EUROPEAN
COMMISSION

Brussels, XXX
[…](2016) XXX draft

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

The ePrivacy Directive ("**ePD**")[1] aims at ensuring an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector and to ensure the free flow of movement of such data and of electronic communications equipment and services in the EU. Its main objective is to implement in EU secondary law the fundamental right to the respect of private and family life including with regard to communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union ("**Charter**").

Since the last revision of the ePD in 2009, the electronic communications sector has significantly evolved from a technological and economical point of view. Consumers and businesses are increasingly relying on new Internet based services enabling inter-personal communications instead of telephony and other traditional communication services. A new typology of players has emerged offering communications services that many end-users perceive as comparable to traditional electronic communications services such as voice telephony and SMS. These so-called Over-the-Top communications services ("**OTTs**") provide their services in the form of applications running over the internet access service (hence "Over-the-Top") and are in general not subject to the current EU electronic communications rules, including the ePD rules[2].

In the Digital Single Market Strategy[3] (hereinafter the "**DSM Communication**"), the Commission set as an objective increasin trust and security in digital services. The reform of the data protection legal framework, initiated in 2012, was key action of the digital single market. In April 2016, the European Parliament and the Council adopted the General Data Protection Regulation ("**GDPR**")[4]. The Commission committed to review, once the new EU rules on data protection were adopted, the ePrivacy Directive with a focus on ensuring a high level of protection for data subjects and a level playing field for all market players. The review must ensure consistency with the GDPR.

Pursuant to this commitment and in line with the 'Better Regulation' requirements, the Commission carried out an *ex post* evaluation. It assessed the effectiveness, efficiency, relevance, coherence and EU added-value of the ePD, and pinpointed areas where there is

---

1 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), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 337, 18.12.2009, p. 11).

2 Popular OTT communication services include Skype, Gmail, WhatsApp, Facebook Messenger, Viber, Telegram, iMessage, Facetime.

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

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).

potential for improvement, adaptation to the evolved technological reality or simplification, without undermining the objectives of the legal framework. It follows from the Better Regulation *ex post* evaluation that the current framework remains sound as far as its objectives and principles. However, it has not prevented fragmentation in the way the ePrivacy Directive is implemented across the Union. Furthermore, while the public in general considers the protection of the confidentiality of communications and information stored in their devices as very important, the current framework has not kept pace with technological developments. The proposal addresses these problems.

1.2. Consistency with existing policy provisions in the policy area

The Data Protection Directive 95/46/EC[5] is the central legislative instrument in the protection of personal data in Europe. The GDPR will repeal and replace Directive 95/46/EC in May 2018 with new modernised rules fit for the digital age.

The proposal, as the current ePD with Directive 95/46/EC, seeks to particularise and complement the newly adopted GDPR by, among others, setting up specific rules concerning the processing of personal data in the electronic communication sector. All matters concerning the processing of personal data in the electronic communications sector which are not specifically addressed by the Proposal will be covered by the GDPR (as of 25 May 2018). For example, this covers the rights of individuals such as the right to obtain access to their personal data.

1.3. Consistency with other Union policies

While this proposal addresses specifically the protection of the fundamental rights to the protection of privacy and confidentiality and the protection of personal data in relation to electronic communications, it builds on and complements existing EU law in several areas.

The proposal maintains the current relationship between the ePD and the regulatory framework of electronic communications[6]. The regulatory framework comprises Framework Directive 2002/21/EC and, on top of the ePD, three specific directives, which are under review and should be replaced by the European Electronic Communications Code ("**EECC**")[7]. Even though not part of the EECC, the proposal relies on the definitions provided by the EECC.

There are also strong synergies between the Radio Equipment Directive 2014/53/EU[8] ("**RED**") and the current ePD. The RED ensures a single market for radio equipment by setting out essential requirements for safety and health, electromagnetic compatibility and the efficient use of the radio spectrum. In particular, it requires that, before being put into the

---

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ, L 281, 23.11.1995).

6 The framework is made of a package of 5 Directives and 2 Regulations: Framework Directive 2002/21/EC; Access Directive 2002/19/EC; Authorisation Directive 2002/20/EC; Universal Service Directive 2002/22/EC; Directive on Privacy and Electronic Communications 2002/58/EC; Regulation (EC) No 1211/2009 on Body of European Regulators for Electronic Communications (BEREC); Regulation (EU) No 531/2012 on roaming on public mobile communications networks.

7 On 14 September 2016, the European Commission published a proposal for a new European Electronic Communications Code, which consists of a horizontal recasting of the four existing Directives (Framework, Authorisation, Access and Universal Service).

8 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).

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[9], the Commission is empowered to adopt measures The proposed regulation will not change the relationship with the RED.

Finally, in line with the European Agenda on Security[10], the proposal does not include any specific provisions in the field of data retention. Therefore, Member States will remain able to establish or maintain national data retention legislation, so far as they comply with the general principles of the Union law, including the respect of fundamental rights under the Charter. The proposal, however, reviews the formulation of Article 15 of the ePD, which provides grounds for limitations to ePrivacy rules.

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 review of the ePD

Article 16 TFEU reaffirms the right to the protection of personal data, already enshrined in the Charter, and 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, bodies, offices and agencies, and by the Member State when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. It also provides that compliance with these rules shall be subject to the control of independent authorities. Since in most of the cases both components of an electronic communication involving a natural person, i.e. 'metadata' and content, will normally qualify as personal data, the protection of natural persons with regard to the confidentiality of communications and processing of such data, also in view of ensuring the protection of privacy, should be based on Article 16. Even if certain communications data would not qualify as personal data as such or if some provisions of the ePrivacy rules go beyond the protection of natural persons with regard to the processing of personal data, such as those aiming at prohibiting the storing of information or accessing of information already stored into users' terminal equipment, or otherwise emitted by such terminal equipment, without users' informed consent, these are merely incidental to the main purpose.

In line with settled case-law of the Court of Justice of the European Union, other components of the act concerning natural persons that are merely incidental to the main purpose have the effect that the act must be based on a single legal basis, namely that required by the main or predominant purpose, in this case Article 16 TFEU.

In addition, the proposal aims at protecting communications and related legitimate interests of legal persons. Article 7 of the Charter contains rights which correspond to those guaranteed by Article 8(1) of the European Convention for the Protection of Human Rights and

---

9 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).

