Position paper

ePrivacy Regulation Proposal

The Federation for European Direct and Interactive Marketing (FEDMA) welcomes the proposal from the European Commission for the review of the ePrivacy Directive. FEDMA would like to take this opportunity to contribute its expertise to the debate and share its experience in the application of the current ePrivacy Directive by the direct marketing industry, as well as its vision for the future legal framework.

1. Relationship between the GDPR and the ePrivacy

GDPR and ePrivacy Directive, what it means for direct marketing

Direct marketing communications fall within the scope of the General Data Protection Regulation (GDPR), which lays out the individual's right to object to the processing of personal data for direct marketing purposes, including related types of processing such as profiling. It also reinforces and creates new rights which are crucial for protecting the privacy of individuals in Europe, such as the right to be forgotten and the right to data portability. **The ePrivacy Directive complements the GDPR** by providing specific privacy rules for sending commercial electronic communication.

The ePrivacy Directive, and the new text to replace it, are lex specialis of the 95/46/EC Directive on the protection of personal data (soon to be replaced by the GDPR), providing specific rules for the electronic communication sector. The GDPR and the ePrivacy Directive are complementary to each other and must be aligned, to ensure a clear, coherent and consistent set of rules for privacy and data protection.

Nevertheless, the ePrivacy directive also includes a number of provisions which regulates the condition for a marketer to send commercial electronic communication to an individual. There is **a clear distinction between the GDPR, which addresses the collection and process of personal data for direct marketing purposes (data protection), and the ePrivacy Directive, which details the condition for a marketer to send a commercial electronic communication to an individual (privacy).** Understanding this distinction is essential to ensure that the new ePrivacy instrument does not duplicate existing rules of the GDPR, but focuses solely on the conditions for sending/receiving commercial electronic communication.

Ensuring Coherency between the 2 texts

One of the objectives of the review of the ePrivacy Directive is to ensure coherency of the text with the newly adopted General Data Protection Regulation (GDPR). This should be done by avoiding any overlap of provisions between both texts which may create confusion and legal uncertainty. Each provisions of the ePrivacy Directive must be evaluated in light of the adopted GDPR in order to assess whether they are already covered by the new broad data protection framework. Furthermore, the effectiveness of each provision must be assessed in light of the objective of the review set up by the European Commission.

FEDMA believes that legislators should refrain from setting in the future ePrivacy instrument new requirements which go above the ones set by the GDPR, in a spirit of coherency and consistency. The GDPR represents an important change organization must get accustomed to. Midway into the implementation period, organization are now putting all their efforts in understanding the GDPR, and apply it to their respective practices. This is a huge work which requires efforts and many resources. It is important that such dedicated efforts are not disrupted in a near future by an additional piece of legislation which may not be fully aligned with the first one.

Focus on processing of electronic communication personal data

In order to efficiently protect both individual's personal data and privacy, the legislators must ensure that the scope of the ePrivacy Regulation applies to personal data, as does the GDPR, and not to any electronic communication data. The broad definition of personal data developed in the GDPR ensure that any data which can directly or indirectly identify a data subject is included in the definition, thus is subject to the GDPR. This definition has been strengthened by the decision of the Court of Justice of the European Union in the case C-582/14[1], which clarified that IP addresses are likely to be considered as personal data even when processed by another controller than the internet service provider. Considering the broad definition of personal data and the objective of the ePrivacy Regulation to protect individual's privacy, FEDMA calls for the new ePrivacy Regulation to focus its material scope to the processing of electronic communication personal data.

Maintaining a risk based approach and pseudonymisation

Coherency and compatibility should also be strengthened by including in the new ePrivacy Regulation important concepts adopted in the GDPR. In particular, the risk based approach and the concept of pseudonymisation which provide the GDPR with its risk based approach should be included in the ePrivacy instrument. Including these two concepts within the new ePrivacy instrument will ensure that both texts benefit from the same flexibility while affording the necessary protection of fundamental rights.

