ACT RESPONSE TO THE DIGITAL OMNIBUS CALL FOR EVIDENCE

CONTEXT

ACT is the voice of commercial television & VoD in Brussels and directly represents 26 commercial broadcasters that operate throughout the European Union and beyond. ACT member companies finance, produce, promote and distribute content and services benefiting millions of Europeans across all platforms.

ACT welcomes the Commission's consultation and the opportunity to share our views regarding the future of the ePrivacy Directive, the GDPR and AI.

GENERAL COMMENTS

ACT strongly supports the simplification agenda. Legal uncertainty and excessive compliance burdens undermine investment in European content and services. The Digital Omnibus is an appropriate tool for delivering pragmatic clarifications, provided the focus remains on targeted simplification rather than wholesale reform.

We welcome the Commission's recognition that the ePrivacy framework leads to both user fatigue and disproportionate costs for service providers. A measured adjustment could enhance legal certainty, reduce unnecessary consent requests, and allow businesses to deploy privacy-preserving technologies.

At the same time, we caution against reopening or destabilising the newly adopted AI Act, recommending instead to direct the focus on the correct implementation thereof.

EPRIVACY - COMPLIANCE COSTS

The lack of alignment between ePrivacy and the GDPR has created unnecessary complexity. The over-reliance on consent under Article 5(3) is costly and does not lead to better outcomes for viewers, resulting in unnecessarily high compliance costs and reduced opportunities for busineeses.

These costs are particularly acute for audiovisual media service providers, who already face heavy compliance obligations (e.g., content quotas, advertising restrictions, cultural investment requirements). Every additional burden reduces their capacity to invest in European production and innovation.

EPRIVACY - ALIGNMENT WITH THE GDPR

At the same time, the framework creates competitive imbalances: large online platforms (so-called "gatekeepers") are able to leverage their ecosystem-wide data access and consent mechanisms, whereas broadcasters and VoD services, who rely largely on first-party and pseudonymised data, face significant compliance hurdles with more limited means.

The current regime creates competitive distortions. Very large online platforms can leverage ecosystem-wide data access and consent flows, while broadcasters and VoD services - which rely mainly on first-party or pseudonymised data - face higher compliance hurdles with fewer resources.

Simplification of Article 5(3) would help level the playing field. ACT sees merit in aligning or incorporating rules on terminal equipment access with the GDPR framework. This would:

- ensure consistency and legal certainty,

- reduce unnecessary administrative burdens, and
- enable proportionate safeguards through the GDPR balancing test.

A useful step would be the creation of a "white list" of essential, low-risk use cases typically exempt from the consent requirement. Such an approach would avoid unnecessary consent requests for benign technical and necessary processes, allowing the deployment of privacy-preserving technologies, while provide clarity and legal certainty for audiovisual service providers.

LOW-RISK, ESSENTIAL AVMS COOKIE USES

Many of the following currently fall within the "strictly necessary for a service explicitly requested by the user" exemption in Article 5(3), or to a certain degree legitimate interest, but explicit clarification would facilitate assessment of appropriate legal basis in a GDPR-only context.

- **Core service delivery & access management**: subscription and account management; login/authentication; DRM and licence checks; software updates and maintenance; service continuity and quality (e.g. adaptive streaming quality, load balancing, caching, CDN routing cookies); accessibility features (e.g., subtitles/closed captions, audio description).
- **Security, fraud prevention & anti-piracy**: detection of bots and invalid traffic; protection against account fraud and credential abuse; cybersecurity monitoring; anti-abuse throttling and session-security tokens (short-lived identifiers to prevent request bursts, replay or hijacking); measures against piracy and unauthorised rebroadcasting.
- **Service improvement & user experience**: first-party analytics (e.g., performance, buffering, error rates); A/B testing and optimisation of interfaces and user journeys; recommender systems (part of editorial responsibility of AVMS).
- **Advertising & monetisation**: ad serving and display; frequency capping and technical measurement (e.g. impressions, viewability); first-party audience measurement carried out by the media service and audience measurement carried out by an independent third party on behalf of the provider of the media service (reach, viewing time, programme performance); contextual advertising; storage of privacy/consent choices; support for monetisation models (e.g., paywalls, ad-based tiers).
- **Use of privacy preserving technologies**: URL-based measurement; pixel authentication; short-lived/session identifiers; aggregation/pseudonymisation; on-device processing.

