

COMMISSION PROPOSAL	PRESIDENCY TEXT	INDUSTRY	JUSTIFICATION
<i>Article 4 - Definitions</i>	<i>Article 4 - Definitions</i>	<i>Article 4 - Definitions</i>	
(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.;	(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.;	(f) 'direct marketing communications' means any form of advertising promotional message , whether written or oral, sent to one or more identified or identifiable end-users of electronic interpersonal communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	<p>Direct marketing and advertising are two different albeit related concepts. Direct marketing is a type of promotional message directed at a specific individual, whereas the broader notion of advertising refers to promotional messages directed at the public at large or groups of the public but not usually specific individuals.</p> <p>As the intent of the proposal is to cover only direct marketing, the article's scope should be limited to promotional messages delivered by means of interpersonal communications services, but not delivered by mass media such as the Internet or other public communication channels in general.</p> <p>In absence of these clarifications any advertising delivered to the public, or groups of the public, over internet protocol would be classified as direct marketing. This is because IP addresses make each user identifiable and the Internet is an electronic communications service.</p>
	(NEW) Article 94a Consent	Article 94a Consent	
	1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.		
	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 placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.	2. Without prejudice to paragraph 4 , Where technically possible and feasible, in particular 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, or by continuing the use of an information society service, having been provided with clear and comprehensive information that this action by the end-user signifies consent.	It should be clarified that consent can be given by the user continuing to actively use a service after having been provided with prominent information that this will be considered consent in line with current practice. Online services should be able to provide necessary information and obtain consent in a manner that does not hinder the normal use of the service.

	<p>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 the possibility to withdraw their consent at periodic intervals of [no longer than 6 12 months], as long as the processing continues.</p>	<p>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 the possibility to withdraw their consent at periodic intervals of [no longer than 6 12 months], as long as the processing continues.</p>	<p>Removing the reminding obligation would better align the provision with the requirements of the GDPR. There is a risk of creating a dual regime for consent and rendering the situation less clear. Articles 4(11) and 7 of Regulation (EU) 2016/679 define the conditions for consent and are sufficient. Moreover, bearing in mind that the end-user should be provided with the option of informed consent and the option to opt-out at any moment, there is no need for constantly reminding of these possibilities.</p>
		<p>NEW (3 a) No service provider shall be obliged to provide full access to its service or content in the absence of end-user consent if such consent is required for conducting the provider's business in accordance with the freedom to conduct a business, the right to property, the right to private and family life, the right to data protection and other fundamental rights and freedoms protected under Union law.</p>	<p>The ePrivacy Regulation requires companies to obtain consent for processing operations such as the use of cookies, and advertising identifiers under Article 8(1), which underpin the business models of advertising-funded online services.</p> <p>Without the existing clarification of Recital 25 of the ePrivacy Directive which states that access to a service can be made conditional on consent, obtaining such consent would be near impossible as users would effectively have the right to use a service without agreeing to the terms under which it is made available on the market.</p> <p>Service providers should have the right to exercise their legitimate economic interests in accordance with the principle of contractual freedom.</p>
<p><i>Article 8 - Protection of information stored in and related to end-users' terminal equipment</i></p>	<p><i>Article 8 - Protection of information stored in terminal equipment of end-users and [related to or processed by or emitted by] end-users' terminal such equipment</i></p>	<p><i>Article 8 - Protection of information stored in terminal equipment of end-users and [related to or processed by or emitted by] end-users' terminal such equipment</i></p>	
<p>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:</p>	<p>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:</p>		

