European Data Union strategy and digital simplification package:

Review of the ePrivacy directive

This note aims to:

- Identify practical implementation and governance challenges related to the ePrivacy Directive.
- Recommend how to address these challenges, and where and how the ePrivacy Directive should be streamlined.
- Outline IAB Europe's perspective on 'centralised consent management'.
- Identify relevant national guidance on the interpretation of Article 5.3 of the ePrivacy Directive and its implications for 'low-risk' digital advertising use-cases (see annex).

ePrivacy directive: challenges

Members of the digital advertising ecosystem are facing key barriers related to the ePrivacy directive, including restrictions of essential digital advertising functions, fragmented interpretation and enforcement across member states, and a lack of transparency and accountability from regulatory bodies (see table below).

Categorisation of 'cookies'	The current implementation of the ePrivacy Directive and its associated guidance requires consent for data storage and access techniques used in digital advertising, even in cases where they have become essential to the functioning of the ad supply chain or enable positive consumer outcomes and do not adversely impact user privacy, such as: • Reducing ad frequency • Ensuring cybersecurity and preventing ad fraud • Storing users' privacy choices. • Displaying ads • Measuring ad delivery These concerns extend to other essential use cases for operating online services, such as: • Cybersecurity and fraud prevention, extending beyond their applications in online advertising. • Software updating/patching and product maintenance. • Analytics, e.g. carried out to improve the website or information society service • Rendering essential information from commercial partners e.g.: banner from a consent management provider. This approach is outdated, not future proof and risks hindering innovative digital advertising services to develop, while degrading the online experience for many users. **Case studies**: Ensure cybersecurity and prevent ad fraud: These techniques play a pivotal role in identifying and preventing fraudulent

	traffic, including internet bots mimicking human activity. These techniques not only foster a safer online environment but also bolster the overall user experience by upholding ad delivery integrity. Reduce the number of ad placements: Our recent study demonstrates that a large majority of European users prefer fewer, targeted and more relevant ads, over numerous untargeted ads which creates a cluttered user experience. Ad frequency: The digital advertising industry has developed solutions to meet user needs, by tailoring and capping the number of times a particular ad is shown to the same user. This avoids users feeling bombarded by an individual ad. Display ads: These techniques are necessary to ensure that the format of the ad fits within content, thus improving users' browsing experiences. They also enable the customisation of ads to resonate with users, taking into account factors such as their country location or language. This customisation not only enhances user engagement but also ensures compliance with specific country rules. Measure ad delivery/effectiveness: The digital advertising industry relies on these techniques to count the number of ad impressions. This allows publishers and the actors of the ad supply chain to determine advertising charges and to be paid. For advertisers, measuring that an ad was effectively delivered is essential to manage their media spend. These practices sustain not only accurate billing but also foster fair

	and efficient revenue allocation in the digital advertising ecosystem.
Overly broad interpretations of key concepts in article 5(3)	The recent EDPB guidance on Article 5(3) presents an overly broad interpretation of "gaining of access" and "stored information." This inadvertently captures techniques that are part of the ordinary operation of the internet (e.g. as part of the Transmission Control Protocol / Internet Protocol) or the device. This approach carries several risks, including: • It expands regulation to essential technologies that do not harm consumer privacy. • It further increases the number of online interactions requiring consent, leading to greater consent fatigue and reduced user engagement with genuine tracking technologies. • It is counterproductive to the online experience of EU users, who would be forced to make 'consent' choices about critical processes in the online ecosystem; • It creates an almost complete overlap between ePrivacy and GDPR for any personal data collected in an online environment. • It undermines the GDPR's purpose limitation principle, which would otherwise allow the onward processing of related data for compatible purposes. More importantly, this expansive interpretation of article 5(3) fails to advance the directive's primary objective, namely protecting user privacy.

Utility of 'cookie' banners	Current regulator guidance prescribes the content and presentation of cookie banners. For example, providers are required to show "strictly necessary" cookies even though users cannot control them. Recent IAB Europe research shows that consumers understand the value exchange between targeted advertising enabled by cookies but increasingly do not find the information in cookie banners useful.
Limited legal base	Following the definition of consent adopted in the GDPR, non-essential cookies used under the ePrivacy Directive require consent and - as noted above - exceptions to this rule are extremely restricted and have become outdated. Insufficient consideration was given to the implications of this for complex supply chains, such as digital advertising. As noted above, compliance has been further complicated by EDPB guidance which brings a wider range of technologies within the definition of 'storage and access'.
Direct marketing restrictions	The ePD requires all organizations to obtain consent before engaging in certain types of electronic direct marketing (e.g., automated phone calls, fax, or "electronic mail" such as email, SMS messages, or push notifications on a device). There is a limited exception for sending direct marketing by electronic mail, i.e. if an organization obtains contact details in the context of a sale of a product or service, it can send marketing messages to those contact details about their own similar products or services, provided it gives the individual the opportunity to opt

