



2017/0003(COD)

22.9.2017

COMPROMISE AMENDMENTS

1 - 33

Draft opinion
Eva Maydell
(PE604.857v01)

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)

Proposal for a regulation
(COM(2017)0010 - C8-0009/2017 – 2017/0003(COD))

Amendment 1
Eva Maydell

Compromise amendment replacing Amendments: 181, 182, 184, 186, 187,188, 189, 190, 191

Proposal for a regulation
Article 1

Text proposed by the Commission

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, ***which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.***

3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.

Amendment

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect private life and communications and the protection of natural persons with regard to the processing of personal data.

2. This Regulation ensures, ***in accordance with Regulation (EU) No 2016/679***, free movement of electronic communications data and electronic communications services within the Union.

3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2. ***Regulation (EU) 2016/679 applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Regulation, including the obligations on the controller and the rights of individuals.***

Amendment 2
Eva Maydell

Compromise amendment replacing Amendments: 17, 18, 214

Proposal for a regulation
Article 3

Text proposed by the Commission

Article 3

Territorial scope and representative

1. This Regulation applies to:
 - (a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;
 - (b) the use of such services;
 - (c) the protection of information related to the terminal equipment of end-users located in the Union.
2. Where the provider of an electronic communications service is not established in the Union ***it shall designate in writing a representative in the Union.***
3. ***The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.***
4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.
5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from

Amendment

Article 3

Territorial scope and representative

1. This Regulation applies to:
 - (a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;
 - (b) the use of such services;
 - (c) the protection of information related to the terminal equipment of end-users located in the Union.
2. Where the provider of an electronic communications service is not established in the Union ***the party identified pursuant to Article 27 of Regulation (EU) 2016/679 shall act as its representative in the Union.***
4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.
5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from

outside the Union to end-users in the Union.

outside the Union to end-users in the Union.

Amendment 3
Eva Maydell

Compromise amendment replacing Amendments: 19, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 233, 20, 234, 235, 236, 237, 238, 239

Proposal for a regulation

Article 4

Text proposed by the Commission

Article 4

1. For the purposes of this Regulation, following definitions shall apply:

(a) the definitions in Regulation (EU) 2016/679;

(b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];

(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC¹.

2. For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Amendment

Article 4

1. For the purposes of this Regulation, following definitions shall apply:

(a) the definitions in Regulation (EU) 2016/679;

(b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];

(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC¹.

2. For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

3. In addition, for the purposes of this Regulation the following definitions shall apply:

- (a) ‘electronic communications data’ means electronic communications content and electronic communications metadata;
- (b) ‘electronic communications content’ means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
- (c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;
- (d) ‘publicly available directory’ means a directory of end-users of electronic 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;
- (e) ‘electronic mail’ means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;
- (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.;

3. In addition, for the purposes of this Regulation the following definitions shall apply:

- (a) ‘electronic communications data’ means electronic communications content and electronic communications metadata;
- (b) ‘electronic communications content’ means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
- (c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;
- (d) ‘publicly available directory’ means a directory of end-users of electronic 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;
- (e) ‘electronic mail’ means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;
- (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.;

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;

(h) ‘automated calling and communication systems’ 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.

¹ Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;

(h) ‘automated calling and communication systems’ 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.

¹ Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).

Amendment 4 **Eva Maydell**

Compromise amendment replacing Amendments: 21, 244, 245, 247, 248, 249

Proposal for a regulation **Article 5**

Text proposed by the Commission

Article 5

Confidentiality of electronic communications 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.

Amendment

Article 5

Confidentiality of electronic communications data

Electronic communications data shall be confidential. Any interference with electronic communications data **during transmission**, such as by listening, tapping, storing, or other kinds of interception, **or** surveillance of electronic communications data, by persons other than the **sender or intended recipients**, shall be prohibited, except when permitted by this Regulation.

Amendment 5

Eva Maydell

Compromise amendment replacing Amendments: 23, 24, 25, 253, 254, 255, 258, 259, 260, 261, 262, 263, 264, 265, 266, 271, 273, 275, 298, 299, 303

Proposal for a regulation

Article 6

Text proposed by the Commission

Article 6

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:

(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

2. Providers of electronic communications services may process

Amendment

Article 6

Lawful processing of electronic communications data

1. Providers of **public** electronic communications networks and **publicly available electronic communications** services may process electronic communications data if:

(a) it is **technically** necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is **technically** necessary to maintain or restore the **availability, integrity, security and confidentiality of the respective** electronic communications networks and services, or **to** detect technical faults and/or errors in the transmission of electronic communications, **or to stop fraudulent use of the service** for the duration necessary for that purpose;

1a. Electronic communications data that is generated in the context of an electronic communications service designed particularly for children or directly targeted at children shall not be used for profiling or behaviourally targeted advertising purposes.

