EUROPEAN
COMMISSION

Brussels, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

(Text with EEA relevance)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

The Digital Single Market Strategy ("**DSM Strategy**")[1] has as an objective to increase trust in and the security of digital services. The reform of the data protection framework, and in particular the adoption of Regulation (EU) 2016/679, the General Data Protection Regulation ("**GDPR**")[2], was a key action to this end. The DSM Strategy also announced the review of Directive 2002/58/EC ("**ePrivacy Directive**")[3] in order to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. This proposal reviews the ePrivacy Directive, foreseeing in the DSM Strategy objectives and ensuring consistency with the GDPR.

The ePrivacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. It also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union ("**Charter**").

In line with the 'Better Regulation' requirements, the Commission carried out an *ex post* Regulatory Fitness and Performance Programme ("**REFIT evaluation**") of the ePrivacy Directive. It follows from the evaluation that the objectives and principles of the current framework remain sound. However, important technological and economic developments took place in the market since the last revision of the ePrivacy Directive in 2009. Consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and web-based e-mail services, instead of traditional communications services. These Over-the-Top communications services ("**OTTs**") are in general not subject to the current Union electronic communications framework, including the ePrivacy Directive. Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services.

1.2. Consistency with existing policy provisions in the policy area

This proposal is *lex specialis* to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The alignment with the GDPR resulted in the repeal of some provisions, such as the security obligations of Article 4 of the ePrivacy Directive.

---

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

2 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).

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

1.3. Consistency with other Union policies

The ePrivacy Directive is part of the regulatory framework for electronic communications. In 2016, the Commission adopted the proposal for a Directive establishing the European Electronic Communications Code ("**EECC**")[4], which revises the framework. While the present proposal is not an integral part of the EECC, it partially relies on definitions provided therein, including that of 'electronic communications services'. Like the EECC, this proposal also brings OTT providers in its scope to reflect the market reality. In addition, the EECC complements this proposal by ensuring the security of electronic communications services.

The Radio Equipment Directive 2014/53/EU ("**RED**")[5] ensures a single market for radio equipment. In particular, it requires that, before being placed on the market, radio equipment must incorporate safeguards to ensure that the personal data and privacy of the user are protected. Under the RED and the European Standardisation Regulation (EU) 1025/2012[6], the Commission is empowered to adopt measures. This proposal does not affect the RED.

The proposal does not include any specific provisions in the field of data retention. It maintains the substance of Article 15 of the ePrivacy Directive and aligns it with specific wording of Article 23 of the GDPR, which provides grounds for Member States to restrict the scope of the rights and obligations in specific articles of the ePrivacy Directive. Therefore, Member States are free to keep or create national data retention frameworks that provide, *inter alia*, for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights[7].

Finally, the proposal does not apply to activities of Union institutions, bodies and agencies. However, its principles and relevant obligations as to the right to respect for private life and communications in relation to the processing of electronic communications data have been included in the Proposal for a Regulation repealing Regulation (EC) No 45/2001[8].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

Article 16 and Article 114 of the Treaty on the Functioning of the European Union ("**TFEU**") are the relevant legal bases for the proposal.

Article 16 TFEU introduces a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, by Member States when carrying out activities falling within the scope of Union law, and

---

4 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)).

5 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62–106).

6 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12–33).

7 See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

rules relating to the free movement of such data. Since an electronic communication involving a natural person will normally qualify as personal data, the protection of natural persons with regard to the privacy of communications and processing of such data, should be based on Article 16.

In addition, the proposal aims at protecting communications and related legitimate interests of legal persons. The meaning and scope of the rights under Article 7 of the Charter shall, in accordance with Article 52(3) of the Charter, be the same as those laid down in Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("**ECHR**"). As regards the scope of Article 7 of the Charter, the case-law of the Court of Justice of the European Union ("**CJEU**")[9] and of the European Court of Human Rights[10] confirm that professional activities of legal persons may not be excluded from the protection of the right guaranteed by Article 7 of the Charter and Article 8 of the ECHR.

Since the initiative pursues a twofold purpose and that the component concerning the protection of communications of legal persons and the aim of achieving the internal market for those electronic communications and ensure its functioning in this regard cannot be considered merely incidental, the initiative should, therefore, also be based on Article 114 of the TFEU.

2.2. Subsidiarity

Respect for communications is a fundamental right recognised in the Charter. Content of electronic communications may reveal highly sensitive information about the end-users involved in the communication. Similarly, metadata derived from electronic communications, may also reveal very sensitive and personal information, as expressely recognised by the CJEU[11]. The majority of Member States also recognise the need to protect communications as a distinct constitutional right. Whilst it is possible for Member States to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of Union rules and would create restrictions on cross-border flows of personal and non-personal data related to the use of electronic communications services. Finally, to maintain consistency with the GDPR, it is necessary to review the ePrivacy Directive and adopt measures to bring the two instruments in line.

