Working document 1.0

DLA PIPER

Proposals for an amendment to the General Data Protection Regulation and repealing the ePrivacy Directive

29 May 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1 INTRODUCTION TO THIS STUDY

This study has been prepared by the international law firm DLA Piper UK LLP (Brussels office), at the request of ETNO. ETNO is the European Telecommunications Network Operator's Association calling for the European legislator to repeal Directive 2002/58/EC (**"ePrivacy Directive"**) through the new General Data Protection Regulation (**"GDPR"**), which is currently under discussion.

The GDPR is meant to apply to all players offering services to European citizens, notwithstanding the sector they are active in, and aims to achieve a full and horizontal harmonisation in the area of privacy, based on the principle of technology neutrality.

While ETNO fully supports this idea, it is convinced that such harmonised privacy area will not be realized as long as the e-Privacy Directive continues to exist next to the GDPR. Although the European Commission announced that the ePrivacy Directive is slated for review after the adoption of the GDPR, ETNO continues to urge to consider the proposed amendments within the scope of the GDPR.

Since the start of the GDPR discussions, and even prior to that, ETNO has expressed its request to repeal the e-Privacy Directive. ETNO believes that the GDPR offers a timely and appropriate instrument to resolve these inconsistencies and market distortions. Otherwise, there is a significant risk that legal uncertainty for consumers as well as telecom providers will continue to last, which is to be avoided at all cost.

Against this background, DLA Piper has been requested by ETNO to investigate the technical and legal feasibility to address the regulatory asymmetries created by the ePrivacy Directive and to propose a way how this could be dealt with in the light of the current on-going discussions in relation to the GDPR. The analysis of this request forms the scope and subject matter of the present document.

The on-going review of the EU Data Protection legal framework is a unique opportunity to achieve a true level playing field in order to ensure that technologically neutral principles apply to all stakeholders, and therefore ETNO urges the policy makers to take into account this proposal. It cannot be denied that in today's converged world, the distortions between sectors are not justifiable and this particular example of asymmetry needs to be addressed without delay. As is illustrated by the conciseness of the amendments, only minor modifications to the legislative framework are needed to remedy the current inconsistencies and issues.

2 STUDY RESULTS

Upon analysing the legal implications of the co-existence of the ePrivacy Directive and the GDPR, DLA Piper comes to the following conclusion:

- first of all, this co-existence will likely lead **to legal uncertainty** and confusion for all stakeholders (telecom providers, consumers and regulatory bodies), notably with regard to the territorial scope of the ePrivacy Directive and with regard to the competent regulatory bodies;
- secondly, while at the time of adoption of the ePrivacy Directive it was justified to have a specific set of privacy rules for the telecom sector, the existence of such a dual legal data protection framework can **no longer be justified** in today's new reality of converged media and communication services and increasingly innovative offers from a myriad of new players. Indeed, telecom providers are subject to the GDPR (if adopted in its current version) and the sector-specific rules of the ePrivacy Directive as regards the processing of personal data (notably location and traffic data), whereas the - mainly US-based - over-the-top players that are offering functionally equivalent services (such as Whatsapp and Skype) are only subject to the GDPR, and not the ePrivacy Directive. This situation needs to be reconsidered: similar services should be subject to the same rules;
- thirdly, as long as the ePrivacy Directive coexists with the GDPR, there will be an **unlevel playing field** between all market players, consumers will not experience comparable digital privacy online and the competitive position of European providers will be compromised, possibly until 2020 if the European legislator does not take immediate action.

As a result of these considerations, and to remedy its consequences, DLA Piper has prepared **an amendment** which aims **to integrate** the data protection related articles of the **ePrivacy Directive into the GDPR**. As will be shown in the attached proposal, DLA Piper considers that such incorporation is not only feasible but instead highly recommendable as it would remedy legal uncertainty on several points and be in line with good policy making practice.

After implementing the proposed amendment, a number of provisions still remain in the ePrivacy Directive. As will be described hereafter, to the extent that those provisions are still relevant, they have little to do with privacy and it would therefore make much more sense to **integrate these provisions into the relevant legal instruments of the Telecoms Package**. DLA Piper is of course prepared to propose an additional amendment in order to reflect these changes.

Upon reading our proposal, it will become clear that only minor modifications to the legal data protection framework are required in order to address and remedy the existing inconsistencies and unjustified differences between the ePrivacy Directive and GDPR. This will be further explained in detail in the document which consists of (i) an explanatory memorandum in which the reasons for preparing said amendments are substantiated, (ii) the proposed amendments to the GDPR (including a justification for each article) as well as a proposal to delete several provisions of the ePrivacy Directive and (iii) a consolidated version of the revised GDPR.

A EXPLANATORY MEMORANDUM

1 INTRODUCTION AND CONTEXT OF THE PROPOSAL

On 25 January 2012 the European Commission proposed a new European General Data Protection Regulation[1], which will repeal the existing Data Protection Directive[2] (hereafter referred to as **"Directive"**). The proposed regulation introduces a number of new concepts and new rights and obligations for both data controllers and data subjects. Over the past 3 years, that legislative process has been on-going, and several amendments have been made to the initial proposal, leading to a consolidated version of the proposal on 19 December 2014 (**"Regulation"** or **"GDPR"**).[3]

The existing Directive has been complemented by a specific set of rules on the processing of personal data in the electronic communications sector, including rules on traffic and location data, as well as data breach notification. Currently, these rules are contained in the Directive 2002/58/EC on privacy and electronic communications[4], as amended by Directive 2006/24/EC and Directive 2009/136/EC[5] (hereafter referred to as **"ePrivacy Directive"** or **"EPD"**), which in itself replaced a previous Directive from 1997. As the growth and development of the electronic communications sector gave rise to specific requirements concerning the protection of personal data and the privacy of the user, the European legislator considered the adoption of different rules for amongst others the treatment of traffic data to be necessary and appropriate.

While the approval of the ePrivacy Directive was considered to be necessary and appropriate at the date of its adoption, it should be emphasised that nowadays the entire area of electronic communications has undergone significant changes, is converging and is no longer exclusively reserved for telecom providers. As the Internet has evolved rapidly, a range of new telecom-alike services (including OTT services) started developing, some of which are functionally equivalent to

[1] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

[2] 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, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[3] See: http://www.eudataprotectionlaw.com/wp-content/uploads/2015/01/Regulation-Council-Draft-Dec14.pdf

[4] 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), see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[5] Consolidated version of 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) amended by (i) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC and by (ii) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

traditional telecom services and also give rise to the collection of location data and traffic data and which are not necessarily subject to the ePrivacy Directive. The existence of different and unequal rules for equivalent services does not only greatly impact telecom providers' ability to compete on equal footing but also creates legal uncertainty and overall confusion for consumers. Moreover, a dual regime is unlikely to lead to a single market in privacy or data and distorts the value in data and innovation in data driven services

After having performed a detailed analysis of the ePrivacy Directive and the Regulation, DLA Piper concludes that there is undoubtedly room for the integration of both legislative acts into one single legal instrument: the proposed Regulation. To illustrate this, we have prepared an **amendment to the Regulation** in order to integrate the relevant definitions of the ePrivacy Directive into the Regulation (notably 'communication' and 'electronic mail') and move the clauses on confidentiality of communications (art. 5 EPD) and unsolicited communications (art. 13 EPD) to the Regulation (see **Section 4.2**), as well as identifying the provisions of the ePrivacy Directive which could be abolished. This analysis and the proposed text forms the scope of the present document.

However, we also see that some of the articles of the ePrivacy Directive do not concern privacy and data protection related topics, but rather general telecom and/or consumer protection related issues. This particularly relates to the clauses on itemised billing (art. 7 EPD), presentation and restriction of calling and connected line identification (art. 8 EPD), exceptions (art. 10 EPD), automatic call forward forwarding (art. 11 EPD), directories of subscribers (art. 12 EPD), technical features and standardisation (art. 14 EPD) and implementation and enforcement (art. 15a). These articles cannot be integrated into the GDPR but it would make a lot of sense to integrate them, provided that they are still of relevance today, into the Telecoms Package[6] (see **Section 4.3**). DLA Piper is prepared to also propose an amendment to the Telecoms Package to reflect this. Such integration can be done rightaway, or one could also wait with this operation until the review of the Telecoms package is more advanced.

As result of these actions, DLA Piper is of the opinion that **the ePrivacy Directive and Regulation 611/2013[7] can easily be repealed**.

This explanatory memorandum presents and further details the proposed amendments to the Regulation in Section 4 (*Proposed amendments*). Before giving an overview of the inconsistencies and unjustified differences that exist between the ePrivacy Directive and the Regulation and the additional arguments supporting the integration of the ePrivacy Directive into the Regulation (*Section 3*), we will briefly discuss the relevant legislatives evolutions as well as market evolutions (*Section 2*) supporting the proposed amendments.

[6] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, as amended by Directive 2009/140/EC and Regulation 544/2009, see: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf

[7] Regulation 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, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

2 LEGISLATIVE & MARKET EVOLUTIONS

2.1 Legislative evolutions

2.1.1 From Directive to Regulation

The Directive - which constitutes the centrepiece of existing European legislation on personal data protection - was adopted in 1995, with a two-fold objective: (i) to protect the fundamental rights to data protection and (ii) to guarantee the free flow of personal data between Member States. It has been complemented by Framework Decision 2008/977/JHA as a general instrument at EU level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters.[8]

Over the past 20 years, rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting increased dramatically, and technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Moreover, individuals increasingly make personal information available publicly and globally, and technology has transformed both the economy and social life.

In regard of those challenges and in order to build trust in the online environment, the European Commission published in 2012 a proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Discussions on the text of the Regulation are still on-going, and a final agreement is planned to be reached in the Spring of 2016.

2.1.2 From ePrivacy Directive to …

In the mid-1990s specific European telecommunication data protection rules were enacted complementing the Directive. Because of the introduction of new advanced digital technologies in public telecommunications networks, the adoption of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[9] (**"Telecommunications Data Protection Directive"**) was considered necessary to protect the fundamental rights and freedoms of natural persons and legitimate interests of legal persons, "*in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users*" .

The telecom sector has been evolving rapidly and still evolves at a high speed. Consequently, over the past years the sector-specific rules had to be changed several times in order to keep up with new developments in the telecom sector.

