Europe

GSMA Europe and ETNO briefing papers on the proposed General Data Protection Regulation

- **Inconsistencies between the GDPR and the e-Privacy Directive**
  Inconsistencies between the 2002 Directive and the proposed Regulation are likely to lead to inconsistent consumer privacy experiences and rights for equivalent services and data. We discuss possible ways to avoid this.
  Articles concerned 2, 3, 4, 31, 89 - Link

- **Applicable law**
  We welcome the proposals in this field, but suggest some key improvements to ensure legal certainty for business and consumers and to ensure European consumers are protected irrespective of from where a service or product is being provided.
  Articles concerned 3, 4, 51 - Link

- **Consent in the online environment**
  We highlight key issues of over-relying on consent and suggest a context-based approach, while highlighting the link with transparency requirements and compatibility issues with the ePrivacy Directive. We propose measures to create consistent and effective privacy experiences for consumers.
  Articles concerned 4, 6, 7, 9, 14, 79 - Link

- **International data transfers**
  We welcome measures to simplify transfers and the codification of Binding Corporate Rules (BCRs). However, we are concerned that related procedural requirements are too strict and call for a review of these.
  Articles concerned 4, 6, 42, 43 - Link

- **Sanctions**
  We highlight the importance that sanctions are not only proportionate but fair, necessary and assist in ensuring effective protection for privacy.
  Articles concerned 15, 28, 32, 79 - Link

- **Documentation obligations**
  We point to the risk that new documentation obligations will lead to costly, time-consuming burdens without improving the protection of personal data.
  Articles concerned 22, 28 - Link

- **Futureproofing the GDPR**
  We express our views on how consistency mechanisms, delegated powers, comitology and self-regulation can play a key role to ensure the future-proofness of this regulation.
  Articles concerned 38, 57, 60, 62, 86, 87 - Link

- **Data Protection Impacts Assessments**
  While supporting PIAs, we suggest improving the text in order to avoid unreasonable burdens to businesses and innovation.
  Articles concerned 33, 34 - Link

- **Data breach**
  We welcome harmonization in this field and point to a few improvements aimed at ensuring that the principle is applied in a fair and proportionate way.
  Articles concerned 31, 32 - Link

GSMA Europe

GSMA Europe and ETNO
Briefing paper on the proposed General Data Protection Regulation (GDPR)

Inconsistencies between the proposed General Data Protection Regulation and the e-Privacy Directive

July 2012

Summary

- data protection rules for telecommunications operators may have been justified in the past. However 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.
- Against a background of global competition in innovative services the co-existence of the e-Privacy Directive (ePD) and the proposed General Data Protection Regulation (GDPR) would be incompatible with technology and service neutrality. The result would be negative for both consumers and businesses.
- Consumers would face inconsistent privacy experiences for functionally equivalent services. They would need to be aware whether the service was being provided by a telecoms operator or an online service provider in order to assess the degree to which their data is protected.
- Telecoms companies and their customers would face dual compliance regimes in terms of national supervision and rights enforcement.
- It would be preferable if all the ePD's provisions were incorporated into the GDPR. Failing this, legislators should ensure that where issues are covered in both instruments, they should be removed from the ePD.
- The GDPR offers a timely and appropriate instrument to resolve these inconsistencies. Consumers and businesses should not need to wait for these legal conflicts to be addressed through future legislative processes.

The proposed rules in the Regulation

The General Data Protection Regulation proposal (GDPR) introduces some of the elements included in the e-Privacy Directive 2002/58/EC[1] (ePD) into general privacy rules, such as data breach notifications. However, it does not sufficiently address the many problems that arise from the asymmetry of regulation for telecoms players in one regime and internet and over-the-top players in the other: most importantly the issue of inconsistent consumer rights and user experiences, but also competitive disadvantages for European telecoms operators. Further, it fails to deliver legal certainty for telecommunications network and service providers and for their customers on which regime to apply.