The risk based approach in the GDPR aligns the level of safeguards and obligation to the level of risks inherent to the processing. Taking the same approach in the ePrivacy Regulation would prevent a "one size fits all" solution where consent is the only way electronic communication data can be processed regardless of the safeguards in place.The concept of pseudonymisation developed in the GDPR is one example of the existing tools for flexibility in the GDPR. While the GDPR clarifies that pseudonymised data is personal data, it also recognizes that data which have been pseudonimized 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 behavioral advertising activities. When personal information about an individual is pseudonymised, advertisers could serve online advertisement on the basis of general

[1] http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf

characteristics, for example, preference for fine food and wine, without having access to specific personal information about them.

The risk based approach enables the marketer 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 technology neutral aspects of the instrument. Failing to introduce this flexibility in the new ePrivacy instrument could severely affect the ability of the European Union to take advantage of the potential of big data.

2. The definition of direct marketing

Direct marketing is defined by its ability to address a message directly to an individual.FEDMA, as the Federation of European direct marketing, has worked extensively in the past to develop a comprehensive definition of direct marketing based on directing of communication to particular individuals. The FEDMA code of practice on the use of personal data for direct marketing defines direct marketing as follow:

The communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc…) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals.

This definition has been approved by the article 29 Working Party in 2010 when the authorities published the opinion 04/2010 on the FEDMA code.The definition at the time was inspired by the UK Data protection act which defines direct marketing as "*the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals*".

The core concept of direct marketing is that the communication is directed to a particular individual. Direct marketing is not defined by the nature of the communication. Such communication can be commercial, political or charitable while being direct marketing. Additionally, direct marketing is not defined by the channel or the communication tool used. It can happen using any communication channel which enables access to particular individuals. It is technology neutral and omnichannel. Direct Marketing is communication of any advertising or marketing material which enables organisations to dialogue with a particular individuals, either on or offline.

FEDMA is concerned that the proposal from the European Commission of a definition of direct marketing communication may not reflect the principles mentioned above. In particular, FEDMA feels that the proposed definition deviates from the core concept that a direct marketing communication must *be directed to a particular individual*, which, as a consequence, may provide for a broader scope (including all advertising and not only direct marketing).

Additionally, while FEDMA understands that the ePrivacy Regulation must focus on electronic communications, it is important to realize that direct marketing communications can also take

place in an offline environment. For this reason, the FEDMA definition remains technology neutral, and FEDMA insists that this clarification is maintained in any definition of direct marketing.

Finally, FEDMA believes it is important to clarify that direct marketing is not spam, as such confusion seems to happen in many discussions on the ePrivacy Regulation. When discussing the provision on unsolicited communication in article 16 of the ePrivacy Regulation proposal, this distinction must be kept in mind. Spam activities are already clearly forbidden. The purpose of article 16 is to determine the condition under which lawful direct marketing communication can take place. Direct marketing communications are unsolicited communications which are send under strict regulated rules (i.e. Article 13 ePrivacy Directive, Unfair Commercial Practices Directive, National legislation), and operates on the recipients consent (either a prior consent, or opt out) depending on the applicable law. Opposed to unsolicited communication, spam is unwanted communication, where the communication is send regardless of the objection of the individual, or without his or her consent, and in complete breach of the rules, and against the user's expressed choice. While direct marketing is authorized and regulated, spam activities are already in breach of the law.

3. Confidentiality of terminal equipment and privacy settings - article 8.1 & 10

Article 8.1 and lawful processing under the GDPR

The proposed article 8.1 of the ePrivacy Regulation proposal aims at protecting users' information stored in and related to end users' terminal equipment. While being technologically neutral, the proposal's main intent is to legislate the use of cookies and other technologies enabling online tracking.

Cookies are personal data. When adopted, the GDPR specifically included online identifiers in the definition of personal data (article 4.1 GDPR) such as "IP address, cookies identifiers or other identifiers such as radiofrequency identification tags" (recital 30 GDPR). The GDPR applies without doubt to the collection of information from end-users terminal equipment, including from software and hardware. Consequently, the collection of personal information from an end-user's terminal equipment is submitted to the rules laid down by the GDPR for the processing of personal data, such as collection, storage and retrieval. The GDPR allows the processing of personal data under seven principles (article 5 GDPR) including the principles of lawfulness, fairness, and transparency, purpose limitation and data minimisation. These principles are binding regardless of the context of the processing, covering processing personal data from a terminal equipment (phone, tablet…) as much as in any other situation.

