NEWS MEDIA EUROPE

Digital Fitness check: European publishers want simple, effective and risk-based digital rules

March 2026

News Media Europe (NME) is the voice of the progressive news media industry in Europe, representing over 2,700 news brands in print, online, radio and TV, through national associations from sixteen countries. Together, we defend key principles which are vital to us: protecting the freedom of the press, championing the digital future of our industry, and ensuring that the value of content is properly protected.

European news publishers see an urgent need to simplify EU digital rules impacting their business, going far beyond what the Commission outlines in the digital omnibus proposal. EU rules are increasingly complex and anchored in burdensome procedures rather than outcomes. This makes them generally more difficult to enforce and to comply with, thereby reducing their overall effectiveness.

In addition, EU digital rules often contain horizontal obligations that must always be complied with irrespective of actual risks, contrary to the often-stated intent of observing a risk-based approach. Too often, the measures proposed to ease the impact of regulations on SMEs are also entirely insufficient. In some cases, EU digital rules have also become far more complicated than the problems they are intended to solve. Therefore, these rules must change and adapt to business realities, such that they remain business-friendly and proportionate.

News Media Europe supports the European Commission's political drive to simplify complex EU rules. This will allow essential services like independent news publishing, whose core mission is to inform the public, to thrive without having to face excessive burdens. News publishing differs fundamentally from other digital services: it has a democratic function, it is editorially accountable and holds legal responsibility for the content published. Publishers rely on direct relationships with audiences and sustainable revenue models, including subscriptions and responsible advertising, to finance independent journalism.

Rules that treat all online services alike risk weakening these models and creating legal uncertainty while offering limited benefits for consumers. A modern rulebook should avoid a one size fits all approach. The European Commission should consider how broad regulatory measures inevitably have effects beyond the practices and sectors that they aim to address. It follows that horizontal rules should only be used when the incidence of, and risks related to, digital harms are sufficiently high across sectors to justify this.

The document contains several sections that address regulatory concerns concerning:

- Digital Omnibus proposal
- General Data Protection Regulation
- Digital Fairness Act

- Political Advertising Regulation
- Digital Markets Act
- Artificial Intelligence Act

Digital Omnibus proposal

Publishers are very concerned that the omnibus is not simplifying, but instead creating new rules that will harm their business and ability to process data. The proposal must be amended so that it may achieve its intended goals of simplification and supporting media services.

While the GDPR is important to protect citizens, its complex overlaps with the ePrivacy Directive are outdated and fail to reflect the realities of the digital economy or to even encourage the use of privacy-friendly technologies. Therefore, these rules should be simplified in the interest of citizens, regulators and the business community.

To succeed, EU privacy rules must shift away from a one-size-fits-all approach and encourage a risk-based framework aligned with the GDPR and the corresponding legal bases for processing data. In addition, the strict rules that apply to global tech platforms because of their invasive data practices should not apply to ordinary SMEs or publishers.

Current rules divert crucial revenue away from European publishers towards foreign platforms, undermining the strategic objectives of the European Democracy Shield and Media Freedom Act.

Publishers appreciate that the Omnibus recognises this risk and the role of editorial media in society through a targeted exemption, but it must go further and create a GDPR data framework that genuinely enables sustainable journalism, treating it as a democratic pillar.

Why data is essential for European media

News publishing is rapidly moving from print to digital where the main currency is data. Access to reliable data is essential to fulfil editorial and social objectives, both in terms of driving engagement and ensuring commercial sustainability. Publishers must be able to:

(a) Use data to know who their audience is. This is crucial to understanding how younger audiences consume news, improving user experience and engagement with quality editorial content that can compete with social media and AI;

(b) Use data to offer advertisers effective, interest-based solutions. This is crucial to ensure sufficient income from digital advertising, which is an essential source of revenue alongside premium content subscriptions.

Problems with the Omnibus proposals

The Omnibus is intended to simplify the current rules. However, it introduces proposals that will make it more difficult for publishers and media services to use data:

1. It maintains the strict ePrivacy consent requirement in Art. 88a (with only a partial derogation for audience measurement) for user devices that contain personal data, while a parallel regime is foreseen in the ePrivacy Directive for devices without personal data.

2. It introduces new consent rules for all websites in Art. 88a (eg. single click rejections and consent request cooling-off periods) that are unworkable, as they require a persistent identification of user devices, and which can starve media of advertising revenues.

3. It introduces centralised consent settings for all websites in Art. 88b (with a media exemption) that would deprive publishers of revenues and create new gatekeepers, against the objectives of the Digital Markets Act.

The current approach means that consent remains the only legal basis for publishers to use cookies and similar technologies. This completely fails to address consent fatigue, restricts flexibility for media services, and excludes more privacy-friendly advertising models based on legitimate interest.

The Omnibus should focus on easing the excessively strict consent requirement that currently applies to many low-risk data processing activities, even where they clearly have no or only a negligible impact on privacy. By reducing the need to obtain consent only where it is really needed, the Omnibus can eliminate the need for centralised consent settings.

So when media services process data in ways that are privacy-friendly, using aggregates, limited data, or on a first-party basis, they should be able to depart from the rigid consent approach. This can be achieved through targeted exemptions for responsible media services or by relying on other legal bases of the GDPR such as legitimate interest.

We oppose the implementation of centralised settings and single-click rejections because of the harm they can inflict to the media sector. While the media exemption is a welcome acknowledgement of this risk, it remains unworkable. In practice, centralised settings will create user expectations about compliance which contradict the operational reality of media services.

This disconnect creates an inevitable risk for consent rates, starving independent publishers of vital advertising revenue and undermining the high level of trust users place in their preferred news brands.

Further to the competition and gatekeeper problems that centralised settings could create, this type of solution would also require advertising technology providers to determine who is a “media service provider” under the Media Freedom Act, and to voluntarily accept significant GDPR risks and liability for breaches of consent. We believe adtech companies are neither willing or capable of doing both.

Suggestions to improve the Omnibus proposal

It is essential to preserve the intent of the omnibus to support the media at this difficult juncture. The Omnibus can actively support the sector in several ways:

1. Introduce alternatives to consent for media services that engage in low-risk data processing activities or use privacy-friendly technologies, by allowing reliance on the other legal bases of the GDPR and expanding the audience measurement derogation.