The GDPR attempts to describe in Article 89 its relationship to, and amends, the ePD as follows:

- Article 89(1) states that *"This Regulation shall not impose additional obligations on 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"*.
- Article 89(2) states that Article 1(2) of the ePD shall be completely deleted. This article sets out that the ePD is lex specialis to the DPD and acknowledges that protections may be extended to subscribers who are legal persons. This deletion may require Member States to adopt national implementation measures of the ePD.
- In Article 88(1) the GDPR repeals the DPD in its entirety. Article 88(2) construes any references to the DPD to the respective provisions of the GDPR. Since the ePD refers in many instances to the DPD, e. g. on key concepts such as consent, the ePD undergoes further changes without changing further rules in the ePD itself.
- Recital 135 of the GDPR clearly states that in order to clarify the relationship b²etween the proposed Regulation and Directive 2002/58/EC, the "*latter Directive should be amended accordingly*." Thereby the Regulator admits the necessity of clarification.

Criticism:
Inconsistencies with the e-Privacy Directive are not sufficiently addressed

As opposed to an EU Regulation, a Directive gives Member States considerable leeway in implementing its rules into law. Many Member States have used that leeway to implement stricter rules than in the ePrivacy Directive (ePD). Since all ePD references to the Data Protection Directive (DPD) will be construed as GDPR references, in consequence, depending on the outcome of the legislative process on the GDPR proposal, national laws transposing the ePD will need to be amended as well. Yet, as these are rules from a Directive, Member States will be free to use their leeway in the implementation again.

In many Member States, data protection authorities (DPA) are not responsible for the supervision of the ePrivacy rules, or may share responsibility with the national regulatory authorities for telecoms. Even if the

rules of the GDPR and ePD are aligned in the EU legal instruments, their co-existence will lead to diverging implementation into national law and application of them. The ePrivacy rules are also not subject to key

[1] as amended by Directive 2009/136/EC

provisions making the GDPR future proof: its consistency mechanism, delegated powers and other key features do not apply.

Therefore a review of the ePD as suggested by Recital 135 GDPR does not guarantee consistent consumer rights and user experience as it will involve a new lengthy legislative procedure involving different players (new constitute European Parliament and appointed Commission as of 2014) and divergent implementations by and supervision in Member States. During the transition period, when the new regulation has come into effect but before the ePD has been adjusted and is being enforced, the ambiguity of which law is applicable will lead to even further legal uncertainty for telecom companies and end users.

Practical impact for consumers and businesses

The e-Privacy Directive (ePD) is considered to be lex-specialis and intended to address specific circumstances of potential privacy risks in the telecommunications sector. But it may be noted that such data is widely used by over-the-top communications and information services without restriction and without the widespread harms that were anticipated. As lex-specialis the ePD is considered to override the current Data Protection Directive (DPD). This has led to the specific imposition of rules over the processing of data by publicly available electronic communications services and networks – ostensibly those services provided by mobile and fixed telecommunications companies. The ePD states in Recital 46 that the DPD "*covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way*."

This means in practice that the ePrivacy rules on traffic and location data do not apply to all players even where they provide functionally equivalent services using functionally equivalent data (for example, GPS data). This has been acknowledged by the Article 29 Working Party in their recent Opinion[2] on geolocation services on smart mobile devices[3].

In 1997 when the first sectoral Directive for the telecommunications sector was adopted (Directive 97/66/EC),, a specific regime for electronic communications was perceived as necessary because of the

unprecedented data those services made it possible to use to identify users, locate them, review their social interaction using SMS/MMS and their voice calls and web pages visited.

While this approach may have been appropriate in the early 2000s, it is highly questionable today, and will be foreseeably wrong in two or three years. Online services outside the scope of the ePD store vast

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[3] An 'electronic communications service' was defined a decade ago in Directive 2002/21/EC. Article 2(c) of the directive defines it as any "*service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.*" The definition does not include information society services, as defined in Article 1 of Directive 98/34/EC, and which services do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

amounts of personal contact information, video, picture and text files online, as well as offering online messaging services (email, chat, voice, video and other services) that are functionally equivalent to telecommunications services. Over the last
decade, interactive services have expanded enormously and functionally equivalent services are being provided in so many new and different ways. Focusing on the underlying technology or business model no longer serves to protect data subjects, but the proposed regime continues to support that focus.

