

IAB EUROPE POSITION ON THE PROPOSED ePRIVACY REGULATION¹

31 October 2018

Summary

- The ePrivacy Regulation should maintain a clear unqualified permission for private actors to make **access to online services conditional on the well-informed consent of the user** to data processing for advertising purposes that is not strictly technically necessary for provision of that service but which is necessary for the monetisation model chosen by that service. Any additional requirements, such as having to make available a paid-alternative, is to be avoided.
- Article 8(1) ePR should be amended to fully align it with the **principles-based approach of the GDPR on lawful processing**, including processing necessary for a legitimate interest where the fundamental rights of a data subject are not overriding, instead of a rigid list of specific exceptions to a general consent requirement.
- **Article 10 should be significantly amended or deleted** in order to avoid requiring browsers to block processing at a technical level. The effect of such a rule would mean in most cases that services requested by users could not function properly without users changing their browser settings. This will result in more user irritation as websites would prompt users to do so.
- Lawmakers should take the necessary time to thoroughly assess and consider any new provisions, also bearing in mind experience and observations gained since the GDPR's implementation rather than pursuing expedited adoption of the ePrivacy Regulation. Experience with the GDPR has shown the importance of a reasonable **transition period of 18-36 months** to afford businesses enough time to assess the new rules and make the necessary changes to their privacy policies, products and services, as well as for industry standards to be adapted to enable compliant processing.

Introduction

Data-driven advertising is the single largest revenue source for European digital media, making up more than 80 per cent of the online revenues for publisher's journalistic content and more than 50 per cent of mobile application revenues.² The proposed ePrivacy Regulation ("ePR") threatens to harm European digital media outlets' economic model by significantly undermining their ability to generate enough revenue to create and provide free online content and services, thus also limiting media pluralism and public debate and discourse online. The free, advertising-funded business model is overwhelmingly preferred by European citizens, 83 per cent of whom prefer free content - with advertising - to being required to pay; indeed 68 per cent of European internet users say they would

¹ IAB Europe is a trade association that represents the online media and advertising industry. For an overview of members see <https://www.iabeurope.eu/membership/member-directory/>. For more information about IAB Europe's position on the ePrivacy Regulation please contact [Matthias Matthiesen, Director – Privacy & Public Policy \(matthiesen@iabeurope.eu\)](mailto:matthiesen@iabeurope.eu).

² IHS Markit, The Economic Contribution of Digital Advertising in Europe, available at http://datadrivenadvertising.eu/wp-content/uploads/2017/09/DigitalAdvertisingEconomicContribution_FINAL-1.pdf

never pay for news content online, even if no free content were available.³ This showcases the importance of the data-driven advertising business model to European consumers.

The GDPR and the ePrivacy Regulation

Businesses and industry organisations, with support from data protection authorities and the European Commission, have been working in good faith toward purposefully applying the GDPR since May 2018. For example, IAB Europe and its members developed the Transparency & Consent Framework, which increases transparency, choice and accountability in relation to how personal data is processed by different actors in the online media and advertising sectors. Already, it is the largest industry program of its kind with over 500 technology company subscribing to its rules and more than 100,000 websites and apps in Europe and beyond having implemented the framework. The prospect of the hard-won compromise rules of the GDPR being altered by the ePrivacy Regulation has therefore created significant legal uncertainty and has raised concerns that efforts and investments already undertaken to achieve GDPR-compliance could be undermined. IAB Europe therefore calls on lawmakers to bear in mind the context of the GDPR in which the discussions around the ePrivacy Regulation takes place, and urges them to understand the interplay and focus on aligning the two instruments rather than introducing divergent rules on the same issues. In addition, IAB Europe calls on lawmakers to ensure a reasonable transition period of 18-36 months to allow adequate time to reflect changes to the law in businesses' privacy policies, products and services, as well as industry standards.

1. Consent as a condition for accessing a service

While IAB Europe believes that the cookie provision should reflect the lawful grounds for processing of the GDPR beyond only consent, IAB Europe also believes it critically important that the future ePrivacy Regulation maintains the clarification that where processing is based on consent, access to an online service may be made conditional on the well-informed consent of the user to data processing that is not strictly technically necessary for provision of that service, for example advertising-related purposes. Failing to do so would put advertising-funded services on the Internet as we know it in jeopardy, result in a steep decrease in the quantity and quality of free services, and/or result in the erection of paywalls for previously free services. The forced erection of paywalls in order to continue offering previously free services is a key concern for the digital media and advertising industry as it is a severe interference in a digital media service's right to choose its own business model and to determine the terms under which it makes its service available to consumers. Such an interference touches on the fundamental right to property and the freedom to conduct business, which must be considered and carefully balanced with the fundamental right to privacy and data protection that the ePrivacy Regulation attempts to protect. IAB Europe does not support an obligation on online services to provide any alternative offers if they wish to continue providing a free, data-driven advertising-funded offering.

³ GfK, Europe online: an experience driven by advertising, available at http://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf.

2. Protection of Information on a user's device (“Cookies”)

All lawful grounds for processing personal data provide ample protection of users, including control and transparency about the processing, while giving the law the necessary flexibility to stand the test of time. IAB Europe does not consider it necessary to change principles adopted as recently as those of the GDPR, however if there were changes they should at minimum respect the flexibility and diversity of legal processing under the GDPR. This could be achieved, for example, by building on the principles of the GDPR and particularising them by requiring additional safeguards be put in place where the ePrivacy Regulation applies. According to the European Commission's impact assessment on the ePrivacy Regulation, derogations from the ePrivacy Regulation's general consent requirement with adequate safeguards such as the one proposed by IAB Europe “could lead to the emergence of innovative, privacy friendly business models and technical solutions” and “stimulate the R&D in privacy preserving technologies” such as anonymisation and pseudonymisation techniques.⁴ IAB Europe welcomes the Council's introduction of new exemptions, such as for security and fraud prevention and security updates, but rather than considering a rigid menu of specific exemptions that may already be outdated by the time the ePrivacy Regulation enters into force, an open norm with safeguards would be a more future-proof alternative.

3. Software privacy settings (Article 10)

IAB Europe welcomes the intention of the European Commission to address the “overload of consent requests for internet users” by allowing users to express their consent on a *general* basis. However, it is doubtful that this would reduce the amount of notices users receive as *general* consent does not meet the specificity requirement of consent under the GDPR, this means users would still face *specific* consent requests in addition to the *general* consent of the software layer.

Where processing is based on consent it is important that legislation does not dictate which technologies must be used to do so, as to not unnecessarily inhibit innovation around providing information and requesting consent in the most appropriate fashion.

IAB Europe also has severe concerns about mandating browsers and other software enabling access to the Internet to provide the option to *prevent* use of processing and storage capabilities of terminal equipment and the collection of information from end-user's terminal equipment. This would make it technically impossible for a service to lawfully collect or display information. Browsers and other software are not able to distinguish between technologies that are necessary for a service to function and technologies that are not strictly necessary, processing that is lawful and unlawful, exempted or non-exempted. As a result, services would not function properly or require users to change their browser settings in order to use a service, thus adding more irritation without added value.

⁴ Ibid, SWD(2017)3 Part 1/3, pp. 40-41.