[8] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ.L.* 350, 30.12.2008, 60-71 (**"Framework Decision"**), see http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN

[9] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

In 2002, the European legislator decided to rename the Telecommunications Data Protection Directive into the ePrivacy Directive. The 'first' ePrivacy Directive modernized and broadened many of the concepts already included in the Telecommunications Data Protection Directive, and more importantly included a different treatment for the processing of location data that was only applicable to telecom providers.

In 2006, the ePrivacy Directive has been amended again by Directive 2006/24/EC[10], also known as the Data Retention Directive. On 8 April 2014 the Court of Justice of the European Union however declared the Data Retention Directive to be invalid, hence those modifications are no longer to be taken into account.[11]

In 2009, the ePrivacy Directive has been amended another time by Directive 2009/136/EC[12], on which moment the so-called the new 'cookie provision', changing the former opt-out regime into an opt-in regime, was introduced. As the cookie provision is not specifically applicable to actors in the telecom sector, but instead to all website operators, it has never been clear for what reason such provision had been included in the ePrivacy Directive.

Recently, notably on 6 May 2015, the European Commission published its Digital Market Strategy for Europe, in which it acknowledges the inadequacy of the current legal framework, and explicitly recognizes the need to reassess the ePrivacy Directive so as to implement a level playing field for all market players, since "*most of the articles of the current e-Privacy Directive apply only to providers of electronic communications services, i.e. traditional telecoms providers. Information society service providers using the Internet to provide communication services are thus generally excluded from its scope.*".[13]

Indeed, the applicability of the majority of the rules set out in the ePrivacy Directive depends on whether or not a particular service qualifies as an 'electronic communications service' (article 2.c of the Framework Directive), meaning "*a service normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks (…)*". According to the general interpretation, most OTT services are considered as not conveying signals on electronic communications networks and thus falling outside the scope of this definition. Consequently, they do not need to comply with most obligations under the ePrivacy Directive. Instead, they are generally considered to fall under the scope of "information society services".[14]

---

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, see: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1431676935830&uri=CELEX:32006L0024

[11] CJEU 8 April 2014, C-293/12 and C-594/12, www.curia.eu.

[12] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, see: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&rid=3.

[13] "A Digital Single Market Strategy for Europe", COM(2015) 192 final, 10, see: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

[14] As defined in the Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

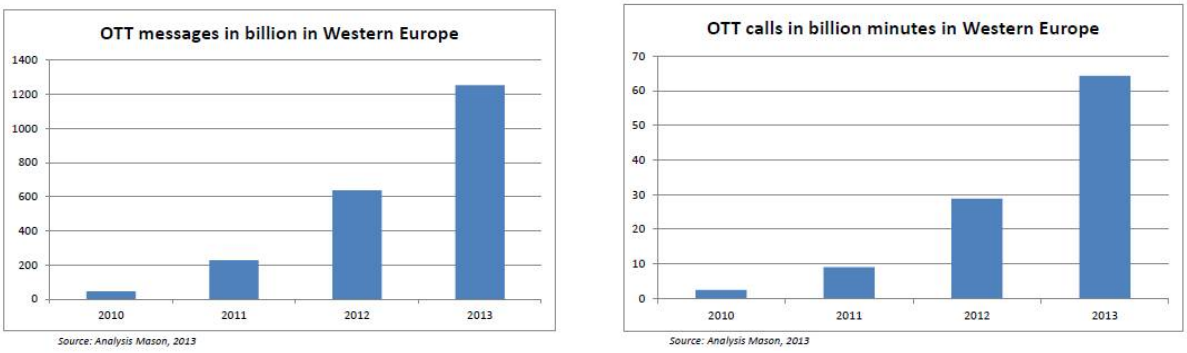
2.2 Market evolutions

The aim of this study is not to present all economic evolutions the telecom sector went through as from the existence of state-owned monopolies, over the liberalization of the market to the current rise of OTT players. We nevertheless consider it highly relevant to briefly discuss the current state of the market, and the important and increasing position of OTT players on the market.

The entire area of electronic communications has undergone significant changes and is no longer exclusively reserved for telecom providers. More in particular, over the last years the telecom sector has witnessed the rise of OTT players offering several competing and functionally-equivalent services.[15]

Communication services offered by OTT players are close substitutes to the corresponding services offered by telecom providers. Well-known substitutes for both traditional SMS and MSS services are Whatsapp, Apple's iMessage, Facebook Messenger, Twitter and Instagram, while Skype, Viber, Apple's FaceTime and Google's Voice/Hangout are well-known substitutes for traditional voice services.

As has been observed by CERRE (Centre on Regulation Europe), the increase of OTT messaging and call volumes has been enormous over the last years, as is illustrated by the following figures.



Source: CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 16.

Whilst in 2010 OTT messages in Western Europe only accounted for **8,31%** of overall messaging traffic, this number had increased to not less than **66,96%** in 2013.[16] Due to the still increasing popularity of smartphones, the ease of installing mobile voice, messaging and video services as applications on such devices and the increasing availability of stable mobile broadband services, it is expected that the popularity of OTT communication services will only increase. Hence, OTT players and OTT services can no longer be ignored.

[15] CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 15, see: http://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf

[16] Data cited in CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 15, see: http://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf.

2.3 Momentum for action

Taking into account (i) that the Regulation is still under discussion and amendments can be brought to the table, (ii) that there is a consensus on the need to revise the ePrivacy Directive in its current form and (iii) that the changing market illustrates the increasing presence of OTT players on the telecom market, there is a momentum for action. Hence, it is of key importance for consumers and telecom providers that the proposed amendments are taken into account at this stage of the decision-making procedure and that the discussion on the ePrivacy Directive is not postponed until after the adoption of the Regulation.

If the process of evaluating and revising the ePrivacy Directive would indeed only be initiated once the Regulation is adopted - which is not to be expected to effectively take place before Spring 2016 - that would imply that the European legislator would need to redo his homework just when it has finished a thorough review of the relevant legal framework on data protection. A review of the ePrivacy Directive will inevitably involve a review of the Regulation. Moreover, if no immediate legislative action is undertaken, that will have considerable negative consequences:

- **Legal uncertainty** - Consumers and data subjects are not aware of the different levels of protection offered by traditional voice and SMS services on the one hand and OTT voice and messaging services (such as Skype and WhatsApp) on the other hand. While the average consumer is likely to expect the same or similar level of protection, in reality, OTT players will not be obliged to offer the same level of protection. For example, the confidentiality of communications principle does not apply as such to OTT services.

- **Unlevel playing field** - Although telecom providers and OTT players increasingly compete for the same public, they are currently not subject to the same rules, and they will not be subject to the same rules for a long time. Indeed, if the review of the ePrivacy Directive is only to start upon the adoption of the Regulation, it is unlikely that a revision and/or integration of the ePrivacy Directive will be effective before 2020. The use of OTT services augmented significantly over the past 4 years, and there are no concrete indications that this growth will stagnate soon. Hence, if the playing field is not levelled soon, the legislative intervention might be 'too little, too late', and domestic telecom providers are very likely to lose ground to - mainly US-based - OTT players. Hence, if the European Union wants telecom providers to compete with the those (US-based) OTT players, notably in the field of big data which the European Commission sees as central to the digital economy and growth path, then immediate action is required.

- **Fragmentation** - If no legal action is undertaken at a European level, it is to be expected that Member States will start regulating OTT players on a national level, leading to a fragmentation of the market and a patchwork of diverging national legislations. In this regard it should be emphasised that Finland is already engaging in unilateral efforts to address the regulatory asymmetry created by the co-existence of the Directive and the ePrivacy Directive. Finland in particular adopted its 'Information Society Code' - which entered into force on 1 January 2015 - pursuant to which OTT players are subordinated to a more stringent set of obligations. This legislation will amongst other oblige social media platforms to ensure the confidentiality of messages exchanged over their messaging services. If more Member States follow suit, this will

add further uncertainty for business and consumers and will lead to further inconsistency and lack of harmonized regulation. It underscores again the urgency of addressing this matter.

3 INCONSISTENCIES BETWEEN THE EPRIVACY DIRECTIVE AND THE REGULATION

In this Section 3 (*Inconsistencies between the ePrivacy Directive and the Regulation*) we will further develop the arguments supporting the integration of the ePrivacy Directive into the Regulation.

3.1 Unclear relationship between the ePrivacy Directive and the Regulation

The adoption of the Regulation may have an adverse impact on the interplay of that Regulation with the ePrivacy Directive. While the ePrivacy Directive specifies that it has been adopted with a view to "*particularise and complement Directive 95/46EC"* (art. 1 § 2 EPD), such reference is missing in the Regulation. Indeed, article 89 § 2 of the Regulation even explicitly states that article 1 § 2 EPD shall be deleted.

Although article 89 § 1 of the Regulation states that it does not intend to impose additional obligations "*in relation to matters for which* [telecom providers] *are subject to specific obligations with the same objective set out in the* [ePrivacy Directive]", recital 135 of the Regulation recognises the unclear character of the relationship and states that "*in order to clarify the relationship between this Regulation and* [the ePrivacy Directive], *the latter directive should be amended accordingly".*

Moreover, as the Directive will be repealed by the Regulation, article 88 of the Regulation specifies that references to the repealed Directive are to be construed as references to the Regulation. Although such clause makes sense from a legislative point of view, it is likely to lead to interpretation issues in this specific case, as is illustrated by the following example. Article 15 of the ePrivacy Directive stipulates that Chapter III of the Directive on judicial remedies, liability and sanctions applies to the ePrivacy Directive. While that Chapter III is rather limited in the Directive, the corresponding Chapter VIII in the Regulation contains a much broader range of sanctions and remedies. Does this mean that all those sanctions and remedies will become applicable to telecom providers or that only those sanctions that are also included in the Regulation but were already included in the Directive are applicable? Moreover, who will be able to impose sanctions? Data protection authorities ('supervisory authorities') as mentioned n Chapter VIII of the Regulation? Or telecom regulators ('national regulatory authorities') as mentioned in the ePrivacy Directive?

The relationship between the ePrivacy Directive and the Regulation is unclear and will lead to interpretation issues and legal uncertainty.

3.2 Overview of inconsistencies and unjustified differences

In this subsection the most important (i) inconsistencies between the Regulation and the ePrivacy Directive as well as (ii) unjustified differences created by the dual regime put in place will be further detailed.

