Position Paper

ePrivacy Regulation - FEDMA proposed Amendments

In the context of the discussion on the review of the ePrivacy legislation, FEDMA has identified a number of concerns in the regulation proposed by the European Commission in January 2017. These concerns are described in details in the FEDMA position paper**.** With discussions now taking place at the European Parliament, FEDMA would like to provide suggestions for amendments, which provide, in the text, solutions to the concerns identified by our industry.

All the amendments presented below follow's FEDMA's objectives:

- Ensuring consistency and coherency between the GDPR and the ePrivacy Regulation, by making sure that the scopes are the same, and that the flexibility provided by the GDPR with the risk based approach is also present in the ePrivacy Regulation.
- Ensuring that the ePrivacy offers protection of confidentiality while enabling the digital world to continue deliver added value to online users and create growth for the economy. In order to be future proof, it is also essential for the ePrivacy Regulation to also be as technology neutral as possible.
- Ensuring that the rules for direct marketing communication are proportionate, enabling users to express their preferences while encouraging industry's best practices. Additionally, the definition of direct marketing should be in line with the reality of our industry practices.

FEDMA would like to encourage the European Parliament to take into consideration the suggested amendments on the below articles and corresponding recitals:

- Article 4: Definitions (recital 32)
- Article 5: confidentiality of electronic communications
- Article 8: Protection of information stored in and related to end-users' terminal equipment (recitals 20, 21, 25 and 41)
- Article 9: Consent (recital 18)
- Article 10: Information and options for privacy settings to be provided (recitals 22, 23 and 24)
- Article 16: Unsolicited communications (recitals 33, 34 and 35)
- Article 18: Independent supervisory authorities

Commission's proposal	FEDMA Amendment	Commission's proposal – recitals	FEDMA Amendment
Article 4 – definitions Direct marketing is defined by its ability to address a message directly to an individual. FEDMA has worked extensively in the past to develop a comprehensive definition of direct marketing based on directing of communication to particular individuals. This definition has been approved by the article 29 Working Party in 2003 and 2010 when reviewing the FEDMA code of conduct. FEDMA would like to encourage the European Parliament to take into consideration the definition proposed by FEDMA below as a basis for their discussion, and suggest an amendment adapted to the specificities of this regulation by referring to interpersonal communication services.			
4.3(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	4.3(f) 'direct marketing communications' means any ~~**form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;**~~ **communication using an interpersonal communication service 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.**	(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.	(32) In this Regulation, direct marketing refers to any **communication using an interpersonal communication service 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** ~~***form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services***~~. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.
4.3 (h) 'automated calling and communication systems'	h) 'automated calling and communication systems' means systems capable of		

means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and communication systems which connect the called person to an individual.	automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including ***pre-recorded messages and*** calls made using automated calling and communication systems which connect the called person to an individual.		
Article 5 – Confidentiality of electronic communications data FEDMA believes that the ePrivacy Regulation should have a clear scope, applying to electronic communication data during their conveyance. Whenever electronic communication data are not in conveyance, the GDPR will apply and protect user's personal data.			
Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Electronic communications data shall be confidential. Any interference with electronic communications data ***during their conveyance***, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.		

Article 8 – Protection of information stored in and related to end-users' terminal equipment			
FEDMA believes that the exception proposed by the Commission for web audience measurement should be further adapted to the technological reality (publisher rarely carry themselves analytics but depends on services provided by third parties), and applies on the basis of the purpose of the processing. Additionally, FEDMA believes that the ePrivacy Regulation should include some of the flexibility adopted in the GDPR, which manage to set the right balance between protection of personal data and free flow of data. Considering the strengthened definition of consent adopted in the GDPR, and which will also apply in the ePrivacy Regulation, FEDMA believes that some other legal ground for processing personal data should also be included in the ePrivacy Regulation, taking into consideration appropriate safeguards to protect the user. Finally, regarding the collection of data emitted by the user's device, FEDMA believes that the ePrivacy Regulation should ensure that user are properly given the required information, while ensuring that the obligation are concretely applicable.			
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	**1.** The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information	(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information
(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is necessary for the sole purpose of ***establishing,*** carrying out ***or demonstrating*** the transmission of an electronic communication over an electronic		