2. Clarify that media services may base the availability of their content on user consent for processing activities that are necessary to finance that content.

3. Stop the introduction of centralised settings and new consent rules because of the harm they could inflict on media services regardless of the exemption, or alternatively make the settings only binding on gatekeepers under the Digital Markets Act.

General Data Protection Regulation

News Media Europe conducted in 2025 a survey of European news publishers following the announcement of the European Commission to simplify aspects of the GDPR. The survey sought feedback on which parts of the GDPR create disproportionate burdens both in editorial activities and commercial operations. Below are the findings of this survey.

Overall experience

- ◊ **Which GDPR obligations are most difficult to manage across your organisation whether in your newsroom, commercial team, or technical departments?**

In general, publishers find it difficult to comply with the GDPR because the regulation is complex and anchored in burdensome procedures rather than outcomes based. In practice, the GDPR contains many obligations that must always be observed irrespective of actual risks in the real world, contrary to the stated intent of the regulation to follow a risk-based approach.

The extensive documentation requirements are inherent in all obligations, which leads to substantial resources spent on data processing activities that sometimes only present a low risk for individuals. This one size fits all approach is a problem and creates a drag on the business of publishers. Below, we identify some of the most difficult obligations to manage:

- Managing the legal bases for processing activities
- Dealing with individual data subject requests
- Overseeing international data transfers
- Reviewing GDPR-related contract provisions
- Applying the definitions of data controllers and processors
- Creating and maintain records of processing activities

Managing **the legal basis for processing activities** is difficult under current practice as it is based on a clear and general preference for consent. This does not result from the contents of

the GDPR, but instead from the selective interpretation and enforcement by data protection authorities.

Besides questions related to how the GDPR should be interpreted, publishers do not believe that consent is always effective as a privacy-enhancing feature and are concerned about cookie fatigue. The technical and legal requirements linked to consent management are also demanding and limit the use of essential analytics and personalization tools, affecting both editorial insight and user engagement.

In many cases, the legitimate interest legal basis can be more beneficial both for users and businesses. However, the significant administrative burden related to the balancing of interests in the case of data processing based on legitimate interest makes it difficult to reap the benefits of this approach.

Individual data subject requests (access, rectification, erasure, and data portability) are also difficult and time consuming. If implemented and executed correctly, the right of access is one of the most burdensome GDPR obligations and it is questionable whether the vast amount of (technical) data which must be provided to data subjects are always desirable.

The GDPR generally lacks substantive and formal rules governing the handling of these requests in practice. This includes procedural standards, verification processes, formats for responses, and criteria for denial or extension, which can lead to legal uncertainty for both data subjects and controllers.

Handling GDPR access and deletion requests involves significant administrative work - preparing legitimate interest assessments and sending them to the data subject. The information provided as part of fulfilling data subject rights can often also include details that conflict with laws concerning the protection of sources. This creates a dilemma for editorial team, particularly in potential future press lawsuits or personality rights cases where disclosed sources or documents can be used against publishers.

Obligations concerning **international data transfers** are another difficult area to manage as they require a lot of time and resources to map and assess any transfer of personal data all the way down the sub-processor chain. Significant resources are also needed to conduct other types of privacy risk assessments related to processing activities. There is a general understanding that Data Transfer Impact Assessments (DTIAs) are too demanding.

For ordinary European publishers, ensuring GDPR compliance when using advertising vendors based outside the EU, especially in the US, has become resource-intensive and legally complex. And while the GDPR is supposed to operate on a risk-based approach, international data transfers are a clear exception to this, where a binary approach prevails: a transfer is either OK (“same level of protection or essentially equivalent”) or it is NOT OK.

The review of contractual agreements with GDPR components is another important area of complexity. Agreements with external parties usually contain GDPR provisions which in principle always need to be reviewed by external lawyers, at least when SMEs are concerned since they do not have in-house GDPR lawyers, to determine whether such agreements are adequate. This results in recurrent significant costs for publishers.

The definitions of data controllers and data processors are unclear which also contributes to this problem and leads to further difficulties when new business partnerships are created.

Deciding on the appropriate role of different partners for every data processing activity is a challenge.

The Record of Processing Activities (RoPA) obligations are also excessively time consuming and create a large administrative burden which achieves little in practice. It is necessary to limit the ROPA obligation to situations where this is necessary, for example to high-risk processing operations.

Editorial matters

◊ **What challenges have you faced when applying the journalistic exemption (Article 85) — for example when responding to data subject requests or legal complaints?**

While **many publishers report minimal difficulty in applying the journalistic exemption**, others report recurrent problems, particularly in specific countries where enforcement by national data protection authorities is incorrect and/or where there are conflicting national rules. This creates legal uncertainty and legal risks.

A common problem for publishers is the **lack of understanding by data subjects about the scope and purpose of the journalistic exemption**. Many data subjects assume that their requests to exercise GDPR rights, such as the right to be forgotten or the right to erasure, are unilaterally enforceable and universally applicable. This is of course incorrect and involves an assessment based on the balancing of competing interests.

Publishers regularly receive GDPR-based **requests for deletion of editorial content** such as news articles (or parts of thereof). Such requests must of course be assessed under the GDPR, but it is the clear view of publishers that they are far more appropriately evaluated under EU and national media laws and the editorial and ethical frameworks governing the journalistic profession.

In general, there are also shared concerns about the **significant administrative burden created by data subject access requests**. Such requests often ask for very detailed information about the processing of personal data, including sources, which journalists cannot disclose due to professional confidentiality and source protection obligations, which can be legally binding.

For these reasons, several publishers advocate for more clearly defined exemptions for journalistic purposes under the GDPR. Some recommend that Article 85 should not leave such exemptions solely to Member States and include an EU-wide standard, and others also believe that the obligations in Chapters II–VII and IX of the GDPR should not apply to personal data processed for journalistic purposes.

These views are notably motivated by the **failure of several data protection authorities to interpret journalistic exemptions sufficiently broadly**, for the GDPR not to inadvertently restrict the work of newsrooms.

A greater focus on this problem is needed as a matter of consistency with other EU laws and policy priorities, such as the European Media Freedom Act, the Directive against Strategic Lawsuits Against Public Participation (SLAPPs), and the forthcoming Democracy Shield.