3.2.1 Territorial scope

A first important issue concerns the territorial scope of the ePrivacy Directive. The articles 1 (*Scope and aim)* and 2 (*Services concerned*) define the material scope of the ePrivacy Directive, but do not contain a clear determination of the territorial scope of the ePrivacy Directive. Both articles merely contain a reference to the words "*in the Community*" without any further explanation.

As the ePrivacy Directive particularise and complements the Directive, the Article 29 Working Party is of the opinion that the territorial scope of the ePrivacy Directive is determined by a combination of both article 3 of the ePrivacy Directive and article 4 § 1 (a) and (c) of the Directive.[17] So, in the absence of clear geographical applicability rules in the ePrivacy Directive itself, data controllers should look to the applicable rules of the Directive.

However, as the Directive will be replaced by a regulation, which is directly applicable and does not need to be transposed in national law, the Regulation does no longer contain any clauses determining the territorial competence of each Member State and/or applicable national law. Hence, once the Regulation will be put in place, it will become nearly impossible to determine whether a telecom provider subject to the ePrivacy Directive will need to comply with ePrivacy laws on a 'country of origin'-basis, on a 'country of destination'-basis or even on another basis. Moreover, it will also be unclear if and how non-EU based players will fit in. One could assume that as the Regulation as well as the ePrivacy Directive remain silent on this question, every Member State would be free to apply its own rules, potentially leading to an even more fragmented market.

Upon adoption of the Regulation, the territorial scope of the ePrivacy can no longer be determined with certainty.

3.2.2 Different data breach notification regimes

For many years the European Data Protection Supervisor has advocated for the extension of the applicability of the data breach notification rules set out in article 4 EPD to a wider scale of data controllers (notably providers of information society services) and to other sectors than the telecom sector. Indeed, the reasons that justify imposing the data breach notification obligation upon telecom providers also exist regarding other organizations processing massive amounts of personal data of

[17] Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising", WP 171, 10, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf, and Article 29 Working Party, "Opinion 1/2008 on data protection issues related to search engines", WP 148, 9-12, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf

which the disclosure may be particularly harmful to data subjects (e.g. online banks, data brokers and online providers processing health data or other sensitive data).[18]

The European Commission answered the European Data Protection Supervisor's call and included in the Regulation articles on the security of processing (article 30 GDPR), the obligation to notify data breaches to the supervisory authority (article 31 GDPR) and to data subjects (article 32 GDPR). The principles set out in those articles are clearly based upon article 4 EPD and on Regulation 611/2013 in which the principles of article 4 EPD are further developed.

Although the European legislator already indicated during the discussions on the Regulation that the data breach notification regime included in the Regulation should be consistent with the ePrivacy Directive, this clearly is not the case:

- While a data controller under the Regulation has 72 hours to notify a data breach to the supervisory authority, a telecom provider will under the ePrivacy Directive only have 24 hours to notify a data breach to the 'competent national authority' (whereby it is uncertain whether the 'competent national authority' is the national telecom regulator or national data protection authority);
- Where a data controller under the Regulation cannot provide all the information required within 72 hours, he may provide some specific information later "*without undue further delay*", while if a telecom provider under the ePrivacy Directive cannot provide all information required within 24 hours, he is only granted a 'grace period' of 3 days for some specific information;
- While a data controller under the Regulation needs to notify a data breach to the supervisory authority in case of a "*high risk for the rights and freedoms of individuals*", a telecom provider will under the ePrivacy Directive need to notify every breach to the competent national authority; and
- While a data controller under the Regulation needs to notify a data breach to the concerned data subject in case of a "*high risk for the rights and freedoms of individuals*", a telecom provider will under the ePrivacy Directive need to notify a data breach to the subscriber in case of a "*particular risk for the security of the network*".

Although the data breach notification regime included in the Regulation is based upon the regime set out in the ePrivacy Directive (and further specified in Regulation 611/2013), there are a number of differences that are unjustified. Moreover, a dual data breach notification regime will lead to complexity for telecom operators who will have to assess for each data breach event which notification procedure they have to apply (e.g. application of the GDPR principles for cloud services, application of e-Privacy Directive principles for internet access services, and uncertainty in relation to events that affect both types of services). There are no objective reasons to maintain such differences and to create operational complexity. Hence, article 4 of the ePrivacy Directive, and Regulation 611/2013, should be entirely substituted by the corresponding articles of the Regulation.

[18] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), see: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf

Maintaining dissimilar data breach notifications rules would create an overly complex situation for telecom providers, stakeholders and regulating authorities. Hence, only the regime currently included in the Regulation should be retained.

3.2.3 Different treatment of location data

The ePrivacy Directive stipulates a specific regime for the processing of location data (other than traffic data). This regime may have made sense in 2002, when such data were still somewhat specific to the telecom sector, but since then the situation has changed significantly, and OTT players are now collecting vast amounts of location data for the performance of their online VOIP and messaging services.

In accordance with article 9 of the ePrivacy Directive, telecom providers may process location data when they are made anonymous or with the consent of the users/subscriber insofar as necessary to provide a value added service. Moreover, users/subscribers must be informed prior to obtaining their consent of the type of location data that is being processed, of the purposes and duration of the processing and on whether the data will be transmitted to a third party (for providing the value added service). Finally, users/subscribers need to be given the opportunity to withdraw their consent at any time.

In the Regulation, a reference to 'location data' is included. in article 4 (1) GDPR, which defines the concept 'personal data',

In 2011 the Article 29 Working Party adopted an opinion on geolocation services on smart mobile devices, in which it observed that with the rapid technological development and wide uptake of smart mobile devices, a whole new category of location based services is developing. In this regard, the Article 29 Working Party explicitly confirmed that the Directive applies in every case where personal data are being processed as a result of the processing of location data, whereas the ePrivacy Directive only applies to the processing of location data (for example base station data) by telecom providers.[19] The ePrivacy Directive does also not apply to the processing of location data by information society services (such Skype and Whatsapp).

In view of the principle of technology neutrality, there no longer is a justification for treating telecom providers processing location data different from OTT players processing location data. Therefore, we propose to delete the specific provisions of the ePrivacy Directive with regard to location data and to continue applying the general regime of the GDPR, where 'consent' will be the main applicable ground for processing location data. In fact, the specific regime set out in the ePrivacy Directive is a mere concretization of the general principles laid down in the Regulation.

The applicability of the Regulation to all data controllers/market players (telecom providers and OTT players) is not likely to reduce the level of protection offered to customers of telecom providers. This can be illustrated by the above-mentioned Article 29 Working Party opinion on geolocation services. Here, the Working Party stressed that while telecom providers must always obtain the user/subscriber's prior consent, the prior informed consent is also the main applicable ground for

[19] Article 29 Working Party, "Opinion 13/2011 on geolocation services on smart mobile devices", WP 185, 7, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

making data processing legitimate when it comes to the processing of the locations of a smart mobile device in the context of information society services.[20] If the default settings of an operating system would allow for the transmission of location data, a lack of intervention by its users should not be mistaken for freely given consent. Moreover, to the extent that developers of operating systems and other information society services actively process location data themselves, they must equally seek the prior informed consent of their users. Such consent cannot be obtained freely through mandatory acceptance of general terms and conditions, nor through opt-out possibilities. Moreover, it should be stressed that users, in accordance with article 7 § 3 GDPR, will have the possibility to withdraw their consent at any time.

In a converged communications landscape, a different treatment of location data processed by telecom providers on the one hand or other data controllers (including OTT players) on the other hand can no longer be justified. Moreover, the general principles on collection of personal data as currently set out in the Regulation offers a similar level of protection for consumers.

3.2.4 Different treatment of traffic data

A specific regime for the processing of traffic data has already been included in 1997 in the Telecommunications Data Protection Directive (the predecessor of the ePrivacy Directive), at a time wherein telecom providers where collecting data that was deemed to be unique to that sector. Traffic data – which may comprise location data – are thus governed by specific rules, even if somewhat "lighter" than the rules applicable to location data (other than traffic data) which are referred to in the former section 3.2.3.

More particularly, in accordance with article 6 of the ePrivacy Directive, traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Telecom providers may however process traffic data for the provision of value added or marketing services with the prior consent of the user/subscriber. Moreover, the user/subscriber must be informed prior to obtaining their consent of the type of traffic data that is being processed and of the purposes and duration of the processing. Finally, users/subscribers need to be given the opportunity to withdraw their consent at any time.

The Regulation does not contain any reference to traffic data. Hence, to the extent that traffic data would include personal data (as defined in article 4 GDPR), the Regulation will apply. For instance if IP addresses are collected (and the user can be identified) or if the duration, date and time of a VOIP call are made by an individual with a subscription, the Regulation will need to be respected.

Although a specific regime for the telecom sector could have made sense at the moment of its adoption, the situation has changed significantly, and OTT players are now collecting vast amounts of

[20] Article 29 Working Party, "Opinion 13/2011 on geolocation services on smart mobile devices", WP 185, 13, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

traffic data for the performance of their online VOIP and messaging services, but yet they fall outside the scope of the ePrivacy Directive and can consequently not only process traffic data with the data subject's consent but also on the basis of other legal grounds set out in article 6 (*Lawfulness of processing*) of the Regulation (for example if such processing would be necessary for the performance of a contract to which the data subject is party or if necessary for the purposes of the legitimate interests pursued by the data controller). In practice, the prior informed consent will nevertheless also be the main applicable ground for making traffic data processing legitimate. Moreover, it should be stressed that users will, in accordance with article 7 § 3 GDPR, have the possibility to withdraw their consent at any time.

As similar services must be submitted to the same privacy rules, there no longer is a justification for treating telecom providers processing traffic data different from OTT players processing traffic data. Moreover, the applicability of the Regulation to all data controllers/market players (telecom providers and OTT players) is not likely to reduce the level of protection offered to customers of telecom providers, as 'consent' will also under the Regulation be the main applicable ground for processing traffic data. It could even be argued that the specific regime set out in the ePrivacy Directive is a mere concretization of the general principles laid down in the Regulation.

In a converged communications landscape, a different treatment of traffic data processed by telecom providers on the one hand or other data controllers (including OTT players) on the other hand can no longer be justified. Moreover, the Regulation offers a similar level of protection for consumers.

3.2.5 Different competent regulatory bodies

Another inconsistency that exists between the ePrivacy Directive and the Regulation is that the Regulation systematically refers to the term 'supervisory authority', meaning the national data protection authority, whereas the ePrivacy Directive refers to the 'competent national authority', without defining that concept.

