INCEPTION IMPACT ASSESSMENT			
TITLE OF THE INITIATIVE	REFIT Evaluation and Impact Assessment of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)		
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	DG CNECT – Unit H4, Trust and Security	**DATE OF ROADMAP**	3/10/2016
LIKELY TYPE OF INITIATIVE	SWD + Legislative proposal(s)		
INDICATIVE PLANNING	Q4 2016		
ADDITIONAL INFORMATION	-		

This Inception Impact Assessment is provided for information purposes only and can be subject to change. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.

A. Context, Subsidiarity Check and Objectives

Context

In the Communication on a Digital Single Market Strategy for Europe of 6 May 2015 (**DSM Communication**), the review of the ePrivacy Directive (hereinafter referred to as the "**ePD**") is presented as one of the key actions under the pillar aiming to create the right conditions for digital networks and services to flourish. More particularly, the DSM Communication emphasises that once the EU rules on data protection are adopted, the ensuing review of the ePD will focus on **ensuring a high level of protection for data subjects and a level playing field for all market players**.

As regards personal data and privacy, the EU is committed to the highest standards of protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. The recently adopted General Data Protection Regulation **(GDPR)** will increase trust in digital services protecting individuals with respect to processing of personal data by all companies that offer their services on the European market.

The ePD (Directive 2002/58/EC on privacy and electronic communications) concerns the protection of privacy and personal data in the electronic communication sector. The ePD was reviewed and amended in 2009 in the context of the review of the telecoms regulatory framework by Directive 2009/136/EC of 25 November 2009.

How does the new initiative relate to past and possible future initiatives?

1. The ePD particularises and complements Directive 95/46/EC on data protection (Data Protection Directive), by setting up specific rules concerning the processing of personal data in the electronic communication sector. It also protects the legitimate interests of subscribers who are legal persons. All matters concerning the protection of personal data in the electronic communications sector which are not specifically addressed by the provisions of the ePD are covered by the Data Protection Directive (and in the future by the GDPR).

The Data Protection Directive is going to be replaced by the General Data Protection Regulation (GDPR) as of 2018. Consequently, the review of the ePD has been dependent on agreement of the reform of the EU general data protection legislation, composed of the GDPR and the Data Protection Directive for Police and Criminal Justice authorities (Police Directive) The evaluation and review of the ePD will in particular look into whether any of the rules of the ePD (or the ePD as a whole) are no longer needed to the extent that are covered by other legal instruments, in particular by the future GDPR. The review is not intended to change any of the provisions adopted in the EU data protection reform. Moreover, an important aspect of the review will be to ensure full consistency with GDPR. This is further explained below in the section on the issues to be tackled.

2. The ePD is part of the electronic communications framework, including the recent Regulation 2015/2120 referred to as Connected Continent. The ePD is part of the **Regulatory Framework for Electronic Communications**, which comprises a Framework Directive 2002/21/EC (the **Framework Directive**) and four specific directives. The ePD is one of these specific directives. It is essential to ensure consistency between the instruments in their review. For example, providers of publicly available electronic communications services are bound by specific security obligations as security is a key precondition for the respect of confidentiality of electronic communications. The review of the ePD will therefore have to be coherent with Art 13a the Framework Directive which deals with security and integrity of network and services.

In the Security agenda it was recognized that communication data Communications data can also contribute effectively to the prevention and prosecution of terrorism and organised crime.

Has the existing policy been evaluated? Is it part of the REFIT policy?

As indicated in the Commission Work Programme 2015, a REFIT evaluation of the performance of the current Regulatory Framework with a focus on regulatory fitness will be carried out in line with the new Commission working methods, REFIT and Better Regulation principles and feed into the Impact Assessment. The ex-post evaluation will assess the five mandatory evaluation criteria and answer questions such as (1) effectiveness: "To what extent have been the objectives of the ePD been achieved?"; (2) efficiency: "To what extent has the ePD been cost effective?"; (3) relevance: Is the ePD still relevant today? ; (4) coherence: "Is the ePD coherent both internal and in relation with other existing regulations?"; (5) EU added value: "What is the additional value resulting from the ePD compared to what could be achieved by Member States at national and/or regional levels?"

Issue

Issues expected to be tackled

At this stage, the main issues that have been identified are explained below. The list of issues will be confirmed once the REFIT evaluation is concluded.