EPRIVACY - CENTRALISATION OF CONSENT

ACT welcomes the Commission's aim of reducing compliance costs by limiting cases where consent must be obtained. However, we strongly caution against introducing centralised consent management tools (e.g., browser-based solutions or universal signals).

Consent will likely remain essential, even by integrating ePrivacy into the GDPR, particularly for the personalisation of content and advertising. Audiovisual media services are amongst the most trusted media sources resulting in higher-than-average opt-in levels. It is therefore key that they be able to ask viewers consent directly.

Moreover, it is difficult to reconcile the GDPR consent criteria, which imply an individual, specific and informed choice, with "unique" third-party solutions implying a prior, global, non-specific and

decontextualised choice aimed at accepting or rejecting, without prior information and with the only criterion for choice being the origin of a cookie rather than its purpose.

Such a centralising approach conflicts with other EU initiatives aimed at limiting the power of gatekeepers in the European Union (e.g., Digital Markets Act). It would also lead to unfair advantages for global digital portals and strengthen their dominant position on the market. Privacy and consumer protections are both key issues, but they should not be instrumentalised in a way that allows online platforms to reinforce their position on the advertising market.

Finally, audiovisual media services invest heavily in original content, be it news, cultural, educational or entertainment content. This investment requires sustainable revenue models to secure returns on investment and fund new content creation. This is in stark contrast with large online platforms and gatekeepers which hold monopolies and extract huge profits from media value chains, at the expense of other actors, without investing in content.

A one-size-fits all approach, which centralises all types of businesses in one consent management system undermine media's ability to connect with its viewers. It is crucial to protect legitimate business models that enable content monetisation. Protecting media companies' freedom to conduct a business is essential to sustain content production and preserve jobs in journalism, editing and production.

The cookie-pledge initiative showed the limits of such an approach and how it would have a negative impact of the media industry. We therefore strongly oppose and advise against any centralised consent management mechanisms, in particular via browser or signals.

EPRIVACY - CROSS DEVICE USE CASE / CONSENT

Rather than centralising users' consent in the browser we would support a decentralised solution. A more effective way to reduce "consent fatigue" would be to explicitly allow cross-device consent.

Today, audiovisual media services must ask the same user for consent separately on each device. This means an individual viewer may receive consent requests from an individual publisher separately for several devices (e.g., PC, smartphone, tablet, set-top box, connected TV).

Clarification that consent given on one device applies to all devices owned by the same user (in full respect of all the GDPR criteria for valid consent) would significantly streamline the user experience.

Obviously, viewers would need to be duly and clearly informed that consent obtained on one of their devices is also valid for other devices in their possession. Such an approach can work, as demonstrated by several French operators, including audiovisual media players, which have successfully implemented cross-device consent following close cooperation with – and approval from – the national regulator.

Although consistent with GDPR principles, current EDPB guidance on consent (05/2020) does not permit this. A targeted clarification in the Digital Omnibus would therefore be both proportionate and effective.

ARTIFICIAL INTELLIGENCE ACT

ACT welcomed the EU's leadership efforts at developing a regulatory framework for Artificial Intelligence. This leadership is critical, as AI interacts with various sectoral regulations, including copyright, and raises complex questions with regard to the protection of Intellectual Property

portfolios, including those of ACT members.

ACT supports focusing on the effective implementation of the copyright *acquis* and of the recently-adopted AI Act, ensuring compliance with established copyright principles and creating the conditions for their application.

The focus today should be on the effective implementation and enforcement of the AI Act. By ensuring that it enables the correct application of established EU copyright *acquis*. The adaptability shown by the EU in the face of technological advances suggests that Gen-AI could be managed under current AI and copyright laws, which provide a robust structure for evaluating potential infringements at both the input and output stages.

We therefore caution against undermining the recently adopted AI act and its interaction with the Copyright *acquis* under the guise of facilitating the "smooth interaction between the AI Act and other EU laws". In our view, this should not be a focus of the Digital Omnibus package.

CONCLUSION

ACT supports the Digital Omnibus as a pragmatic opportunity to streamline compliance with certain rules, specifically Article 5(3) ePrivacy. Clarifications that would reduce unnecessary consent requests, recognise low-risk use cases, and enable cross-device consent would deliver tangible benefits for both users and businesses.

However, centralised consent mechanisms must be avoided, and the AI Act must remain intact.

ACT stands ready to engage further with the Commission to ensure that simplification measures enhance both competitiveness and user trust in the digital ecosystem.