Under the Directive 2002/21/EC ("**Framework Directive**"), the 'national regulatory authority', meaning the national telecom regulatory body, has been appointed for monitoring the telecom sector and specifically performing the obligations assigned to it under the Framework Directive (and the other directives of the Telecoms Package). A number of Member States however also attributed the rights and obligations of the 'competent national authority' under the ePrivacy Directive to said national telecom regulatory body. In other Member States the data protection authority is competent for the national implementation of the ePrivacy Directive, while in even other Member States responsibilities may be shared between the data protection authority and the telecom regulator as not all provisions of the ePrivacy Directive relate to privacy and/or telecom.

In particular with regard to the dual data breach notification regime, this uncertainty may lead to interpretation issues. For instances, should a telecom provider notify a data breach related to its telecom activities to its national data protection authority and/or to its national telecom regulator in

accordance with article 4 of the ePrivacy Directive and Regulation 611/2013? And if a telecom provider notices a data breach that is not related to its telecom activities but instead to its HR and payroll administration, should the telecom provider notify its national data protection authority and/or to its national telecom regulator of such data breach in accordance with article 4 of the ePrivacy Directive and Regulation 611/2013 and/or should the telecom provider notify such data breach to the data protection authority in accordance with the procedure set out in the Regulation?

When not all data protection related articles are joined in one instrument and different national regulatory authorities may be competent for judging over the same rules, this is likely to lead to diverging national interpretations of said rules.

3.3 Other arguments in support of the integration of the ePrivacy into the Regulation

In addition to the inconsistencies and unjustified differences between the ePrivacy Directive and the Regulation, as set out above, also the following arguments support the integration of the ePrivacy Directive into the Regulation.

3.3.1 Regulation vs. directive

The choice for a regulation instead of a new or revised ePrivacy Directive will not only exclude the risk on inconsistencies, but will also enhance legal certainty and guarantee a consistent application of data protection rules within the single market. As a regulation is directly applicable in all Member States, data controllers and users will more easily know their rights and obligations, regardless of where the data controller is established.

While the ePrivacy Directive has been transposed in national laws, resulting in 28 different implementations and interpretations of the same directive, issues of interpretation are likely to be reduced when said rules are placed in a regulation, that is not to be further transposed by the Member States.

The choice for a regulation is likely to ensure a more consistent application of privacy rules across the European Union.

3.3.2 One set of data protection rules.

The coexistence of two different sets of rules creates legal uncertainty and confusion for consumers, which does not play in favour of a coherent consumer policy online.

When all European rules related to data protection would be integrated into one legislative instrument, this would be beneficial for all stakeholders and increase legal certainty, as businesses and consumers will only have to look to one legal instrument in order to understand their rights and obligations in respect of the processing of personal data. Moreover, by creating one set of rules all stakeholders will clearly know what is expected from them. It goes without saying that the Regulation is the most appropriate instrument in which all rules are to be included.

In order to increase legal certainty and trust, all data protection related rules should be combined into one legal instrument, notably the Regulation.

3.3.3 Level playing field

While specific data protection rules for telecom operators may have been justified in the past, today, it makes little sense to single out one particular sector when there are such a broad range of online service companies collecting and processing large volumes of personal data. As has been demonstrated by a recent study published by CERRE[21], today, there is little economic rationale for treating OTT players offering communication services (such as Skype and Whatsapp) differently and imposing different privacy and data security requirements to telecom providers and OTT players.

Moreover, while it would make sense to impose additional obligations for the processing of sensitive data (such as medical data), it can even be considered discriminatory to apply additional rules to one specific sector irrespective of the data processed, without there being a justification for such different treatment.

By creating one set of uniform data protection rules that apply to telecom providers, OTT players as well as all other data controllers, the level playing field between different services providers will be restored.

It cannot be denied that the ongoing review of the EU Data Protection legal framework is a unique opportunity to achieve a true level playing field in order to ensure that technological neutral principles apply to all stakeholders. This is also a key element in the debate towards more internal market and more competitiveness. In the current converged world, the distortions between sectors are not justifiable and it is necessary to avoid competition distortions among the players of the digital ecosystem. Including data protection related EPD articles within the GDPR would make the ePrivacy Directive unnecessary.

By creating one set of data protection rules that applies to all data controllers and data processors, notwithstanding the sector in which they are operating, the level playing field between telecom providers and OTT player can be restored.

[21] CERRE, Study on Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets, see: http://www.cerre.eu/sites/default/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final_0.pdf

3.3.4 Consumer trust

Communication services provided by telecom providers and by OTT players are close substitutes. Not only services provided by telecom providers, but also OTT services that fall outside the scope of the ePrivacy Directive store vast amounts of personal information, identifiers, traffic and location data, without being regulated in the same way as telecom providers.

As stated before, the ePrivacy Directive leads to increase legal uncertainty and an asymmetry of data protection and privacy laws, and leaves consumers to assess which rules and rights apply to functionally-equivalent services. As consumers often do not know to which legal regime the provided communication is subject, they also do not know that different levels of protection may be available.

To build trust and increase legal certainty for consumers, it is key to simplify the applicable legal framework, which can be done by applying one set of data protection rules to all market players.

Consumers face inconsistent privacy experiences for functionally-equivalent services, often without being aware. To resolve the legal uncertainty, similar rules should be applied to similar services.

3.3.5 Redundant ePrivacy Directive

A number of clauses included in the ePrivacy Directive, notably on (i) location data, (ii) traffic data and (ii) data breach notifications, could be considered as necessary and revolutionary at their time of adoption. However, as set out above, it cannot be denied that a number of those rules are no longer required in regard of the current text of the Regulation.

- With regard to the data breach notifications, the Regulation contains a data breach notification regime that has been inspired upon the one set out in the ePrivacy Directive. Hence, there is no need to a separate regime that only is applicable to telecom providers.
- With regard to location data and traffic data, it has been stated above that a mere application of the principles laid down in the Regulation will lead to the same level of protection. More in particular, the specific regimes set out in the ePrivacy Directive are not more than a concretization of the general principles set out in the Regulation.

In regard of the foregoing, it must be concluded that a mere deletion of sector-specific rules on data breach notifications, traffic data and local data is not likely to reduce the level of protection for the concerned data subjects.

The data protection related articles of the ePrivacy Directive (notably on location, traffic data and data breach notifications) have become redundant and are no longer required in regard of the current text of the Regulation.

3.3.6 Material scope of the ePrivacy Directive

3.3.6.1 Not only related to the telecom sector

Although the aim of the ePrivacy Directive has initially been to harmonize the processing of personal data in the telecom sector, it contains several articles which have a scope that is not merely limited to telecom providers.

- The principle of confidentiality of communications (although limited to electronic communications services and networks) applies to any person that would intercept users' communications, and not only to telecom providers (article 5 § 1 EPD);
- The so-called cookie provision applies to all website operators placing cookies (article 5 § 3 EPD); and
- The anti-spam provision applies to anyone considering to send unsolicited communications (article 13 EPD).

As the scope of those articles is not limited to the telecom sector or to telecom providers, it would have been more logical to include them in legislation (such as the Regulation) that has a general field of application.

The ePrivacy Directive contains a number of articles, notably on the confidentiality of communications, cookies and unsolicited communications, with a scope that cannot be limited to the telecom sector. Hence, it would make sense to include said articles in the Regulation.

3.3.6.2 Not only related to privacy and data protection

Although the ePrivacy Directive aims to particularize and complement the Directive for the processing of personal data and the protection of privacy in the telecom sector, it must be observed that the ePrivacy Directive contains a significant number of articles that are not (directly) related to the processing of personal data or that cannot be introduced in the Regulation in a generalized way.

Said articles are notably related to itemised billing (art. 7 EPD), presentation and restriction of calling and connected line identification (art. 8 EPD), exceptions (art. 10 EPD), automatic call forwarding (art. 11 EPD), directories of subscribers (art. 12 EPD), technical features and standardisation (art. 14 EPD) and the implementation and enforcement of the ePrivacy Directive (art. 15a EPD).

It can be questioned whether these provisions are still relevant in the current status of the telecommunication sector. .

If not, the provisions should be taken away in their entirety.

If yes, these clauses are in all circumstances related to the traditional telecom services, and therefore it would be more logical to integrate them into the Telecoms Package.

Non-privacy related - to the extent still relevant - articles of the ePrivacy Directive should be moved to the relevant legal instrument of the Telecoms Package.

4 PROPOSED AMENDMENTS

4.1 Approach

In this section we propose an **amendment to the Regulation**[22] in order to integrate the relevant definitions of the ePrivacy Directive into the Regulation (notably 'communication' and 'electronic mail') and move the clauses on confidentiality of communications (art. 5 EPD) and unsolicited communications (art. 13 EPD) to the Regulation (see **Section 4.2**).

After implementing this amendment, several non-privacy related provisions remain, more in particular the clauses on itemised billing (art. 7 EPD), presentation and restriction of calling and connected line identification (art. 8 EPD), exceptions (art. 10 EPD), automatic call forward forwarding (art. 11 EPD), directories of subscribers (art. 12 EPD), technical features and standardisation (art. 14 EPD) and the implementation and enforcement of the ePrivacy Directive (art. 15a EPD) (see **Section 4.3**). We consider that it would be far more appropriate to integrate these provisions **into the Telecoms Package** and we are prepared to prepare an additional amendment in that sense.

As result of those two actions, **Regulation 611/2013 and the ePrivacy Directive are to be repealed**, including the following EPD clauses (see **Section 4.4**):

- the clauses that introduced specific obligations for telecom providers and that are no longer justifiable in the current telecom landscape, notably the clauses on traffic data (art. 6 EPD), location data (art. 9 EPD) and the specific data breach notification regime (art. 4 EPD), including the related Regulation 611/2013 on the notification of data breaches, and the definitions that are consequently no longer required (notably 'traffic data', 'location data', 'consent', 'value added service' and 'personal data breach').
- The clauses that do no longer serve a purpose due to the proposed amendments, notably the clauses on the scope and aim of the ePrivacy Directive (art. 1 EPD), the services concerned (art. 3 EPD), the Committee procedure (art. 14a EPD), the application of certain provisions of the Directive (art. 15 EPD), transitional arrangements (art. 16 EPD), transposition (art. 17 EPD), review (art. 18 EPD), repeal (art. 19 EPD), entry into force (art. 20 EPD) and art. 21 (addressees).