10 Communication from the Commission to the European Parliament, the Council, the Eruopean Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM(2015) 185 final.

Fundamental Freedoms ("ECHR"). In accordance with Article 52(3) of the Charter, Article 7 thereof is this to be given the same meaning and the same scope of Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights. Concerning the scope of Article 7 of the Charter as concerns legal persons, case-law of the Court of Justice of the European Union and of the European Court of Human Rights confirm that professional activities of legal persons may not be excluded from the protection of the right guaranteed by both, 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 (for non-exclusive competence)

Subsidiarity

The subsidiarity principle requires the assessment of the necessity and the added value of the EU action. The need for EU level legislation on the protection of the rights to privacy and confidentiality and the protection of personal data in the electronic communications and the free movement of such data and of electronic communications equipment and services was already recognized by the European legislator with the adoption of the ePD.

As electronic communications, especially those based on Internet protocols, have a global reach; the dimension of the problem goes well beyond the territory of a single Member State. Member States cannot effectively solve the problems in the current situation. In order to achieve the internal market in electronic communications, it is necessary to reduce the current fragmentation of national rules and ensure an equivalent level of protection of end-users across the whole EU. Moreover, the proper functioning of the internal market requires that the rules ensure a level playing field for all economic operators in the electronic communications sector.

The technological developments and the ambitions of the DSM strategy have strengthened the case for action at EU level. The success of the EU DSM depends on how effectively the EU will be on bringing down national silos and barriers and seize the advantages and economies of a truly European digital single market. Moreover, as Internet and digital technologies know no borders, a level playing field for economic operators and equal protection of users at EU level are requirements for the DSM to work properly.

Respect for communications is a fundamental right recognised in the Charter. It is also in line with constitutional traditions common to the Member States: the majority of Member States also recognise the need to protect communications as a distinct constitutional right and usually have a distinct body of national law regulating this area. However, national rules on the protection of communications differ widely on scope and content. 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 EU rules and would create restrictions on cross-border flows of personal and non-personal data related to the use of electronic communications services to other Member States that do not meet the same protection standards.

Finally, in order to maintain consistency with the general data protection rules (GDPR), it is necessary to review the current sector-specific rules on ePrivacy and adopt measures required to bring the two instruments in line.

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

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

The Commission has carried out an assessment under the Regulatory Fitness and Performance Programme to examine whether these rules have contributed to ensuring an adequate protection of privacy and confidentiality of communications in the EU and also thought to identify possible redundancies.

The Directive is still **relevant** to meet its objectives but some of its rules are no longer fit for purpose in light of technological and market developments and changes in the legal framework. This is the case for the security provision as the new GDPR includes similar rules applicable broadly to data controllers.

The REFIT evaluation has emphasised that some of the rules have not been fully **effective** in reaching their intended objectives. Unclear drafting and ambiguity in legal concepts is a common issue but some specific flaws were also put in evidence. Critics were also made on the ineffectiveness of the consent imposed upon information society services engaged in on-line tracking by storing cookies in and/or accessing, **terminal equipment** (Article 5.3). The banners used to obtain consent impair the user's browsing experience and often not provide sufficient and clear information about purpose pursued by cookies. Also, the way consent is obtained was considered not to be freely given. As for the rules on **unsolicited communications,** difficulties arose firstly to the discretion left to Member States to choose whether end-users are protected by an opt-out or an opt-in regime. Moreover, the rules differ widely according to the technology used, which adds a layer of complexity and undermine legal certainty.

While it is necessary to acknowledge the difficulty to obtain reliable and representative quantitative data, most of the compliance costs experienced today seem to be associated to the "cookie" consent provision (Article 5.3), which due to its extensive coverage (i.e. all businesses running a website with tracking cookies), amounts to approximately EUR 1.8 billion. The evaluation identified scope for simplification of this provision.

The evaluation concluded that the ePrivacy rules still have substantial **EU added-value** to better achieve 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 legislations, although certain redundancies have been identified vis-à-vis the new General Data Protection Regulation (e.g. the rules on notification of personal data breach mentioned above).

3.2. Stakeholder consultations

The stakeholder consultation aimed to deliver a high quality and credible evaluation of current rules while allowing interested parties to contribute with suggestions for possible policy options to revise the directive. It also aimed to ensure transparency and accountability in the Commission's work.

Results of the public consultation

A dedicated 12-week open public consultation was conducted and gathered a total of 421 replies, almost half of which were from citizens[11]. The key findings of the public consultation as to the way forward are the following:

- **Need for special privacy rules:** 83.4% of the responding citizens and civil society believe that there is an added value in having special rules for the electronic communications sector to ensure the confidentiality of electronic communications.
- **Extension of scope to new communication services:**76% of citizens and civil society and 93.1% of public authorities believe the scope should be broadened to cover so-called over-the-top service providers while only 36.2% of respondents from industry favour such an extension
- **Preferred legal instrument:** A majority of citizens, consumer- and civil society organisations (66.3%) and of public authorities (66.7%) believe that a regulation would be a better instrument than a Directive. 47% of industry representatives suggest other options. 24.1% are against the idea of a regulation, while 28.9% are in favour of a regulation.
- **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 replying to the public consultation prefer not to broaden the exemptions to the confidentiality of traffic and location data, while 36% of the industry favour extended exemptions, e.g. to allow the use of this data for statistical purposes; while 2/3 of industry advocates to the mere repeal of the provisions on the processing of these data
- **Support for solutions proposed to the cookie consent issue:** Citizens had the strongest support for introducing provisions to prevent specific behaviours, irrespective of users' consent (86.7%), imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated. The option to support self/co-regulation received most support from industry (58.3%). The options most supported by public authorities were the introduction of rules prohibiting specific abusive behaviour (70.4%), and placing obligations on manufacturers (63%).
- **Need to limit the number of competent authorities:** Close to 70% of the combined total responses from industry, citizens and civil society say that one single national authority should be entrusted to enforce the rules. However, half of the public bodies who responded to the consultation are not convinced that this is needed. For respondents who consider that one single authority should enforce ePrivacy rules, a majority, across all categories, find that the national data protection authority is the best suited authority.
- **Opt-in or opt-out for direct marketing calls:** All groups of respondents agree that Member States should not retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for direct marketing calls to citizens. 90% of citizens, civil society and public authorities favour an opt-in regime, whereas 73% of industry favours an opt-out regime.