In order to be lawful, the processing of personal data must be based on at least one of the legal grounds described in article 6 of the GDPR. The legal grounds for processing personal data include the data subject's consent, the performance of a contract and the legitimate interest of the data controller under certain conditions. The article 29 Working Party stated in opinion 06/2014 that

consent has an important role but this doesn't exclude the possibility, depending on the context, for other legal grounds to be more appropriate depending on the context.

While the GDPR, and its predecessor, Directive 95/46, have always recognised the principle of different legal basis for processing of personal data, the ePrivacy proposal restricts the processing of personal data to the sole legal ground that is the user's consent. This focus solely on consent creates a "one size fits all" solution, which in reality is unworkable for both online users and organisations. Unlike the GDPR which offers a risk based approach, the ePrivacy proposal does not take into consideration the context in which the processing takes place, nor the impact on the individual's privacy. This approach goes against the incentives created by the GDPR to process personal data, in a way which limits the impact on individual's privacy. Where consent is the only way forward to process data, controllers have limited interest to adopt additional safeguards to limit the privacy impact.

Introducing additional legal grounds and safeguards besides consent

From a practical point of view, a systematic consent requirement, as proposed by the European Commission, would continue to impact heavily users online browsing habits with consent requests, and is unlikely to be solved by the Commission's proposal described in article 10 (see section: Article 10: developing workable privacy settings solutions**)**. A systematic consent requirement would not necessarily increase the level of protection of the users, while lowering the effectiveness of the consent requirement. Indeed, the study on implementation of the last ePrivacy Directive recognised that the consent rules did not reach its objectives "due to the fact that users currently receive a warning message with regard to the use of cookies on almost every website". The high level of consent requirement prevents users from making the difference between consenting to processing with little privacy impact with to more privacy intrusive activities.

FEDMA believes that the ePrivacy Regulation should include certain flexibility, to adapt the rules and the level of safeguards to the impact an activity would have on an individual's privacy. Consequently, FEDMA believes that article 8.1 of the ePrivacy Regulation should recognise other legal grounds for the processing of personal data beyond the user's consent. Additionally, FEDMA would encourage legislators to introduce in the ePrivacy regulation a number of safeguards adopted in the GDPR, such as pseudonymisation and data protection impact assessment. Besides strengthening coherency between GDPR and ePrivacy, such safeguards would ensure that user's privacy is respected in the online environment.

Welcomed clarification on web audience measurement

Not all cookies include identifiers and are used to collect and process personal data. Such cookies do not fall under the GDPR and should not be submitted to the consent requirement under the future ePrivacy instrument. Indeed, some cookies have other tasks than collecting personal data, for example, strictly necessary cookies (essential in order to enable you to move around the

website and use its features, such as accessing secure areas of the website), performance cookies (to know how visitors use a website), functionality cookies (allows the website to remember choices you make) where the data can be anonymised.

With regards to these, cookies, FEDMA welcomes the effort put forward by the European Commission's proposal. In particular, Article 8.1.d, together with recital 21 clarifies that web audience measurement generates no or very limited intrusion of privacy. This provision will bring important added value to the confusing situation many online publishers are currently facing.

In order to be effective and enabling publishers to have a clear understanding of their web traffic, this provision should also apply when the web audience measurement is done by a partner of the first party. In many situation, first parties are not doing their analytics themselves but depend on third parties to obtain such necessary service in an easy way. This agreement between a publisher and an analytic partner (which can act as a processor) clarifies that the data collected for analytics can only be used for such purposes. The ePrivacy Regulation proposal clarifies that this exception is solely for web audience measurement. Consequently, the provision enabling web audience measuring should not be limited to the provider of the information society service requested by the end users but also include its partners.