Section 4.2 contains an overview of the EPD articles that are to be integrated in the Regulation, including (i) the current wording of the concerned articles, (ii) the proposed amendments to those articles (if any) and (iii) a justification for the proposed amendments. All modifications have been highlighted in bold, whereby deletions are marked as struck-through bold text (e.g. ~~**deletion**~~) and additions are marked as italic bold text (e.g. ***addition***).

[22] The unofficially consolidated version of the Regulation of 19 December 2014 has been taken as a starting point.

Section 4.3 merely contains an overview of the EPD articles which are non-privacy related and which, in our view, could perfectly be integrated in the relevant legal instrument(s) of the Telecoms Package, either now or in the context of the future discussions on the reform of the Telecoms Package.

Section 4.4 merely contains an overview of the EPD articles that are to be deleted, whereby we justify for each article why it should be deleted.

4.2 Amendments to the Regulation

Current wording of the ePrivacy Directive	Proposed wording to integrate into the GDPR
▪ **Recitals EPD**	▪ **Recitals GDPR**
(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.	(~~**3**~~ ***59a***) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.
(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.	(~~**21**~~ ***59b***) Measures should be taken to prevent unauthorised access to ***digital*** communications in order to protect the confidentiality of ***digita*****l** communications, including both the contents and any data related to such communications~~**, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.**~~
(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. 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.	(~~**23**~~ ***59c***) Confidentiality of ***digital*** communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. ~~**Directive 95/46/EC applies to such processing.**~~ Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded **digital** 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.
(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal	(~~**24**~~ ***59d***) Terminal equipment used by individuals to make digital communications and any information stored on such equipment are part of the private sphere of the ~~**users**~~ **individuals** requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the

without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.	~~user's~~ ***individual's*** terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the ~~user~~ ***individual*** and may seriously intrude upon the privacy of these ~~users~~ ***individuals***. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the ~~users~~ concerned ***individuals***.
(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.	(~~25~~ ***59e***) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of ~~users~~ ***individuals*** engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that ~~users~~ ***individuals*** are provided with clear and precise information in accordance with ~~Directive 95/46/EC~~ ***this Regulation*** about the purposes of cookies or similar devices so as to ensure that ~~users~~ ***individuals*** are made aware of information being placed on the terminal equipment they are using. ~~Users~~ ***Individuals*** should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where ~~users~~ ***individuals*** other than the original ~~user~~ ***individual*** have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the ~~user's~~ ***individual's*** terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.
(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a	(~~40~~ ***57a***) Safeguards should be provided for ~~subscribers~~ ***individuals*** against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may

burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an

impose a burden and/or cost on the ~~**recipient**~~ ***addressee***. Moreover, in some cases their volume may also cause difficulties for ~~**electronic communications**~~ networks and terminal equipment ***on which these communications are being sent***. For such forms of unsolicited communications for direct marketing, it is justified to require that prior ~~**explicit**~~ ***unambiguous*** consent of the ~~**recipients**~~ ***individuals*** is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(~~**41**~~ ***57b***) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with ~~**Directive 95/46/EC**~~ ***this Regulation***. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(~~**42**~~ ***57c***) Other forms of direct marketing that are more costly for the sender and impose no financial costs on ~~**subscribers and users**~~ ***the addressees*** such as person-to-person voice telephony calls, may justify the maintenance of a system giving ~~**subscribers or users**~~ ***addressees*** the possibility to indicate that they do not want to receive such calls. ~~**Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.**~~

(~~**43**~~ ***57d***) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(~~**44**~~ ***57e***) Certain electronic mail systems allow ~~**subscribers**~~ ***addressees*** to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails

additional tool to the general obligations established in this Directive. (45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) are fully applicable.	or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this ~~**Directive**~~ ***Regulation***. (~~**45**~~ ***57f***) This ~~**Directive**~~ ***Regulation*** is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) are fully applicable. ~~**Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.**~~

Justification

The recitals listed above are those recitals of the ePrivacy Directive that are relevant for the interpretation of the clauses on confidentiality of communications and unsolicited communications that have been proposed to be integrated into the Regulation. A further explanation on the changes made can be found below under the corresponding articles and paragraphs.

As the order of the recitals follows the order of the articles, the numbering of the recitals transposed from the ePrivacy Directive has been selected in this respect.

▪ /	▪ **Recital 25b GDPR**
	(25b) To the extent that traffic data relate to an identified or identifiable person, such data is to be qualified as personal data. An example includes the duration, date and time of a telephone or VOIP call made by an individual with a subscription.

Justification

Although not all traffic data can be qualified as personal data, we deem it recommended to specify in the recitals of the Regulation that traffic data could in certain circumstances indeed qualify as personal data. Consequently the Regulation will apply to the processing of such data.

▪ Recital 135 Regulation	▪ /
(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.	~~**(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.**~~
Justification	
As the relevant articles of the ePrivacy Directive are incorporated into the Regulation, there is no longer a need to keep this recital 135.	
▪ **Article 2 EPD (Definitions)**	▪ **Article 4.12(c) GDPR (Definitions)**
(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;	(~~**d**~~ ***12.c***) '***digital*** communication' means any information exchanged ~~***or conveyed***~~ ***by electronic means*** between a finite number of parties ~~**by means of a publicly available electronic communications service**~~. This does not include any information conveyed as part of a broadcasting service to the public ~~**over an electronic communications network**~~ except to the extent that the information can be related to ~~**the identifiable subscriber or user receiving the information**~~ ***one or more parties to the digital communication***;
Justification	
The concept 'communication' is relevant for the interpretation of the articles on the confidentiality of communications (art. 5 EPD) and on unsolicited communications (art. 13 EPD). As those concepts are to be integrated into the Regulation, the definition of 'communication' also needs to be integrated into the Regulation. To avoid confusion and as the word 'communication' as such is already used in a generic way in the Regulation (e.g articles 11 and 12) the concept has been renamed to 'digital communication' . Moreover, the definition has been redrafted in such a way that it is not limited to communication over a publicly available electronic communications service, but also covers communication by other electronic means (such as over Whatsapp and Skype).	
▪ **Article 2 EPD (Definitions)**	▪ **Article 4.12(d) GDPR (Definitions)**
(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected	(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the ~~**recipient's**~~ ***addressee's*** terminal equipment

by the recipient;	until it is collected by the ~~**recipient**~~ ***addressee***;

Justification

This definition is required for the interpretation of article 13 (Unsolicited communication) and should therefore be integrated into the Regulation.

In regard of the existence of a definition of 'recipient' in article 4.7 of the Regulation that is not suited to interpret 'electronic mail' (notably "a natural or legal person, public authority, agency or any other body other than the data subject, the data controller or the data processor to which the personal data are disclosed; however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients"), the term 'recipient' has been renamed to 'addressee'.

▪ **Article 5 § 1 EPD (Confidentiality of communications)**	▪ **Article 20a § 1 GDPR (Confidentiality of digital communications)**
1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.	***Section 4a - Confidentiality of digital communications*** ~~**1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.**~~ ***A natural or legal person shall respect the confidentiality of the content of digital communications and shall refrain from listening, tapping, storing, intercepting or surveilling of the content of digital communications unless and insofar as:*** ***(a) the parties to the digital communication have unambiguously consented;*** ***(b) those acts are necessary to protect the integrity and security of the communication or information society service offered by the concerned natural or legal person;*** ***(c) those acts are necessary for the conveyance of a digital communication and do not prejudice the principle of***

	confidentiality; ***(d) those acts are necessary to comply with a legal obligation or judicial order.***

Justification

As a preliminary remark we propose to include the provisions on the confidentiality of digital communications in the Regulation under a new Section 4a (Confidentiality of digital communications).

Today, only the confidentiality of communications over public communications networks and electronic communications services is protected by the ePrivacy Directive. In a digital era in which also other services such as Skype and Whatsapp - that are not subject to the ePrivacy Directive - are increasingly used by consumers to communicate, it is of key importance that such communications also remain confidential. For that reason article 5 § 1 EPD has been modernized and redrafted in a generalized way.

In accordance with article 5 § 1 EPD, the member states are competent to further detail the principles laid down in that paragraph. As it is not recommended to transpose such a high-level approach to the Regulation, the proposed text is a further developed clause that has been based upon the Dutch implementation of the ePrivacy Directive (notably article 11.2 of the Dutch Telecommunications Act).

▪ **Article 5 § 2 EPD (Confidentiality of communications)**	▪ **Article 20a § 2 GDPR (Confidentiality of digital communications)**
2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.	2. Paragraph 1 shall not affect any legally authorised recording of ***the content of digita*****l** communications ~~**and the related traffic data**~~ when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Justification

This paragraph 2 has only been slightly modified in order to reflect the modified concept 'digital communication' and the deletion of the concept 'traffic data'.

▪ **Article 5 § 3 EPD (Confidentiality of communications)**	▪ **Article 20a § 3 GDPR (Confidentiality of digital communications)**
3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a	3. ~~**Member States shall ensure that the**~~ **The** storing of information, or the gaining of access to information already stored, in the terminal equipment of ~~**a subscriber or user**~~ **an individual** is only allowed on condition that the ~~**subscriber or user**~~ concerned **individual** has given his or her **unambiguous** consent, having been provided with clear and comprehensive information, in accordance with ~~**Directive 95/46/EC**~~ ***article 14***, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole

communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.	purpose of carrying out the transmission of a ***digital*** communication ~~**over an electronic communications network**~~, or as strictly necessary in order for the provider of an information society service explicitly requested by the ~~**subscriber or user**~~ ***individual*** to provide the service.

Justification

As this paragraph - also known as the cookie provision - already applies to all website operators placing cookies, and consequently is not limited to telecom providers, this paragraph does not belong in the ePrivacy Directive. Moreover, it can be easily integrated into the Regulation. In order to remain consistent, the terms 'subscriber' and 'user' have been replaced by the more neutral term 'individual'. This however does not have an impact on the scope, which will remain unchanged.

▪ **Article 13 § 1 EPD (Unsolicited communications)**	▪ **Article 19a § 1 GDPR (Unsolicited communications)**
1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.	***Section 4 - Right to object, unsolicited communications and profiling*** 1. ***Notwithstanding article 19,*** ~~**The**~~ ***the*** use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of ~~**subscribers or users**~~ ***addressees*** who have given their prior consent.