This approach of sector-specific rules for telecommunications operators has led to an increased legal uncertainty and an asymmetry of data protection and privacy law. It disadvantages providers of equivalent services and leaves consumers alone to assess whether a specific service is being provided using telecoms data or online data in order to understand the level of protection individual data receives. At the same time telecoms operators have to face dual compliance regimes from the two legal instruments.

The GDPR affects the meaning, scope and application of the key matters listed in Annex I.

Policy considerations

Clarity and consistency are required between the two instruments in order to create
effective privacy experiences and drive the digital economy. As the GDPR currently stands it
manifests dual standards and uncertainty for consumers and dual compliance regimes for telecoms operators.

Ideally, the ePD should be fully integrated in the GDPR. However, taking political realities into account, this is not in reach in this legislative process. Since the ePD is a Directive and the GDPR is a Regulation it will be difficult to ensure consistency. Thus legislators must at least go the extra mile to require that all issues covered by articles both in the ePD and the GDPR are repealed in the ePD through the GDPR – as it has already begun in Article 89. This does not extend the scope or change the meaning of the GDPR but ensures that consumers can benefit from transparent and consistent rights and user experiences for functionally equivalent services.

Annex I

Key areas for consideration and recommendations

GDPR Proposal	e-Privacy Directive To Date	Issue and Practical Implications	Recommendation
Article 2: Definitions	**Article 2: Definitions** Stipulates that the future GDPR definitions should be applied if not otherwise provided herein.	• Personal data/ location data, recipients and other expression of the ePD will in future be defined by the GDPR.	• Ensure that there isn't duplication of rules by repealing in the ePD the ones conflicting with the GDPR.
Article 3: Territorial Scope Covers: • EU established companies (Art 3(1)) • Companies not established in the EU but targeting EU customers (Art 3(2)).	**Article 3: Territorial scope** Covers only EU established companies.	• For example, the 'cookie provision' would not apply to companies covered by companies targeting EU residents from non-EU countries.	• Ensure that there isn't duplication of rules by repealing in the ePD the ones conflicting with the GDPR.
Article 4(2) and (1): Personal Data The definition of personal data is extended to include "*any information relating to a data subject*" that can identify directly or indirectly, a natural person by means reasonably likely to be used by the data controller ... in particular by reference to an identification number, location data, online identifier …."	**Article 2 1st sentence; (c); (b); Articles 6 and 9: Personal Data** • Personal data in general are not expressly defined and refers to future GDPR. • But location data is covered and defined by the ePD in Art 2(c) and Art 9. • Traffic data is being defined in Art	• The lack of clarity and alignment may lead to certain categories of data being subject to both the GDPR and the ePD. For example, location data and identifiers that fall under traffic data. • GDPR and ePD do require legal grounds for processing of location data being personal data and not be-	• In order to treat equivalent services in the same way the provisions of the ePD related to location data should be repealed.

GDPR Proposal	e-Privacy Directive To Date	Issue and Practical Implications	Recommendation
	1(b) and 6.	ing rendered anonymous. Consent is the only legal ground for processing accepted within the ePD. Article 6 of the GDPR provides for more legal grounds of processing as e.g. contract related or a legitimate interest of the controller. This creates a disadvantage for those service providers covered by the ePD.	
Article 4(8) and 7: Consent Consent obligations are significantly strengthened: • Where required, consent will need to be a "freely given, informed and explicit 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". See also Recital 25. • Consent cannot have a legal basis where there is a significant imbalance between individual and the data controller. • Where consent is given in written	**Articles 2(f), 6(3) and 9(1), 13(2): Consent** • Art 2(f) – the definition of consent refers to the future GDPR. • Art 6(3) requires 'prior consent' to use traffic data for the purpose of marketing electronic communications services. • Art 9(1) requires individuals be given prior information and their consent obtained before their location data can be processed for providing a location based value added service.	• The GDPR introduces the need to obtain explicit consent compared to the current requirement for 'prior consent' in the ePD, for traffic and location data. Location data is classified as 'personal data' under the GDPR and it is unclear which consent standard will apply to this data category. Likewise, traffic data may include online or device identifiers now caught by the GDPR. • The GDPR removes the possibility of assuming consent or securing tacit consent as currently permitted under the ePD. • Consent will not be valid where there is significant imbalance in the	• Ensure that GDPR consent requirements apply to data processed in electronic communications networks. • Adapt the notion of consent to the context it is given in and grade consent requirements to the sensitivity of the data under question and potential risks.