Article 10: developing workable privacy settings solutions

FEDMA appreciates the effort of the European Commission in developing solutions facilitating the way for individuals to express their privacy preferences. Article 10 of the ePrivacy Regulation proposal provides for software permitting electronic communications, including the retrieval and presentation of information on the internet to include privacy settings.

FEDMA welcomes the approach taken by the Commission to look for a centralised solution. "Web browser (…) are in a privileged position to play an active role to help the end user control the flow of information to and from the terminal equipment" (recital 22). However, it is crucial that this solution is workable in the online environment, enabling all players of the online ecosystem to interact lawfully and in an easy manner with the end users.

For this reason, FEDMA is concerned that the proposal uses web browsers as "gatekeepers" (recital 22). Requiring browsers to prevent third parties to access the device would provide them with a disproportionate power against the other players of the online ecosystem. Often, first parties rely on third parties to provide the users with certain information and services on the website they visit. Additionally, first and third parties may want to engage in a dialogue with end users to encourage them to consent to online tracking (for example to help publishers finance their services). With such a system, it becomes impossible for first parties, and third parties to engage in a dialogue with the end users, in order to ask for consent, unless the web browser enables such dialogue. Additionally, consent collected by a first party would be meaningless, unless the web browser creates an exception and allow the party to access the device. The internet could only function if web browser create "white list" of parties benefitting from the end user's consent.

While the distinction between first and third party access is technologically easy to make for a web browser, the distinction between cookies that require consent according to the proposed ePrivacy Regulation, and the ones that don't (e.g. web audience cookies) is more difficult. Additionally, as mentioned above, on many occasions, first party uses third party for services which fall within the situation described by article 8.1.a and 8.1.b (providing the information society services requested, or web audience measurement). In such situation, the ability of the browser to differentiate between third and first parties is not aligned with intention of the legislator. Finally, such a system would concentrate all information related to the user within the hands of the few major browser companies which already dominate the European market.

FEDMA would like to encourage the legislator to adopt rules which both provide a centralised privacy tool for users, while enabling the internet ecosystem to thrive, and dialogue with the user when consent is needed. One solution to be considered is the use of privacy tools which communicate to all first and third parties the user's privacy preferences, instead of preventing access to third parties as proposed by the Commission. Such a mechanism, based on the expression of the choice of the user, would provide more flexibility for actors to dialogue with users and ask for consent when necessary. As explained in recital 22, "the choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on and enforceable against any third parties". While, maintaining the same level of control as proposed by the Commission, this solution would have the added value of providing flexible way for the online ecosystem to interact with the user, and would avoid concentrating user's data and power within few online players.

4. Confidentiality of data emitted by the user's device – article 8.2

FEDMA welcomes the approach taken by the European Commission, in article 8.2, regarding the collection of information emitted by a terminal equipment. The Commission's proposal allows today's technology to continue providing value added services based on data emitted by device, while ensure the protection of individual's privacy, through obligations of transparency and user's control.

However, it is important that this provision does not generate too much visual impact in public spaces, in particular in cities major shopping streets, highways, or any other public area where such data collection may take place. While the notice must be visible for all individuals, it should be of a reasonable size, in order to avoid disproportionate impact on landscape. The visual impact of such notice could be reduced by having on said notice an internet address where all the required information, according to article 13 of the GDPR, would be provided, and kept up to date.

5. Unsolicited communication – Article 16

Unsolicited communication is not similar to unwanted communication, **spam, phishing and other malicious attempts,** and remains one of the main possibilities for new companies to enter the market, or companies promoting new products or services to inform individuals about them, gain and sustain customers' relations. Without prejudice to the current ePrivacy Directive, Persistent and unwanted commercial communications are forbidden under the Unfair Commercial Practices Directive (black list point 26).

The Direct Marketing industry uses many different channels of communication from the most traditional such as fax and telemarketing to the most modern such as social media. Each channel is a different way to communicate and interact with customers and potential customers and each channel has its own specificities. Marketers will use different channels for different audiences, different strategies and at different costs. They will use channels in a complementary manner ensuring an omnichannel experience for the consumer.

Recognizing existing standards for consent for unsolicited communication

The direct marketing industry has developed many guidance, including codes of conduct, to ensure that consent is collected appropriately whenever required for email marketing. FEDMA has developed an on-line annex to its code of practice for the use of personal data in direct marketing, dedicated to electronic communication. The Annex has been approved by the Article 29 Working Party in 2010, and includes clear guidance, as well as concrete examples on how consent can be collected for email marketing. FEDMA believes that the standards developed in the annex already meet the new criteria for a valid consent defined in the GDPR, and should be considered when adopting the new ePrivacy Regulation.

More clarification of the Soft opt-in provision

The on-line annex developed by FEDMA also provides standards and guidance for the collection of consent for email marketing in the context of a sale. The Annex has been approved by the Article 29 Working Party in 2010. In particular, the Annex includes concrete wording examples of what can qualify as best practices and as not acceptable for the collection of consent for email marketing in the context of a sale. FEDMA believes that the standards developed in the annex already meet the new criteria for a valid consent defined in the GDPR.

Telemarketing rules should remain national

FEDMA appreciates the effort of the European Commission in understanding the particularities of telemarketing calls "given that they are more costly for the sender and impose no financial costs on end-users" (recital 36). Additionally, the importance of the language (You expect to reach or being reached out by a telemarketer who speaks the same language as you) makes telemarketing

a very local industry. Finally, in order to facilitate user's choice, and in particular his or her ability to object to receiving marketing calls, both government and industry have invested substantial resources in the development of Robinson lists. Subscribers are able to express their preferences regarding telemarketing calls by adding their numbers to the list if they want to unsubscribe/opt-out of all unsolicited telemarketing calls. 16 Robinson lists dealing with B2C telemarketing have been developed in Europe, mostly in countries which enable telemarketing on an opt-out basis.

FEDMA believes that the possibility for Member States to maintain the status quo should be as easy as possible. The Commission's proposal already provides for a definition of direct marketing communication (article 4.3f) and a more specific sub definition of direct Marketing voice-to-voice calls (article 4.3.g). This distinction and the way article 16 is written highlights the fact that voice to voice calls is a specific form or direct marketing. Considering the specific nature of telemarketing, as mentioned in recital 36, FEDMA believes the ePrivacy Proposal should recognize specifically for telemarketing voice to voice calls the ability for Member States to decide between and opt-in and an opt-out scenario. Indeed, the flexibility given by the current ePrivacy Directive to Member States to decide between opt-in and opt-out solutions for telemarketing has led to a regime that both the industry and users have become familiar with.

Common prefix, a technical challenge:

FEDMA is concerned by the proposal of the European Commission in article 16.3.b, of presenting a "specific code/or prefix identifying the fact that the call is a marketing call". FEDMA is a strong supporter of transparency. Any marketing communication should be identified as such, providing transparency to the individual. All phone numbers should be visible (no hidden commercial phone number). In particular, the GDPR already requires that the individual be informed of the identity and the contact details of the controller (GDPR 13.1.a and GDPR 4.1.a)), the right to access, rectification or erasure (GDPR 13.2.b and GDPR 14.2.c), and a right to object at any time to processing of personal data for direct marketing purposes (GDPR 21.2). This last right must be brought to the attention of the individuals and shall be presented clearly and separately (GDPR 21.4).

Being in line with the GDPR, FEDMA welcome the obligation to "present the identity of a line on which they (the marketers) can be contacted" (article 16.3.a), but is concerned by the alternative proposal to have a specific code/prefix to identify such marketing calls.

FEDMA would like to highlight that the development of a specific prefix number, common to all marketing calls will prove to be technically difficult to implement. Such provision would then, require a disproportionate effort from the industry, considering that many countries already have in place mechanisms enabling individuals to object to telemarketing.

Additionally, the use of a common prefix number can be counterproductive for the individuals. The idea of a common prefix number, which can easily blocked by the individual, would lead to situations where individuals who wish to be contacted and have given their consent for that

purpose could not be reached out by the marketer if marketing calls with a common prefix number have been blocked. From the marketers' point of view, such a system would render useless the users' consent, because the call would be blocked. This approach would actually undermine the consent given by the user.