<p>(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or</p>	<p>(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or</p>		
<p>(b) the end-user has given his or her consent; or</p>	<p>(b) the end-user has given his or her specific consent; or</p>		
<p>(c) it is necessary for providing an information society service requested by the end-user; or</p>	<p>(c) it is necessary for providing an information society service requested by the end-user; or</p>		
<p>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.</p>	<p>(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 or by a third party on behalf of the provider of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.;</p>	<p>(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 or by a third party on behalf of the provider or with the provider's permission. of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.;</p>	<p>In the advertising context, audience measuring is used to determine, amongst others, whether an advertisement has been viewed, as well as to confirm that a conversion (determined by the advertiser, e.g. user went on to purchase a shoe) has occurred. These audience measuring activities are often carried out by the advertiser who purchases advertising space on a service's property, or on its behalf, and not by the service provider accessed by the user, or on its behalf. This is because in order for an advertiser to trust the measurement, it must be done by an entity under its control rather than the sellers control. Forcing advertisers to rely on the measurement of their sellers, would be analogous to students grading their own homework.</p>
	<p>(e) it is necessary for a security update provided that the privacy settings chosen by the end-user are not changed in any way, the end-user is informed in advance and is given the possibility to postpone or turn off the automatic installation of these updates.</p>		
		<p>NEW (f) it is necessary to maintain or restore the security of information society services and services, or detect technical faults and/or errors and/or attacks against information society services, for the duration necessary for that purpose.</p>	<p>Information society services rely on information provided by or stored on users terminal devices, such as cookies, mac addresses, etc., to maintain or restore the security of their services.</p> <p>Information society services should not be prevented from processing information for security purposes, just like electronic communications services are not prevented from processing information to keep their property secure.</p>

		<p>NEW (g) it is necessary for billing, calculating payments, detecting or stopping fraudulent, abusive, or otherwise unauthorised use of information society services; or</p>	<p>Information society services rely on information provided by or stored on users terminal devices, such as cookies, mac addresses, etc., to detect and prevent fraud or other unauthorized use of their service as well as to bill advertisers for the advertising space they sell to them.</p> <p>Information society services should not be prevented from processing information necessary for receiving payment for services rendered, or to prevent fraud and other unauthorised use of their property.</p>
		<p>NEW (h) 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 collected, as well as any measure the 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 measures and the application of organisational measures, which shall include inter alia pseudonymisation, to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.</p>	<p>In order to reduce the number of consent requests that users receive due to the ePrivacy Regulation, no consent should be needed where non-sensitive information is collected, for example for advertising purposes.</p> <p>It should be possible to collect pseudonymous or anonymous information for legitimate purposes while applying appropriate technical and organisational measures to ensure an adequate level of security in line with the requirements of the GDPR, and the user is provided with prominent information as required by the GDPR, as well as given the possibility to stop or minimise the collection in line with the GDPR.</p>
		<p>NEW (i) it is necessary to comply with a legal obligation under Union or Member State law.</p>	<p>Information society services have legal obligations under Union and Member State law that require it to collect and process information stored on the terminal equipment of its users, including to provide information and to trigger a consent notice.</p> <p>Compliance with a legal obligation should not be contingent on the user's consent.</p>
Article 9 - Consent	Article 9 – Consent	Article 9 -	
1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	DELETED	DELETED	

<p>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.</p>	<p>DELETED</p>	<p>DELETED</p>	
<p>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.</p>	<p>DELETED</p>	<p>DELETED</p>	
<p><i>Article 10 - Information and options for privacy settings to be provided</i></p>	<p><i>Article 10 - Information and options for privacy settings to be provided</i></p>	<p><i>Article 10 - Information and options for privacy settings to be provided</i></p>	
<p>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.</p>	<p>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 any other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.</p>	<p>DELETED</p>	<p>Article 10 would prevent online services from collecting and processing information in accordance with the law and user choices, and force online services to rely on mechanisms put in place by a limited number of browser developers.</p> <p>Furthermore, Article 10 would also reinforce the dominant position of browsers/platforms and aggravate serious competition concerns linked to their dominance and ensuing levels of bargaining power vis-a-vis online service providers by cementing their role as “gatekeepers” of the online ecosystem. This is dangerous as such browsers/platforms are not only competing with online service providers for marketing revenue, but also increasingly for content. Altogether, Article 10 risks concentrating market power in the digital space and aggravating existing and/or creating new competition concerns by further strengthening the position of browsers/platforms.</p> <p>We also note that the absence of regulation has not prevented browser developers from offering services aimed at improving privacy. Since there are</p>

			market-based solutions, it is not necessary to interfere in online services' legal compliance capabilities by designating a few companies as gatekeepers for their ability to conduct business and meet their obligations under the law.
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	2. Upon installation or first usage , the software referred to in paragraph 1 shall inform the end-user about the privacy settings options and, to continue with the installation or usage , require the end-user to consent to a setting.	DELETED	
	2.(a) The software referred to in paragraph 1 shall provide in a clear manner easy ways for end-users to change the privacy setting consented to under paragraph 2 at any time during the use.	DELETED	
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 [25 August 2018].	DELETED	