Workshops and meetings with stakeholders

[11] 162 contributions from citizens, 33 from civil society and consumer organisations; 186 from industry and 40 from public bodies, including competent authorities to enforce the ePrivacy Directive.

The European Commission organised a series of workshops to collect further views of stakeholders.

The **first workshop** was open to all stakeholders and took place on 12 April. There were around 120 participants, representing industry, competent authorities and civil society. Representatives of the telecom industry argued for the need for the rules to be made flexible. Representatives from consumer organizations supported an ambitious instrument that would increase the level of protection of privacy and confidentiality of communications throughout Europe. The **second workshop** gathered the **national competent authorities** in order to receive their specific inputs to the review. The discussions focused on the cookie rule, rules on traffic and location data, the need for a security provision, the provisions on subscriber's directories and unsolicited communications. A **round table** with 17 key stakeholders from all fields, the European Data Protection Supervisor and the Article 29 Working Party, was organised to gather views in a later stage of the review. Stakeholders expressed their views on, *inter alia*, the preferred legal instrument, the extension of the scope to OTT communication services, the need of having sector specific rules on traffic and location data, how to simplify the requirement to obtain consent before placing cookies or other identifiers, how to address online tracking.

Eurobarometer on e-Privacy

Between the 7th and 8th July 2016, around 27,000 citizens from different social and demographic groups were interviewed throughout the EU via telephone (mobile and fixed line) on questions related to the protection of their privacy. Below is a summary of the results of this Eurobarometer survey[12].

- Almost eight in ten say it is very important that personal information on their computer, smartphone or tablet can only be accessed with their permission (78%).
- More than seven in ten (72%) state that it is very important that the confidentiality of their e-mails and online instant messaging is guaranteed.
- A majority agree that there should be a range of measures available to protect their privacy, while almost two thirds have taken at least one action to protect their personal information when surfing online. 60% have already changed the privacy settings on their Internet browser (e.g. to delete browsing history or cookies) while 40% avoid certain websites because they are worried their online activities would be monitored.
- Almost nine in ten respondents (89%) agree with the proposal that the default settings of their browser should stop their information from being shared.
- Nine in ten agree they should be able to encrypt their messages and calls, so they can only be read by the recipient (90%).
- More than six in ten (61%) of respondents say they receive too many unsolicited commercial calls. An almost similar number would like commercial calls to be displayed with a special prefix (59%).

3.3. Collection and use of expertise

The Commission relied on the following external expert advice:

[12] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

-**Targeted consultations** of EU expert groups[13]
- **External expertise** collected in two studies:

– **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). In addition, a number of other studies have provided input to the review process (Annex I of the Staff Working Document on ex-post REFIT evaluation of the ePrivacy Directive).

3.4. Impact assessment

The executive summary of the impact assessment and the positive opinion of the Regulatory Scrutiny Board can be found on the website [add hyperlinks] of the Commission.

The following policy options to achieve the objective were examined against the three core 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 **best 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 means of a technologically neutral definition, which extends the scope of the legal instrument to include new functionally equivalent electronic communication services. In addition, the Regulation enhances user's control by clarifying that where consent is requested, it can be expressed through appropriate technical settings.

– Enhancing protection against unsolicited communications, with the introduction of 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.

Economic impacts of the preferred option

The compliance costs of the preferred option are expected to decrease overall, given the additional harmonisation and simplification introduced. **OTT communication services** would have to incur some compliance costs for revising the legality of their business models. However, such costs are not expected to be significant. **Website publishers** may incur some small adaptation costs. **Browsers** and similar applications permitting electronic communications,would have to incur significant costs for putting in place privacy by design

[13] Opinion of the Article 29 Working Party; the EDPS; views of BEREC; views of ENISA; views of members of the Consumer Protection and Cooperation Network ('CPC network').

settings. Traders would incur some costs following the introduction of the prefix for marketing calls.

The main impacts on national budgets and administration would derive from the implementation of the consistency mechanisms. The impact is not considered to be major, as synergies with already existing consistency mechanisms (e.g. in the field of data protection) might be exploited. No other significant impacts were identified.

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. The measures aim to ensure effective privacy and confidentiality of electornic communications for end-users and the protection of personal data, while providing clarity and simplification to reduce compliance costs and efforts of businesses that occur due to the obligations set forth. The proposed changes include specifically:

- Use of technologically neutral definitions to apprehend new services and technologies in order to ensure the Regulation is future-proof;
- Repeal of the security and notification of personal data breach rules, which will eliminate regulatory duplication;
- Clarification of scope, which would help to eliminate/reduce the risk of divergent implementation by Member States;
- Clarification and simplification of the consent rule for the use of cookies and other identifiers, to help eliminate/reduce the risk of divergent application and render the rule more effective in protecting end-users, while lowering compliance costs for businesses;
- Introduction of the consistency mechanism set forth under the GDPR for matters covered under Chapter II of this Regulation and advisory role of the European Data Protection Board for the remaining Chapters, to significantly improve the uniform interpretation of this Regulation

3.6. Impact on fundamental rights

The proposal for a regulation seeks to implement fundamental rights and principles recognised by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union: the right to respect for private and family life and communications is a fundamental right in the EU as is the right to the protection of personal data. The proposed measures aim at increasing the level of protection of privacy and personal data processed in relation with electornic communication, ensure greater legal certainty, and make EU confidentiality of communication more effective. The proposal seeks to complement and particularise the General Data Protection Regulation (Regulation 2016/679/EU)[14]. Protecting confidentiality of communications is essential as the effectiveness of this right is a necessary condition for exercising the freedom of expression and other related rights, such as personal data protection or the freedom of thought.

[14] 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).

4. BUDGETARY IMPLICATIONS

The proposal has no implications for the EU budget.

5. OTHER ELEMENTS

5.1. Implementation plans and monitoring, evaluation and reporting arrangements

The Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council every four years. The reports shall be made public and details the effective application and enforcement of this Regulation.

5.2. Detailed explanation of the specific provisions of the proposal

5.2.1. CHAPTER I - GENERAL PROVISIONS

Article 1 defines the subject matter and the objectives of the Regulation.
Article 2 determines the material scope of the Regulation.
Article 3 determines the territorial scope of the Regulation.
Article 4 contains definitions of terms used in the Regulation. While some definitions are taken over from Directive 2002/58/EC, others are modified, complemented with additional elements, or newly introduced. The Regulation also refers back to definitions enshrined in Regulation 2016/679/EU and in the proposal for a Directive establishing the European Electronic Communications Code.

