



ETNO-GSMA comments on EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

January 2024

The protection of customer privacy and the confidentiality of their communications is at the core of the services offered by telecom operators. While these rules establish the foundation for delivering secure, trusted telecommunications services in Europe, they must also provide a degree of flexibility to enable European telcos to use data to improve customer experience, bring societal benefits, and, in general, keep pace with innovation and competition.

Now that the General Data Protection Regulation (GDPR) has been in force for over seven years, a significant body of experience and jurisprudence has developed regarding its application. It is crucial that the e-Privacy rules align with the GDPR, enabling the European industry to remain competitive in the growing field of data analytics and take a leadership role in responsible artificial intelligence.

ETNO and the GSMA regret that the old e-Privacy Directive (ePD) has become untenable in light of and legal and technological developments that have occurred over the past decade. A series of EU regulations governing the use of personal and non-personal data, such as the Data Act, Data Governance Act, Digital Markets Act, and the soon-to-come Artificial Intelligence Act, have been added to the GDPR. Together, they form a richer framework that combines data privacy with the promotion of competitiveness and innovation. The ePD no longer fits this evolving regulatory landscape.

Furthermore, with specific reference to the subject of the EDPB Guidelines 2/2023, the GDPR has *de facto* compelled data controllers to revamp their cookie policies and notices. At the same time, there is a general realization that an excessive reliance on user consent can lead to 'cookie fatigue,' diminishing the significance of consent itself. The European Commission has openly raised concerns about the 'cookie fatigue' and initiated a reflection on how to better empower consumers to make effective choices regarding tracking-based advertising models.

Overreliance on consent poses particular challenges in the telecom sector. Telco customers often use terminal equipment, such as Wi-Fi routers or industrial equipment, that may lack a digital interface. This absence complicates the collection and management of consent. Furthermore, such equipment is typically shared among different users, like a family, creating additional identification challenges in seeking consent from the correct user.

Given the above, we are concerned that the EDPB's attempt to contextualize Article 5(3) ePD in light of emerging tracking tools highlights the evident misalignment of the ePD with modern data processing technologies and user expectations. The overly broad interpretation of the applicability of Article 5(3) ePD to any information storage and access in any terminal equipment may pose unjustified challenges to operating ecosystems based on the Internet of Things and Edge computing. Such an interpretation may also create legal uncertainty, impeding the consistent application of the ePD itself in the telecom sector. This is due to the broad interpretation presented by the EDPB, which may, at the same time, trigger the application of Article 5(3) and Articles 5(1) and (2) ePD in certain situations. This is especially relevant when telcos engage in communication protocols or instructions from/to the terminal equipment, enabling users to connect and access core services such as internet access and TV.

In fact, this broad interpretation of Article 5(3) leads to some artificial constructs that would be unrealistic to implement in practice, such as requesting consent for URL tracking or pixel tracking, often used solely for counting impressions without containing any other information. If consent is required for these techniques, it might lead companies to revert to using cookies, which often store more information and are less privacy-preserving. Additionally, the broad interpretation extends to the concept of 'gaining access', encompassing examples that could be deemed essential for the provision of services.

It is the right time to thoroughly reassess whether the e-Privacy rules remain an adequate component of the existing EU data framework and whether they impede, rather than advance, the EU's goals of a flourishing data economy and trustworthy artificial intelligence. The failure of EU institutions to adopt a new e-Privacy Regulation (ePR) seven years after the draft law was proposed by the Commission also calls for serious reflection, especially considering that the proposed ePR is now outdated. In this context, the recent [European Commission's study on digital advertising](#) has called for a more transparent, balanced, and sustainable digital advertising ecosystem. Ultimately, it advocates for a reform of the digital advertising ecosystem, as the *status quo* is deemed unsustainable for European publishers, advertisers, and citizens. The study highlights gaps in the regulatory framework, such as Article 5(3) ePD, which allow many identified imbalances to persist. The current legislative framework strengthens the position of online players with the most control and insight into people's online behavior, while weakening the ability of other companies, especially advertisers and publishers, to communicate directly with their customers. This imbalance has resulted in an accountability crisis in digital advertising, where individuals are expected to navigate a complex web of myriad companies to control the types of ads they see online.

The e-Privacy rules should undergo a thorough reconsideration, maintaining a strong focus on the principle of confidentiality of communications while acknowledging the broad applicability of the GDPR to any personal data, including the possibility to process electronic communication metadata based on clear safeguards and protections in full alignment with the GDPR regime. Such a framework would effectively safeguard the privacy of citizens, adapt to rapid technological developments, and promote the responsible use of data as a key driver for innovation and competitiveness in European industry.