The technological developments and the ambitions of the DSM strategy have strengthened the case for action at the Union level. The success of the EU DSM depends on how effectively the EU brings down national silos and barriers and seize the advantages and economies of a European digital single market. Moreover, as internet and digital technologies know no borders, the dimension of the problem goes beyond the territory of a single Member State. Member States cannot effectively solve the problems in the current situation. A level playing field for economic operators providing substitutable services and equal protection of end-users at Union level are requirements for the DSM to work properly.

2.3. Proportionality

To ensure the effective legal protection of respect for privacy and communications, an extension of scope to cover OTT providers is necessary. While several popular OTT providers already comply, or partially comply with the principle of confidentiality of communications, the protection of fundamental rights cannot be left to self-regulation by industry. Also, the

---

9 See C-450/06 *Varec SA*, ECLI:EU:C:2008:91, §48.

10 See, *inter alia*, ECHR, judgments *Niemietz v Germany*, judgment of 16 December 1992, Series A n° 251-B, §29; *Société Colas Est and Others v France*, no 37971/97, §41; ECHR 2002-III; *Peck v The United Kingdom* no 44647/98, §57, ECHR 2003-I; and also *Vinci Construction and GTM Génie Civil et Services v. France*, n°s. 63629/10 and 60567/10, § 63, 2 April 2015.

11 See footnote 7.

importance of the effective protection of privacy of terminal equipment is increasing as it has become indispensable in personal and professional life for the storage of sensitive information. The implementation of the ePrivacy Directive has not been effective to empower end-users. Therefore the implementation of the principle by centralising consent in software and prompting users with information about the privacy settings thereof, is necessary to achieve the aim. Regarding the enforcement of this Regulation, it relies on the supervisory authorities and the consistency mechanism of the GDPR. Moreover, the proposal allows Member States to take national derogatory measures for specific legitimate purposes. Thus, the proposal does not go beyond what is necessary to achieve the aims and complies with the principle of proportionality as set out in Article 5 of the Treaty on European Union. The obligations put on affected services are kept to a level as minimum as possible, while not impinging on the fundamental rights concerned.

2.4. Choice of the instrument

The Commission puts forward a proposal for a Regulation in order to ensure consistency with the GDPR and legal certainty for users and businesses alike by avoiding divergent interpretation in the Member States. A Regulation can ensure an equal level of protection throughout the Union for users and lower compliance costs for businesses operating across borders.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

3.1. Ex-post evaluations/fitness checks of existing legislation

The REFIT evaluation examined how efficiently the ePrivacy Directive has contributed to an adequate protection of the respect for private life and confidentiality of communications in the EU. It also sought to identify possible redundancies.

The REFIT evaluation concluded that the above objectives of the Directive remain **relevant**. While the GDPR ensures the protection of personal data, the ePrivacy Directive ensures the confidentiality of communications, which may also contain non-personal data and data related to a legal person. Therefore, a separate instrument should ensure an effective protection of Article 7 of the Charter. Other provisions, such as the rules on the sending of unsolicited marketing communications, have proven to remain relevant too.

In terms of **effectiveness and efficiency**, the REFIT evaluation found that the Directive has not fully met its objectives. The unclear drafting of certain provisions and ambiguity in legal concepts have jeopardized harmonization, thereby creating challenges for businesses to operate cross-border. The evaluation further showed that some provisions have created an unnecessary burden on businesses and consumers. For example, the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent. The consent rule is over-inclusive, as it also covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. Finally, its implementation can be costly for businesses.

The evaluation concluded that the ePrivacy rules still have **EU added-value** for better achieving the objective of ensuring online privacy in the light of an increasingly transnational electronic communications market. It also demonstrated that overall the rules are **coherent** with other relevant legislation, although a few redundancies have been identified vis-à-vis the new GDPR (see in Section 1.2).

3.2. Stakeholder consultations

The Commission organised a public consultation between 12 April and 5 July 2016 and received 421 replies[12]. The key findings are the following[13]:

– **Need for special rules for the electronic communications sector on confidentiality of electronic communications**: 83.4% of the responding citizens, consumer and civil society organisations and 88.9% of public authorities agree, while 63.4% of industry respondents do not agree.

– **Extension of scope to new communications services (OTTs)**: 76% of citizens and civil society and 93.1% of public authorities agree, while only 36.2% of respondents from industry favour such an extension.