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 ('Privacy and Electronic Communications Regulation)

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. The respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of communications guarantees that information exchanged between parties and the external elements of such communication (e.g. when it has been sent, from where, to whom, etc.) will not be revealed to anyone other than to the communicating parties. The principle must apply to current and future means of communication, including calls, Internet access, instant messaging applications, e-mail, internet phone calls and personal messaging through social media.

(2) Electronic communications data may reveal highly sensitive information about the 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, and embarrassment. In addition to the content of communications, electronic communications metadata, which includes the numbers called, the websites visited, one's geographical location, the time, date and duration when an individual made a call, etc, may also expose very sensitive and personal information, allowing precise conclusions to be drawn regarding the private lives of the persons, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. Moreover, electronic communications data may reveal information concerning legal entities, such as

---

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

busines secrets or other sensitive information that has economic value. The protection of confidentiality of communications is also an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of expression and information.

(3) Article 8(1) of the Charter of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. 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 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[4]. Electronic communications data may include personal data as defined under Regulation (EU) 2016/679, in the form of spoken words, text messages, files exchanged but also data related to the external elements of these communications ('metadata').

(4) In order to ensure adequate protection of the fundamental rights protected under Article 7 and Article 8 of the Charter, it is necessary to lay down specific rules concerning the protection of private life and communications and the processing of personal data in connection with the provision and use of electronic communications. This Regulation, therefore, harmonises the provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the the respect for private life and the protection of personal data in connection with the provision and use of electronic communications services and to ensure the free movement of such data and services in the European Union.

(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 of the European Parliament and of the Council as regards electronic communications data that constitutes personal data. In relation to electronic communications data. Regulation (EU) 2016/679 applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Regulation, including the obligations on controllers and processors and the rights of individuals. Insofar as the provisions of this Regulation conflict with the provisions of Regulation (EU) 2016/679, the provisions of this Regulation shall prevail.

(6) While the objectives and principles 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 inconsistent or not sufficiently effective protection of privacy and confidentiality in relation to electronic communications, in some fragmentation in the implementation of

---

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), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 337, 18.12.2009, p. 11).

its provisions in the internal market and a general perception that the confidentiality of communications is not fully guaranteed. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.

(7) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary. The latter will ensure legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and will provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities. A regulation will also serve to ensure consistency with Regulation (EU) 2016/679, in particular in the light of the lex specialis- lex generalis relationship between these instruments.

(8) The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited by Member States for reasons connected with the protection of natural or legal persons with regard to the processing of electronic communications data. Nonetheless, Member States should be allowed, within the limits of the provisions of this Regulation, to determine more precisely the conditions under which the processing of electronic communications data is lawful. In this respect, they may maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation where this is necessary to ensure an effective application and interpretation of such rules and does not conflict with any provisions of this Regulation. The margin of discretion which Member States have in this regard can therefore be used only in accordance with the objective pursued by this Regulation and of maintaining a balance between the protection of private life and the free movement of electronic communications data.

(9) This Regulation sets forth rules that 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. It also applies to natural and legal persons who use electronic communications services to send direct marketing commercial communications and/or collect information related to or contained in end-users' terminal equipment.

(10) This Regulation does not address issues of protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of electronic communications data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union. When the processing of electronic communications data by private bodies falls within its scope, this Regulation should provide for the possibility for 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 important interests including 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. Therefore this Regulation does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 11 of this Regulation, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal

law. Consequently, this Regulation does not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law and 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 rulings of the European Court of Human Rights and the Court of Justice of the European Union.

(11) In order to provide a strong and coherent data protection framework in the Union, this Regulation and the [New Regulation 45/2001] shall be governed by the same general principles with regard to the protection of privacy and confidentiality in relation to the processing of electronic communications data.

(12) 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 the processing takes place in the Union or not. Moreover, in order not to deprive end-users who are in the Union of the protection of privacy and confidentiality of electronic communications, this Regulation also applies to electronic communications data processed in connection with the provision of electronic communication services from outside the Union to end-users in the Union.

(13) New online players have emerged offering communications services which many users perceive as comparable to traditional electronic communications services such as voice telephony and SMS. These so-called over-the-top service providers ("OTTs") provide their services in the form of applications running over the internet access service (hence "over-the-top") and are in general not subject to Directive 2002/58/EC. This creates a void of protection of confidentiality for the users of these services. Moreover, it generates an uneven playing field between these providers and electronic communications service providers, as services which are perceived by users as functionally equivalent are not subject to the same rules. It is therefore necessary to update the scope of Directive 2002/58/EC so as to ensure that the protection of confidentiality is guaranteed, irrespective of the technological medium chosen. To this end, this Regulation uses the definition of electronic communication services set forth in the proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code[6], which encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communication services, which may be number-based or number independent. The latter category covers OTTs.

(14) With the development of the Internet of Things, connected devices and machines increasingly communicate with each other by using electronic communications networks. The transmission of machine-to-machine communications regularly consists in the conveyance of signals and hence usually constitutes an electronic communications service. Such transmission of machine-to-machine services may

---

6 Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM(2016 590 final of 14.09.16).

6 OJ C [...], [...], p. [...].

6

include personal data as defined under Regulation (EU) 2016/679 or sensitive business information. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation applies to the transmission of machine-to machine communications. Therefore the principle of confidentiality enshrined in this Regulation also applies to the transmission of machine-to-machine communications.

(15) The spreading 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 private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls, hospitals, etc. To the extent that these networks are provided to an undefined group of users, the confidentiality of these communications should be protected. The fact that wireless communication services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications and application of this Regulation. On the other hand, this Regulation does not apply to closed user groups and corporate networks.

(16) This Regulation applies to any exchange of information using electronic communication services and public communications networks, including content and metadata. Information conveyed or exchanged that is part of a broadcasting service provided over a public communications network, such as for example, news or other audio-visual content intended for a potentially unlimited audience does not constitute a communication in the sense of this Directive.

(17) 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, and the date, time, duration and the type of communication. It should also include data necessary to identify end-users' terminal equipment and the location of such equipment. 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 metadadata and therefore be subject to the provisions of this Regulation. Location data, such as for example, the location of a terminal equipment from or to which a mobile phone call or an Internet connection has been made or the Wi-Fi hotspot that his/her phone connected to, is also considered electronic communications metadata.

(18) Electronic communications data should be treated as confidential. This means that any interference with the conveyance of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of the communicating parties is prohibited. Interception of communications may occur, for example, when someone other than the communicating parties, listens calls, reads and stores the content of text messages for purposes other than the exchange or conveyance of communications The storage and further processing of electronic communications content, once the electronic communication has been conveyed to its recipient(s), shall be governed by Regulation

(EU) 679/2016. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc without the consent of the 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 phones over targeted areas, such as the so-called IMSI catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, and analysis of customers' traffic data, for example to determine users' interests and deliver targeted advertising without the consent of the concerned end-users.

(19) Processing of electronic communications data, by providers of electronic communications services, however, may be permitted in certain limited circumstances, for specified purposes and under clearly defined conditions. Permitted uses include the processing of electronic communications metadata that is necessary to maintain or restore the security of electronic communications networks and services, to ensure the ability of the electronic communications' network to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise its availability, authenticity, integrity and confidentiality of stored or transmitted communications data.

(20) Providers of electronic communications services may be obliged to ensure certain quality of service and ensure, for example, that the service does not suffer degradation or that the traffic is not unduly slowed down; for which, in some limited circumstances, it may be necessary to analyse metadata in real time and respond to fluctuations in traffic. Certain electronic communications metadata is necessary to enable providers to correctly bill end-users for the services used and to allow end-users to verify that the costs incurred correspond to their actual usage. The processing and storage of such data for such purposes should therefore be permitted without requiring consent by the end-user concerned.

(21) The processing of electronic communications metadata can be useful for businesses, consumers and society as a whole. End-users may benefit from value-added services such as traffic information, find nearby services, etc. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communication services to process electronic communications data, based on end-users consent. 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). Providers may request users' consent for purposes un-related ot the provision of services to the customer, including the transfer of this information to marketers and other clients. Providing more leeway to providers of electronic communications services to process metadata may foster a data market and encourage innovation in the Union. Polls and studies, however, show that 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. The risk to individuals' privacy may increase when such data is transferred to third parties for unrelated purposes. Therefore, the processing of electronic communications metadata for one or more specified purposes should be permitted, after having been adequately informed, only if the user has given his or her prior consent for the processing of his or her electronic communications data.

(22) 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 as the data subject's consent as defined and further specified in Regulation (EU) 2016/679. End-users should receive all relevant information about the intended processing in a clear and easily understandable language, such information should be given separately from the terms and conditions to the service. The provision of electronic communication services shall not be made conditional upon obtaining the end-user's consent to the processing of their electronic communications metadata; whether end-users consent is freely given, shall be assessed on a case by case basis; relevant aspects to determine whether the end-user has a genuine or free choice; shall include whether similar services are available at affordable prices; currently the market offers great variety of free or paid services, such as instant messaging, web mail; at least for Internet access services and voice communication services, the European Electronic Communications Code ensures that all end-users in the Union have access at an affordable price to such services.

(23) Terminal equipment of users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored on 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 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 very sensitive information, 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 malicious or unwanted tracking tools can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information, to trace the activities of the user or to instigate certain technical operations or tasks, often without the knowledge of the user, and may seriously intrude upon the privacy of these users.

(24) Any interference with the end-user's terminal equipment, for example, by using the terminal equipment processing capabilities, by storing or retrieving information from such equipment or by collecting information remotely from the equipment for the purpose of identification should be allowed only with the user's prior informed consent and for specific and transparent purposes. A high and equal level of protection of the private sphere of users' needs to be ensured therefore in relation to the privacy and confidentiality of users' terminal equipment content, functioning and use. Techniques that surreptitiously monitor the actions of users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the users' terminal equipment pose a serious threat to the privacy of users.

(25) Exceptions to the obligation to provide information and obtain the prior consent should be limited to situations which have no or only limited privacy intrusiveness. For instance, consent shall not be requested for authorizing the technical storage or access which is necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include user interface customization cookies set for short periods of time, for example, to remember language preferences. It also includes the storing of cookies to keep track of the user's input when filling online forms over several pages. Cookies can also be a legitimate

and useful tool, for example, in measuring web traffic to a site. Websites that engaging in configuration checking to provide the service in compliance with the end-users settings and the mere logging of the fact that the user's device is unable to receive content requested by the end-user shall not constitute access to such a device or use of the device processing capabilities.

(26) The methods of providing information and obtaining user's consent should be as user-friendly as possible. Taking into account the fact that especially in the online world users are increasingly requested to provide consent for online processing of their personal data, and the information overload related to these requests, the use of centralized, transparent and user-friendly settings of privacy preferences should be strongly encouraged. Where it is technically possible and effective, in accordance with the relevant provisions of Regulation (EU) 2016/679, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The choices made by users when establishing its general privacy settings of a browser or other application shall be binding on, and enforceable against, any third parties.

(27) 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 user to control the flow of information to and from the terminal equipment. More particularly web browsers may act as gatekeepers, thus helping users to prevent information from their terminal equipment (e.g. smart phone, tablet, computer etc.) from being accessed or stored. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. For web browsers to be able to convey users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of cookies for tracking purposes, they should, among others, require an affirmative action from the user to signify his or her agreement to the storage of, access to or use of the equipment computing capabilities. Such affirmative action may be given if the browser presents the user with settings that include 'accepting third party tracking cookies' and users are required to actively select 'tracking' to confirm their agreement. If browsers are equipped with such functionality, websites that want to set cookies for behavioral advertising purposes may not need to put in place banners requesting their consent insofar as users may provide their consent by selecting the right settings in their browser. Web browsers are encouraged to provide easy ways for end-users to change the private settings.

(28) While such banners serve to empower users, at the same time, they may cause irritation because users are forced to read the notices and click on the boxes, thus impairing Internet browsing experience. It is therefore necessary to provide for the obligation of providers of software enabling the terminal device's basic functions, including the retrieval and presentation of information on the Internet, to configure the software so that the software is offered on the market with privacy-friendly settings as a means to provide consent and to reinforce user's control over online tracking and over the flow of data from and into their terminal equipment. Users shall be prompted at the moment of the first use of the software to choose their privacy settings among a specifically established set of privacy options, ranging from higher (e.g. 'never accept cookies') to lower (e.g. 'always accept cookies'). In case of no active choice or action from the user, the web browser shall be set so that it blocks by default the storage of third party cookies or other type of trackers. Some web browsers detect that the settings of end-users and convey information from a visited website, for example 'The website X wishes to set a cookie'. This functionality offers enhanced transparency and

constitutes a valuable tool to empower usersto make decisions on a case-by case basis.. Browser providers are encouraged to include these functionalities

(29) Communication networks require the regular broadcast 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 broadcasting of active signals containing unique identifiers such as MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI (International Mobile Subscriber Identity), etc. A single wireless base station (i.e., a transmitter and receiver), such as 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 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 users as they enter, for example 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 repeats visits to specified locations. Providers engaged in such practices shall display prominent notices informing users that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and any measure the end-user of the terminal equipment can take to minimize or stop the collection and adequate safeguards are applied.

(30) Restrictions concerning specific principles and the rights and obligations set out in this Regulation may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, the safeguarding against and the prevention of threats to public security, 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. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(31) Where necessary and legally authorized under Union or Member State law, electronic communications may be recorded for the purpose of providing evidence of a commercial transaction. In such case, all the parties to the communications should be informed prior to the recording about the recording, and of its purpose. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged

(32) It is necessary, as regards calling line identification, 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. It is necessary, as regards connected line identification, 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. Providers of publicly available number-based interpersonal communication services should inform their subscribers of the existence of calling and

connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the end-usersto make an informed choice about the privacy facilities they may want to use.

(33) 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 shall 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. For the purpose of tracing nuisance calls, Member States should adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of end-users concerned.

(34) Technology exists that enables providers of communication services to limit the reception of unwanted calls by end-users in different ways, including blocking them at network level, blocking silent calls as well as other fraudulent and nuisance calls. Providers of publicly available number-based interpersonal communication services should provide end-users with such technology against the nuisance calls and free of charge. Such technology shall facilitate the possibility for end-users to stop the forwarded calls or unwanted incoming calls being passed on to their terminals. Providers should disseminate the existence of such functionalities to end-users, for instance by publicizing it on their webpage and on their bills.

(35) 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 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 to be included in a directory.

(36) If end-users that are natural persons give their consent to have their data included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (e.g. name, email address, home address, user name, phone number). In addition, providers of publicly available directories should, before including them in the directory, inform the end-users of the purposes of the directory and of the search functions of the directory. End-users should be able to determine by consent the categories of personal data on the basis of which 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.

(37) 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 indentified or identifiable end-users using electronic communications services. This includes the offering of products and services for commercial purposes. Political parties that contacts natural persons directly via electronic communications services in order to promote their parties are considered to provide direct marketing falling into the remit of this Regulation. The same applies to messages sent by other no-profit organisations to support the purposes of the organisation.

(38) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes which intrude into the private life of end-users of electronic communication services. 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 phone calls instant messaging applications, SMS, MMS, Bluetooth, emails, etc. It is therefore justified to require that prior consent of the end-user is obtained before commercial communications for direct marketing purposes are sent to end-users in order to effectively protect citizens 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 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 2016/679/EU.

(39) Having consented to receiving unsolicited communications for direct marketing purposes end-users 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 be clearly recognizable as such and should indicate the identity of legal or the natural person who transmits 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.

(40) 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, which can be easily be used by 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 shall 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.

(41) Voice-to-voice direct marketing calls, given that they are more costly for the sender and impose no financial costs on end-users, justify the possibility for Member States to establish and or maintain national systems only allowing such calls to end-users who have not objected.

(42) 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-usesof 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 2016/679/EU.

(43) When designating the supervisory authorities responsible for monitoring this Regulation, Member Sates shall ensure that such authorities are completely independent in accordance with Article 16 of the TFEU and Article 8(3) of the Charter of Fundamental Rights of the European Union. Requirements for independence applicable to the supervisory authorities responsible for the monitoring of Chapter II of this Regulation should be those set forth under Regulation 2016/679/EU. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. However, the supervisory authorities responsible for monitoring the application of Regulation 2016/679/EU shall also be responsible for monitoring the application of Chapter II of this Regulation. Such authorities shall also be responsible for monitoring the application of this Regulation regarding electronic communications data that refers to legal entities. Such additional tasks shall not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation Regulation 2016/679/EU and this Regulation. Where more than one supervisory authority is established in a Member State, such authorities shall cooperate with each other. They shall also cooperate with the authorities appointed to enforce the European Electronic Communications Code.

(44) The enforcement of the provisions of this Regulation often requires cooperation between the national supervisory authorities of two or more Member States, for example in combating interferences with the confidentiality of the terminal equipment. In order to ensure smooth and rapid cooperation in such cases, the procedures of the cooperation and consistency mechanism established under Regulation 2016/79/EU should apply to Chapter II of this Regulation. Therefore, the European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, in particular by issuing opinions in the context of the consistency mechanisms or by adopting binding decisions in the context of dispute resolution as provided in article 65 of Regulation 2016/679/EU as regards Chapter II of this Regulation.

(45) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks, including adopting binding decisions, conferred on it in accordance with this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, 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 To this end, this Regulation provides national authorities shall have the relevant tasks and powers as set forth under Articles 57 and 58 of Regulation 2016/679/EU. These tasks and powers do not include those which relate to specifici provisions of the Regulation 2016/679/EU, such as those set forth under Art 57 (a), (j), (k), (l), (n), (o) and Art 58 (c), (e), (h).

(46) 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 TFEU for those purposes.

(47) 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 TFEU should be delegated to the Commission. 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 marketing calls, which will identify voice-to-voice marketing calls. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(48) 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 (TEU). 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.

(49) Directive 2002/58/EC and Commission Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications[7] should be repealed by this Regulation.

HAVE ADOPTED THIS REGULATION:

[7] Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (OJ L 173 26.06.2013 p. 2).

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject-matter and objectives

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons, 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, in connection with the provision and use of electronic communications services.

2. This Regulation ensures free movement of electronic communications data and electronic communication 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 for the purposes mentioned in paragraphs 1 and 2 insofar as it concerns the processing of personal data.

Article 2
Material Scope

1. This Regulation applies to the processing of electronic communications data processed 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:

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

(b) to activities of the Member States which fall within the scope of Chapter 2 of Title V of the TEU;

(c) in relation to electronic communication services which are not publicly available;

(d) to 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. For the processing of electronic communications data by the Union institutions, bodies, offices and agencies, pursuant to Regulation (EU) 00/0000 [new EDPS regulation] applies.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, 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 Directive 2014/53/EU, in particular of the rules on essential requirements in Article 3 of that Directive.

Article 3
Territorial scope

1. This Regulation applies to:

(a) to electronic communications data processed in connection with the provision of electronic communications services in the Union, regardless of whether the processing takes place in the Union or not; to the use of such services, and to the protection of information related to the terminal equipment of end-users located in the Union;

(b) to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union;

(c) to electronic communications data processed in connection with the provision of electronic communications services from outside the Union, but in a place where Member State law applies by virtue of public international law.

2. Where paragraph 1(b) applies, the natural or legal person not established in the Union 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 services are located.

4. The representative shall have the power to represent the natural or legal person referred to in paragraph 1, in addition or instead of that person, and for that purpose to answer questions and provide information , in particular, to supervisory authorities, courts and end-users, on all issues related to processing, 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, the definitions of Regulation (EU) 2016/679/EU shall apply. Furthermore, the definitions of Directive 00/0000/EU [Directive establishing the European Electronic Communications Code] shall also apply and in particular the definition of 'electronic communications network' [Article 2 (1)], 'electronic communications service' [Article 2(4)], 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service' [Articles 2(5), (6) and (7) respectively], 'user' [Article 2(13)], 'end-user' [Article 2(14)], and 'call' [Article 2(21)].

2. The following definitions shall also apply:

(a) 'electronic communication' means the exchange or conveyance of electronic communications data between a finite number of parties by means of electronic communications services or an electronic communications network;

(b) 'electronic communications data' means electronic communications content and metadata;

(c) 'electronic communications content' means the content such as text, voice, images, and sound exchanged by means of an electronic communications services or via an electronic communications network;

(d) 'electronic communications metadata' means data related to an end-user of electronic communications services, processed for the purposes of transmitting, distributing or exchanging electronic communications content; including but not limited to, data to trace and identify the source and destination of a communication, and the date, time, duration and the type of communication. It includes data broadcasted or emitted by the terminal equipment to identify end-users' communications and/or terminal equipment in the network and enable it to connect to such network or to another device.

(e) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published and or made available to members of the public or a section of the public, including by means of a directory enquiry service;

(f) 'electronic mail' means any message containing information such as text, voice, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the recipient's terminal equipment;

(g) '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; this includes the use of automated calling and communication systems with or without human interaction, electronic mail and SMS etc.;

(h) 'voice to voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;

(i) '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;

(j) 'terminal equipment' means equipment within the meaning of Article 1 (1) of Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment[8].

[8] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162 21.06.2008 p. 20).

CHAPTER II
PROTECTION OF ELECTRONIC COMMUNICATIONS AND OF INFORMATION RELATED TO END-USERS' TERMINAL EQUIPMENT

Article 5
Confidentiality of electronic communications

Electronic communications shall be confidential. Any processing of, including interference with, electronic communications by any natural or legal person without the consent of the end-users concerned, such as by listening, tapping, storing, monitoring or other kinds of interception and surveillance shall be prohibited, except when provided otherwise in this Regulation.

Article 6
Lawfulness of processing of electronic communications metadata

1. Providers of electronic communications services may process electronic communications metadata if:

(a) 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;

(b) Iti s necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation 2015/2120;

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

(d) it is necessary for emergency services as set forth under Article 13 of this Regulation;

(e) the end-user to whom electronic communications metadata relate has given his or her prior consent to the provider of electronic communications services to process electronic communications metadata relating to him or her for one or more specified purposes, including for the provision of value added services to such end-user, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous and the conditions set forth under paragraph 2 of this Article are fulfilled

2. For the purpose of paragraph 1(e) 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, Articles 35 and 36 of the GDPR shall apply.

Article 7

Erasure of electronic communications data

1. Electronic communications metadata shall be erased or made anonymous as soon as the communication has taken place unless one of the lawful grounds for processing as set out in Article 6 (1) apply.
2. Where the processing of electronic communications metadata for the purpose of billing in accordance with Article 6(1)(c), 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;
3. For the conveyance of communications, the technical storage of electronic communications data during the time necessary for such conveyance;
4. Electronic communications data may be stored by the parties communicating or by a third party entrusted by them to store such data, provided that the parties communicating have sole control over the use of the communications data.

Article 8

Protection of information related to end-users' terminal equipment

1. The use of terminal equipment's processing and storage capabilities and the collection of information about end-users' terminal equipment, including software and hardware, by natural or legal persons other than end-users concerned shall be prohibited, except in the following cases:

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

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

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

2. The collection of data emitted by terminal equipment to enable it to connect to another device and or network equipment by natural or legal persons other than end-users concerned shall be prohibited, except:

(a) if it is done exclusively in order and for the time necessary to establish a possible connection;

(b) if a clear and prominent notice is displayed to the public informing of, at least, the modalities of the collection, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection, and,

When such data is used for direct marketing and profiling, the end-user shall have the right to object as provided for in Artice 21 of the GDPR; and,

(c) appropriate technical and organization measures to ensure a level of security appropriate to the risks, as set forth under Article 32 of Regulation (EU) 2016/679/EU, have been applied.

3. The information to be provided pursuant to paragraph 2(b) may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the collection.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article [xx] for the purpose of determining the information to be presented by the icon and the procedures for providing standardized icons.

Article 9
Consent

1. The conditions for consent provided for under Article 7 of Regulation (EU) 2016/679/EU shall apply.

2. Where technically possible and effective, in particular for the purposes of Article 8(1)(c), consent may be expressed by using the appropriate technical settings of a software application enabling access to the Internet.

3. End-users who have agreed to the processing of electronic communications data as set forth under Articles 6(e) shall be given the possibility to withdraw their consent at any time as set forth under Art 7(3) of Regulation (EU) 2016/679/EU and on periodic intervals of 6 months, as long as the processing continues.

Article 10
Privacy by design

1. The settings of all the components of the terminal equipment placed on the market shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities.

2. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the Internet, shall be configured to by default prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

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, 6, 7, and 8 of this Regulation when such a restriction respects the essence of the fundamental rights and is a necessary, appropriate and proportionate measure in a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or of unauthorised use of electronic communications systems. Any legislative measure referred to in paragraph 1 shall be in accordance with the Charter of Fundamental Rights of the European Union, in particular with Articles 7, 8, 10 and 52 thereof.