	communications network; or	already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.	already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs ***and*** hidden identifiers, ~~***tracking cookies and other similar unwanted tracking tools***~~ can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that ~~**surreptitiously**~~ monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment ***without his or her knowledge may*** pose a ~~***serious***~~ threat to the privacy of end-users. ***At the same time, the same technologies can be used for legitimate and useful purposes such as verifying the identity of end- users engaged in on-line transactions and understanding the effectiveness of website design and advertising. Where such technologies, for instance cookies, are used for a legitimate purpose, such as to facilitate the provision of information society services, such use should be allowed on condition that it meets the principle of lawfulness, fairness and transparency.*** Therefore, any such ***use***
(b) the end-user has given his or her consent; or	(b) the end-user has given his or her consent; or		
(c) it is necessary for providing an information society service requested by the end-user; or	(c) it is necessary for providing an information society service requested by the end-user; or		
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.	(d) if it is necessary for ~~***web***~~ ***verifying, invoicing or valuing*** audience ~~***measuring; or ,***~~ provided that ***it*** ~~***such measurement is carried out***~~ ***is authorized by, or on behalf of*** the provider of the information society service, ***and the data processing is strictly limited to the primary purpose*** ~~***requested by the end-user.***~~		
	(d)a. (new) if it is necessary for pursuing a legitimate interest and the person responsible undertakes to comply with specific privacy safeguards; or		
	(d)b. (new) it is necessary to maintain or restore the security of information society services, or detect technical faults and/or errors in the functioning of information society services, for the duration necessary for that purpose.		

	1a. (new) For the purpose of point (d)a (new) of paragraph 1 the following specific privacy safeguards apply: ***(a) the responsible person has put in place appropriate technical measures, such as pseudonymisation or encryption.*** ***(b) the data processed do not constitute special categories of personal data as defined by Article 9 of Regulation (EU) 2016/679; and***		***~~interference~~*** with the end-user's terminal equipment should be allowed only with the end-user's consent ***or some other legitimate basis*** and for specific and transparent purposes***.***
		(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy ***of the end-user concerned and in accordance with Regulation (EU) 2016/679***. ***In order to ascertain whether a situation involves no, or only limited, impact on the privacy of the end-user concerned, the entity responsible, after having met all the requirements for the lawfulness of using the end-user's terminal equipment, including with respect to transparency, should take into account inter alia: the purpose for which the processing and storage capabilities of the terminal equipment or information accessed are used; the context in which information is collected, in particular the reasonable expectations of end-users based on their relationship with the controller as to the information's further use; the consequences of the intended processing for end-users; and the existence of appropriate safeguards such as encryption or pseudonymisation.*** For instance, ***~~consent should not be requested for authorizing~~*** the technical storage or access which is strictly necessary and proportionate for ***~~the legitimate purpose of~~*** enabling the use of a specific service

			explicitly requested by the end-user ***may be regarded as carried out for a legitimate interest.*** This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool for ***other legitimate purposes,*** for example**,** ***helping to secure a service,*** ~~**in**~~ measuring web traffic to a website ***or delivering and measuring the effectiveness of advertisements.***
2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or (b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are	2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or (b) a clear ~~**and prominent**~~ notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are	(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive	(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used ~~***for more intrusive***~~

collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection, ***or informing end-users as to where such information is available,*** The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.	~~***purposes, such as***~~ to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. ~~***Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection.***~~ Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	***Delete***		
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be	***Delete***		

presented by the standardized icon and the procedures for providing standardized icons.			
Article 9 – Consent While ensuring the consistency between the GDPR and the ePrivacy with regard to the definition of consent, FEDMA believes it is important to clarify that information society services remain free to determine the condition of access to their services, as any such obligation would prevent them from defining their own business model.			
1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provided for under Articles 4(11) and 7**(1), 7(2) and 7(3**) of Regulation (EU) 2016/679/EU shall apply.	(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment. (	(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. ***It is the prerogative of an information service provider to determine the condition of access to its service.*** ~~***In such context, service providers should have the possibility to limit access to end users who have denied consent.***~~ For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same ***definition*** ~~***meaning and be subject to the same conditions***~~ as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. ~~***Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice,***~~
	1a. (new) Access to information society services may be made conditional on the well-informed consent of end-users.		
2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.	2. Without prejudice to ~~***paragraph 1 Regulation (EU) 2016/679/EU***~~, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed **or withdrawn** by using ~~***the***~~ appropriate technical settings of ~~***a***~~ ***any*** software application ~~***enabling access to the internet.***~~		
3. End-users who have consented to the processing of electronic communications	3. End-users who have consented to the processing of electronic communications		

data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 ~~and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.~~		~~or is unable to refuse or withdraw consent without detriment.~~
Article 10 – Information and options for privacy settings to be provided FEDMA believes that software permitting electronic communications should offer options for the user to express/withdraw his or her consent. However, such software should enable any other digital player, which may need consent in order to provide their services to the user, to request consent, and to modify the settings accordingly.			
1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.	1. Software ~~placed on the market~~ permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option ~~to choose appropriate technical settings referred to in article 9(2) option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment~~.	(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. 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.	(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using ~~the~~ appropriate *technical* settings. ~~of a browser or other application.~~ The choices made by end-users when establishing its general privacy settings *of software* ~~of a browser or other application should be binding on, and~~
2. Upon installation, the software shall inform the end-user about the privacy settings	2. ~~Upon installation,~~ The software shall ~~inform~~ *make available to* the end-user		