GDPR Proposal	e-Privacy Directive To Date	Issue and Practical Implications	Recommendation
form concerning two different matters, it must be 'distinguishable in its appearance' from the other matter.		relationship between the individuals and data controller. This will impact on standard terms currently developed under the ePD and used to secure implied consent or to wrap up consent. • Under Art 19 GDPR personal data can be used for direct marketing so long as individuals are given the opportunity to object. This creates a lower threshold for non-telecoms providers as the former will be subject to higher consent requirements of the ePD (Art 13(2). This results asymmetrical regulation between EU players and other online actors covered by the GDPR only.	
Article 31: Data Breach Art. 31 requires notification of a personal data breach to the supervisory authority 'without undue delay and not later than 24 hours'.	Art 4(3) requires the provider of a 'publicly available electronic communications network' to report 'without undue delay' a 'personal data breach … in connection with the provision of a publicly available electronic communications service'.	• Creates a new security obligation for MNOs and establishes dual notification regimes or telcos – one under national implementations of the ePD and one for other personal data as defined in the GDPR. • This will add additional cost and complexity to operations. • Art 79(6)(h) of GDPR introduces fines	• Remove 24 hour obligation and propose adoption of 'without undue delay' as a standard. • Ensure GDPR proposals are aligned with current work by DG Infso and ENISA (who are working on SBN guidelines and standard forms of notification to NRAs etc). • Call for harmonised regime of en-

GDPR Proposal	e-Privacy Directive To Date	Issue and Practical Implications	Recommendation
		of up to 2% of worldwide turnover for failing to meet Art 31 security breach obligations. These penalties are inconsistent with those adopted under national implementing measures for the ePD.	forcement and sanctions regarding personal data security breaches.
Article 89(2): Amending ePD Art 89(2) states that Art 1(2) ePD shall be deleted.	**Article 1(2): Lex specialis** The deleted paragraph states that the ePD is lex specialis to the DPD (95/46/EC).	• It is highly questionable if the ePD would not be lex specialis – even if this reference is deleted. • If the ePD continues to rule only telecoms providers (and in few cases information service providers) on matters as well regulated in the GDPR the risk of double regulation arises.	• Avoid duplication of compliance regimes for telecoms operators.

About GSMA
The GSMA represents the interests of mobile operators worldwide. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA also produces industry-leading events such as the Mobile World Congress and Mobile Asia Congress.
For more information, please visit Mobile World Live, the online portal for the mobile communications industry, at www.mobileworldlive.com or the GSMA corporate website at www.gsmworld.com.

In the European Union the GSMA represents over 100 operators providing more than 600 million subscriber connections across the region. www.gsmworld.com/gsma_europe

About ETNO

ETNO, the European Telecommunications Network Operators' Association, is the voice of Europe's leading providers of e-communications services and investors in tomorrow's services and infrastructure.

ETNO's 38 member companies and 11 observers from Europe and beyond represent a significant part of total ICT activity in Europe. They account for an aggregate annual turnover of more than €600 billion and employ over 1.6 million people. ETNO companies are the main drivers of broadband and are committed to its continual growth in Europe.

ETNO contributes to shaping an investment-friendly regulatory and commercial environment for its members, allowing them to roll out innovative, high-quality services and platforms for the benefit of European consumers and businesses.

More information: www.etno.eu

GSMA Europe
Martin Whitehead
Director GSMA Europe
Park View, 4th floor
Chaussée d'Etterbeek 180
1040 Brussels
T: +32 2 792 05 56
E: mwhitehead@gsm.org

ETNO
Daniel Pataki
Director ETNO
Avenue Louise, 54
1050 Brussels
T: +32 2 219 32 42
E: pataki@etno.be