Justification

As a preliminary remark, we propose to modify the title of Section 4 by including a reference to unsolicited communications.

Paragraphs 1 of article 13 EPD does not only impose obligations on telecom providers, but also on all other natural and legal persons wishing to send unsolicited communications via the listed means. In regard of its broad field of application, this clause should never had been placed in the ePrivacy Directive. Instead, it can be easily integrated into the Regulation without changing its material scope. In order to remain consistent, the terms 'subscriber' and 'user' have been replaced by the more neutral term 'addressee'.

In order to clarify the relationship with the right to object as set out in article 19 of the Regulation, a reference to that article has been included.

▪ **Article 13 § 2 EPD (Unsolicited communications)**	▪ **Article 19a § 2 GDPR (Unsolicited communications)**
2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for	2. Notwithstanding paragraph 1, 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 Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.	electronic mail, in the context of the sale of a product or a service, in accordance with ~~**Directive 95/46/EC**~~ ***this Regulation***, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

Justification

Apart from updating the reference to the Directive, no changes are required to integrate paragraph 2 of article 13 EPD into the Regulation.

▪ **Article 13 § 3 EPD (Unsolicited communications)**	▪ **Article 19a § 3 GDPR (Unsolicited communications)**
3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.	3. ~~**Member States shall take appropriate measures to ensure that unsolicited**~~ **Unsolicited** communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed ~~**either**~~ without the ***unambiguous*** consent of the ~~**subscribers or users concerned**~~ ***addressee*** ~~**or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user**~~.

Justification

This third paragraph allows Member States to choose between either requiring the prior consent of the subscribers/users on the one hand, or giving the opportunity to subscribers/users to express their wish not to receive such communication. To maintain a consistent application of these principles throughout the European Union, we deem it recommended to directly make a choice in the Regulation, instead of leaving this up to the Member States. Hence, we have redrafted this paragraph in such a way that the addressee's unambiguous consent is required, leading to a higher level of protection for the addressee as well as to a higher level of harmonization.

▪ **Article 13 § 4 EPD (Unsolicited communications)**	▪ **Article 19a § 4 GDPR (Unsolicited communications)**
4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such	4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the ~~**recipient**~~ ***addressee*** may send a request

communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.	that such communications cease or which encourage ~~**recipients**~~ ***addressees*** to visit websites that contravene that Article ~~**shall be**~~ ***are*** prohibited.
Justification	
This paragraph only required minor modifications in order to integrate it into the Regulation.	
▪ **Article 13 § 5 EPD (Unsolicited communications)**	▪ **Article 19a § 5 GDPR (Unsolicited communications)**
5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.	5. Paragraphs 1 and 3 shall apply to ~~**subscribers**~~ ***addressees*** who are natural persons. ~~**Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.**~~
Justification	
As the main aim of the Regulation is to protect individuals with regard to the processing of personal data, the reference to the obligation for Member States to ensure that legal persons are also protected with regard to unsolicited communications has not been retained.	
▪ **Article 13 § 6 EPD (Unsolicited communications)**	▪ */*
6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.	~~**6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article**~~
Justification	
A reference to the article on unsolicited communications has been integrated into article 79a of the Regulation on administrative fines (see infra),	

allowing supervisory authorities to impose administrative fines. Moreover, article 74 of the Regulation gives each natural and legal person a right to a judicial remedy against a (legally binding of a) supervisory authority, while article 75 of the Regulation gives each data subject the right to a judicial remedy against a controller or processor. Hence, the Regulation already offers similar guarantees to the involved stakeholders.

▪ */*	▪ **Article 79a § 3 GDPR (Administrative fines)**
	3. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year, on a controller or processor who, intentionally or negligently: (...) ***(p) does not comply with Article 19a.***

Justification

As explained with regard to article 13 § 6 EPD a reference to the article on unsolicited communications has been integrated in order to allow supervisory authorities to impose administrative fines.

▪ **Article 19 EPD (Repeal)**	**Article 88a GDPR (Repeal of Directive 2002/58/EC)**
Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1). References made to the repealed Directive shall be construed as being made to this Directive.	***1. ~~Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).~~ Directive 2002/58/EC and Regulation 611/2013 are repealed.*** ***2.*** References made to ***articles 4, 5 and 13 of*** the repealed Directive ***2002/58/EC*** shall be construed as being made to ***~~this Directive~~ respectively articles 30, 20a and 19a of this Regulation***. ***3. References made to the repealed Regulation 611/2013 shall be construed as being made to this Regulation.***

Justification

This article should be replaced by an article stating that the ePrivacy Directive will be repealed and that references made to the privacy-related articles of the ePrivacy Directive that have been integrated into the Regulation shall be construed as being made to the corresponding articles of the Regulation.

Article 89 GDPR (Relationship to and amendment of Directive 2002/58/EC)	▪ */*
1. This Regulation shall not impose additional obligations on natural	***~~1. This Regulation shall not impose additional obligations on~~***

or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC. 2 Article 1(2) of Directive 2002/58/EC shall be deleted.	**~~natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.~~** **~~2 Article 1(2) of Directive 2002/58/EC shall be deleted.~~**

Justification

As all data protection related rules - including those that were included in the ePrivacy Directive - are to be combined in the Regulation and as the ePrivacy Directive is to be repealed, an article governing the relationship with said repealed directive is no longer needed.

4.3 Non-privacy related articles

The following provisions of the ePrivacy Directive have no or little relation with privacy or data protection, but rather with the general telecom framework and/or specific telecom consumer protection rules: recitals 19, 33, 34, 36-39, itemised billing (art. 7 EPD), presentation and restriction of calling and connected line identification (art. 8 EPD), exceptions (art. 10 EPD), automatic call forward forwarding (art. 11 EPD), directories of subscribers (art. 12 EPD), technical features and standardisation (art. 14 EPD) and implementation and enforcement (art. 15a).

Some of these provisions may no longer be of relevance today, in which case they should be repealed. Additionally, in our opinion it is highly recommended to integrate the remainder of these provisions into the other directives of the Telecoms Package rather than to maintain the ePrivacy Directive with this limited number of provisions.

This could either be done in the context of the general review of the Telecoms Package, or rightaway. In the latter case, DLA Piper can of course prepare an amendment in that sense.

4.4 Deletion of remaining clauses of the ePrivacy Directive

In this section an overview of the ePrivacy Directive articles that are not to be integrated into the Regulation or Telecoms Package is given, whereby for each article a justification is given on the reason for deletion.

Deletion of remaining clauses of the ePrivacy Directive	
▪ **Article 1 EPD (Scope and aim)**	▪ **Justification for deletion**
1. This Directive provides for the harmonisation of the national provisions required to ensure 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 communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.	Paragraph 1 merely sets out the aim of the ePrivacy Directive, with a clear focus on the electronic communication sector. As the idea is to adopt one set of data protection rules that applies to all data controllers, regardless of the sector their operating in, and move the other relevant provisions to the Telecoms Package, this paragraph is no longer needed. Article 1 of the Regulation and the Telecoms Package already describe their respective subject matter and objectives.
2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.	This paragraph does no longer serve a purpose as all data protection related provision are combined into the Regulation. Moreover, in accordance with article 89 § 2 of the Regulation, this paragraph will be deleted in any event (*"Article 1(2) of Directive 2002/58/EC shall be deleted."*).
3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.	A similar article has been provided for in article 2.2 (*Material scope*) of the Regulation.
▪ **Article 2 EPD (Definitions)**	▪ **Justification for deletion**
Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework	As the amendments proposed to the Regulation aim to create a true level playing field with uniform rules applicable without restrictions throughout all sectors, the Regulation should not contain any references to Directive 2002/21/EC (Framework Directive).

Directive) (8) shall apply. The following definitions shall also apply:	Moreover, as the Regulation is meant to be technology neutral and in order to avoid creating another set of sector-specific rules under the Regulation, the concepts 'electronic communications network', 'electronic communications service', 'public communications network', 'subscriber', 'user', 'provision of an electronic communications network' should not be used.
(a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;	This definition of 'user' is relevant for the interpretation of the articles 7 EPD (*Itemised billing*), 8 EPD (*Presentation and restriction of calling and connected line identification*) and 14 EPD (*Technical features and standardization*), that we propose to integrate into the Framework Directive, but not for the interpretation of the articles that are to be integrated into the Regulation. The Framework Directive however already contains a definition of 'user', notably "*a legal entity or natural person using or requesting a publicly available electronic communications service*". Although this definition is broader in that it also includes legal entities, this does not appear to have any impact as regards the concrete provisions of the ePrivacy Directive that would be included in the Telecoms Package. By way of example, it can be emphasized that the Belgian implementation of the Telecoms Package and the ePrivacy Directive (in particular the Act of 13 June 2005 on electronic communications) does not make a distinction between 'user' within the meaning of the Framework Directive and 'user' within the meaning of the ePrivacy Directive. Notably, article 130 of the Belgian Act on electronic communications on the presentation and restriction of calling and connected line identification refers to the concept of 'end-user' as defined in article 2(n) of the Framework Directive. In regard of the foregoing, we propose to delete the definition of 'user' included in the ePrivacy Directive. Alternatively, it could be considered to integrate this specific definition and apply it only to the clauses that are to be integrated.
(b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;	As a separate treatment of traffic data under the Regulation is not recommended, this definition is not to be integrated into the Regulation, not even in a generalized way without any reference to the telecom sector. However, to avoid any interpretation issues, a recital is included in the Regulation stating that traffic data could in specific circumstances indeed be qualified as personal data, and

	hence be subject to the Regulation.
(c) 'location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;	Since the European legislator did not consider it necessary to define the concept 'location data' in the Regulation, this definition should not be retained
(e) […]	
(f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;	This definition merely contains a cross-reference to the definition of 'consent' in the Directive.
(g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;	The definition of 'value added service' is only relevant for the interpretation of article 6 EPD (*Traffic data*) and article 9 (*Location data other than traffic data*). As the Regulation currently does not foresee a different treatment for location data and traffic data, and the introduction of such regime for all data controllers is deemed to be undesirable and burdensome, this concept does no longer serve a purpose and can be deleted.
(i) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.	The Regulation already contains a definition of 'personal data breach'. More in particular, the definition of 'personal data breach' set out in article 4 § 9 of the Regulation is a generalized '*copy*' of the definition set out in the ePrivacy Directive, and is as follows: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal, transmitted, stored or otherwise processed*".
▪ **Article 3 EPD (Services concerned)**	▪ **Justification for deletion**
This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.	This article further specifies the aim and scope of the ePrivacy Directive, as set out in article 1. As the idea is to adopt one set of data protection rules that applies to all data controllers, regardless of the sector their operating in, this article no longer serves a purpose. The Regulation as well as the Telecoms Package contain comparable clauses that set out their respective objectives.
▪ **Article 4 EPD (Security of processing)**	▪ **Justification for deletion**
1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures	As the purpose of this proposal is to evolve to one general data protection regime, for telecom providers and all other data