This is particularly important in light of recently documented cases of **weaponisation of the GDPR by malicious actors to censor journalistic content through SLAPPs against news publishers**. Such cases, which typically seek to abuse defamation and libel laws, have led to the adoption of the SLAPP Directive and an accompanying recommendation to Member States. Greater efforts are urgently needed to ensure that the GDPR is not misused to such ends.

◊ **Have you faced compliance problems related to editorial archives?**

Participants report that the **GDPR creates pressure on editorial archives due to the way search engines surface their contents.** Since news articles are indexed by search engines, they can appear prominently as search results or as sources referenced by online chatbots powered by artificial intelligence.

As a result, **data subjects frequently submit erasure or anonymisation requests based on the right to be forgotten.** Where news publishers decide to honour such requests, based on a case-by-case assessment of whether the rights of the data subject take precedence over the public interest, the personal data are removed from editorial content such as news articles.

The consequence is important as **the historical and journalistic continuity of the archives is compromised** since the original editorial content loses the links that would otherwise connect it to any future coverage and the ability to access information about the the past is lost. While this must remain a case-by-case assessment, the lack of clear guidance on what constitutes a public interest and on the need to interpret freedom of expression as broadly as possible in this context, creates an unacceptable risk of censorship.

Without clear boundaries, continued overenforcement by data protection authorities and national courts risks leading to a scenario where European journalistic archives are gradually stripped of their integrity. Over time, this could result in a reality where historical records are routinely altered or erased, creating a dystopian environment reminiscent of Orwell's vision in 1984 — one in which the past can be rewritten at will.

Editors therefore argue that **Article 85 should go further to shield journalistic archives.** They stress that altering, pseudonymising or deleting historic material risks distorting the public record and, by extension, rewriting history. In their view, any regulatory outcome that compels permanent changes to past reporting amounts to censorship and is incompatible with the democratic role of a free press in Europe.

Even where no formal compliance breach has yet occurred, several news publishers are concerned about the **burdensome internal work to draw up and apply retention rules** that distinguish between preparatory materials for editorial content, unused information and copies, and final published content that has undergone editorial review and been approved. Deciding how long to keep each category, and under what legal basis, has proved administratively burdensome and demands staff attention.

Finally, publishers are also concerned that **editorial archives can retroactively generate problems.** One respondent noted that older press releases which were once assumed to be lawful in their entirety were later challenged on grounds that personal data had been carried over without sufficient justification. As a result, some newsrooms now spend time every year deleting or anonymising a handful of past articles.

We believe that article 85 should provide media archives with effective protection tool for media archives as well to protect journalistic freedom. No, but in principle it is paramount that GDPR does not imply any censorship or altering of historic archives, which also would mean the altering of history as documented through editorial media over time.

Audience measurement, analytics & subscriptions

- ◊ **How does GDPR compliance affect your use of audience analytics and personalisation (eg. headlines, paywalls, or newsletters)?**

Personalisation is increasingly viewed as critical to the relevance and viability of editorial content. Tailored newsletters, dynamic paywalls, and behavioural recommendation engines help improve reader engagement, boost subscriber loyalty, and ultimately generate revenue—revenue that supports the independence of quality journalism.

However, GDPR compliance, particularly when combined with ePrivacy requirements, significantly constrains the use of audience analytics and personalisation tools by news publishers. Respondents broadly agree that the requirement to obtain user consent limits the audience data available for analysis. This loss of data harms the ability to tailor content, recommend articles, test headlines, or optimise user journeys.

There is also a shared concern that these limitations weaken the competitiveness of publishers in a digital economy dominated by global tech platforms. Younger audiences in particular expect personalised content and are less likely to engage with digital products that lack it. This puts editorial media at a structural disadvantage, not only in terms of user engagement and reach but also in their ability to develop business models based on subscriptions and digital advertising.

Many publishers are of the view that the different legal bases of the GDPR for processing data (such as legitimate interest or contract) can offer a better alternative to consent. However, the ePrivacy Directive, which takes precedence when cookies or similar technologies are involved, imposes strict conditions. In general, publishers see that ePrivacy rules are poorly explained by national data protection authorities and inconsistently interpreted.

Furthermore, some participants express frustration at how low-risk data points — such as IP addresses or browser fingerprints — are treated under GDPR. They argue that these identifiers, while technically personal data, pose significantly less risk than other forms of personally identifiable information. Yet, under current regulation, the level of risk has no impact on the rules that must be observed. This approach, they say, disproportionately affects smaller or editorially controlled publishers, while larger tech companies continue to exploit such data with, in many cases with little to no accountability.

Another area of concern is the broader effect on innovation and product development. With many users rejecting analytics cookies, media organisations lose the ability to make data-driven decisions about product features and editorial strategies. In markets such as the UK or US, publishers appear to face fewer restrictions when sending newsletters or marketing messages, whereas GDPR places a much higher burden of consent, complicating subscription growth and retention efforts within the EU.

Finally, several respondents point to contradictions between regulatory intent and market practice. For instance, Consent Management Platforms (CMPs) often function in ways that conflict with regulatory guidance, making compliance harder in practice. In summary, while there

is widespread support for user privacy and data protection, the current GDPR and ePrivacy implementation—especially the rigid requirement for consent and the lack of harmonisation—severely limits publishers' ability to engage their audiences effectively, develop sustainable digital business models, and remain competitive in a personalised media ecosystem.

◊ **What is your experience in managing consent for editorial emails (eg. newsletters, content alerts)? Are the current rules clear and proportionate?**

Respondents generally report that the rules concerning consent for editorial emails, such as newsletters and content alerts, are relatively clear. In most cases, it is well understood that subscribers must opt in to receive such communications. This process is largely seen as functioning smoothly, with no significant compliance difficulties reported.

However, views on the proportionality and coherence of the rules vary more widely. Several publishers point out that while the basic framework for consent is understandable, practical application becomes more complex when additional national laws come into play — such as those concerning direct marketing rules.

In such cases, there is a lack of clarity about the extent to wich a distinction can or should be drawn between editorial and marketing communications. Some national laws classify any form of mailing that even indirectly promotes a product or service as "direct marketing," requiring full consent under GDPR — even for newsletters that are editorial in nature. This is seen as disproportionate, especially when the primary intent of a newsletter is to deepen reader engagement rather than drive sales.