Business to Business unsolicited communications

FEDMA welcomes the approach from the European Commission to delegate to Member States the responsibility to ensure that legal persons receiving unsolicited communications are sufficiently protected.

Indeed, while the main objective of the ePrivacy Regulation proposal is to protect individuals' privacy, including privacy of communication, unsolicited communication send to individuals in a professional capacities does not have a direct impact on their private life. Unsolicited communication send in a BtoB context aims at providing information to existing customers, or prospect about product and services which may be interesting. In their professional capacities, many individuals have purchasing responsibilities, including responsibilities to compare offers to ensure the organisation gets the product or services which suits best. In such context, unsolicited marketing communication plays an important role for the daily running of an organisation, while having little impact on individual's privacy. Consequently, it is justified to benefit from a lighter regime which ensure sufficient flexibility for BtoB marketing communications. This approach is in line with the principles of proportionality and subsidiarity.

Additionally, it is always unclear, who should give consent, when required, on behalf of a legal person.

Finally, in their professional capacities, individuals are usually supported by technologies which enables them a better control of the unsolicited communication they receive, and they are also more aware of the existing solutions to oppose to such communication.

4. Keeping user in control, the role of self-regulation

In reviewing the ePrivacy Directive, the European Commission should leave room for industry self and co-regulation. Self-regulation and best practices have raised consumer trust at national level for email marketing (e.g. FEDMA online annex to its code of practice for the use of personal data in direct marketing includes guidance and examples on how consent can be collected for email marketing), **for telemarketing** (16 Robinson lists dealing with B2C telemarketing have been developed in Europe, mostly in countries which enable telemarketing on an opt out basis) **and for Online Behavioural Advertising** with the Pan European Self-Regulatory programme on OBA (offering information, control and complain mechanism for consumers for OBA).

According to the European Advertising Consumer research report 2015, between 20% and 56% of the respondents, depending on the country, said that having the option to manage their preferences through the self-regulatory online behavioural advertising programme increased their levels of trust in the brand being advertised. Furthermore, between 26% and 59% of respondents are more favourable to the concept of OBA through the European Self-Regulatory programme. These results demonstrate that a well-informed opt-out mechanism can reach the objective of increasing trust online.

5. Icons

FEDMA understand the approach of the Commission regarding the use of icons, and a solutions to provide information to individuals regarding their privacy and data protection. However, FEDMA is concerned that this approach may be a one size fits all which would miss its objective.

Indeed, the use of standardized icons, would provide a one size fits all solutions where organisations would be deprived from the flexibility to communicate their practices and activities in their own way, and develop creative solutions for it. As an example, some organisation may use a short video to describe their personal data processing activities (i.e. The Guardian privacy policy). Additionally, the use of icons is likely to miss its objective to properly inform individuals. Indeed, individuals generally do not understand fully the message the aimed at being transmitted through a visual icon. While the use of descriptive icons, such as icons used on food product, provide an easy to understand information, it is likely to be more difficult, in the field of privacy, to provide icons which inform about legal assessment, which are not simple. The transmission of a simple message using an icons, must not scare the user away from a legal service, nor should it mislead him or her regarding the actual processing taking place.

FEDMA believes that the use of standardized icons to describe personal data processing or privacy related activities may not be the one size fits all solutions. Industries should be able to develop the most suitable solutions to inform users about their respective practices.

6. Delegated acts

FEDMA believes that the use of delegated acts should be as limited as possible within the new ePrivacy instrument in order to avoid increasing the great legal uncertainty which data controllers currently have to face with regards to the implementation of the GDPR, impacting further Europe's economic development. FEDMA believes that alternative solutions should be promoted, entailing the use of industry self-regulation or co-regulation to clarify legislative acts. The Commission should only produce delegated acts in cases where the relevant stakeholders do not develop their own self- regulatory or co- regulatory measures within a reasonable timescale and after consulting with industry stakeholders and legislators. As an example taken from the GDPR, FEDMA believes

that the creation of mandatory icons to inform data subjects about processing of data, using delegated acts is counterproductive, and prevents the industry from deciding how to best communicate and be transparent to data subjects.