	out at the time of collection of their contact details (articles 13(1) (2)).
Absence of lead authority	While GDPR is overseen by a single lead regulator for cross border processing activities - which are often the norm in the digital world - all member states have authority to oversee and enforce the ePrivacy directive. In some member states, different regulators oversee GDPR and the ePrivacy Directive. In others, some cases dealing with cookies have been enforced solely on the basis of the GDPR by data protection authorities. This results in fragmentation, uncertainty, duplicative oversight and enforcement, and ultimately greater compliance costs and risk, as well as reticence to innovate. As a result, enforcement of cookie rules has been inconsistent and the selection of cases is not always risk-based. In some cases, enforcement action was taken against some providers before: • Regulatory guidance was available to inform compliance. • The end of the grace period to implement the same regulatory guidance. This has made cookie uses more risky for some providers, and has resulted in no enforcement against others for non-compliance.

Lack of transparency and accountability from regulatory authorities	The European Data Protection Board (EDPB) and national data protection authorities lack transparency and clear processes for consulting and engaging stakeholders to inform their interpretation of data protection rules and regulatory guidance. They often adopt a top-down approach, developing complex and unworkable guidelines without prior consultation with businesses. There is no requirement to enable continuity of business or support the EU's competitiveness agenda. For example, the EDPB consultations on guidelines are ad hoc and where consultation does occur it appears as a cursory exercise with no transparency as to how feedback is evaluated and potentially incorporated in the final version which may have been predetermined. Businesses or trade bodies are not allowed to be heard by the EDPB. This lack of accountability from the EDPB and national DPAs discourages businesses from investing time in responding to consultation and contributing to the development of soft law.

IAB Europe recommendations on the review of the ePrivacy directive

General recommendations

IAB Europe supports the European Commission's ambition to simplify and streamline existing EU data legislation and in particular the ePrivacy directive. This is important to remove unnecessary complexity and reduce administrative burdens while safeguarding EU consumers, and ultimately restore the competitiveness of the digital (advertising) industry in Europe. The future European Data Union Strategy should provide a solid foundation to achieve these objectives.

Since its adoption in 2002 as part of the telecoms package, the ePrivacy directive has undergone several reforms, transforming it into a multi-faceted instrument that attempts to regulate a non-homogenous group of services/providers and advance disparate policy goals, ranging from privacy protection to market regulation, consumer protection, security, and law enforcement. Simplification can address the unintended consequences by bringing some of its current provisions into existing laws where they fit better, e.g:

- Processing currently under Article 5(3) should be moved into the GDPR and benefits from a wider range and more open legal bases. This would allow organizations to rely on legitimate interests for essential, low-risk processing. If kept in, low-risk processing should be rendered more flexible by allowing cookie placement without consent (see section on "specific recommendations").
- The list of 'essential' purposes that do not require consent should be revised to reflect the modern internet.
- The direct marketing rules in article 13, could be deleted and simply absorbed into the GDPR.

Beyond the scope of pure online advertising, further simplification measures should be considered, such as absorbing the provisions on metadata in the GDPR and modernizing the provisions on confidentiality of content.

Specific recommendations

The Commission should adopt a risk-based approach, in line with the GDPR, and support the digital industry in delivering the best possible user experience. The Commission should examine the effects of the prevailing interpretation of 'storage and access' and build understanding of what techniques are necessary to operate a digital publishing/commerce site in order to promote a more flexible, risk-based approach to data access and storage on user devices, consistent with the principles of the GDPR. Ultimately, this should result in tangible changes, including:

- User consent should not be required for 'low-risk' digital advertising use cases, which have become essential to the operation of a vibrant and open digital advertising market (see section "Challenges" above). These exemptions to the consent obligation could be expanded to encompass other low-risk and essential processing, e.g. for cybersecurity, anti-fraud, analytics, software updates and product maintenance goals.
- The Commission should exclude from the scope of article 5(3) ephemeral storage (such as pre-load scripts needed to interface with commercial partners e.g. to display consent banners) as well as information communicated as part of the ordinary operation of the internet (e.g., as part of Transmission Control Protocol

/ Internet Protocol) or the device, provided it is not specifically targeted by the sender or recipient (see section "Challenges" above).