Others highlight the complications arising from the overlap between GDPR and the ePrivacy Directive, especially in relation to email tracking and analytics. Practices such as pixel tracking to monitor open rates or click-through behavior also require consent, and trigger GDPR principles like data minimisation and storage limitation. When such tracking is tied to third-party advertising platforms (e.g., Facebook Pixel or Google Ads audiences), the line between editorial and commercial activities blurs further.

Some publishers credit sectoral self-regulation and the relatively low enforcement priority placed on these rules by national authorities for smoother implementation. Nonetheless, there is an underlying concern that while the rules are technically clear, they often lack proportionality and flexibility, especially when applied uniformly to very different kinds of email communication. The burden of legal compliance can deter publishers from using newsletters as an effective editorial and engagement tool, even though such tools are critical in maintaining a loyal reader base and driving growth.

In summary, while there is broad agreement that managing consent for editorial emails is operationally manageable and conceptually clear, many respondents question whether the current regulatory framework strikes the right balance. The overlap of GDPR, national marketing laws, and the ePrivacy Directive can lead to inconsistent interpretations and disproportionate obligations—particularly when editorial and commercial boundaries are not clearly distinguished.

Some suggest that a more nuanced regulatory approach, one that differentiates between direct marketing and editorial communications, would better support the legitimate role newsletters play in modern journalism.

Advertising

◊ **What are the biggest compliance challenges you face when working with advertising vendors (eg. ad tech platforms such as SSPs and CMP providers)?**

Most publishers are concerned about the legal and compliance risks they must shoulder as data controllers, while having only a limited influence or even insight over the activities of advertising vendors. The main difficulty lies in understanding the GDPR role of vendors: the same supply-side platform or measurement firm may present itself as a processor for one purpose, a controller for another, or a joint controller when reusing data across multiple clients.

Because different vendors attach different roles to nearly identical activities, publishers struggle to give their readers clear privacy notices and to honour individual data subject requests, such as requests for access, erasure, rectification or portability. Consent management aggravates this problem as even if consent management platform can transmits user choices correctly, publishers cannot easily verify that every downstream vendor fulfil their obligations.

Observance with the principles of data minimisation, purpose limitation and storage limitation are therefore impossible to audit for large publishers, let alone smaller ones. The result is a gap between the formal collection of consent and the practical control of data. Publishers also face difficulties in implementing mechanisms to inform advertising vendors about withdrawal of consent and thereby ensure that any data collected based on such consent is also deleted by third-party recipients.

And so publishers understand that the challenges in handling the buy-side technology are substantially more important from a privacy perspective. And yet the biggest challenge appears to be that the GDPR and the way it is enforced by data protection authorities does not encourage privacy in programmatic advertising, but rather encourages focus to be had on the collection and communication of consent.

Meanwhile, the contract negotiations that publishers have with vendors perpetuate problems about data control, particularly for smaller publishers. Large adtech providers present standard terms that cap liability, limit audit rights and blur the boundary between service provision and independent data exploitation — for instance by reserving data for “product development” or AI-model training under the vendor’s own legitimate-interest claim. In the absence of advertising-specific Standard Contractual Clauses (SCCs) under Article 28, every deal requires costly legal review, yet publishers rarely have the leverage to demand changes.

Many publishers point out that the rules treat first-party and third-party data alike, even though the privacy risks differ sharply. Information gathered directly by a news site within a trusted reader relationship is subjected to the same constraints as data that is arbitrarily pooled across dozens of ad-tech intermediaries. This uniform approach, they argue, burdens responsible publishers while permitting larger tech platforms to profit from practices that remain difficult for regulators to police.
In practice, the GDPR has led to a situation where publishers are held accountable for chains of processing they neither initiate nor fully understand. Some publishers are therefore cutting business ties with intermediaries altogether, especially those outside the EU and who apply different data protection standards, accepting revenue losses in exchange for a more defensible compliance posture.

Respondents call for clearer distinctions between first- and third-party data, stricter transparency obligations for vendors, and contract templates that prevent unilateral shifting of liability, warning that without such reforms programmatic advertising may prove irreconcilable with the spirit—and perhaps even the letter — of GDPR.

GDPR governance

- ◊ **What internal resources do you currently devote to GDPR compliance (eg. staffing, legal review, technology)? What takes up the most time or cost?**

Survey respondents describe GDPR compliance as a resource-intensive effort that involves multiple functional teams, legal expertise, and continuous technological adjustments. These teams are often or even entirely supported by external lawyers, particularly for contract review and case-specific legal interpretation.

For smaller publishers, GDPR duties are often assigned as a secondary responsibility to existing staff, which limits bandwidth and capacity for proactive compliance work. Meanwhile, larger organizations report having formal privacy structures in place, that include the appointment of a full-time Data Protection Officer (DPO).

The single most time-consuming and costly area of compliance is consistently identified as adtech. This includes managing consent for programmatic advertising, staying current with evolving legal interpretations (such as case law around frameworks like IAB's TCF), and maintaining privacy-aware configurations across web and mobile platforms. Adtech compliance requires both legal and deep technological knowledge, especially for assessing how third-parties behave and whether they meet consent requirements. Ensuring that tracking technologies are only triggered after valid user consent is in place takes significant coordination between functional teams.

Technology investments are also a major factor. The costliest areas include licensing Consent Management Platforms (CMPs), configuring tag managers to sync with user consent preferences, and integrating those systems with internal databases, analytics tools, and advertising servers. CMP implementation and ongoing updates demand continual developer time, especially when dealing with the complexities of header bidding, SSP integrations, and yield optimization strategies. These tasks must now incorporate privacy-by-design principles, often slowing down product development or limiting personalization features.

Contract negotiations with service providers also consume a large share of resources. Some publishers point to a lack of standard templates or harmonised guidance from authorities, which could reduce the burden of reviewing and negotiating data processing agreements or joint controller agreements. Many suggest that if providers adopted templates approved or certified by authorities, legal review processes could be streamlined, saving both time and legal costs.