to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.	controllers, only one data breach notification regime should be retained. The data breach notification regime set out in the Regulation has been inspired upon the one currently set out in the ePrivacy Directive, and therefore we propose to retain the current wording of the Regulation. Furthermore, it should be borne in mind that the regime in the ePrivacy Directive has been further developed in Regulation 611/2013. Hence, Regulation 611/2013 would need to be repealed.
1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least: - ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, - protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and, - ensure the implementation of a security policy with respect to the processing of personal data, Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.	Although article 1.a of the ePrivacy Directive is not copied entirely into the articles 1.a to 2.b of the Regulation, the Regulation provides sufficient safeguards in this regard. The supervisory authority has been attributed a general investigative power to carry out investigations in the form of data protection audits.
2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers 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.	As it has already been expressed by the European legislator that the Regulation should be consistent with the ePrivacy Directive in this regard, we propose to delete paragraph 2 of the ePrivacy Directive. Article 3 § 4 of Regulation 611/2013 is in line with the Regulation by stating that the notification to the subscriber or individual should be made without undue delay. It should be stressed that the Regulation requires the communication of only slightly less information than Regulation 611/2013 (see Annex II to that regulation).
3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national	As it has already been pronounced by the European legislator that the Regulation should be consistent with the ePrivacy Directive in this

authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.	regard, we propose to delete paragraph 3 of the ePrivacy Directive. Another point of legal uncertainty is caused by the reference to 'competent national authority' in the ePrivacy Directive, and the reference to 'supervisory authority' in the Regulation. By only retaining the general regime in the Regulation, it will be clear that the notification will need to be done to the supervisory authority (meaning the data protection authority). Moreover, it should be stressed that the general regime would give telecom providers as much time to notify as all other data controllers (notably 72 hours instead of the 24 hours that are foreseen in Regulation 611/2013). The obligation to inform subcontracted providers (art. 5 Regulation 611/2013) corresponds to article 31 § 2 of the Regulation.
4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the	Although the Regulation does not contain a similar article, we do not consider this to be an issue. In the Regulation, general audit powers are foreseen for the supervisory authorities. Moreover, the European Data Protection Board may issues guidelines, recommendations and best practices in order to encourage consistent application of the Regulation.

competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.	
5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).	This article becomes redundant when all relevant rules would be combined in a regulation. Noteworthy is that the current Regulation 611/2013 is the result of an initiative based upon article 4 § 5 of the ePrivacy Directive, of which the main aim is to ensure consistency. Although the Regulation delegates the power to amend/implement specific parts of the Regulation to the Commission, the European legislator did not deem it required to provide such a possibility for the data breach notification regime. Further arguments can be found in Section 3.2.2 (*Different data breach notification regimes*).
▪ **Article 6 EPD (Traffic data)**	▪ **Justification for deletion**
1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. 3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data	Telecom providers need the subscriber's/user's prior consent for processing traffic data, while other actors (such as OTT players) that are only subject to the Regulation, will also be able to process traffic data on the basis of other legal grounds and for other purposes (for example if the processing is necessary for the performance of a contract to which the data subject is party or if necessary for the purposes of the legitimate interests pursued by the controllers). For the reasons set out in Section 3.2.4 (*Different treatment of traffic data*), this article should be deleted.

referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

▪ **Article 9 EPD (Location data other than traffic data)**	▪ **Justification for deletion**
1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.	Telecom providers need to make location data anonymous or obtain the subscriber's/user's prior consent for processing location data for value-added services, while other actors (such as over-the-top players) that are only subject to the Regulation, will be able to process anonymous as well as non-anonymous location data on the basis of other legal grounds and for other purposes (for example if the processing is necessary for the performance of a contract to which the data subject is party or if necessary for the purposes of the legitimate interests pursued by the controllers). For the reasons set out in Section 3.2.3 (*Different treatment of location data*), this article should be deleted.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.	The possibility to withdraw consent has been explicitly included in article 7 of the Regulation. Hence, this paragraph can be deleted.
3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service	This paragraph can also be deleted as the Regulation contains safeguards on the use of personal data and restrictions on the purposes for which personal data can be processed.
▪ Article 14a EPD (Committee procedure)	**▪ Justification for deletion**
1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).	The Framework Directive contains a nearly identical article (notably art. 22). Although the Regulation also foresees a Committee procedure in article 87 of the Regulation, the committee is not further specified. It however is unlikely that the Communications Committee[23] will obtain any authority over general data protection law. To ensure consistency, it is recommended to accept the competence of the committee appointed under the Regulation.
2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.	Only article 4 § 6 of the ePrivacy Directive concerning the data breach notification regime - which is to be deleted - referred to this paragraph. Hence, it does no longer serve a purpose.
3. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.	No clause of the ePrivacy Directive refers to this paragraph. Hence it has no purpose.
▪ Article 15 EPD (Application of certain provisions of Directive 95/45/EC)	**▪ Justification for deletion**
1. Member States may adopt legislative measures to restrict the	An article similar to article 13 § 1 of the Directive and to article 15 of

[23] See http://ec.europa.eu/digital-agenda/en/communications-committee

scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.	the ePrivacy Directive has been included in article 21 (*Restrictions*) of the Regulation, permitting the Member States to limit the scope of the rights and obligations provided for. Only the reference to article 8 EPD (*Presentation and restriction of calling and connected line identification*) is to be retained.
1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1(1) of that Directive.	This paragraph has been included by Directive 2006/24/EC, to which is referred. That directive however has been declared invalid by the Court of Justice of the European Union.[24] Hence, it should not be copied into the Regulation.
1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.	As the Regulation currently does not contain a similar obligation for other data controllers, we do not deem it appropriate to retain this obligation only for providers of electronic communications services/networks.
2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.	Upon an integration of the ePrivacy Directive into the Regulation, its entire Chapter VIII (*Remedies, Liability and Sanctions*) will become applicable. This would also resolve the uncertainty as whether to only the articles corresponding to Chapter III of the Directive, notably article 74 (*Right to a judicial remedy against a supervisory authority*), article 75 (*Right to a judicial remedy against a controller or processor)* and article 77 (*Right to compensation and liability*) would apply upon the approval and entry into force of the Regulation.

[24] CJEU 8 April 2014, C-293/12 and C-594/12, www.curia.eu.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.	This paragraph will no longer offer an added value once all data protection articles have been incorporated in the Regulation. For the sake of completeness, it should be mentioned that the Article 29 Working Party will be replaced by the European Data Protection Board.
▪ Article 16 EPD (Transitional arrangements)	**▪ Justification for deletion**
1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force. 2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.	This article governs the transition to the ePrivacy Directive, and will no longer serve a purpose.
▪ Article 17 EPD (Transposition)	**▪ Justification for deletion**
1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States. 2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.	No transposition will be required for the clauses integrated into the Regulation. Member states will however be required to adapt their national legislation on electronic communication in order to avoid any inconsistencies between their national legislation and the Regulation. It should nevertheless be stressed that Member States will in any event also need to repeal their general data protection laws. From a theoretical point of view, the directive amending the Telecoms Package will need to contain a similar article, allowing members to transpose the amendments. However, from a practical point of view, no changes will be required as the wording of the provisions moved to the Telecom Package nearly did not change.

▪ Article 18 EPD (Review)	▪ Justification for deletion
The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.	Similar provisions are already foreseen in article 90 (*Evaluation*) of the Regulation and article 25 (*Review procedures*) of the Framework Directive.
▪ Article 20 EPD (Entry into force)	**▪ Justification for deletion**
This Directive shall enter into force on the day of its publication in the *Official Journal of the European Communities*.	A similar provision is foreseen in article 91 (*Entry into force and application*) of the Regulation. In the directive amending the Telecoms Package however a similar article will need to be included.
▪ Article 21 EPD (Addressees)	**▪ Justification for deletion**
This Directive is addressed to the Member States.	The Regulation is automatically directed to and directly applicable to the Member States, and the Telecom Package already contains an identical article (e.g. article 30 (*Addressees*) of the Framework Directive).

* * *

B CONSOLIDATED AMENDMENTS

This Section of the proposal contains a consolidated version of the Regulation.

Given the length of the Regulation, only the chapters that contain one or more amended articles have been included.

All modified articles have been presented as bold italic text.

REVISED REGULATION

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Whereas:

[…]

(25b) To the extent that traffic data relate to an identified or identifiable person, such data is to be qualified as personal data. An example includes the duration, date and time of a telephone or VOIP call made by an individual with a subscription.

[…]

(57a) Safeguards should be provided for individuals against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the addressee. Moreover, in some cases their volume may also cause difficulties for networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior unambiguous consent of the addressees is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(57b) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with this Regulation. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(57c) Other forms of direct marketing that are more costly for the sender and impose no financial costs on the addressees such as person-to-person voice telephony calls, may justify the maintenance of a system giving addressees the possibility to indicate that they do not want to receive such calls.