The term "direct marketing" should be explicitly defined to ensure that all national regulators interpret it in the same way. This means covering marketing material that is directed to a specific individual (article 13). Additionally, any replacement legislation should clarify that the term "electronic mail" – which the Directive defines as any message that "can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" – applies to emails, SMS messages, and the like, but not to banner or similar ads displayed on apps and websites that are loaded and displayed when a user visits a particular page.

There is a need to unify regulatory oversight in a single jurisdiction, mirroring the GDPR model. This would increase legal certainty, while limiting the risk of duplicative guidance and enforcement. This proposal would also ensure more cost-effective compliance for businesses, which is one of the key objectives of the EU competitiveness agenda.

The operation of regulatory oversight should be reviewed to ensure it supports the EU's innovation and competitiveness goals. The roles and procedures of national DPAs and the EDPB should be reviewed to improve transparency and accountability. Concrete steps could include introducing explicit duties for them to have regard to harmonisation across EU countries as well as avoiding interpretations that lead to inconsistencies with other digital laws. In addition, some core principles should be embedded in their working methods to ensure their interpretations of EU rules are workable and support both business continuity and long term commercial decision-making. For example, they should evaluate the effect on innovation, competition and growth, aid company compliance and consult on annual programmes of work, enforcement strategies and draft guidance and opinions. National DPAs in particular should introduce frameworks for consulting their national stakeholders in order to inform their participation in EDPB discussions. National DPAs should make greater use of powers to endorse certification schemes and industry codes.

IAB Europe's perspective on 'centralised consent management'

IAB Europe remains concerned about any policy that would lead to mandatory centralised consent management for market participants, due to the following main reasons:

- **Centralised consent management may not align with all user preferences online.** Users value the ability to make choices about data collection on a per-website/app basis, often making different choices depending on the digital content or service. Centralized consent management reduces this agency. A recent IAB Europe study confirms that consumers are more willing to accept data collection when they trust and are familiar with the website.

- **This approach would impede publishers' capacity for direct and meaningful engagement with their audience regarding content financing.** Publishers, serving as the primary point of contact with users, are best positioned to provide context-specific information regarding consent requests, particularly for data collection related to digital advertising. They are also ideally placed to explain how digital advertising financially supports their online services. This is consistent with GDPR which requires the controller to obtain and record user consent.

- **'Consent gatekeepers' could emerge from centralised consent management, especially if managed by end-user agents like web browsers or operating systems**. The way these agents present user choices risks creating bias and discriminating against industry stakeholders, leading to competition issues. Apple's App Tracking Transparency (ATT) prompt, and its negative impact on app publishers and irreversibility for consumers, is a tangible example of this.

Annex: Overview of national and EU guidance on the application of article 5.3 of the ePrivacy directive

Juridiction	**Approach to 'low-risk' digital advertising use-cases**
France Guidance: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience	Cookies placed for audience measurement can be exempt from consent under certain conditions.

Spain	
Guidance: https://www.aepd.es/documento/guia-cookies.pdf	Exemption for the use of technologies such as cookies for the management of advertising spaces: *"Also belonging to this category, due to their technical nature, are those cookies that allow the management - in the most efficient way possible - of the advertising spaces. These spaces, as another element of design or layout of the service offered to the user, are included by the editor in a web page, application, or platform based on criteria such as the edited content, without collecting information from users for other purposes, such as personalizing that advertising content or other content."*
Guidance: https://www.aepd.es/guias/guia-cookies-analiticas-externas.pdf	Audience measurement solutions can be exempt from consent under certain requirements of the ePrivacy Directive.
Finland Guidance: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Sanoma%20Media%20Finland%20Oy.pdf	Exemption for the using of technologies such as cookies for the management of advertising spaces: *"According to Traficom's assessment, the purpose of the non-personalized distribution cookie on the front page is to enable a specific advertisement to be shown to Helsingin Sanomat readers once a day. Traficom considers that the non-personalized distribution cookie on the front page is necessary in the sense of Section 205 subsection 2 of the SVPL to*

	provide a service explicitly requested by the subscriber or user."
Italy Guidance: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876	Audience measurement solutions can be exempt from consent under certain requirements of the ePrivacy Directive.
Luxembourg Guidance: https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/cookies/CNPD-LD-Cookies.pdf	Audience measurement solutions can be exempt from consent under specific requirements. The document outlines conditions for exceptions concerning certain analytical cookies.
EU Guidance: EDPB Guidelines on Legitimate Interest	Using legitimate interest for the purpose of fraud prevention might be justified but it requires case-by-case assessment (reference to recital 47 GDPR as well).