In some cases, respondents point out r indirect impacts, such as editorial self-censorship that arises from fear of litigation under GDPR. For emerging areas like AI, respondents report that the compliance requirements are particularly heavy and underdeveloped, requiring intensive legal analysis for each new use case. Overall, the feedback suggests that while the principles of GDPR are broadly supported, the practical demands of compliance are burdensome and require further standardisation.

- ◊ **Do you conduct data protection impact assessments for editorial or commercial activities? What makes these easy or difficult to complete?**

Most publishers conduct Data Protection Impact Assessments (DPIAs) in accordance with Article 35 of the GDPR, though the frequency and depth of such assessments varies significantly. For some publishers, DPIAs are relatively infrequent because only a limited number of high-risk processing operations are identified within their organisations. In these cases, DPIAs are not seen as a major burden, especially when activities are straightforward or limited in scope, such as a well-defined personalised email marketing initiative.

However, where high-risk processing is involved—particularly in more complex or evolving areas such as targeted advertising or data profiling—the DPIA process becomes significantly more challenging. The complexity of these activities often demands multidisciplinary collaboration involving legal, technical, editorial, and commercial teams. Gathering the necessary information across departments is time-consuming and can delay the completion of assessments. For larger publishers, the need to coordinate data sharing across entities for commercial purposes adds another layer of difficulty.

One of the main complaints is the lack of consistent and clear guidance. Although DPIAs are legally required, the criteria for when and how to perform them can be vague. Publishers note that while data protection authorities have published useful guidelines, these are not always aligned or detailed enough to reduce uncertainty. As a result, even when companies outsource DPIA work to external legal or compliance experts, the internal effort remains significant due to the need for internal knowledge and coordination. Moreover, outsourcing is often very costly and not always feasible.

Some publishers stress that keeping DPIAs up to date is a challenge. Technical systems and data uses tend to evolve quickly after a DPIA is first completed, making the original assessments obsolete if not reviewed regularly. Implementing the recommended risk mitigation measures from a DPIA also requires clear coordination and project management, especially when resources are stretched.

A key concern raised is the asymmetry between smaller publishers and big tech who benefit from vast legal and technical teams. Some publishers suggest that if digital service providers developing new solutions were required to conduct DPIAs for their tools and before making them available to customers, it would reduce redundancy and ease the compliance burden for smaller organisations. Overall, while publishers understand that they are required to conduct DPIAs in certain cases, the process is often hindered by complexity, fragmentation of internal knowledge, evolving technologies, and a lack of scalable solutions.

GDPR simplification

- ◊ **If you could change one or two aspects of the GDPR to make compliance more workable for publishers, what would it be and why?**

Publishers express a strong desire for targeted changes to the GDPR that would make compliance more practical and proportionate to their day to day realities, without undermining the fundamental rights the regulation seeks to protect. A common theme across responses is the call for a more risk-based and context-sensitive approach that recognizes the specific role and limitations of media organisations, particularly smaller publishers.

There is a consensus about the need to reduce the formal and documentation-heavy obligations, especially for low-risk processing activities. This would allow publishers to focus their limited resources on genuinely high-risk operations, such as complex profiling or the use of third-party data for targeted advertising. For example, they suggest simplifying or waiving requirements like appointing dedicated GDPR roles for small companies, while maintaining the core data protection principles for all.

The most frequent and pressing concern is the overlap and inconsistency between the GDPR and the ePrivacy Directive, particularly around cookie consent rules. Publishers argue that these rules make it unnecessarily difficult to use basic, first-party data for editorial and analytical purposes, and they limit audience engagement. And so they call for a clearer distinction between first- and third-party data — especially where the processing supports editorial goals and democratic functions, such as audience measurement or product development.

Several publishers call for expanded use of “legitimate interest” as a lawful basis for certain types of non-invasive processing—such as contextual advertising, frequency capping, audience measurement, basic campaign analytics, and non-profiling A/B testing. They propose a “light-touch” legal basis or exemption for such purposes, provided there are strong safeguards, such as no use of persistent identifiers and easy opt-outs. This would help reduce reliance on consent for routine processing that does not pose significant risks to individuals.

Another significant issue raised is the overcomplexity and ambiguity of GDPR roles (controllers, processors, joint controllers). Publishers report that these distinctions are often impractical in real-world data flows, particularly in digital advertising, where the power dynamics are often reversed (e.g. processors like platforms or ad tech vendors have far more control than the publisher). Respondents suggest abolishing or simplifying these role definitions, replacing them with a more general requirement for clear contracts when data is shared.

There is also a strong desire for institutional reform. Respondents report a lack of trust in data protection authorities (DPAs) and argue that the enforcement model is structurally too fragmented, unpredictable, and lacks transparency. They recommend creating “privacy sandboxes” to allow publishers and DPAs to engage in open dialogue about complex processing in a non-punitive environment. They also call for more effective promotion of codes of conduct and certification mechanisms. The approval processes for such instruments should also be made faster and more efficient.

Publishers also want to be exempted from certain GDPR obligations altogether when acting in their journalistic or editorial capacity, citing Article 85 of the GDPR. They argue that the current implementation of this article is inconsistent across the EU and often too vague or narrow. In practice, this legal uncertainty can lead to overcompliance or self-censorship, particularly when processing personal data as part of investigative reporting or editorial projects. Without a more balanced and consistent interpretation of this provision, the GDPR can be misused as a tool to restrict press freedom, rather than protect individuals’ privacy in a proportionate way.

Overall, the publishers are not seeking to weaken data protection, but rather asking for more proportionate, practical, and context-aware application of the rules. Without these reforms, there is concern that GDPR compliance will continue to disproportionately burden publishers, especially smaller and editorially independent ones, while advantaging big tech platforms that already dominate digital markets and aggravate existing harms linked to this.

Digital Fairness Act (DFA)

While the specific contents of the upcoming DFA are yet to be determined, the Commission has already indicated interest in horizontal rules across different issues such as subscriptions, personalised advertising, dark patterns, and the protection of minors.

The inherent risk associated with horizontal rules is that creating one-size-fits-all obligations inevitably overlooks sectoral specificities and imposes unnecessary administrative burdens, at a time where the priority should be to simplify EU digital rules to make it easier to do business in Europe. This is a priority for publishers too, many of which are SMEs that find it difficult to navigate the EU's digital rulebook.

These concerns find reason in the current evidence base presented in the Fitness Check which, in our view, is insufficient to justify new legislation. The quantitative analysis informing the Fitness Check relies heavily on opinion-based data, and struggles to isolate and attribute impacts directly to gaps in the existing Directives.

We therefore urge the European Commission to prioritise better enforcement of existing consumer protection legislation before considering the introduction of new, far-reaching obligations that could add complexity and legal uncertainty. Doing so would support the stated aim of legislative simplification, reduce the risk of fragmentation, and enable a unified interpretation and effective enforcement.

It is crucial that any potential legislative proposals adopt a risk-based approach. This approach should be targeted and prioritise sectors and practices where actual consumer harm or unfairness is demonstrably occurring, rather than adopting broad horizontal measures that risk unintended negative impacts on news publishers.

The Digital Fairness Act could directly impact how publishers design, deliver and monetise their digital services. While addressing manipulation or deception is legitimate, the proposed rules must avoid unintended consequences for editorial freedom and innovative user engagement.

For example, many of the concerns raised relating to "dark patterns" lack a clear and consistent definition, which are likely to lead to overenforcement. Such enforcement could subsequently create spillover effects in the enforcement of different but related fields of law, such as data protection.

Our main concern is therefore that overly generic rules could further undermine the economic and editorial challenges faced by independent news media, thereby threatening their ability to provide trusted journalism. A targeted, evidence-driven focus will ensure that consumer protection is both effective and proportionate.

Subscriptions

Digital subscriptions are essential for the sustainability and growth of Europe's news media sector. They allow both small and large news publishers to invest in the creation of diverse, high-quality content for European citizens. In a rapidly evolving digital landscape, subscription models are one of the few viable revenue streams that support independent journalism and pluralistic editorial media offerings.

To develop a stable reader base and foster long-term relationships with audiences, news publishers rely on tools such as free trials, discounted introductory offers, and added-value incentives (e.g. welcome gifts). These offers are not only legitimate business practices, but they are also vital to building trust with new readers, encouraging experimentation with different news sources, and creating lasting engagement with reliable local, national, and international journalism.

Personalised offers also allow publishers to reach specific groups that might otherwise be difficult to engage, such as students, young readers, or low-income households, by tailoring subscription models to their needs and preferences. These targeted incentives help ensure that diverse audiences can access independent, fact-checked news, contributing to a more informed society. It is therefore essential that the Digital Fairness Act does not restrict the ability of publishers to offer personalised pricing and promotions.

Free or discounted trials and payment information

Free or discounted trails are key tools in attracting new readers as they allow users to experience news services. When payment details are requested, this serves several legitimate and proportionate functions:

Preventing abuse, such as repeated trial use or identity manipulation.
Protecting content, for example from bots or unauthorised redistribution.
Enabling service improvement, by collecting feedback from users who choose not to subscribe.
Simplifying conversion, helping users move seamlessly from trial to subscription once properly informed.

Importantly, any transition from free to paid or a higher fee must be fully transparent, based on explicit consent, and accompanied by clear pre-contractual information. These principles are already enshrined in current EU consumer law. Free trials are already regulated under the CRD and the UCPD, which impose clear pre-contractual information requirements and have been further clarified through detailed guidance.

The real question, however, is what constitutes transparency. Too much information can be counterproductive: if users are overwhelmed with legal detail, this may hinder, rather than help, informed decision-making. Therefore, rather than prescribing specific formats or separating trial periods from the main contract, rules should focus on substance over form. Trials are, by definition, part of a broader paid agreement, and consumers already benefit from protection as long as information is accurate, clear, and not misleading.

When consumers sign up, businesses must ensure that payment obligations are explicitly acknowledged, and that terms relating to trials, expiration dates, and the start of billing periods are clearly and visibly communicated. This protects users while maintaining the flexibility for businesses to offer introductory promotions, an essential tool for onboarding new customers and encouraging editorial media engagement.

Stricter, one-size-fits-all obligations would reduce the availability of trial offers, ultimately leading to higher entry costs for consumers and limiting their ability to experience and assess digital content before committing.

Ultimately, transparency should empower the user, not drown them in complexity. The Digital Fairness Act should avoid overly prescriptive requirements and instead support practical, innovation-friendly transparency, grounded in existing law and tailored to consumer behaviour in the digital age. Such commercial practices fall squarely within the freedom to conduct a business, a principle enshrined in the EU Charter of Fundamental Rights. Publishers must retain the ability to innovate in how they reach and retain subscribers, including through the responsible use of consumer data and payment information.

Subscription management and cancellation rights

European news publishers fully support clear, simple, and fair processes for subscription management and cancellation. Consumers should be able to subscribe, unsubscribe, or modify their contracts easily, especially when logged into an account. This aligns with obligations under the Consumer Rights Directive (CRD) modified as recently as 2023 with new obligations coming into force in June 2026, the Unfair Commercial Practices Directive (UCPD), and the Digital Services Act (DSA).

However, it is equally important to recognise that subscription contracts are legally binding on all parties of the agreements. While cancellation must not be made unnecessarily difficult, businesses should retain the ability to apply reasonable conditions, such as notice periods or minimum terms, provided these are communicated transparently and comply with consumer law.

Proposals to mandate specific interface designs (such as standardised cancellation buttons or uniform contract management layouts) risk undermining legitimate business flexibility, without providing clear added value for consumers. The focus should remain on identifying and sanctioning genuinely harmful practices, such as hidden cancellation options or misleading language, rather than restricting innovation in how businesses design user experiences.

No need for new withdrawal requirements

The current EU consumer protection framework already provides strong and flexible safeguards for digital subscriptions:

- CRD Article 11(1)(a) requires an easily accessible withdrawal function for online contracts.
- UCPD Article 9(d) prohibits barriers to contract termination and addresses subscription traps.
- DSA Article 25(1) bans interface manipulation that makes cancelling harder than subscribing.

These provisions, supported by detailed Commission guidance, strike the right balance between consumer protection and business freedom. Introducing new or overlapping withdrawal rules, such as mandatory additional confirmation steps or requiring a complete separation of trial and paid contracts, would create regulatory confusion and harm subscription-based business models.

Such measures would also reduce the availability of free or discounted trials, ultimately disadvantaging consumers who would lose access to risk-free opportunities to explore new services.