– **Amending the exemptions to consent for processing traffic and location data**: 49.1% of citizens, consumer and civil society organisations and 36% of public authorities prefer not to broaden the exemptions, while 36% of the industry favour extended exemptions and 2/3 of industry advocate the mere repeal of the provisions.

– **Support for solutions proposed to the cookie consent issue**: 81.2% of citizens and 63% of public authorities support imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated, while 58.3% of industry favour the option to support self/co-regulation.

In addition, the European Commission organised two workshops in April 2016, one open to all stakeholders and one open to national competent authorities, addressing the main questions of the public consultations. The views expressed during the workshops reflected the outcome of the public consultation.

To obtain views from citizens, a Eurobarometer survey on ePrivacy[14] was conducted throughout the EU. The key findings are the following[15]:

– 78% say it is very important that personal information on their computer, smartphone or tablet can only be accessed with their permission.

– 72% state that it is very important that the confidentiality of their e-mails and online instant messaging is guaranteed.

– 89% agree with the suggested option that the default settings of their browser should stop the sharing of their information.

3.3. Collection and use of expertise

The Commission relied on the following external expert advice:

– Targeted consultations of EU expert groups: Opinion of the Article 29 Working Party; Opinion of the EDPS; Opinion of the REFIT Platform; views of BEREC; views of ENISA and views of members of the Consumer Protection and Cooperation Network.

– External expertise, particularly the following two studies:

---

12 162 contributions from citizens, 33 from civil society and consumer organisations; 186 from industry and 40 from public authorities, including competent authorities enforcing the ePrivacy Directive.

13 The full report is available: https://ec.europa.eu/digital-single-market/news-redirect/37204.

14 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

15 The full report is available: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– Study "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/007116).

– Study "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" (SMART 2016/0080).

3.4. Impact assessment

An impact assessment was carried out for this proposal on which on 28 September 2016, the Regulatory Scrutiny Board issued a positive opinion[16]. To address the recommendations of the Board, the impact assessment explains better the scope of the initiative, its coherence with other legal instruments (GDPR, EECC, RED) and the need for a separate instrument. The baseline scenario is further developed and clarified. The analysis of the impacts is strengthened and made more balanced, clarifying and reinforcing the description of the expected costs and benefits.

The following policy options were examined against the criteria of effectiveness, efficiency and coherence:

– **Option 1:** Non-legislative ("soft law") measures;

– **Option 2:** Limited reinforcement of privacy/confidentiality and simplification;

– **Option 3:** Measured reinforcement of privacy/confidentiality and simplification;

– **Option 4:** Far reaching reinforcement of privacy/confidentiality and simplification;

– **Option 5:** Repeal of the ePrivacy Directive.

Option 3 was, in most aspects, singled out as the **preferred option** to achieve the objectives, while taking into account its efficiency and coherence. The main benefits are:

– Enhancing protection of confidentiality of electronic communications by extending the scope of the legal instrument to include new functionally equivalent electronic communications services. In addition, the Regulation enhances end-user's control by clarifying that consent can be expressed through appropriate technical settings.

– Enhancing protection against unsolicited communications, with the introduction of an obligation to provide the calling line identification or a mandatory prefix for marketing calls and the enhanced possibilities to block calls from unwanted numbers.

– Simplifying and clarifying the regulatory environment, by reducing the margin of manoeuvre left to Member States, repealing outdated provisions and the broadening of the exceptions to the consent rules.

The economic impact of Option 3 is expected to be overall proportionate to the aims of the proposal. Business opportunities related to the processing of communications data are opened up for traditional electronic communications services, while OTT providers become subject to the same rules. This implies some additional compliance costs for these operators. However, this change will not substantially affect those OTTs that already operate on the basis of consent. Finally, the impact of the option would not be felt in the Member States that have extended these rules to OTTs already.

By centralising the consent in software such as internet browsers and prompting users to choose their privacy settings and expanding the exceptions to the cookie consent rule, a significant proportion of businesses would be able to do away with cookie banners and notices, thus leading to potentially significant cost savings and simplification. However, it

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

may become more difficult for online targeted advertisers to obtain consent if a large proportion of users opt for "reject third party cookies" settings. At the same time, centralising consent does not deprive website operators from the possibility to obtain consent by means of individual requests to end-users and thus maintain their current business model. Additional costs would ensue for some providers of browsers or similar software as these would need to ensure privacy-friendly settings.

The external study identified three distinct implementation scenarios of Option 3, according to the entity who will establish the dialogue box between the user having chosen "reject third party cookies" or "do-not-track" settings and websites visited wishing the internet user to reconsider his/her choice. The entities who could be put in charge of this technical task are: 1) software such as internet browsers; 2) the third party tracker; 3) the individual websites (i.e. information society service requested by the user). Option 3 would lead to overall savings in terms of compliance cost compared to baseline scenario of 70% (€948.8 million savings) in the first scenario (browser solution), implemented in this proposal. Cost savings would be lower in other scenarios. As overall savings largely derive from a very significant decrease of the number of affected businesses, the individual amount of compliance costs for one business is expected to incur – on average – would be higher than today.

3.5. Regulatory fitness and simplification

The policy measures proposed under the preferred option address the objective of simplification and reduction of administrative burden, in line with the findings of the REFIT evaluation and Opinion of the REFIT Platform[17].

The REFIT Platform issued three sets of recommendations to the Commission:

– The protection of citizen's private life should be strengthened through an alignment of the ePrivacy Directive with the General Data Protection Regulation;

– The effectiveness of citizens protections against unsolicited marketing should be enhanced by adding exceptions to the ‘consent’ rule for cookies;

– The Commission addresses national implementation problems and facilitates the exchange of best practice amongst Member States.

The proposal include specifically:

– Use of technologically neutral definitions to apprehend new services and technologies to ensure that the Regulation is future-proof;

– Repeal of the security rules to eliminate regulatory duplication;

– Clarification of scope to help eliminate/reduce the risk of divergent implementation by Member States (point 3 of the Opinion);

– Clarification and simplification of the consent rule for the use of cookies and other identifiers, as explained in Sections 3.1 and 3.4 (point 2 of the Opinion);

– Alignment of the supervisory authorities with the authorities competent to enforce the GDPR and reliance on the consistency mechanism of the GDPR.

3.6. Impact on fundamental rights

The proposal aims to make more effective and increase the level of protection of privacy and personal data processed in relation with electronic communications in accordance with Articles 7 and 8 of the Charter and ensure greater legal certainty. The proposal complements and particularises the GDPR. Effective protection of the confidentiality of communications is

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

essential for exercising the freedom of expression and information and other related rights, such as the right to personal data protection or the freedom of thought, conscience and religion.

4. BUDGETARY IMPLICATIONS

The proposal has no implications for the Union budget.

5. OTHER ELEMENTS

5.1. Implementation plans and monitoring, evaluation and reporting arrangements

The Commission will monitor the application of the Regulation and submit a report on its evaluation to the European Parliament and to the Council and the European Economic and Social Committee every three years. These reports will be public and detail the effective application and enforcement of this Regulation.

5.2. Detailed explanation of the specific provisions of the proposal

Chapter I contains the general provisions: the subject matter (Article 1), the scope (Articles 2 and 3) and its definitions, including references to relevant definitions from other EU instruments, such as the GDPR.

Chapter II contains the key provisions ensuring the confidentiality of electronic communications (Article 5) and the limited permitted purposes and conditions of processing such communications data (Articles 6 and 7). It also addresses the protection of terminal equipment, by (i) guaranteeing the integrity of the information stored in it and (ii) protecting information emitted from terminal equipment, as it may enable the identification of its end-user (Article 8). Finally, Article 9 details the consent of end-users, a central lawful ground of this Regulation, expressly referring to its definition and conditions as provided by the GDPR, while Article 10 imposes an obligation on providers of software permitting electronic communications to help end-users in making effective choices about privacy settings. Article 11 details the purposes and conditions for Member States to restrict the above provisions.

Chapter III concerns the rights of end-users to control the sending and reception of electronic communications to protect their privacy: (i) the right of end-users to prevent the presentation of the calling line identification to guarantee anonymity (Article 12), with its limitations (Article 13); and (ii) the obligation for providers of publicly available number-based interpersonal communication to provide for the possibility to limit the reception of unwanted calls (Article 14). This Chapter also regulates the conditions under which end-users may be included in publicly available directories (Article 15) and the conditions under which unsolicited communications for direct marketing may be conducted (Article 17). It also relates to security risks and provides for an obligation upon providers of electronic communications services to alert end-users in case of a particular risk that may compromise the security of networks and services. The security obligations in the GDPR and in the EECC will apply to the providers of electronic communications services.

Chapter IV sets out the supervision and enforcement of this Regulation and entrusts it to the supervisory authorities in charge of the GDPR, in view of the strong synergies between general data protection issues and confidentiality of communications (Article 18). The powers of the European Data Protection Board are extended (Article 19) and the cooperation and consistency mechanism foreseen under the GDPR will apply in case of cross-border matters related to this Regulation (Article 20).

Chapter V details the various remedies available to end-users (Articles 21 and 22) and the penalties that can be imposed (Article 24), including the general conditions for imposing administrative fines (Article 23).

Chapter VI relates to the adoption of delegated and implementing acts in accordance with Article 290 and 291 of the Treaty.

Finally, Chapter VII contains the final provisions of this Regulation: the repeal of ePrivacy Directive, the monitoring and review, the entry into force and application. Concerning the review, the Commission intends to evaluate, *inter alia*, whether a separate legal act remains necessary in the light of legal, technical or economic developments and taking into account the first evaluation of Regulation (EU) 2016/679 which is due by 25 May 2020.

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Having regard to the opinion of the European Data Protection Supervisor[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties involved in a communication. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media.

(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

---

1 OJ C , , p. .
2 OJ C , , p. .
3 OJ C , , p. .

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.

(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 Council[4], 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.

(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include personal data as defined in Regulation (EU) 2016/679.

(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation.

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[5] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.

(7) The Member States should be allowed, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, the margin of discretion, which Member States

---

4 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).

5 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

(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.

(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union.

(10) Radio equipment and its software which is placed on the internal market in the Union, must comply with Directive 2014/53/EU of the European Parliament and of the Council[6]. This Regulation should not affect the applicability of any of the requirements of Directive 2014/53/EU nor the power of the Commission to adopt delegated acts pursuant to Directive 2014/53/EU requiring that specific categories or classes of radio equipment incorporate safeguards to ensure that personal data and privacy of end-users are protected.

(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 Code[7]]. 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.

(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

---

6 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

7 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)).

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.

(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. 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.

(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor

browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

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

(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 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.

(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the

data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.

(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.

(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited,

intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.

(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings

among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.

(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI 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.

(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 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).

(27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.

(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.

(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by end-users in different ways, including blocking silent calls and other fraudulent and nuisance calls. Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against nuisance calls and free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

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

(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.

(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

(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.

(34) When end-users have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.

(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called or present a specific code identifying the fact that the call is a marketing call.

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

(37) Service providers who offer electronic communications services should inform end-users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.

(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

(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.

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of

13 April 2016[8]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(43) Directive 2002/58/EC should be repealed.

HAVE ADOPTED THIS REGULATION:

[8] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).

CHAPTER I
GENERAL PROVISIONS

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.

Article 2
Material Scope

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

2. This Regulation does not apply to:

(a) activities which fall outside the scope of Union law;

(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;

(c) electronic communications services which are not publicly available;

(d) activities of competent authorities for the purposes of 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;

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC[9], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.

---

[9] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

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 outside the Union to end-users in the Union.

Article 4
Definitions

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/EC[10].

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;

---

[10] 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).

(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.

CHAPTER II
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT

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.

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 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) 2015/2120[11] 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 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.

Article 7
Storage and erasure of electronic communications data

1. Without prejudice to point (b) of 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.

---

[11] 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).

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.

Article 8

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:

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

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

(c) it is necessary for providing an information society service requested by the end-user; or

(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

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.

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.

Article 9

Consent

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

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the

appropriate technical settings of a software application enabling access to the internet.

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.

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 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.

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 interests.

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.

CHAPTER III
NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

Article 12
Presentation and restriction of calling and connected line identification

1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following:

(a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;

(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;

(c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;

(d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user.

2. The possibilities referred to in points (a), (b), (c) and (d) of paragraph 1 shall be provided to end-users by simple means and free of charge.

3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries.

4. Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of paragraph 1.

Article 13

Exceptions to presentation and restriction of calling and connected line identification

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

2. Member States shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.

Article 14

Incoming call blocking

Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge:

(a) to block incoming calls from specific numbers or from anonymous sources;

(b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.

Article 15
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 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.

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 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.

Article 17
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.

CHAPTER IV
INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT

Article 18
Independent supervisory authorities

1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.

2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].

Article 19
European Data Protection Board

The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks:

(a) advise the Commission on any proposed amendment of this Regulation;

(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation.

Article 20
Cooperation and consistency procedures

Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each

other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.

CHAPTER V
REMEDIES, LIABILITY AND PENALTIES

Article 21
Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.

2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.

Article 22
Right to compensation and liability

Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.

Article 23
General conditions for imposing administrative fines

1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation.

2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;

(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;

(c) the obligations of the providers of publicly available directories pursuant to Article 15;

(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.

3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.

5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.

Article 24
Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.

CHAPTER VI
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 25
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].

3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European

Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 26
Committee

1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011[12].

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VII
FINAL PROVISIONS

Article 27
Repeal

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

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

Article 28
Monitoring and evaluation clause

By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and

[12] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).

Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.

Article 29
Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*