2. Providers of electronic communication services shall establish internal procedures for responding to requests for access to users' pesoanl data based on national provisions, adopted pursuant to parraagpha 1. They shall provide the compeetnat national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoiked and their response.

3. Member States law and Union law may set forth conditions allowing the recording of communications data for the purpose of providing evidence of a commercial transaction or of any other business communication.

CHAPTER III
END-USERS ' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

Article 12
Presentation and restriction of calling and connected line identification

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

(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;

(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 detailed in paragraph 1(a), (b) (c) and (d) shall be provided to the end-user by simple means and free of charge.

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

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

Article 13
Exceptions to presentation and restriction of calling and connected line identification

1. Regardless of any elimination of the calling line identification by the calling end-user, where the call is made to emergency services, providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of 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, law enforcement agencies, ambulance services and fire brigades, 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 Block Calling

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

(a) to block incoming calls from specific numbers;

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

Article 15
Publicly available directories

1. Providers of publicly available directories shall obtain the consent of end-users who are natural persons prior to including their personal data in the directory and, if so, which categories of personal data shall be included, 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. Providers of publicly available directories shall inform end-users who are natural persons whose personal data are in the directories of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.

3. Providers of publicly available directories shall provide end-users that are legal persons with the possibility to object against the data related to them to be included in the directory. Providers shall give end-users that are legal persons the means to verify, correct and delcting 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. The use of electronic communications services by natural or legal persons for the purposes of transmitting direct marketing communications is allowed only in respect of end-users who have given their prior consent.

2. Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Regulation 2016/679/EU, the same 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 on the occasion of each message.

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

(a) present the identity of a line on which he or she 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 voice-to-voice live calls to natural and legal persons shall only be allowed in respect to persons who have not expressed their objection to receiving these communications.

5. 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, about the identity of the legal or natural person on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner,to receiving further marketing communications.

6. The Commission shall be empowered to adopt implementing measures in accordance with Article [xx] for the purpose of specifying the code to identify marketing calls.

CHAPTER V
SECURITY RISKS

Article 17

Information about detected security risks

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

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT

Article 18
Independent supervisory authorities

1. Each Member State shall provide for one or more independent authorities to be responsible for monitoring the application of this Regulation ('supervisory authorities').

2. Insofar as different supervisory authorities in Member States are in charge of monitoring the application of this Regulation, such authorities shall cooperate with each other.

3. Supervisory authorities shall cooperate with national regulatory authorities pursuant to the European Electronic Communications Code.

Article 19
Supervisory authorities entrusted with monitoring the application of Regulation 2016/679

1. The supervisory authorities responsible for monitoring the application of Regulation 2016/679/EU shall also be responsible for monitoring the application of Chapter II of this Regulation.

2. For the purpose of this Article, the tasks and powers of the supervisory authorities shall be exercised in regard to end-users.

Article 20
Tasks and Powers

1. For the purpose of monitoring the application of Chapter II, Chapter VI and VII of Regulation 2016/679/EU shall apply mutatis mutandis.

2. Insofar as monitoring the application of Chapter III, IV and V of this Regulation is entrusted by Member States to independent authorites other than those provided for under paragraph 2 of Article 19, such independent authorities shall have the same tasks and powers as those provided for under Articles 57 and 58 of Regulation 2016/679/EU. Such tasks and powers shall be exercised with regard to end-users.

Article 21
European Data Protection Board

The European Data Protection Board, established under Article 68 of Regulation 2016/679/EU, shall be competent to ensure the consistent application of Chapter II of this Regulation. To that purpose, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation 2016/679/EU. 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 22
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 2016/79/EU regarding the matters covered by Chapter II of this Regulation.

CHAPTER VI
REMEDIES, LIABILITIES AND PENALTIES

Article 23
Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the end-user considers that his or her rights under this Regulation have been infringed in accordance with this Regulation.

2. Without prejudice to any other administrative or non-judicial remedy, every end-user of electronic communications services shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her or where that supervisory authority does not handle a complaint or does not inform the end-user within three months on the progress or outcome of the complaint lodged. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

3. Every end-user of communications services shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed. Such proceedings shall be brought before the courts of Member State of the habitual residence of the end-user.

4. 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 communication services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect to such infringements.

5. End-users shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data and the protection of privacy to lodge the complaint on his or her behalf, to exercise the rights referred to in paragraphs 1, 2 and 3 of this Article on his or her behalf, and to exercise the right to receive compensation referred to in Article 23 on his or her behalf where provided for by Member State law.

6. Member States may provide that a body, organisation or association independently of the end-user's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to paragraph 1 of this Article and to exercise the rights referred to in paragraphs 2 and 3 of this Article if it considers that the rights of the end-user under this Regulation have been infringed.

Article 24
Right to compensation and liability

Every end-user of 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.

Article 25
General conditions for imposing administrative fines

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

2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1 of this Article be subject to administrative fines up to 10 000 000 EUR, 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(2);

(b) the obligations of the provider of terminal equipment and or software enabling electronic communications, pursuant to Article10 ;

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

3. Infringements of the following provisions shall, in accordance with paragraph 2 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:

(a) the principle of confidentiality of communications, permitted uses, time limits for erasure pursuant to Articles 5, 6, 7 and 8 (1).

4. Member States shall lay down the rules on penalties for infrigmentns of Articles 12, 13, 14, 16 and 17 of this Regulation.

5. Non-compliance with an order by the supervisory authority as referred to in Article 20, paragraph 2 shall, in accordance with paragraph 2 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.

6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 19 each Member State may lay down the 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 26
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 xx, 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, by xxx and, without delay, any subsequent amendment affecting them.

Chapter VII
DELEGATED ACTS

Article 27
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 [xx] 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 [XX] 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 [XX] 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 28
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. For the implementation measures referred to in paragraph 6 of Article 16, the Committee shall be the Communications Committee established under Article 110 of the Directive establishing the European Electronic Communications Code.
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
4. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER VIII
FINAL PROVISIONS

Article 29
Repeal of Directive 2002/58/EC

1. Directive 2002/58/EC and Commission Regulation 611/2013 are repealed with effect from XXXX.
2. References to the repealed Directive shall be construed as references to this Regulation.

Article 30
Commission reports

By XX and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

Article 31
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 … [six] months from the date of entry into force of this Regulation].

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

Done at Brussels,

For the European Parliament
The President

For the Council
The President