As the Commission considers new measures under the Digital Fairness Act, we urge policymakers to take a balanced, evidence-based approach that recognises the role of subscriptions in supporting independent journalism. The goal must be to protect consumers without undermining the business models that enable the production of trusted, professional news.

Ensuring proper enforcement of existing rules, rather than layering new regulatory burdens, will contribute both to consumer trust and to the long-term health of Europe's information ecosystem.

Avoiding one-size-fits-all obligations

The ability to advertise freely and lawfully is essential for the economic viability of independent news media. The processing of personal data for advertising, measurement, and performance analysis is indispensable for news publishers to understand their audience, improve services and demonstrate value to advertisers.

However, European publishers face an increasing regulatory burden, including GDPR, ePrivacy, DSA and voluntary initiatives like the Cookie Pledge, often designed with the dominant practices of large tech platforms in mind. These one-size-fits-all rules risk creating additional barriers for news media, particularly smaller news titles, while failing to address the real imbalances in the digital advertising market. Big tech platforms can easily absorb compliance costs; independent news media cannot.

To support news media independence and digital sustainability, the Digital Fairness Act must avoid rigid, prescriptive rules that unintentionally restrict legal, responsible, and

privacy-compliant business models in the news media sector. It should observe a risk-based approach, where the rules that must be observed reflect the nature of the actors and practices involved.

Instead, enforcement should focus on ensuring informed consent, preventing deceptive or manipulative practices, and supporting genuine user choice, while leaving room for diverse and legitimate monetisation models that fund journalism and protect the public interest.

Protecting the freedom to advertise is essential for the diversity of opinion, innovation, and editorial independence that underpins European democracy. The Digital Fairness Act should strengthen, not weaken, the ability of European news publishers to operate fairly and sustainably in a digital economy.

Design and engagement: a responsible use of digital features by news publishers

News publishers invest heavily in the development of their digital platforms to provide citizens with trusted, relevant, and diverse information. In an increasingly crowded and competitive online environment, where users are constantly exposed to countless stimuli, it has become more challenging to capture and maintain attention.

To ensure that users are able to discover and engage with high-quality journalism, news publishers make use of digital design features that enhance the user experience and help surface relevant content in a clear and appealing manner.

It is important to stress that news websites must remain freely accessible without age verification or other access restrictions. Press publications are primarily aimed at adult audiences and, unlike online platforms, typically do not require user profiles. Introducing an obligation to verify the age of all users would be disproportionate, technically burdensome, and would deter citizens from accessing trusted editorial content.

The Digital Fairness Act rightly highlights concerns about addictive design patterns, such as infinite scrolling, autoplay, or recommender systems that aim to prolong user engagement beyond intention. These concerns are valid, particularly where design choices are used to manipulate or exploit vulnerable consumers. However, it is important to distinguish between designs that are manipulative and those that responsibly improve relevance and accessibility.

In this context, recommender systems should not be treated as inherently problematic. In the case of news media, these systems serve a valuable role in guiding readers to relevant articles, improving personalisation, and increasing exposure to verified information. Rather than creating dependency, well-designed recommender systems support informed engagement and content diversity, helping readers stay up to date with current events and topics of personal or societal importance.

Similarly, autoplay can be a meaningful and non-intrusive feature when applied responsibly, for instance to play relevant video news clips that enrich the article content. The intent is not to trap the user, but to present journalistic content in a format that aligns with user preferences and current digital standards. Finally, we do not view infinite scrolling as inherently negative in the context of news consumption. News publishers aim to inform citizens about developments in the world around them, and infinite scrolling can support this by offering readers seamless access to a broader range of articles.

Publishers are aware of their societal responsibility and the importance of ethical design, particularly in relation to young or vulnerable audiences. This is reflected in editorial standards and business practices that put trust and user welfare first. We therefore urge policymakers to apply a balanced and evidence-based approach. Not all engagement-enhancing features are addictive by nature. Context, purpose, and proportionality should guide assessments of digital design.

The goal is not to manipulate engagement, but to ensure that quality journalism remains discoverable and accessible in a modern digital environment. In the case of the news media sector, well-regulated design tools are essential for the sustainability of quality journalism and public access to reliable information.

Political Advertising Regulation

These new rules are motivated by real concerns about protecting democracies against foreign interference. However, they have become very complicated and burdensome to implement due to the extensive requirements which are imposed on publishers of political advertisements (eg. media companies).

The regulation essentially forces publishers of political advertisements to engage in extensive data collection and verification exercises relating to the advertisements they display on their properties, and for which they are fundamentally not responsible for (the advertisers are).

The regulation also introduces restrictions on the targeting of political advertisements to individuals, when using personal data. Several of those restrictions, however, go significantly beyond and diverge from the applicable rules already found in the existing GDPR/ePrivacy framework.

The rules apply to publishers and online platforms in the exact same way irrespective of size, and so small publishers, local parties, and SMEs face the same requirements as large platforms.

Overall, the regulation failed to meet a simple common sense test: there is a real risk that compliance costs may exceed the limited revenues of this small advertising segment. And by the same token, the regulation has become overly complex and burdensome relative to the size of the market it regulates.

This has already led the largest dominant market actors such as Google, Meta and Microsoft to terminate their political advertising services in Europe, because of the burden created by those new EU rules.

Digital Markets Act (DMA)

The promise of the DMA was that a clear list of do's and don'ts would steer gatekeepers away from commercial practices that are known to harm business users and digital markets. In addition, that it would also facilitate swift and effective enforcement, while taking into account evolutions in the services of gatekeepers.

Unfortunately, the impact of the DMA on the business of news publishers has generally been disappointing. Fundamentally, the DMA has not led to meaningful changes in the commercial practices of gatekeepers that are most concerning and pressing for publishers.

While the DMA has had some early successes, these wins have mostly targeted consumer-facing issues rather than systemic imbalances affecting publishers, who remain constrained by the control of gatekeepers over advertising markets and traffic distribution.

Ambiguities and general lack of clarity in the obligations, leading to different interpretations

One of the main challenges is the ambiguity and lack of clarity in some of the DMA obligations, which results in diverging interpretations by gatekeepers, regulators, and business users.

Many of the DMA obligations such as those about self-preferencing and fair access to data, are broadly framed. For example, what constitutes "fair" or "reasonable" terms for access to data or ranking remains open for debate.