(57d) ***To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.***

(57e) ***Certain electronic mail systems allow addressees to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Regulation.***

(57f) ***This Regulation is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) are fully applicable.***

[…]

(59a) ***Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.***

(59b) ***Measures should be taken to prevent unauthorised access to digital communications in order to protect the confidentiality of digital communications including both the contents and any data related to such communications.***

(59c) ***Confidentiality of digital communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded digital 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.***

(59d) ***Terminal equipment of individuals and any information stored on such equipment are part of the private sphere of the individuals requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the individual's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the individual and may seriously intrude upon the privacy of these individuals. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned individuals.***

(59e) ***However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of individuals engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that individuals are provided with clear and precise information in accordance with this Regulation about the purposes of cookies or similar devices so as***

to ensure that individuals are made aware of information being placed on the terminal equipment they are using. Individuals should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where individuals other than the original individual have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the individual's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

[…]

(135) (…)

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

2a. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for other specific processing situations as provided for in Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law (…);

(b) (…);

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V the Treaty on European Union;

(d) by a natural person (…) in the course of (…) a personal or household activity;

(e) by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and, for these purposes, safeguarding of public security, or the execution of criminal penalties.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

(2) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination or erasure;

(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(7) 'recipient' means a natural or legal person, public authority, agency or any other body other than the data subject, the data controller or the data processor to which the personal data are disclosed; however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients;

(8) 'the data subject's consent' means any freely-given, specific and informed (…) indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means data related to the physical or mental health of an individual, which reveal information about his or her health status;

(12a) 'profiling' means a form of automated processing of personal data intended to (…) use a profile to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;

(12b) 'profile' means a set of data characterising a category of individuals that is intended to be applied to a natural person;

(12c) 'digital communication' means any information exchanged by electronic means between a finite number of parties. This does not include any information conveyed as part of a broadcasting service to the public except to the extent that the information can be related to one or more parties to the digital communication;

(12d) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the addressee's terminal equipment until it is collected by the addressee;

(13) 'main establishment' means

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, In this case the establishment having taken such decisions shall be considered as the main establishment. If no decisions as to the purposes and means of the processing of personal data are taken in the Union, the establishment of the controller in the Union where the main processing activities take place;

- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place;

- Where the controller exercises also activities as a processor, the main establishment of the controller shall be considered as the main establishment for the supervision of processing activities;

- Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking shall be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking;

(14) 'representative' means any natural or legal person established in the Union who, designated by the controller in writing pursuant to Article 25, represents the controller with regard to the obligations of the controller under this Regulation;

(15) 'enterprise' means any natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or group of enterprises engaged in a joint economic activity;

(18) (…)

(19) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 46;

(19a) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing, because the controller or processor is established on the territory of the Member State of that supervisory authority or because data subjects residing in this Member State are or likely to be substantially affected by the processing.

(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

[…]

CHAPTER II

PRINCIPLES

[…]

CHAPTER III

RIGHTS OF THE DATA SUBJECT

[…]

SECTION 4

RIGHT TO OBJECT*, UNSOLICITED COMMUNICATIONS* AND PROFILING

Article 19

Right to object

1. The data subject shall have the right to object, on reasoned grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (f) of Article 6(1); the personal data shall no longer be processed unless the controller demonstrates legitimate grounds for the processing which override the interests or rights and freedoms of the data subject.

1a. Where an objection is upheld pursuant to paragraph 1, the controller shall no longer process the personal data concerned except for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Article 19a

Unsolicited communications

1. Notwithstanding article 19, the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of addressees who have given their prior consent.

2. Notwithstanding paragraph 1, 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 this Regulation, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic

contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed without the unambiguous consent of the addressee.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the addressee may send a request that such communications cease or which encourage addressees to visit websites that contravene that Article are prohibited.

5. Paragraphs 1 and 3 shall apply to addressees who are natural persons.

Article 20

Profiling

1. The data subject shall have the right not to be subject to a decision evaluating personal aspects relating to him or her, which is based solely on automated processing, including profiling, and produces legal effects concerning him or her or significantly affects him or her.

1a. A data subject may be subject to a decision referred to in paragraph 1 only if it

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; or

(b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's explicit consent.

1b. In cases referred to in paragraph 1a) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision:

2. (…)

3. Decisions referred to in paragraph 1a shall not be based on special categories of personal data referred to in Article 9(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's legitimate interests are in place.

SECTION 4a

CONFIDENTIALITY OF DIGITAL COMMUNICATIONS

Article 20a

Confidentiality of digital communications

1. A natural or legal person shall respect the confidentiality of the content of digital communications and shall refrain from listening, tapping, storing, intercepting or surveilling of the content of digital communications unless and insofar as:

(a) the parties to the digital communication have unambiguously consented;

(b) those acts are necessary to protect the integrity and security of the communication or information society service offered by the concerned natural or legal person;

(c) those acts are necessary for the conveyance of a digital communication and do not prejudice the principle of confidentiality;

(d) those acts are necessary to comply with a legal obligation or judicial order.

2. Paragraph 1 shall not affect any legally authorised recording of digital communications when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. The storing of information, or the gaining of access to information already stored, in the terminal equipment of an individual is only allowed on condition that the concerned individual has given his or her unambiguous consent, having been provided with clear and comprehensive information, in accordance with article 14, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a digital communication, or as strictly necessary in order for the provider of an information society service explicitly requested by the individual to provide the service.

[…]

CHAPTER IV

CONTROLLER AND PROCESSOR

[…]

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

[…]

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES

[…]

CHAPTER VII

CO-OPERATION AND CONSISTENCY

[…]

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS

Article 73

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single 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 data subject considers that the processing of personal data relating to him or her does not comply with this Regulation.

2. (…)

3. (…)

4. (…)

5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant Article 74420 or, as regards decisions taken by the European Data Protection Board pursuant to Article 76b.

Article 74

Right to a judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority competent in accordance with Article 51 does not deal with a complaint or does not inform the data subject within three months or any shorter period provided under Union or Member State law on the progress or outcome of the complaint lodged under Article 73.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 75

Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 73, a data subject shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in noncompliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority acting in the exercise of its public powers.

Article 76

Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf 434 and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf.

1a. Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1436 shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51 if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.

Article 76a

Suspension of proceedings

1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings involving the same processing activities are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 76b

Actions before the Court of Justice of the European Union against decisions by the European

Data Protection Board

1. Actions may be brought before the Court of Justice of the European Union in accordance with Article 263 TFEU, in order for it to review the legality of decisions taken by the European Data Protection Board pursuant to Article 58a. Such actions may be brought before the Court of Justice of the European Union by supervisory authorities, Member States and the Union institutions as well as by natural or legal persons to whom decisions taken by the European Data Protection Board have been notified or to whom such decisions are of direct and individual concern, including data subjects who have lodged a complaint in accordance with Article 73.

2. The expiration of the time-period provided for in the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court shall not bar the persons referred to in paragraph 1 from calling in question the lawfulness of any decision taken by the European Data Protection Board before the national courts in accordance with Article 74 or 75 and those national courts from requesting the Court of Justice of the European Union a preliminary ruling concerning the validity of any decision taken by the European Data Protection Board in accordance with Article 267 TFEU.

3. Where the European Data Protection Board notifies its decision in accordance with Article 58a(6), such a notification shall state the possibility for the persons referred to in paragraph 1 to bring an action for annulment before the General Court of the European Union in accordance with Article 263 TFEU as well as the time-period for such an action in accordance with the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court. It shall also refer to the additional right conferred on that person pursuant to paragraph 2.

4. In the event that the European Data Protection Board has an obligation to act and fails to take a decision, proceedings for failure to act may be brought before the Court of Justice of the European Union in accordance with Article 265 TFEU.

5. The European Data Protection Board shall be required to take the necessary measures to comply with the judgment of the Court of Justice of the European Union.

Article 77

Right to compensation and liability

1. Any person who has suffered damage as a result of a processing operation which is not in compliance with this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Where more than one controller or processor or a controller and processor are involved in the processing which gives rise to the damage, each controller or processor shall be jointly and severally liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors.

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

4. Court proceedings for exercising the right to receive compensation shall be brought before the courts with jurisdiction for compensation claims under national law of the Member State referred to in paragraph 2 of Article 75.

Article 78

Penalties

(…)

Article 79

General conditions for imposing administrative fines

1. Each supervisory authority competent in accordance with Article 51 shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 53.

2. Administrative fines imposed pursuant to Article 79a shall in each individual case be effective, proportionate and dissuasive.

2a. When deciding whether to impose an administrative fine in addition to, or instead of, measures referred to in points (a) to (f) of paragraph 1b of Article 53 and deciding on the amount of the administrative fine in each individual case due regard shall be had to the following:

(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned;

(b) the intentional or negligent character of the infringement,

(c) the number of data subjects affected by the infringement and the level of damage suffered by them;

(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;

(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;

(f) any previous infringements by the controller or processor;

(g) any financial benefits gained, or losses avoided, directly or indirectly from the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with these measures ;

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;

(k) (…)4;

(l) (…);

(m) any other aggravating or mitigating factor applicable to the circumstances of the case.

2b. (…).

3. (…)

3a. (…)

3b. 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.

4. The exercise by the supervisory authority competent in accordance with Article 51 of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.

Article 79a

Administrative fines

1. The supervisory authority competent in accordance with Article 51 may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] % of its total worldwide annual turnover of the preceding financial year, on a controller who, intentionally or negligently:

   (a) does not respond within the period referred to in Article 12(2) to requests of the data subject;

   (b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.

2. The supervisory authority competent in accordance with Article 51 may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual turnover of the preceding financial year474, on a controller or processor who, intentionally or negligently:

   (a) does not provide the information, or provides incomplete information, or does not provide the information timely or in a sufficiently transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;

   (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19;

   (c) (…);

   (d) (…);

   (e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24;

   (f) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4).

   (g) (…)

3. The supervisory authority competent in accordance with Article 51 may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year, on a controller or processor who, intentionally or negligently:

   (a) processes personal data without a (…) legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;

   (b) (…);

   (c) (…);

   (d) does not comply with the conditions in relation to profiling pursuant to Article 20;

   (e) does not implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 and 30;

   (f) does not designate a representative in violation of Article 25;

   (g) processes or instructs the processing of personal data in violation of Articles 26;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;

(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);

(j) (…);

(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).

(n) (…)

(o) (…)

(p) does not comply with Article 19a.

3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.

Article 79b

Penalties

1. For infringements of the provisions of this Regulation not listed in Article 79a Member States shall lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. (…).

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

CHAPTER IX

PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

[…]

CHAPTER X

DELEGATED ACTS AND IMPLEMENTING ACTS

[…]

CHAPTER XI

FINAL PROVISIONS

Article 88

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 88a

Repeal of Directive 2002/58/EC

1. Directive 2002/58/EC and Regulatin 611/2013 are repealed.

2. References made to articles 4, 5 and 13 of the repealed Directive 2002/58/EC shall be construed as being made to respectively articles 30, 20a and 19a of this Regulation.

3. References made to repealed Regulation 611/2013 shall be construed as being made to this Regulation.

Article 89

(…)

1. (…)

2 (…)

Article 89a

Relationship to previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked.