Centre for Information Policy Leadership
Hunton & Williams LLP

Centre for Information Policy Leadership's Response to the European Commission's Public Consultation on the ePrivacy Directive

5 July 2016

1. Introduction

1.1 The Review of the ePrivacy Directive

On 6 May 2015, the European Commission ("Commission") adopted the Digital Single Market Strategy for Europe ("DSM Strategy").[1] The DSM Strategy has three main pillars:

a. Provide consumers and businesses with better access to digital goods and services across Europe;

b. Create the right conditions and a level playing field to enable digital networks and services to flourish; and

c. Maximise the growth potential of the European digital economy.

As part of the DSM Strategy plans, following the adoption of General Data Protection Regulation ("GDPR"),[2] on 12 April 2016, the Commission launched a public consultation ("ePrivacy Consultation") on the evaluation and review of Directive 2002/58/EC ("ePrivacy Directive"). [3] The ePrivacy Directive forms part of the Regulatory Framework for Electronic Communications.[4] The ePrivacy Directive is also a "lex specialis" which particularises and complements Directive 95/46/EC ("Data Protection Directive")[5] which will be replaced by the GDPR on 25 May 2018.

The ePrivacy Consultation takes the form of an electronic questionnaire. The first part of the electronic questionnaire aims to evaluate the performance of the ePrivacy Directive against the five mandatory criteria of the Commission's "Better Performance Guidelines", namely, effectiveness, efficiency, relevance, coherence and EU added value. The second part of the e-questionnaire aims to assess the current ePrivacy Directive in light of the DSM Strategy.[6]

1.2 Introducing CIPL and the CIPL GDPR Project

CIPL is an independent global data privacy and information policy think tank, based in Brussels, London and Washington DC. In March 2016, CIPL launched its two year project on the consistent implementation, interpretation and enforcement of the GDPR ("CIPL GDPR Project").[7]

The CIPL GDPR Project aims to establish a forum for an expert dialogue amongst industry representatives, the European data protection authorities ("EU DPAs"), the European Data Protection Supervisor, the Commission, the ministries of the Member States and academic experts

---

[1] http://ec.europa.eu/priorities/digital-single-market_en.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN >. The GDPR will apply on 25 May 2018.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L 201) 37 (EC) as amended by Directive 2009/136/EC, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML. The 2009 amendments are *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0136-20091219. In this document, all references to the ePrivacy Directive are references to the amended ePrivacy Directive. See Article 1(2), ePrivacy Directive.

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24216a.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[6] https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016.

[7] https://www.informationpolicycentre.com/eu-gdpr-implementation.html.

on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and reports.

The objectives of the CIPL GDPR Project are set out in Appendix 1. The five focus topics of the CIPL GDPR Project, namely (a) data privacy programmatic management, (b) core principles and concepts, (c) individual rights, (d) international data transfers and (e) the relationships of and with EU DPAs, enforcement and sanctions, are fully set out in Appendix 2.

1.3 CIPL's Response

CIPL draws on its unique position as a neutral international think tank which brings together a broad range of industry from various sectors, including classic telecommunication providers, broadcasters and other information service providers to respond to the ePrivacy Consultation.

CIPL's response to the ePrivacy Consultation is written by the CIPL President, Bojana Bellamy, and the CIPL GDPR Fellow, Dr Asma Vranaki. CIPL's response focuses on the interplay between the ePrivacy Directive and the GDPR. This response evaluates two keys areas, namely:

a. Avoiding overlaps and ensuring consistency between the revised ePrivacy Directive, the GDPR and the wider European regulatory framework; and

b. The issues raised if the scope of the ePrivacy Directive is expanded.

2. Consistency between the Revised ePrivacy Directive and Other European Laws

In the interest of **legal certainty**, **legal coherence** and the **harmonisation of the European data protection law package**, it is of pivotal importance that the revised ePrivacy Directive is consistent with and does not duplicate existing European legislation.

Consistency between the revised ePrivacy Directive and other European legislation revolves around (1) clarifying the **relationship** between the GDPR and the revised ePrivacy Directive, (2) the **form** of the revised ePrivacy Directive and (3) avoiding **overlaps or inconsistencies** between the ePrivacy Directive and **other relevant European laws**.

2.1 Clarifying the relationship between the revised ePrivacy Directive and the GDPR

In the pre-GDPR era, the ePrivacy Directive had a complementary relationship with the Data Protection Directive. Given that the GDPR is replacing the Data Protection Directive, going forward, it is essential that the **relationship between the GDPR and the revised ePrivacy Directive** is clearly set out to ensure **legal certainty, legal coherence** and a **harmonised European data privacy regulatory framework** as well as achieve the goals of the **DSM Strategy**.

<u>GDPR Provisions on the ePrivacy Directive</u>

The GDPR approaches its relationship with the ePrivacy Directive in the following manner:

a. The GDPR "should apply to all matters concerning the protection of fundamental rights and freedoms 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 of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons;"[8]

b. The ePrivacy Directive should be amended once the GDPR is adopted to further clarify the relationship between the two instruments;[9]

c. The GDPR "shall not impose additional obligations on natural or legal persons in relation to processing 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;"[10]and

d. The Data Protection Directive is repealed by the GDPR although it remains in force until it is amended, repealed or replaced. [11]Any reference to the Data Protection Directive shall be construed as a reference to the GDPR.[12]

CIPL Recommendations

In the interest of **legal certainty**, **legal coherence**, a **consistent European data protection law regime** and achieving the **goals of the DSM Strategy**:

- The revised ePrivacy Directive should further **flesh out its relationship** with the GDPR.
- The revised ePrivacy Directive should clarify which legal instrument takes **precedence in cases of conflict** with the GDPR.
- The **GDPR** should take **precedence** in cases of conflict with the revised ePrivacy Directive. The GDPR is a modern, progressive, flexible and future-proof European data protection legislation which sets out the general data protection and accountability principles which apply directly across Europe.
- It will also take some time before the revised text of the ePrivacy Directive is agreed and formally adopted. It is likely that the revised ePrivacy Directive may not be agreed or in force by the time the GDPR applies. It is essential that decisions made pursuant to the GDPR during the revision period are not later on invalidated because of conflicts with the approved text of the revised ePrivacy Directive.

[8] Recital 173, GDPR.
[9] Recital 173, GDPR.
[10] Article 95, GDPR.
[11] Recital 171, GDPR.
[12] Article 94, GDPR.

2.2 Form of the Revised Legislative Instrument

CIPL Recommendations

The Commission should amend the form of the ePrivacy Directive from a **directive** to a **regulation** because:

- If the GDPR and the amended ePrivacy Directive have **different legislative forms**, this would lead to **legal uncertainty** and **incoherence** for all relevant stakeholders (e.g. telecommunication providers, OTT players, consumers and regulatory bodies), especially in cases of conflict between the two instruments. Legal uncertainty and incoherence would have a negative impact on the **DSM Strategy**;
- If the amended ePrivacy Directive remains a directive, this would impede the establishment of a **harmonised European data protection law regime**. There is a real danger that the directive may be inconsistently transposed in Europe. Past experiences about the national transpositions of both the Data Protection Directive and the ePrivacy Directive have highlighted the divergent approaches of member states when implementing such directives; and
- Inconsistent implementation of the ePrivacy Directive would also result in the lack of an **equivalent level of protection for the data protection and privacy rights** of individuals in Europe. This would prevent Europe from achieving one of the main aims of the GDPR which is to ensure the consistent interpretation, implementation and enforcement of European data protection laws.

2.3 Potential Areas of Overlap and Inconsistencies with European Legislation

In order to ensure **legal coherence, legal certainty** and a **harmonised European data protection law regime**, it is essential to avoid any inconsistency or overlap between the amended ePrivacy Directive and the following European legislation, namely, the GDPR, the upcoming NIS Directive,[13] the Framework Directive and the European Convention on Human Rights.

[13] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN ("NIS Directive"). On 7 December 2015, the European Parliament and Council reached agreed on the proposals of the Commission on the NIS Directive. See https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation. The new text of the NIS Directive will be available when it is adopted.

2.3.1 Applying the GDPR to "Publicly Available Electronic Communications Network and Service Providers"

CIPL is of the view that the GDPR provisions will apply to "publicly available electronic communication network and service providers" that:

a. Fall within the "material scope" of the GDPR; [14]

b. Fall within the "territorial scope" of the GDPR; [15] and

c. Qualify as either "controllers"[16] or "processors"[17] ("Qualifying Conditions").

CIPL Recommendations

- The GDPR should apply to all providers of publicly available electronic communication services that meet the Qualifying Conditions in respect of **the data protection matters** currently covered by ePrivacy Directive. This is essential in order to **avoid duplication, conflicts, promote a more sector-neutral, forward thinking, future-proof and technology-proof data privacy regulation** which would support emerging technologies, such as cloud computing and the Internet of Things.

- The GDPR is well-placed to deal with the **new data privacy challenges** raised by **innovative technologies** , with its **enhanced data compliance and accountability provisions** for controllers and processors, its **risk-based approach**, its strict safeguards for "**high risk" processing** and its **more robust individual rights** provisions. For example, the risk based approach allows organisations to modulate data privacy compliance in proportion to the risk level of personal data processing operations.

[14] Article 2, GDPR.
[15] Article 3, GDPR.
[16] Article 4(7), GDPR defines a "controller" as "the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." Article 4(2), GDPR defines "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Article 4(1), GDPR provides that "personal data" mean "any information relating to an identified or identifiable natural person…an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person…"
[17] Article 4(8), GDPR defines a "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

2.3.2 Data Breach Notification

The GDPR contains detailed provisions on data breach notification which are substantially similar to the **data breach notification** provisions found in the ePrivacy Directive.[18] The GDPR data breach notification provisions will apply to "publicly available electronic communication service and network" providers (and their processors) that meet the Qualifying Conditions.

CIPL Recommendation

- To avoid **unnecessary duplication**, the revised ePrivacy Directive should not address **data breach notification** as this is already covered by the GDPR.

2.3.3 Security

The following **European legislation** deal with several aspects of "security" which are relevant to the operations of "publicly available electronic communications service and network" providers.

a. The **GDPR** introduces detailed **security obligations** which will apply to "publicly available electronic communication services and network providers" which satisfy the Qualifying Conditions. These provisions also apply to processors that provide services to such controllers.

   Key security measures in the GDPR include the obligations on controllers and processors to implement the "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" taking into account the "state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[19]

   Examples of such measures include pseudonymisation, encryption, ensuring "ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;"[20]

b. The upcoming **NIS Directive** imposes comprehensive **security obligations** on **network and information service providers**.[21]

   The Commission's proposed text for the NIS Directive excludes "publicly available electronic communications service and network providers" from the ambit of the NIS directive because they current fall within the ambit of the ePrivacy Directive.[22]

c. Article 13a of Directive 2002/21/EC (as amended) ("**Framework Directive**")[23]requires providers of publicly available electronic communication networks and services to take **appropriate measures** to manage **the risks posed to the security of the networks and services**. It also requires them to guarantee the integrity of their networks and continuity of supply; and

[18] Article 4(3), ePrivacy Directive.
[19] Article 32(1), GDPR.
[20] Ibid.
[21] E.g. Article 14, NIS Directive.
[22] Article 1(3), NIS Directive.
[23] 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 Regulation (EC) No 717/2007, Regulation (EC) No 544/2009 and Directive 2009/140/EC.

d. The **Radio Equipment Directive** sets out the regulatory framework for "the making available on the market and putting into service … of radio equipment".[24]

The Radio Equipment Directive empowers the Commission to adopt a number of **delegated acts** "in respect of the specification of categories or classes of radio equipment that have to comply with one or more of the additional essential requirements" set out in this directive in order address various needs including the **personal data and privacy protection** of the individuals.[25] Radio equipment within certain categories or classes shall be so constructed that it complies with a number of essential requirements including incorporating measures to protect the personal data and privacy of individuals.[26]

CIPL Recommendations

In the interest of **legal certainty, legal coherence, a harmonised European regulatory regime and achieving the goals of the DSM**:

- "Security" provisions in European legislation must be consistent, complimentary and not overlap with each other.
- The **ePrivacy Directive "security" provisions** should be **deleted** in the revised ePrivacy Directive.
- The **GDPR "security" provisions** should apply to "publicly available electronic communication service and network" providers that meet the Qualifying Conditions.
- The **Article 1(3) exclusion of the NIS Directive** should be deleted in the official text of the NIS Directive so that the comprehensive security provisions in the NIS Directive apply to "publicly available electronic communications service and network providers."
- Article 13a of the **Framework Directive** should apply to "publicly available electronic communications service and network providers" which fall within its ambit.
- Where necessary, the **Commission** could use its power to enact **delegated acts** under the **Radio Equipment Directive** to specify new categories or classes of radio equipment, which are not covered by existing European laws.

[24] Article 2(1) of the Radio Equipment Directive defines "Radio equipment" as "an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination."
[25] Recital 18, Radio Equipment Directive.
[26] Article 3(2)(e), Radio Equipment Directive.

2.3.4 Location and Traffic Data

Currently, the ePrivacy Directive applies 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."[27]

In plain terms, "electronic communications service and network" refer to services and networks that consist partly or fully of conveyance of signals.[28] The ePrivacy Directive establishes a specific and stricter legal regime for the processing of location and traffic data by "publicly available electronic communications services and networks" providers.[29] In essence, traffic and location data can only be processed by such providers for the provision of services. Processing for any other purpose, including value added services, can only take place with individual's consent or where data is anonymised.

As noted by various data protection experts, the current scope of the ePrivacy Directive can lead to circumstances where functionally equivalent services do not fall within the remit of the directive and are not subject to the same stricter legal regime.[30] As an example, the ePrivacy Directive regime for **traffic and location data** may have been appropriate in 2002 when location and traffic data were mostly used by the telecommunications sector. However, since 2002, due to technological innovation and the converged communications landscapes, Over-The-Top ("OTT ") providers and other communication service and information society providers, also collect large amount of traffic and location data for various purposes, including delivering their messaging services. [31]

Nonetheless, **OTT providers and other information society providers** do not fall within the scope of ePrivacy Directive and are not subject on location and traffic data. In the era of **convergence and technological neutrality**, it is not appropriate to impose different data protection obligations on providers of functionally equivalent services depending on whether they are OTT and other information society providers or traditional telecommunications companies.

This is even more problematic from the perspective of individuals and considering the fact that the ePrivacy Directive has been **inconsistently transposed** in Europe. Consequently, in some Member States, services which are functionally equivalent to "electronic communication services" may often fall within the remit of multiple laws, such as data protection, consumer and other information society services laws. This means that European individuals receive **different levels of data protection** depending on what type of "electronic communication service" they are using and the jurisdiction in which they are based. Most **consumers are not aware** that different levels of data privacy protection are afforded to their communications depending on whether they use the services and products of traditional telecommunication providers or OTT, such as WhatsApp and

[27] Article 3, ePrivacy Directive.
[28] 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 Directive), Articles 2(a) and (c) define "electronic communications service and network".
[29] Art. 6 and 9, ePrivacy Directive.
[30] E.g. European Commission, "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (2015) available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962; DLA Piper, "Proposals for an amendment to the General Data Protection Regulation and repealing the ePrivacy Directive," (29 May 2015) available at https://www.etno.eu/datas/publications/studies/DPTS_study_DLA_31052015_Final.pdf.
[31] OTT providers refer to content providers which provide audio, visual and other types of media (e.g. messages) over the Internet.

Skype. With this in mind, is the ePrivacy Directive still the appropriate legal instrument to regulate traffic and location data?

In our opinion the **GDPR** is the right instrument to regulate **traffic and location data** because:

- Both **location and traffic data** are **personal data** and will be subject to the GDPR. The GDPR already explicitly recognises **location data** as a type of "personal data". Although the GDPR does not contain any specific provision about **traffic data**, as long as traffic data relate to an identifiable or identified individual, such data fall within the ambit of the GDPR.

- The GDPR contains comprehensive provisions to enable the **lawful processing of location and traffic data**, while **preserving individuals' rights**, both in the context of the provision of services and for other purposes, such as value added services. In particular, Art. 6 of the GDPR provides several grounds which legitimise the processing of traffic and location data, including consent, legitimate interest and necessity for contract. Currently, the ePrivacy Directive enables companies to process traffic and location data for purposes other than service provision in cases where they have obtained the relevant consent. This regime will impede innovation and hinder future legitimate uses of these data. It is essential that organisations have an option to apply the **legitimate interest ground** for processing of traffic and location data, where such processing is in the legitimate interest of the organisation, or a third party and the rights and freedoms of individuals are not prejudiced. In the rapidly evolving world of connected devices, internet of things, machine to machine communication, it is essential to preserve the flexibility that GDPR provides for any future communications and processing of personal data

- The **GDPR risk provisions** will also enable companies to modulate their data privacy compliance in proportion to the **level and magnitude of risk** to individuals raised by their processing operations. This will afford **greater protection** to the **personal data and privacy rights of individuals.** Companies will have to adopt **context-specific privacy protective measures** which are proportional to the risk level of processing specific personal data categories, such as location and traffic data.

- GDPR provisions on **enhanced transparency**, **automated decision-making** and **stronger individual rights** also provide for the effective protection of individuals, which are also applicable in respect of processing of traffic and location data.

- There is no legal rationale to subject **traffic and location data** to the stricter legal regime of the ePrivacy directive. In essence, retaining these provisions in the amended ePrivacy Directive would create two conflicting data protection regimes given the GDPR provsions. This would create confusion for both businesses and individuals. It may also have unintended consequences to extend the reach of ePriavcy directive well beyond the original intent to any communications in the future information society (including Internet of things and machine to machine) and diminish the applicability of the GDPR.

CIPL Recommendations

- The **revised ePrivacy Directive** should not contain any provisions on **location and traffic data.**
- The **GDPR** should apply in cases where companies meeting the Qualifying Conditions process **location and traffic data**.

2.3.5 Confidentiality of Communications

Currently, other than the ePrivacy Directive, three European legislative instruments regulate the "confidentiality of communications."

Firstly, Article 8(1) of the **European Convention of Human Rights** ("ECHR") provides that "everyone has the right to respect for his private and family life, his home and his correspondence." The Article 8 right is a qualified right which may be limited in scope in prescribed circumstances, such as public interest and national security. Article 8 is a broad-ranging right that is often closely connected with other rights such as freedom of religion, freedom of expression, freedom of association and the right to respect for property.

The **"respect for private life"** right is multi-faceted and covers various aspects of "confidential communications" prescribed by the ePrivacy Directive including:

- Respect for **private and confidential information**, particularly the storing and sharing of such information;
- The right not to be subject to **unlawful state surveillance**; and
- The right to control the **dissemination of information** about one's private life, including photographs taken covertly.

The **"respect for correspondence right"** explicitly covers the right of individual to **uninterrupted and uncensored communication** with other. This right is particular relevant to matters, such as phone-tapping and electronic communication surveillance (e.g. email), which are key concerns in an age of increased covert and overt state and unauthorised third-party surveillance of such communications era.

Secondly, the Charter of Fundamental Rights of the European Union also contain various provisions which are relevant to the confidentiality of communications.[32]

Thirdly, the **GDPR** requires controllers and processors "to implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." Examples of such measures including the ability to "ensure the ongoing **confidentiality**, integrity, availability and resilience of processing systems and services."[33] Maintaining the "confidentiality" of personal data processing systems and services extends, to a

[32] E.g. Article 7, Charter of Fundamental Rights of the European Union.
[33] Article 32(1)(b), GDPR.

variable extent, to the protection of the confidentiality of communications passing through these systems and services.

CIPL Recommendations

- Aspects of **"confidentiality of communications"** which are covered by the **ECHR** and the **Charter of Fundamental Rights of the European Union** should not be replicated in the revised ePrivacy Directive
- The revised ePrivacy Directive should not duplicate the **GDPR security provisions** to the extent that such provisions are relevant to the "confidentiality of communications"

3. Conclusion

CIPL's response to the ePrivacy Directive Consultation has highlighted:

- The importance of **avoiding overlaps and inconsistencies** between the revised ePrivacy Directive, the GDPR and other European laws in the interest of **legal certainty, consistency and promoting the aims of the DSM Strategy**;
- The **GDPR** will apply to electronic communication service providers and networks that meet the Qualifying Conditions. The GDPR provisions on **security, data breach notification and confidentiality of communications** will apply in such cases. The revised ePrivacy Directive should not contain similar provisions;
- Other than the GDPR, various other European laws, such as the NIS Directive and the Framework Directive, contain **security provisions** which would apply to electronic communication service providers and networks in specific cases. Given the existence of comprehensive security provisions in various European laws, the revised ePrivacy Directive does not need to contain any similar security provisions;
- The **comprehensive, future-proof, technology-neutral GDRP rules** will apply to the processing of personal data including **location data and traffic data** (that contain personal data). The revised ePrivacy Directive should not contain any provisions on location and traffic data as this would lead to fragmentation, legal uncertainty and incoherence;
- The revised ePrivacy Directive should be in the form of a **regulation** to ensure that consistency with the GDPR. The **relationship** between the revised ePrivacy Directive and the GDPR should also be further clarified; and
- The revised ePrivacy Directive should not contain provisions on the **"confidentiality of communications"** which replicate existing provisions in the GDPR and the Charter of Fundamental Rights of the European Union the ECHR.

Appendix 1

OBJECTIVES OF THE CIPL GDPR PROJECT

The CIPL GDPR Project aims to establish a forum for an expert dialogue between industry representatives, EU DPAs, the European Data Protection Supervisor (EDPS), the Commission, the Member States representatives and academic experts through a series of workshops, webinars and white papers with the following specific objectives:

- Informing and advancing **constructive and forward-thinking** interpretations of key GDPR requirements;
- Facilitating **consistency in the interpretation** of the GDPR across the EU;
- Facilitating **consistency in the further implementation** of the GDPR by Member States, the Commission and EDPB;
- Examining **best practices**, as well as **challenges**, in the implementation of the key GDPR requirements;
- **Sharing industry experiences and views** to benchmark, coordinate and streamline the implementation of new compliance measures; and
- Examining how the new GDPR requirements should be interpreted and implemented to **advance the DSM and data-driven innovation**, while protecting the privacy of individuals and respecting the fundamental right to data protection.

Appendix 2

FOCUS TOPICS OF THE CIPL GDPR PROJECT
"5 BUCKETS"

1. **Data Privacy Programmatic Management**

   - Accountability and its elements under the GDPR for controllers and processors;
   - Appointment and role of the DPO;
   - Assessing risk under the GDPR – privacy impact assessments, privacy by design, breach notification;
   - Evidencing and demonstrating accountability externally;
   - Privacy seals, certifications, codes of conduct; and
   - Harmonisation and consistent implementation.

2. **Core Principles and Concepts**

   - Legitimacy (consent/age of consent, legitimate interest), decisions based on profiling, transparency, purpose limitation, pseudonymisation.

3. **Individual Rights**

   - Data portability, new aspects of data erasure and right to object, transparency.

4. **International Data Transfers**

   - Adequacy decisions, BCRs, model contracts, the new EU-US Privacy Shield, derogations, seals and certifications, Art. 48, interoperability with non-EU mechanisms.

5. **Relationship with the EU DPAs, Enforcement and Sanctions**

   - Smart regulation;
   - Main establishment, "one-stop-shop" and relationship with EU DPAs;
   - Role and powers of the EU DPAs;
   - Role and powers of the EDPB;
   - Consistency procedure;
   - Sanctions and liability; and
   - Links with EU strategy for digital single market and smart regulation.