This lack of precision creates legal uncertainty for businesses meant to benefit from the DMA, such as news publishers, advertisers and app developers, who cannot rely on consistent enforcement or clear rights.

This also unnecessarily burdens the European Commission with the task of issuing clarifications or case-specific enforcement decisions. Ultimately, these ambiguities risk diluting the DMA's effectiveness, as protracted legal arguments delay meaningful changes in the market.

A more detailed example is that of Article 6(8) which requires gatekeepers to provide advertisers and publishers with the "data necessary" to carry out their own "independent verification" of the "advertisement inventory", including aggregated and non-aggregated data.

The meaning of several of those terms is unclear. Platforms may interpret this narrowly, disclosing only limited aggregate data rather than full, transaction- and auction-level details that would enable the meaningful auditing of gatekeeper services.

For publishers, this lack of clarity means they continue to face significant information asymmetries in digital advertising markets, limiting their ability to verify value, optimise revenues, and compete effectively. Instead of increasing transparency, vague provisions allow gatekeepers to comply formally while withholding the granularity of data that publishers need.

Lack of ambition and insufficient obligation concerning online advertising

Access to auction-level data is critical to achieve meaningful transparency in online advertising. Without insight into how individual impressions are priced and allocated in real time, publishers and advertisers remain dependent on the opaque and questionable self-reporting practices. This means that publishers are unable to verify the integrity and fairness of auctions or whether hidden fees and self-preferencing practices distort outcomes. Aggregate or delayed data is inherently insufficient because it masks discrepancies in bidding behaviour, pricing strategies, and demand.

Auction-level transparency would enable publishers to understand the real value of their inventory, strengthen their negotiating position, and foster competition among advertising technology intermediaries. In this sense, it is a catalyst for accountable competition in online advertising.

More broadly, the DMA is insufficiently far-reaching in addressing structural conflicts of interest in online advertising. The dual presence on the buy- and sell-sides gives gatekeepers the ability to unfairly set rules for auctions in which they participate, such that competition is artificially reduced.

This vertical integration creates inherent incentives for self-preferencing and discriminatory practices that transparency obligations alone cannot remedy. To ensure fairness, contestability and fair competition in the advertising ecosystem, the Commission should mandate structural separation between buy-side and sell-side functions.

Designating generative AI services as a core platform service

The integration of generative AI in search engines and other core platform services is shaping how users access information, content, and advertising. Yet standalone generative AI services are not a core platform service under the DMA, meaning the obligations on fairness, transparency, and non-discrimination may not apply.

This creates a regulatory gap. For example, when a generative AI system delivers answers directly to users, traffic to third-party sites including publisher sites can be diverted without transparency or fair compensation.

Without clear designation as a core platform service, regulators lack the authority to impose obligations and prohibitions such as those about audience measurement and self-preferencing. To keep pace with technological change, the DMA should explicitly cover generative AI services deployed by gatekeepers.

Google's AI Overviews: an enforcement case study

Google's launch of AI Overviews illustrates the urgent need for the enforcement of rules on self-preferencing and on fair, reasonable, and non-discriminatory (FRAND) terms. By presenting AI-generated summaries directly on top of search results, Google diverts significant traffic away from publishers, and towards their own products and properties.

This dynamic mirrors past concerns over Google's preferential treatment of its shopping service, which the Commission previously sanctioned. If AI Overviews systematically reduces the visibility of publishers while keeping users within Google's ecosystem, this amounts to self-preferencing. Moreover, ensuring FRAND terms is essential so that publishers are not excluded from the new AI-driven interfaces.

Without strong and consistent enforcement, AI Overviews are a direct threat to the business model of media companies, their financial sustainability, and by extension to media pluralism and freedom. The Commission must act decisively to clarify obligations in this area and prevent gatekeepers from using AI as a new means of entrenching dominance.

If the Commission's assessment is that this is not possible or justified, then the DMA should be amended to facilitate this kind of enforcement action.

Sector-specific enforcement guidelines for the media

To complement the various points already raised in this submission, the Commission should consider developing specific DMA enforcement guidelines for the media sector.

This is both necessary to better achieve the objectives set out in the DMA but also to protect the integrity and resilience of Europe's information space requires, a political priority already recognised across multiple EU initiatives.

It follows that better coordination between the DMA and the European Media Freedom Act (EMFA), which was adopted to support media pluralism, and the European Democracy Shield initiative must be facilitated.

Such guidelines should at least seek to:

- minimise algorithmic bias against media
- ensure a diverse range of sources in recommender systems

- clarify the application of FRAND terms to media content
- clarify the application of the prohibition against self-preferencing
- align the DMA and EMFA enforcement of provisions on audience measurement
- align the DMA and EMFA enforcement of provisions on the notification of concentrations.

Artificial Intelligence (AI) Act

While the AI Act rightly obliges providers of General Purpose AI to publish a “sufficiently detailed” summary of training data, the template released by the AI Office is alarmingly superficial. It lacks the specificity and granularity necessary for rightsholders to verify whether their copyright-protected content has been exploited, let alone to enforce their rights effectively.

Despite extensive consultations, the final outcome reflects the interests of major AI providers far more than those of Europe’s creative sector. The reliance on broad categorizations, undisclosed datasets, and narrative generalities makes it nearly impossible to determine whether protected journalistic content was used – especially content hidden behind paywalls or accessed in violation of scraping rules.

This means that the interpretation and implementation by the European Commission and its AI Office of the AI Act provision related to copyright lose their utility and effectiveness (effet utile). The failure to enable meaningful transparency means that the way in which the Commission chooses to enforce the AI Act prevents rightsholders from exercising their other rights acquired under EU copyright law.

The AI Act – and particularly Recital 107 – clearly states that summaries should empower rightsholders to exercise and enforce their rights. Yet the current Template enables opacity, not transparency. Requiring providers to reveal only the “top 10%” of scraped domains while shielding the majority of datasets from scrutiny renders enforcement a legal guessing game.

If the AI Act does not facilitate and enable the exercise of rights through meaningful transparency, then rightsholders must at least be able to operate in markets on the basis of a presumption that their content protected under copyright law has been used. That presumption must be codified in European law as a matter of urgency.