Digital Omnibus: Bertelsmann Position on Article 88a & Article 88b

Executive Summary

The currently discussed provisions (in both the Commission's proposal and the latest Council compromise proposal) pose a significant threat to the viability and refinancing of digital media services while failing to achieve their stated objective of reducing consent fatigue and simplifying the regulatory framework.

Rather than simplifying the existing regime, the proposals would introduce new technical, legal and operational complexities, create substantial uncertainty for businesses and risk strengthening existing or creating new digital gatekeepers at the expense of European media providers and digital businesses. This is particularly problematic because consent rates are not merely an operational metric: for advertising-funded media services, they directly affect the ability to finance journalistic and editorial offerings, provide personalized services and innovate.

Against this backdrop, the co-legislators should pause the work on the current proposals and urge the Commission to carry out a holistic assessment and evaluation of the data protection acquis, with a view to identifying workable, balanced solutions for all stakeholders. Rather than maintaining strict consent requirements while simultaneously preventing companies from effectively requesting consent, the EU should assess ways to address issues such as consent fatigue in a way that preserves both user choice and the viability of European digital business models.

Not addressing the core issue

The Digital Omnibus is presented as a simplification initiative intended to reduce consent fatigue and regulatory burdens. However, the current proposal does not materially reduce the situations in which consent remains necessary.

Consent continues to be the default and only legal mechanism for most forms of access to and storage of information on consumer devices. While the proposal introduces certain additional exemptions, these remain narrow and do not address the underlying structural problem.

Most importantly, the proposal fails to resolve the long-standing mismatch between the rules governing access to terminal equipment and the broader and more flexible risk-based approach of the GDPR, with a set of legal bases available and adequate levels of protection also in the online environment. As a result of the proposal, consent would continue to be required for many activities involving device access even where the subsequent processing of personal data could lawfully rely on other legal bases such as legitimate interests or contractual necessity.

This issue extends far beyond browsers, websites and cookies. By maintaining consent as the default gateway for access to terminal equipment, the proposal affects a wide range of digital business models that rely on connected devices, including media services, connected TV environments, e-commerce and emerging AI-enabled products. Given the broad interpretation of the ePrivacy framework by supervisory authorities, under which establishing an internet connection itself falls within the scope of Article 5(3) ePrivacy Directive, these restrictions affect virtually any internet-connected device.

The Council text improves the audience-measurement exemption for consent by covering anonymous aggregated usage information where measurement is carried out by the provider or by a third party acting together with or on behalf of the provider, including audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083. This is welcome and fundamental, as reach is the central currency for advertising-funded private media and must be measurable through independent and comparable systems such as AGF. However, it remains a limited correction exemplifying where consent should not be necessary.

At the same time, the proposal introduces additional restrictions on how consent may be requested, including prescriptive UI requirements and limitations on renewed consent requests. These restrictions do not adequately reflect operational realities or the need for continuous product development and innovation. In practice, organizations may need to seek renewed consent not only for new purposes, but also where there are material changes to existing processing activities, technologies, service features or business models that affect how a previously consented purpose is implemented. Limiting the ability to re-engage users in such situations risks creating legal uncertainty and may discourage the improvement of digital services. Rather than reducing complexity, these requirements would increase operational complexity for digital services, including established Pay-Or-Consent models, personalized offerings and innovative digital products.

As a result, the proposal has implications far beyond digital advertising and risks creating unnecessary barriers to the development, financing and improvement of digital products and services across the European digital economy.

Introducing complexity without resolving consent fatigue

Article 8a GDPR (formerly Article 88b GDPR) introduces automated and machine-readable indications of users' choices, effectively moving consent decisions towards browser-, operating-system- or intermediary-level mechanisms. The user-facing benefit of this approach is highly questionable: as valid consent must remain specific, informed and tied to concrete purposes, controllers and processing contexts, there is little to no room for generic automated choices to meaningfully reduce the need for consent requests.

At the same time, Article 8a GDPR would create a new mandatory compliance layer whose technical, legal and operational foundations are undefined. It remains unclear how such systems would support all relevant processing purposes, controllers, devices and interaction scenarios; how conflicts between automated signals, service-level choices and account-based preferences would be resolved; and who would define, govern and control the relevant details – especially given the scope covering any digital service and business model, its purposes and data processing details.

Standardization cannot resolve these concerns on its own. A technical standard may define formats, interfaces or signal transmission, but it cannot solve the underlying legal and commercial questions: whether a centralized or automated signal can constitute specific and informed consent, how all possible purposes and controllers should be represented, who controls the user interface, and how conflicts between intermediaries, platforms and digital services are resolved. If these questions are left to later standardization, the proposal would create a binding obligation before its legal and operational feasibility has been established.

Furthermore, this approach would extend the role of existing digital gatekeepers or create new ones. Browser, operating-system and platform providers are not neutral infrastructure actors. Many of them operate their own advertising, data, app-store, distribution, search, content or AI-related businesses and therefore have their own commercial interests in how user choices are framed and implemented. If these actors control the interface for consent decisions, they could influence default settings, the granularity of available choices, the language and design of prompts, the transmission of signals and the resolution of conflicts between browser-level settings and service-level choices.

Nor would the problem be solved by shifting this role to a new layer of specialized consent intermediaries. On the contrary, this would add further complexity: digital services would then have to assess, integrate and continuously support multiple third-party consent systems, each potentially using different user interfaces and user journeys. Instead of simplifying consent management, the proposal could create a fragmented intermediary market in which media providers are forced to deal with numerous additional actors between themselves and their users.

This would give third parties a structurally privileged position in the digital value chain. Media providers would lose the ability to explain their own services, financing models, personalization features and product-specific processing purposes in the concrete context of use. Instead, user choices could be shaped by intermediaries whose incentives may not be aligned with the financing of independent media or with fair competition in digital advertising markets.

This would not reduce complexity. It risks creating years of uncertainty until workable standards and interpretations emerge, while requiring European digital businesses to integrate mechanisms that may be controlled or shaped by actors with competing commercial interests. As a result, the proposal would strengthen existing or create new gatekeepers, weaken the direct relationship between media providers and users, reduce consent rates in practice and create significant risks for digital business models and AI-enabled use cases.

The media exemption does not solve the underlying problems

The proposal contains a media exemption for media service providers within the meaning of the European Media Freedom Act. While welcome in principle, it does not address the core concerns associated with Article 8a GDPR.

The exemption allows media providers to continue requesting consent directly when providing their services. However, the economic viability of digital media depends on a broader ecosystem of advertising, measurement and technology partners that support the financing and monetization of content. Many of these activities are unlikely to fall within the narrow concept of the provision of the media service itself.

As a result, the exemption risks being of limited practical value. Media providers may retain the ability to request consent for certain activities while facing restrictions for essential advertising, audience measurement and monetization functions carried out through third-party partners. The media exemption therefore cannot compensate for the structural shortcomings of Article 8a GDPR.