2. Providers of electronic communications **networks and** services

electronic communications metadata if:

(a) it is necessary *to meet mandatory* quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration necessary for that purpose; or

(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

3. Providers of the electronic communications services may process electronic communications content *only*:

(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or

(b) if *all* end-users *concerned have given their consent* to the processing of their electronic communications content *for one or more specified purposes that cannot be*

may process electronic communications metadata if:

(a) it is necessary *for quality of service purposes, including network management and* quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration necessary for that purpose; or

(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(bb) the further processing of the metadata for another specified purpose is compatible with the purpose for which the data were initially collected and is subject to specific safeguards, especially pseudonymisation, as set forth in Article 6(4) of Regulation (EU) 2016/679;

(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

3. Providers of the electronic communications services may process electronic communications content:

(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or

(b) if *service providers' end-users have consented* to the processing of their electronic communications content *pursuant to* Regulation (EU) 2016/679 or.

fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

(b a) for the sole purpose of the provision of a specific service explicitly requested by an end-user in the course of a purely personal, household or business activity, if the end-user concerned has consented to the processing of his or her electronic communications content and that service cannot be provided without the processing of such content; or

²⁸ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

²⁸ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

Amendment 6

Eva Maydell

Compromise amendment replacing Amendments: 26, 306

Proposal for a regulation

Article 7

Text proposed by the Commission

Amendment

Article 7

Article 7

Storage and erasure of electronic communications data

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of

Without prejudice to point (b) of Article

Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a *third* party entrusted by *them* to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

6(1) and points (a), **(aa)** and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a party, ***which could be the provider of the electronic communication service, specifically*** entrusted by ***the end-user*** to record, store or otherwise process such data. ***The end-user may further process the content*** in accordance with Regulation (EU) 2016/679, ***if applicable***.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous ***or pseudonymous*** when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

Amendment 7

Eva Maydell

Compromise amendment replacing Amendments: 27, 30, 314, 317, 318, 319, 323, 324, 327, 329, 330, 331, 332, 333, 335, 336, 339, 340, 341, 343, 344, 345, 347, 352, 358, 362, 363, 364, 365, 366, 368, 377, 378, 379, 380, 381, 382, 383

Proposal for a regulation

Article 8

Text proposed by the Commission

Amendment

Article 8

Article 8

Protection of information stored in and related to end-users' terminal equipment

Protection of information stored in and related to end-users' terminal 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:

1. The use of processing and storage capabilities of terminal equipment and the collection of **personal data** 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

(a) it is **technically** 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

(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 **a service requested by the end-user especially in order to secure the integrity, security and access of the information society service or for measures to protect against unauthorised use or access to the information society services in agreement with the terms of use for making available the service to 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 audience measuring, provided that such measurement is carried out by, **or on behalf of** the provider of the information society service requested by the end-user, **including measurement of indicators for the use of information society services in order to calculate a payment due, and provided that such audience measurement does not adversely affect the fundamental rights of the end-user or it is necessary in order to obtain information about the technical quality or effectiveness of an information society service that has been delivered and has no or little impact on the privacy of the end-user concerned. Where audience measuring takes place on**

behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or

(da) it is necessary to protect privacy, security or safety of the end-user, or to protect confidentiality, integrity, availability, authenticity of the terminal equipment.

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 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.

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 *sole* purpose of establishing a connection *requested by the user*; or

(ab) the data are anonymised and the risks are adequately mitigated; or

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

(b) *the end-user has given his or her consent after being informed by* a clear and prominent notice *for*, 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.

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 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 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

4 a. Terminal equipment that is intended particularly for children's use shall implement specific measures to prevent access to the equipment's storage and processing capabilities for the purpose of profiling of its users or tracking their behaviour with commercial intent.

Amendment 8

Eva Maydell

Compromise amendment replacing Amendments: 385, 386, 387, 388, 401

Proposal for a regulation

Article 9

Text proposed by the Commission

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.