options and, to continue with the installation, require the end-user to consent to a setting.	*information* about the privacy settings options ~~***and, to continue with the installation, require the end-user to consent to a setting.***~~	Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored. (	~~***enforceable against, any third parties***~~. ***Such privacy settings must not prevent an information society services from overriding other software privacy setting with the end-users consent or another lawful ground .*** ~~***Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.***~~
	2a. (NEW) The software shall provide easy ways for information society services to request and transcribe consent or withdrawal of consent from end-users in accordance with Article 9(1) and to change the technical settings referred to in Article 9(2).		
3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with ~~***at the time of the first update of the software, but***~~ no later than ***12 months after the application of this regulation.***	(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be	(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option **for end-users to express their privacy preference using appropriate technical settings.** ~~***To prevent third parties from storing information on the terminal***~~

		offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in an easily visible and intelligible manner.	~~***equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies').***~~ Such privacy settings should be presented in an easily visible and intelligible manner.
		(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the	(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party ***tracking*** cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end***, it is necessary to require*** providers of software enabling access to internet ***should inform*** ~~***that, at the moment of installation,***~~ end-users ~~***are informed***~~ about the possibility to choose ~~***the***~~ privacy settings among ~~***the***~~ various options ~~***and ask them to make a choice.***~~ Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about ***the purposes for which*** ~~***the risks associated to***~~

		computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.	***~~allowing~~*** third party cookies ***~~to be~~*** stored in the computer ***may be processed***, including ***~~the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising.~~*** ***using information about an end-user's browsing habits to build up an anonymous profile which may determine what type of advertising they are shown.*** Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the end-user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.
Article 16 – unsolicited communications FEDMA believes that the ePrivacy Regulation should further clarify the scope of the rules on unsolicited communications by referring to communications using interpersonal communication services. The detailed definition of interpersonal communication services in the draft European Electronic Communication Code Directive ensures clarity to the scope of this article, and offer protection to users with regard to all these communications. Additionally, FEDMA believes that the ePrivacy Regulation should incentivise the industry efforts to develop Do Not Call register, instead of creating mandatory code/prefix identifying telemarketing calls, and such code may lead to situations where users, who have consented to calls, may not receive such calls as it is being block for technical reasons. Finally, FEDMA believes that individuals in a BtoB context have a greater interest in receiving commercial offers which contribute to informed business decisions, thus deserve a separate set of rules as proposed by the European Commission and as it is currently the case.			
1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural	1. communications services for the purposes of sending direct marketing communications, ***Using interpersonal communication service*** to end-users who are	(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of	(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of

persons that have given their consent.	natural persons that have given their consent.	technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.	technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users ***using interpersonal communication service ~~in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons~~***. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications ***using interpersonal communication services*** remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of e-mail contact details ***and phone numbers*** within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.
2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.	2. Where a natural or legal person obtains electronic contact details for electronic mail ***or phone number*** from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services ~~only if~~ ***Provided that*** customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use ***of electronic contact details***. The right to object shall be given at the time of collection and ~~each time a message is sent~~ ***on the occasion of each direct marketing communication in case the customer has not initially refused such use.***		
3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for	3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for	(34) When end-users have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an	(34) When end-users have provided their consent to receiving ~~***unsolicited***~~ communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an

the purposes of placing direct marketing calls shall: (a) present the identity of a line on which they can be contacted; or (b) present a specific code/or prefix identifying the fact that the call is a marketing call.	the purposes of placing direct marketing calls shall~~:~~ ~~(a)~~ present the identity of a line on which they can be contacted; ~~or~~ ~~(b) present a specific code/or prefix identifying the fact that the call is a marketing call.~~	easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.	easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and ~~provide~~ **make available** the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.
4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.	4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons ~~shall~~ ***is*** only ~~be~~ allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications, ***or is allowed with the consent of the subscriber.*** ***The choice between these options is to be determined***	(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called or present a specific code identifying the fact that the call is a marketing call.	(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called ~~*or present a specific code identifying the fact that the call is a marketing call*~~.

	by national legislation, taking into account that both options must be free of charge for the end-users.		
7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.	***Delete***		
Article 18 – Independent supervisory authority FEDMA believes it is important to clarify the relationship between the ePrivacy proposal and the Consumer Protection Cooperation Network proposal which include a reference to article 13 of the ePrivacy Directive 2002/58. It is important to ensure that the independent supervisory authority described are solely responsible for the enforcement of this proposed regulation.			
1. The independent supervisory authority or authorities responsible for monitoring the application of the Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation.	1. The independent supervisory authority or authorities responsible for monitoring the application of the Regulation (EU) 2016/679 shall ***exclusively*** be responsible for monitoring the application of this Regulation.		