Council of the European Union

Brussels, 22 March 2018
(OR. en)

7207/18

Interinstitutional File:
2017/0003 (COD)

TELECOM 66
COMPET 161
MI 182
DATAPROTECT 35
CONSOM 68
JAI 230
DIGIT 40
FREMP 34
CYBER 43
CODEC 395

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	6726/18 TELECOM 53 COMPET 125 MI 128 DATAPROTECT 24 CONSOM 51 JAI 184 DIGIT 22 FREMP 24 CYBER 40 CODEC 298
No. Cion doc.:	5358/17 TELECOM 12 COMPET 32 MI 45 DATAPROTECT 4 CONSOM 19 JAI 40 DIGIT 10 FREMP 3 CYBER 10 IA 12 CODEC 52
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency discussion paper

I. INTRODUCTION

For the purposes of the WP TELE meeting of 28 March, delegations will find in Annex a revised text of the ePrivacy proposal (ePR), focusing on Articles 8, 10, 15 and 16 and the related recitals. The revisions are inspired by WP TELE discussions held on the basis of the Presidency discussion papers (doc. 5165/18 and 5569/18) and on the written comments provided by delegations in this context. For ease of reference, the latest changes to the text are underlined.

During the WP TELE of 28 March, the Presidency would like to invite delegations to provide comments on:

– **the above mentioned proposals as presented in Section II and in Annex**.

– additionally, in order to further advance the debate on the proposal, **on articles 18 to 29, as presented in doc. 15333/17**.

II. AMENDMENTS TO THE TEXT

a. ARTICLE 8: Protection of end-users' terminal equipment information

The **title of art. 8** has been simplified.

The Presidency has deleted **point (f) of art. 8(1)** on the location of a caller of an emergency calls, as this issue is now addressed in art. 13.

A sentence has been provided in **recital 20** to clarify that a one-off consent for a cookie in the context of one website is possible.

In **recital 21**, it has been made clear that access to a website may be made conditional on the well-informed acceptance of a cookie.

b. ARTICLE 10: Privacy settings

Following the discussion on the Presidency option paper (doc. 5165/18), the Presidency has proposed to amend **art. 10(2).** The provision now requires information to be provided to the end-user about the possibility to choose a setting, without however prompting the end-user to agree with the settings upon installation or first usage. The Presidency has also proposed to include periodic reminders about the privacy settings.

Art. 10(2a) has been slightly amended to mirror the changes in art. 10(2).

It should be noted that recitals related to art. 10, and in particular recital 24, will be updated following the discussion on 28 March.

c. ARTICLE 15: Publicly available directories

In order to clarify the concept of a publicly available directory, the Presidency has amended the **definition in art. 4(3)(d) and the corresponding recital 30.** The idea is to distinguish publicly available directories under ePR from other types of directories or lists by clarifying that the ePR targets directories, the main function of which is to enable to identify end-users of number-based interpersonal communications services (NB-ICS).

Following the discussion on the Presidency option paper (doc. 5569/18), the Presidency proposes to keep the basic obligation of giving end-users the opportunity to determine whether they wish to be included in a directory (**art. 15(1)**) for providers of NB-ICS. However, the Presidency proposes to address the other obligations provided for in **art. 15(1a), (2), (3), (3a)**, to providers of NB-ICS and/or to providers of publicly available directories. This would, in the Presidency's view, allow Member States to maintain their current regimes with regard to the addressee of the obligation. Corresponding **recital 31** has been amended accordingly.

Art. 15(2) has been amended to clarify that the obligation to inform end-users of available search functions only applies to search functions not based on name, as searching by name seems to be the basic function of any directory.

In addition, following comments from a number of delegations, the Presidency has clarified in **recital 30** that end-users who are natural persons acting in a professional capacity should be treated as legal persons.

d. ARTICLE 16: Direct marketing communications

More details on the right to object have been included in **art. 16(2)** on direct marketing to customers.

New **art. 16(2a)** allows Member States to set a time limit for using customers' contact details for direct marketing.

Art. 16(6) has been restructured to provide a clear overview of obligations regarding information to be provided in the context of direct marketing.

To address concerns that online advertising would be captured by the provisions on direct marketing, new **art. 16(6a)** explicitly excludes advertisements on websites that are displayed to the general public and do not require end-users' contact details.

In response to concerns of some delegations, flexibility has been introduced in **recital 32** with regard to messages sent by political parties for promotion purposes.

Recitals related to article 16 might need further adjustments following the discussion on 28 March.

(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~~ **processed by** or emitted by or **stored in** 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**, including the privacy of one's communications,** 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 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. **The end-user's consent to storage of a cookie or similar device may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.**

(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**, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket**. **Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.**

(21a) Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example by helping to** measure~~ing web traffic to~~ **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site**. 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. **Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception.**

(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. 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.

(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 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 a 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 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.

(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**, the WiFi signal** 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 **physical movements'** tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, **such as** providing data on the number of people waiting in line, ascertaining the number of people in a specific area, ~~etc~~ **referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level if security appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is not longer needed for this purpose**. **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.** This information may be used for more intrusive purposes, **which should not be considered statistical counting,** 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~~ **as well as** 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.~~

(30) ~~**Publicly available directories of end-users of electronic communications services are widely distributed.**~~ Publicly available directories means any directory or service containing ~~**categories of**~~ **information on** end-users ~~information~~ ~~**personal data**~~ **of number-based interpersonal communication services** such as **name,** phone numbers (including mobile phone numbers), email address ~~contact details~~**, home address** and includes inquiry services, **the main function of which is to enable to identify such end-users**. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are ~~asked for consent before their personal data are included in a directory~~**able to determine per category of personal data whether their personal data are included in a directory**. The legitimate interest of legal ~~entities~~ **persons** requires that end-users that are legal ~~entities~~ **persons** have the right to object to the data related to them being included in a directory. **End-users who are natural persons acting in a professional capacity should be treated as legal persons.**

(31) ~~If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, p~~**P**roviders of ~~publicly available directories~~ **number-based interpersonal communications services and/or providers of publicly available directories** should inform the end-users **who are natural persons** ~~of the purposes of the directory and~~ of the search functions of the directory **and obtain their additional consent** before ~~including them in that directory~~**enabling such search functions related to their personal data**. ~~End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched.~~ The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same.

(~~30a~~31a) For the purposes of the provisions relating to direct marketing communications, electronic message should include e-mail, SMS, MMS and functionally equivalent applications and techniques.

(32) In this Regulation, direct marketing **communications** refers to any form of advertising by which a natural or legal person sends **or presents** direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. **The provisions on direct marketing communications do not apply to any other form of marketing, e.g. displaying advertising to the general public on a website which is not directed to any specific identified or identifiable end-user.** In addition to the offering of products and services for commercial purposes, ~~this should~~ **direct marketing communications ~~also~~ may** include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same ~~should~~ appl~~y~~**ies** to messages sent by other non-profit organisations to support the purposes of the organisation.

(33) Safeguards should be provided to protect end-users against ~~unsolicited~~ **direct marketing** communications ~~for direct marketing purposes~~, which intrude into the ~~private life~~ **privacy** of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of 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**s who are natural persons** is obtained before ~~commercial electronic communications for~~ direct marketing **communications** ~~purposes~~ are sent **or presented** to ~~end-users~~ **them** in order to effectively protect ~~individuals~~ **them** 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~~ **direct marketing** communications remain future-proof justify the need to define **in principle** a single set of rules that do not vary according to the technology used to convey these ~~unsolicited~~ **direct marketing** 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 **for electronic message** 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 **for electronic message** in accordance with Regulation (EU) 2016/679.

(~~36~~**33a**)Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems~~, given that they~~ are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users **who are natural persons and** who have not objected.

(34) When end-users **who are natural persons** have provided their consent to receiving ~~unsolicited~~ **direct marketing** communications ~~for direct marketing purposes~~, they should still be able to withdraw their consent at any time in an easy manner **and without any cost to them**. To facilitate effective enforcement of Union rules on ~~unsolicited messages for~~ direct marketing **communications**, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending **or presenting** ~~unsolicited commercial~~ **direct marketing** communications ~~for direct marketing purposes~~. ~~Unsolicited~~ **Direct** marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person ~~transmitting~~ **sending or presenting** the communication or on behalf of whom the communication is ~~transmitted~~ **sent or presented** and provide the necessary information for ~~recipients~~ **end-users who are natural persons** to exercise their right to ~~oppose~~ **withdraw their consent** to receiving further ~~written and/or oral marketing messages~~ **direct marketing communications, such as valid contact details (e.g. link, e-mail address) which can be easily used by end-users who are natural persons to withdraw their consent free of charge**.

(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~~ **present** their identity line on which the company can be called**. Member States are encouraged to introduce by means of national law** ~~or present~~ a specific code **or prefix** identifying the fact that the call is a **direct** marketing call **to improve the tools provided for the end-users in order to protect their privacy in more efficient manner**. **Using a specific code or prefix should not relieve the legal or natural persons sending or presenting direct marketing call from the obligation to present their calling line identification.**

Article 4

Definitions

…

(d) 'publicly available directory' means a directory of end-users of ~~**electronic**~~ **number-based interpersonal** communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service **and the main function of which is to enable to identify such end-users**;

…

Article 8

Protection of ***end-users' terminal equipment*** *information* ~~***stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment***~~

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:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; 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

(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**~~.~~**; or**

(e) it is necessary for a security update provided that:

(i) security updates are necessary and do not in any way change the privacy settings chosen by the end-user are not changed ~~in any way~~,

(ii) the end-user is informed in advance each time an update is being installed, and

(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or

~~(f) it is necessary to locate, at the time of the incident, a caller of an emergency call from the terminal by organisations dealing with emergency communications.~~

2. The collection of information emitted by terminal equipment **of the end-user** to enable it to connect to another device and, or to network equipment shall be prohibited, except ~~if~~ **on the following grounds**:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

(b) the end-user has given his or her consent; or

(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.

~~(b)~~**2a. For the purpose of paragraph 2 points (b) and (c),** a clear and prominent notice ~~is~~ **shall be** 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 end-user of the terminal equipment can take to stop or minimise the collection.

2b. **For the purpose of paragraph 2 points (b) and (c),** ~~T~~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.

3. The information to be provided pursuant to ~~point (b) of~~ paragraph 2**a** 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.

4. **[**The Commission shall be empowered to adopt delegated acts in accordance with Article 2~~5~~**7** determining the information to be presented by the standardized icon and the procedures for providing standardized icons.**]**

…

Article 10

Information and options for privacy settings to be provided

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.

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~~ shall remind the end-users of the availability of privacy settings with periodic intervals**.

2a. **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.**

3. In the case of software which has already been installed on **[**~~25 May 2018~~ **the date of entry into application]**, 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 months after the date of entry into application]**.

…

Article 15

Publicly available directories

1. The providers of ~~publicly available directories~~ **number-based interpersonal communications services** shall ~~obtain the consent of~~ **inform end-users who are natural persons about the possibility to include their personal data in a publicly available directory and give** ~~**end-users who are natural persons**~~ **them** ~~to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data~~ **the opportunity to determine per category of personal data whether their personal data are included in the publicly available directory**, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory.

1a. **The** ~~P~~providers **of number-based interpersonal communications services and/or providers of publicly available directory** shall give end-users who are natural persons the means to verify, correct and delete ~~such~~ data **included in a publicly available directory**.

2. The providers of ~~a publicly available directory~~ **number-based interpersonal communications services and/or providers of publicly available directory** shall inform end-users who are natural persons whose personal data are in the directory of ~~**the available**~~ **any** search function~~**s**~~ **that is not based on name** ~~**of**~~ **in** the directory and obtain **the additional consent of** end-users' ~~consent~~ before enabling such search functions related to their own data.

3. The providers of ~~publicly available directories~~ **number-based interpersonal communications services and/or providers of publicly available directory** shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory.

3a. **The** ~~P~~providers **of number-based interpersonal communications services and/or providers of publicly available directory** shall give ~~such~~ end-users that are legal persons the means to verify, correct and delete ~~such~~ data **included in a publicly available directory**.

4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Article 16

~~Unsolicited~~ ***Direct marketing*** *communications*

1. Natural or legal persons may use electronic communications services for the purposes of **[**sending **or presenting]** direct marketing communications to end-users who are natural persons that have given their consent.

2. **Notwithstanding paragraph 1,** ~~**W**~~**w**here a natural or legal person obtains ~~electronic~~ contact details for electronic ~~mail~~ **message** from ~~its customer~~ **end-users who are natural persons**, 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~~ **such end-users** 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 **of such end-users' contact details** and**, if that end-user has not initially refused that use,** each time **that natural or legal persons sends a message to that end-user for the purpose of** ~~**such**~~ **direct marketing** ~~**communication is [sent or presented]**~~.

2a. Member States may provide that natural or legal person may use its customer's contact details for direct marketing purposes only where the sale of the product or service occurred not more than twelve months prior to the sending of an electronic message for direct marketing.

3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(a) present the ~~identity of a~~ **calling** line **identification** on which they can be contacted~~; or~~**.**

(b)**3a. Member States may require natural or legal person using electronic communications services for the purposes of placing direct marketing calls to** present a specific code~~/~~or prefix identifying the fact that the call is a **direct** marketing call **in addition to the obligation set out in paragraph 3. Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons who use electronic communications services for the purposes of direct marketing calls**.

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.

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to ~~unsolicited~~ **direct marketing** communications **[**sent **or presented]** by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to ~~transmit~~ **[**send **or present]** direct marketing communications shall**, each time a direct marketing communication is [sent or presented]:**

(a) reveal his or its identity and use true return addresses or numbers;

(b) inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the **direct marketing** communication is ~~transmitted~~ **[**sent **or presented]**;

(c) ~~**and shall**~~ provide the necessary information for ~~recipients~~ **end-users who are natural persons** to exercise their right to **object or to** withdraw their consent, in an easy manner **and free of charge**, to receiving further **direct** marketing communications;

(d) clearly and distinctly give the end-users who are natural persons a means to object or to withdraw their consent, free of charge, at any time, and in an easy and effective manner, to receiving further direct marketing communications. This means shall also be given at the time of collection of the contact details according to paragraph 2. It shall be as easy to withdraw as to give consent.

6a. Advertisements on a website that are displayed to the general public and do not require any contact details of end-users should not be subject to this article.

~~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.]~~