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.

Amendment

Article 9

1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679 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.

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.**

2b. Where access to a service requires processing of information that is not strictly necessary for the provision of the service and an end-user has refused to give his or her consent to such processing, the end-user shall be given other fair and reasonable options to access the service.

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. **It shall be as easy to withdraw as to give consent.**

Amendment 9

Eva Maydell

Compromise amendment replacing Amendments: 32, 425

Proposal for a regulation

Article 10

Text proposed by the Commission

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 parties from storing** information on the terminal equipment of an end-user or processing information already stored on that equipment.

2. Upon installation, the software shall inform the end-user about the privacy

Amendment

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 **the storage of** information on the terminal equipment of an end-user or **the processing of** information already stored on that equipment.

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*.

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*.

settings options. *The technical settings shall consist of multiple options for the end-user to choose from, including an option to prevent the storage of information on the terminal equipment of an end-user and the processing of information already stored on, or processed by, that equipment. These settings should be easily accessible during the use of the software.*

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 *one year after entry into force of this Regulation*.

Amendment 10 **Eva Maydell**

Compromise amendment replacing Amendments: 435, 436, 437, 439,

Proposal for a regulation **Article 11**

Text proposed by the Commission

Article 11

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard *one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such*

Amendment

Article 11

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard *national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences*.

interests.

1a. Member States law may not require the removal or the corruption of technical protection measures, such as end-to-end encryption; nor should it otherwise determine the nature of such measures, where these are applied directly by the provider of the electronic communications network, service or terminal equipment, or by the end-user.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Amendment 11

Eva Maydell

Compromise amendment replacing Amendments: 36, 37, 446, 447, 448, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462.

Proposal for a regulation

Article 15

Text proposed by the Commission

Amendment

Article 15

Article 15

Publicly available directories

Publicly available directories

1. ***The providers of publicly available directories shall obtain the consent of end-users who are natural persons 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, to the extent that such data are***

1. ***Without prejudice to Member States national law the providers of electronic information, communication and telecommunication services shall give end-users who are natural persons the right to object to data related to them being included in directories and shall provide a transparent information about the data***

relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.

2. The providers of a publicly available directory shall *inform* end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and *obtain* end-users' *consent before enabling* such search functions related to their own data.

3. The providers of *publicly available directories* shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct *and* delete such data.

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.

being included in the directory and the means to verify, correct, update and delete such data.

2. The providers of a publicly available directory shall *provide accessible and intelligible information to* end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and *provide* end-users' *the option to disable* such search functions related to their own data.

3. The providers of *electronic information, communications and telecommunications services* shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct, *update, supplement* and delete such data. *Natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons.*

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

4a. The provisions of paragraphs 1 to 4 shall not apply to data and information published in other publicly accessible sources and data provided by end-users themselves, nor shall it apply to data published in publicly available directories before this Regulation enters into force unless the end-users have expressed their objection against their data being included in the directory or against available search functions related to their data pursuant to Article 17 of Regulation (EU) 2016/679.

Amendment 12

Eva Maydell

Compromise amendment replacing Amendments: 469, 470, 471, 472, 473, 474, 469

Proposal for a regulation

Article 16

Text proposed by the Commission

Article 16

Unsolicited communications

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

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.

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 line on**

Amendment

Article 16

Unsolicited communications

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

2. Where a natural or legal person obtains electronic contact details for **e-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 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 customer shall be informed about the right to object and shall be given an easy way to exercise it** at the time of collection and each time a message is sent.

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 **present the identity of a line on which they can be contacted and may present a specific code/or prefix identifying the fact that the call is a marketing call.**

which they can be contacted; or

(b) present a specific code/or prefix identifying the fact that the call is a marketing call.

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 communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.

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.

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users shall only be allowed in respect of end-users who have not expressed their objection to receiving those communications. ***Member States may provide that users can object to receiving the unsolicited communications via a national Do Not Call Register, thereby also ensuring that the end-user is only required to opt out once.***

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 communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.

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.

Amendment 13
Eva Maydell

Compromise amendment replacing Amendments: 487, 488

Proposal for a regulation
Article 17

Text proposed by the Commission

Amendment

Article 17

deleted

Information about detected security risks

In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.

Amendment 14
Eva Maydell

Compromise amendment replacing Amendments: 526, 527,

Proposal for a regulation
Article 27

Text proposed by the Commission

Amendment

Article 27

Article 27

Repeal

Repeal

1. Directive 2002/58/EC is repealed with effect from **25 May 2018**.

1. Directive 2002/58/EC **and Commission Regulation 611/2013 are** repealed with effect from **[XXX]**.

2. References to the repealed Directive shall be construed as references to this Regulation.

2. References to the repealed Directive shall be construed as references to this Regulation.

Amendment 15
Eva Maydell

Compromise amendment replacing Amendments: 1, 46, 47, 49

Proposal for a regulation
Recital 2

Text proposed by the Commission

(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, *from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment.* Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing *precise* conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, *such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.*

Amendment

(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing conclusions to be drawn regarding the private lives of the persons involved in the electronic communication. *The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.*

Amendment 16
Eva Maydell

Compromise amendment replacing Amendments: 50, 51, 52, 53

Proposal for a regulation
Recital 3

(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council²¹, also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council²¹, also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

Amendment 17
Eva Maydell

Compromise amendment replacing Amendments: 5, 64, 65

Proposal for a regulation
Recital 8

Text proposed by the Commission

(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing **commercial** communications or collect information related to or stored in end-users' terminal equipment.

Amendment

(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing communications or collect information related to or stored in end-users' terminal equipment.

Amendment 18
Eva Maydell

Compromise amendment replacing Amendments: 71, 72

Proposal for a regulation
Recital 11

Text proposed by the Commission

(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. **In order to ensure** an effective and equal protection of end-users when using functionally equivalent services, **this** Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code²⁴]. That

Amendment

(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. ***This Regulation aims at ensuring*** an effective and equal protection of end-users when using functionally equivalent services, ***so as to ensure the confidentiality of their communication, irrespective of the technological medium chosen.*** ***This*** Regulation uses the definition of electronic communications services set

definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.

forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code²⁴]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.

²⁴ Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

²⁴ Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

Amendment 19

Eva Maydell

Compromise amendment replacing Amendments: 73, 74

Proposal for a regulation

Recital 12

Text proposed by the Commission

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic

Amendment

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic

communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications.

Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications.

Nevertheless, in the context of automated supply-chains and elsewhere in the manufacturing or industrial context, where communication by the machines involved is not inter-personal and does not involve natural persons, this Regulation should not apply.

Amendment 20

Eva Maydell

Compromise amendment replacing Amendments: 7, 79, 77, 78, 80, 81

Proposal for a regulation

Recital 13

Text proposed by the Commission

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. ***The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation.***

Amendment

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. ***Therefore, this Regulation should apply to electronic communications data using electronic communications services which are targeting the general public, and public communications networks. In addition, this Regulation should also apply to closed social media profiles and groups that the***

Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.

user has restricted or defined as private. This Regulation should not apply to other kind of closed groups such as corporate networks, access to which is limited to members of the corporation. Such networks are offered to a defined group of end-users. However, even if undefined end-users use the network in question in the context of the activities of the defined group of end-users it should not preclude them from being considered outside the material scope of the Regulation. For example, an enterprise's collaboration platform primarily used by its employees that allows third parties to call-in or otherwise engage in the workspace should not be covered. The mere act of requiring a password should not be considered as providing access to a closed group of end-users if the access is provided to an undefined group of end-users.

Amendment 21
Eva Maydell

Compromise amendment replacing Amendments: 89, 90, 91, 92

Proposal for a regulation
Recital 16

Text proposed by the Commission

(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission ***in the electronic communications network***. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats ***such as the presence of malware*** or the processing of

Amendment

(16) The prohibition of storage of communications ***during transmission*** is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission. ***This Regulation also*** should not prohibit either the processing of electronic communications data to ensure the security, ***confidentiality, integrity, availability, authenticity*** and continuity of the electronic communications services ***and networks***, including checking security

metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.

threats *related to the respective service* or the processing of metadata *of the respective service* to ensure the necessary quality of service requirements, such as latency, jitter etc.

Amendment 22

Eva Maydell

Compromise amendment replacing Amendments: 9, 94, 97, 98, 99

Proposal for a regulation

Recital 17 Proposal for a regulation

Text proposed by the Commission

(17) The processing of electronic communications **data** can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, **based on end-users consent**. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to **obtain end-users' consent to process** electronic communications metadata, which should include data on the location of the device **generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing** electronic communications services **should not be considered as** metadata. Examples of commercial usages of electronic communications metadata by providers of

Amendment

(17) The processing of electronic communications **metadata** can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to **further** process electronic communications metadata. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to **comply with Regulation (EU) 2016/679 when processing** electronic communications metadata, which should include data on the location of the device. **The processing of** electronic communications metadata **for purposes other than those for which the personal data were initially collected should be allowed in cases where consent was obtained for the initial collection and the further processing is compatible in accordance with Article 6(4) of Regulation (EU) 2016/679**. Examples of

electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. *Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.*

commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.

Amendment 23
Eva Maydell

Compromise amendment replacing Amendments: 11, 106, 107

Proposal for a regulation
Recital 19

Text proposed by the Commission

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications

Amendment

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications

protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to *adequate* safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. *Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service.* After electronic communications content has been sent by the *end-user* and received by the intended *end-user or end-users*, it may be recorded or stored by the *end-user, end-users* or by *a third* party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. *For services that are provided to users engaged in purely personal, household or business activities, the consent of the end-user requesting the service should be sufficient. Where an electronic communication service that is based on new technologies is likely to result in a high risk to the rights and freedoms of natural persons after taking into account the nature, scope, context and purposes of the service the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The obligation does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing. After electronic communications content has been sent by the sender and received by the intended recipient(s), it may be recorded or stored by the sender, the recipient(s) or by another party entrusted by them to record or store such data. For communications, which do not happen in real time, such as email and messaging, the transmission is completed as soon as the communication is delivered to the trusted service provider or collected by the addressee.* Any processing of such data must comply with Regulation (EU) 2016/679. *It should be possible to process electronic*

communications data for the purposes of providing services requested by a user for personal or work-related purposes such as search or keyword indexing functionality, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools for instance by persons with disabilities. This should be possible without the consent of all users who are part of the communication, but may take place with the consent of the user requesting the service.

Amendment 24
Eva Maydell

Compromise amendment replacing Amendments: 112, 113, 115, 116, 117

Proposal for a regulation
Recital 21

Text proposed by the Commission

(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

Amendment

(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, ***or processed by,*** terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a service requested by the end-user. This may include the storing of ***information (such as cookies and identifiers)*** 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. ***This may also cover situations where end-users use a service across devices for the purpose of service personalisation and content***

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.

recommendation. Cookies, if implemented with appropriate privacy safeguards, can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Such measuring could also be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service. Similarly, providers of terminal equipment and the software needed to operate such equipment regularly need access to configuration and other device information and the processing and storage capabilities to maintain the equipment or its use, and correct problems related to the equipment's operation. Therefore, consent should also not be necessary if the information processed or stored is necessary to protect privacy, security or safety of the end-user, or to protect confidentiality, integrity, availability and authenticity of the terminal equipment. Information society providers and electronic communications service 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 user's device is unable to receive content requested by the end-user should not constitute illegitimate access.

Amendment 25
Eva Maydell

Compromise amendment replacing Amendments: 118, 120, 122, 123, 124

Proposal for a regulation
Recital 22

Text proposed by the Commission

(22) The methods used for providing information and obtaining end-user's

Amendment

(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*.

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 *or to object* by appropriate *technical* settings. 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, *unauthorised* parties, *provided that there is no separate specific consent given by the end-user*. 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. *On the other hand, in light of the pace of innovation, the increasing use and range of devices that permit communications and the increase of cross-device tracking, it is necessary for this Regulation to remain technology neutral to meet its objectives*. More particularly web browsers, *applications or mobile operating systems should not abuse their position as gate-keepers and still allow for possibilities for the user to individually give consent with regard to a certain specific service or service provider. Such consent should prevail over the privacy settings chosen at an earlier date or at the*

point of installation of the software.

Amendment 26

Eva Maydell

Compromise amendment replacing Amendments: 13, 126, 128, 129, 130, 138, 139

Proposal for a regulation

Recital 23

Text proposed by the Commission

(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*** easily visible and intelligible manner.

Amendment

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to ***inform the end-user about the possibility to express or withdraw his or her consent using appropriate technical settings. The end-user should be offered multiple options to choose from, including to prevent the storage of information on the terminal equipment. End-users should be offered a set of privacy setting options, ranging from, for example, rejecting cookies or trackers that are not necessary for the functionality of the website or other software to, for example, accepting tracking necessary for the functionality of the website or other software as well as for other purposes or, for example, accepting tracking necessary for the functionality of the website or other software and tracking for other purposes by parties that demonstrate the compliance with Article 40 and 42 of Regulation (EU) 2016/679, and the possibility to opt out from cross-device tracking. These options may also be more fine-grained and, among other aspects, reflect the possibility that another party might act as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service. In cases where a business model is based on targeted***

advertising, consent should not be considered as freely given if the access to the service is made conditional on data processing. The end-user should therefore be able to choose between accepting cookies or being provided fair and reasonable options to access the service, such as subscription, payment or limited access to parts of the service or other options. Where the end-user accepts cookies for purpose of targeted advertising, the end-user should also be able to correct the information gathered about him or her to prevent the possible harm caused by inaccurate information. Such privacy settings should be presented in an easily visible and intelligible manner. Information provided may include examples of benefits and risks associated with allowing cookies to be stored in the computer. Such obligations do not arise where the software already seeks to prevent the storage of information on the terminal equipment of an end-user or the processing of information already stored on that equipment.

Amendment 27
Eva Maydell

Compromise amendment replacing Amendments:135, 136, 137

Proposal for a regulation
Recital 24

Text proposed by the Commission

Amendment

(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

Deleted

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.

Amendment 28
Eva Maydell

Compromise amendment replacing Amendments: 144, 146, 147

Proposal for a regulation
Recital 25

Text proposed by the Commission

(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

Amendment

(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 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.

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 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 *ask for the end-user's consent, or where consent is not possible, such practices should be limited to what is strictly necessary for the purpose of statistical counting, be limited in time and space, or should carry out data protection impact assessment and in this case the data collected is or is rendered pseudonymous or anonymous or erased as soon as it is no longer needed for this purpose. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, prior consultation with the supervisory authority, as prescribed in Article 36 of Regulation (EU) 2016/679, should be carried out. Providers should display or make available 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.

Amendment 29
Eva Maydell

Compromise amendment replacing Amendments: 14, 148, 150, 151,

Proposal for a regulation
Recital 26

Text proposed by the Commission

(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, ***including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory***

Amendment

(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction ***is targeted at persons suspected of having committed a criminal offence and*** constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance

function connected to the exercise of official authority for such interests.

Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 27 of ***Regulation (EU) 2016/679. Providers of electronic communications services should not be obliged by Union or Member States competent authorities to weaken any measures that ensure the integrity and confidentiality of electronic communications.***

Amendment 30 **Eva Maydell**

Compromise amendment replacing Amendments: 156, 157,

Proposal for a regulation **Recital 30**

Text proposed by the Commission

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. 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. The legitimate interest of legal entities requires

Amendment

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person ***acting in a professional capacity*** requires that end-users that are natural persons ***provided with transparent information about the data being*** included in ***the*** directory ***and the***

that end-users that are legal entities have the right to object to the data related to them being included in a directory.

means to verify, correct, update, supplement and delete data relating to them free of charge, as well as the possibility of objecting to their data being included in public directories.. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

Amendment 31 **Eva Maydell**

Compromise amendment replacing Amendments: 159, 160, 161

Proposal for a regulation **Recital 31**

Text proposed by the Commission

(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, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory ***before including them in that directory. 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.***

Amendment

(31) If end-users that are natural persons ***do not object to the inclusion of*** their data being included in such directories, they should be able to ***make an objection on which categories directories, they should be able to*** determine which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories ***or the providers of electronic communications services*** should inform the end-users of the purposes of the directory and of the search functions of the directory.

Amendment 32
Eva Maydell

Compromise amendment replacing Amendments: 166, 167, 168,

Proposal for a regulation
Recital 33

Text proposed by the Commission

(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 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.

Amendment

(33) Safeguards should be provided to protect end-users against unsolicited communications, ***including*** 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 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 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.

Amendment 33
Eva Maydell

Compromise amendment replacing Amendments: 176, 177

Proposal for a regulation
Recital 40

Text proposed by the Commission

(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.

Amendment

(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty. ***Double penalties resulting from the infringement of both this Regulation and Regulation (EU) 2016/679 for the same act or omission should be avoided.***