FEDMA
Federation of European Data and Marketing

FEDMA Response to the European Commission's Call for Evidence: Digital Omnibus (Digital Package on Simplification)

FEDMA welcomes the Commission's initiative to simplify and streamline the EU's digital regulatory landscape through the Digital Omnibus. We strongly support efforts to reduce administrative burdens, enhance legal clarity, and ensure the digital rulebook is fit for purpose in a rapidly evolving environment. In particular, we urge the Commission to address the persistent complexity and fragmentation caused by the coexistence of the ePrivacy Directive (EPD) and the General Data Protection Regulation (GDPR), and to pursue a harmonized, future-proof approach to privacy and data protection, as well as better coordination between national supervisory authorities, before contemplating the need for new rules.

We therefore advocate for the **repeal of the existing ePrivacy Directive (EPD)** and the **integration of relevant privacy and security provisions into existing horizontal frameworks** such as the GDPR, the European Electronic Communications Code (EECC), and the forthcoming Digital Network Act (DNA).

FEDMA would like to stress the following key areas for simplification

a) Security of Processing

The EPD's requirements for security of processing and breach notification are already comprehensively addressed by Article 32 of the GDPR and related provisions. The dual notification regimes under the EPD and GDPR create confusion and unnecessary administrative burden. FEDMA recommends repealing EPD Article 4 and relying solely on the GDPR's advanced, horizontal security framework.

b) Traffic and Location Data

Both traffic and location data are now recognized as personal data under the GDPR, subject to its robust legal bases and transparency requirements. The EPD's sector-specific restrictions are redundant and should be repealed, with the GDPR providing the necessary safeguards for all actors, not just telecom providers.

c) Confidentiality of Communications

The GDPR already guarantees confidentiality for communications involving personal data. For non-personal data, such as data related to legal persons, any additional confidentiality requirements should be addressed in the EECC or DNA, not in a separate privacy instrument. Furthermore, this aspect is also part of protecting business secrets, which is already protected by national laws and EU laws, such as the Directive on trade secrets, the Cyberresilience Act, the NIS Directives, and the Cybersecurity Act, which is part of the digital omnibus itself. Any new regulatory layer will just add more confusion for all stakeholders.

d) Unsolicited Communications

The GDPR's requirements for a legal basis (consent or legitimate interest) and the right to object provide effective safeguards for direct marketing. GDPR's risk based approach allows direct marketing taking place through different electronic channels, i.e. telemarketing, email- and text messages marketing, each associated with different levels of risks to data subjects, to be governed effectively. The EPD's technology-specific rules are unnecessary and should be repealed.

e) Cookies and Similar Technologies

FEDMA strongly supports the Commission's aim to reduce "consent fatigue" and improve user experience. The EPD's blanket consent requirement for cookies has proven ineffective and burdensome. We recommend **regulating cookies under the GDPR**, allowing for legal grounds beyond consent (e.g., legitimate interest for analytics and certain advertising cookies) and **implementing a risk-based, purpose-driven approach** to cookies, with clear transparency, user control, and privacy-enhancing technologies.

Use case of defending telemarketing under the ePrivacy Directive

FEDMA recognizes the importance of telemarketing as a legitimate and valuable channel for businesses to reach consumers, promote products and services, and support economic growth. The EPD currently regulates unsolicited communications, including telemarketing, by requiring either prior consent (opt-in) or providing users with the opportunity to object (opt-out), depending on national implementation. Telemarketing remains an essential tool for businesses, especially SMEs, to connect with customers (both existing and prospects), inform them about relevant offers, and support competition in the digital single market. Overly restrictive rules risk stifling innovation and limiting consumer choice.

The opportunities provided by PETs

The broad interpretation of personal data by some data protection authorities has blurred the line between personal and non-personal data. The lack of a clear boundary complicates data reuse, hinders effective data governance mechanisms, and puts Europe's data economy at risk. But following the CJEU SRB case, regulators have an opportunity to agree collectively on the criteria that would determine that data is non reasonably and legally identifiable and is not personal data and therefore not subject to the GDPR. That would bring much needed legal certainty, helping all public or private organisations of all sizes to figure out quickly which legal regime applies to their data related activities. Instead of introducing additional layers of complications, a practical approach would be to promote the use of Privacy-Enhancing Technologies (PETs), which the marketing industry has been embracing for many years. For example, a regional supermarket and a car dealer collaborating on a music festival ticket giveaway would want to avoid sending duplicate offers to the same customers. Instead of exchanging customer databases directly, which

would expose personal data, they can use a PET to securely match and deduplicate records. A service provider can then manage the campaign messaging on their behalf, ensuring customer privacy. Such protection results in striking the right balance between the protection of personal data while allowing organisations to be innovative and carry out effective marketing campaigns.

Interplay with the AI Act:

Because AI is trained on vast amounts of data, the data laws and in particular the GDPR also apply to the training of AI models/systems with personal data. The risk classification of the AI Act does not align with the risk based approach of the GDPR and its interpretation by the data protection authorities. They tend to consider that the use of new technologies and the processing of large scale of personal data is high risk and therefore requires a data protection impact assessment (DPIAs). The AI Act only requires a fundamental right impact assessment in limited circumstances (article 27). The digital omnibus offers a key opportunity to clarify that DPIAs are only required for AI model/system training that fall under Annex III of the AI Act. This clarification will drive greater clarity, consistency, and legal certainty, ultimately benefiting AI innovation.

Also for AI, the use of PETs, in particular the pseudonymisation and anonymisation techniques enable to protect the right to personal data, while allowing AI models/systems to be trained in a robust, responsible manner.

Conclusion

FEDMA believes that the Digital Omnibus presents a unique opportunity to modernize and simplify the EU's digital regulatory landscape. By repealing the EPD and relying on the GDPR and updated sectoral legislation, the European Commission can achieve its objectives of reducing administrative costs, enhancing legal clarity, and supporting innovation, while maintaining a high level of data protection and privacy for individuals. Instead, the Digital Omnibus can incentivise organisations to make use of PETs which can strike the right balance between effective protection of data and innovation.

We remain at your disposal for further consultation and look forward to contributing to the next steps and related initiatives.

FEDMA

Federation of European Data and Marketing

Federation of European Data and Marketing
155 rue de la Loi, 1040 Brussels
+32 2 779 4268 www.fedma.org