Position paper

02 February 2021

FEDMA's renewed recommendations on the proposal for an ePrivacy Regulation

Aware of the frustrations, and to a certain degree exhaustion, created by the proposal for an ePrivacy regulation after four years of negotiations, FEDMA feels that, **despite some progress under the current Presidency, a number of issues do remain unsolved** and their adverse implications are also becoming clear in other policy areas (e.g. competition, Artificial Intelligence, Big Data). Specifically, we believe that the proposed Regulation reaches beyond its scope of confidentiality of communication and privacy to cover processing of personal data, which is already regulated by the GDPR.

In this context, FEDMA calls to:

I. Fully integrate the GDPR's risk-based approach into the ePrivacy by **deleting Article 8 1(a) which provides that only anonymous data can be shared with third parties**. This deletion will support EU's efforts to reap the benefits of the Data Economy within the EU data protection framework. This deletion will also ensure contestability of digital markets dominated by gatekeeper platforms.

II. Fully apply the GDPR to B2C relationships based on soft opt-in by **deleting in Article 16(2a) the possibility of a horizontal time limit for consent**.

III. Preserve end-user's individual consent over telecom providers' technical solutions blocking direct-marketing calls by **deleting in Article 14 (3) the possibility for telecom to automatically block all incoming marketing calls**.

You fill find hereunder explanations to justify our calls.

I. Fully integrate the GDPR's risk-based approach into the proposed ePrivacy Regulation.

Setting the rules on how to access information on an end-user terminal equipment falls under the scope of the ePrivacy. However, as it is now, the proposed ePrivacy regulation is moving in the direction of restricting the processing of personal data to the sole ground of user's consent. As cookies in usually contain personal data, **the processing of information from end-user's terminal equipment is without doubt subject to the GDPR's principles set out in Art.5 which are binding on all processing of personal data, whichever the lawful ground relied upon under Art.6.** FEDMA believes that a consent-only scenario creates a one-size-fits-all solution which overlooks the GDPR's risk-based approach, thus undermining EU's efforts to uptake the data economy and ensuring fair and open digital markets. In doing so, the GDPR supports a flexible risk-based approach which aligns the level of safeguards and obligation to the level of risks inherent to the processing. The **concept of pseudonymisation developed in the GDPR is one example of the existing tools for flexibility**.

Federation of European Direct and Interactive Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

While the GDPR clarifies that pseudonymised data is personal data, it also recognizes that data which have been pseudonymized present less risk to the data subject (GDPR recital 28). *As an example, the concept of pseudonymisation can apply to cookies/online identifiers, used for online behavioural advertising activities: when personal information about an individual is pseudonymised, advertisers could serve online advertisement on the basis of general characteristics, for example, preference for fine food and wine, without having access to specific personal information about them.*

Such risk-based approach enables marketers to take into consideration all the relevant factors that impact personal data processing (e.g. whether in a BtoB or BtoC environment) and to apply the necessary safeguards in order to protect individuals, while furthering innovation and the technology neutral aspects of the instrument. However, the consequences of failing to introduce this flexibility in the proposed ePrivacy reugulation go beyond the data marketing sector and would severely undermine Europe's ability to take advantage of the potential of big data in the areas of artificial intelligence, energy transition, manufacturing, cooperative intelligent transport systems, medical technology, etc., thus jeopardizing the objectives stated in the European Data Strategy. *For instance, the use of mobility data which is proving essential to contain the spread of coronavirus and contribute significantly to the twin transitions of digital and green would be adversely affected by the restrictive rules of the proposed regulation.*

Restricting user's consent as the sole legal basis in Art.8 would also deepen the asymmetrical access to data in the EU Digital Single Market at the advantage of few dominant digital players. Specifically, while individual websites will have significantly fewer users consenting to the collection of terminal equipment's data, global digital platforms will increasingly benefit of their "login data ecosystems" which allow them to easily obtain consent from end-users in exchange for access to an increasingly broad range of services. The resulting asymmetrical concentration of aggregated user data in the hands of a few digital platforms will increase the dependency of the European marketing and publishing economy on these global players, strengthening entry barriers for newcomers. FEDMA therefore believes that such scenario defies current EU's effort to ensure the contestability of digital markets under the proposed Regulation for a Digital Markets Act (DMA) and hinders the objective of having a competition neutral regulation.

II. Fully apply the GDPR to B2C relationships based on soft opt-in

Enabling Member States to set a horizontal time limit on soft opt-in (Article 16(2a)) represents a further example on how the proposed ePrivacy Regulation reaches beyond its scope of confidentiality of communication and privacy to cover processing of personal data, which is already regulated by the GDPR. **This will create confusion with the implementation of the GDPR principles under article 5 (e.g. lawfulness of processing, data minimization and accuracy).** Indeed, Regulation 2016/679 provides for consent and, in line with accountability, consent is valid on a case-by-case basis unless it is withdrawn by the Data Subject (Article 21(2) provides that recipient of direct marketing communication shall always have the right to object to the processing of his/her data at any time for direct-marketing purposes). For example, a consumer receiving regular newsletters with opt out

Federation of European Direct and Interactive Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

options, can at any point choose to opt out. In addition, the Data Subject must also be informed on storage period of the data or the criteria to determine that period.

Furthermore, **there cannot be a one-size-fits-all time limit for a soft opt in as this relies on various criteria such as the life cycle of the product as well as the possibility to win back the Customer,** when there is a significant response rate and Return on Investment (ROI). The GDPR already recognizes that this time limit cannot be horizontally set in a specific manner and provides the principles to help controllers remain accountable with a risk-based approach. This especially applies in the context of direct marketing where, for instance, the retention of a consumer's data following the sale of a car is expectedly longer than for the sale of a pair of shoes. In this case, should a Member State decide to set a narrow time limit on the soft opt-in, the added value of that soft opt-in for the car would not only be unfairly lower than for the pair of shoes, but it would also overrule the GDPR. Such a horizontal time limit also increases the reliance of SMEs on major stakeholders operating within walled gardens, where time limits are much easier to overcome.

III. Preserve end-user's individual consent over telecom providers' technical solutions blocking direct-marketing calls.

The Council's pending proposal requiring providers of communication services to offer users the possibility to choose to automatically block all incoming marketing calls (Art.14(3)), that *may be* required to be labelled as such through a prefix or code (Art.16(3)a) risks making the end-user's individual consent irrelevant, thus jeopardizing well-established relationships between marketers and customers.

In the context of a common prefix for all marketing calls, longstanding customers, having consented to telemarketing, might decide to activate the prefix option from their telecom provider, no realizing the impact on their favorite brand. The telecom could automatically block all marketing calls, including the ones those customers had previously given their consent to receiving. In other words, the technical solution implemented by the telecom provider would override the individual consent of customers to specific marketing calls**. This would therefore create a situation similar to where software settings prevail over consent directly expressed by an end user: a scenario currently prohibited under Art.4(2)aa of the latest proposal by the Portuguese Presidency.** Additionally, bad companies who do not apply the prefix could easily circumvent the telecoms' blockage, thus gaining an unfair competitive advantage over compliant businesses and creating disincentives towards non-compliance in countries where the prefix will be introduced.

Federation of European Direct and Interactive Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org