- **The current legal framework is complex and needs updating** in the light of the recently adopted GDPR/other legal instruments: Some stakeholders argue that some provisions of the ePD are no longer needed in light of the GDPR and could be repealed or transferred into other legal instruments. Some of its provisions may be simplified. After establishing, among others the effectiveness, efficiency, relevance, coherence, EU added value of each one of the articles of the ePD, the Commission will consider changes that are needed in order to ensure full consistency with the GDPR and the electronic communications regulatory framework.
- **The scope of the ePD has been outpaced by with the new market and technological realities:** As the other directives of the electronic communications regulatory framework, the ePD mostly applies to traditional telecommunication service providers, i.e. those providers who are responsible for carrying signals over an electronic communications network. It does not apply to the so-called over-the-top (OTT) services which provide communication services (voice, messaging). This may result in both a void of protection and in an uneven playing field. The Data Protection Directive and the recently adopted GDPR applies to the processing of personal data carried out by OTTs but the enhanced protections provided in the ePD do not apply. Moreover, while the rules of the Data Protection Directive apply to closed (private) user groups and corporate networks, the enhanced protections of the ePD, for example as regards confidentiality obligations, do not apply.
- **Confidentiality of communications may not be sufficiently protected against intrusions**: Cyber-attacks and other publicly reported breaches have put into question the effectiveness of the current protection afforded to security and confidentiality of electronic communications. In addition, the ePD ensures protection against intrusions into users devices, for example by taking information stored in these devices (e.g. contact lists) or by inserting identifiers into such devices. Under Article 5(3), storing information, or accessing information already stored, in the terminal equipment requires the prior informed consent of the user or subscriber. If the information is personal data, in order to further process the information collected or stored, The Data Protection Directive and the GDPR will apply. Importantly, unlike to the GDPR, Art 5(3) applies even if the information collected or stored is not personal data. The effectiveness and efficiency of this provision has been contested. Moreover, the rapid pace of technology has shown that some techniques for tracking using browsing activities may not be entirely captured by Article 5(3), such as device fingerprinting. Finally, it has been argued that the exceptions to the consent rule need to be widened in order to include the storing/accessing of information in users' device which are not privacy invasive, such as first party web-analytics. Against this background, the review of the ePD will consider, also in light of the GDPR, whether changes are needed in order to ensure effective and efficient protection of security confidentiality of communications.
- **Fragmented implementation and inconsistent enforcement:** There is evidence suggesting that some provisions of the ePD may be formulated in too broad and general terms. As a consequence, key provisions and concepts may have been implemented and transposed differently by Member States. Moreover, the enforcement of the ePD provision at national level is entrusted to a "competent national authority" (Article 15a of the ePD), without further defining that authority or body. This has led to a fragmented situation in the EU, where some Member States have allocated competence to data protection authorities (DPAs), others to the telecom national regulatory authorities (NRAs) and others to yet another type of body (consumer protection bodies), possibly causing overlapping competences and legal uncertainty. The review will consider whether the above has limited the effectiveness or efficiency of the ePD and whether, also in light of the GDPR, changes are needed.

EU dimension

- EU action is justified by the requirement in the current regulatory framework (Art. 18 ePD) to review periodically the functioning of the current rules.
- The EU Data Protection laws requires a review of the ePD, to adapt it to the recently adopted general data protection framework and in particular to ensure consistency with the GDPR.

Affected stakeholders

Providers of electronic communication services; providers of information society services; manufacturers of electronic communications equipment; including operative systems; all individuals who are users and subscribers of electronic communications services and information society services; public administrations in the EU Member States; policy makers and administrations at national, regional and local level; regulators; Europol; European Union economy and society as a whole.

Subsidiarity check

On the choice of possible legal basis, it will depend on the aim and contents of the possible future act. Possibilities include the following:

The legal basis for any possible initiative that concerns the protection of personal data of individuals will be Article 16 of the Treaty on the Functioning of the European Union (TFEU). But taking into account that the ePD also covers aspects related to the protection of privacy (as opposed to "data protection"), consumer issues and the protection of legal persons, Article 114 of the TFEU may also be the legal basis.

Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU.

Main policy objectives

The general objectives are to assess which elements are no longer fit for purpose via a REFIT evaluation (backward-looking exercise) and to identify/assess possible policy options for the modernisation of the regulatory framework via the impact assessment (forward-looking exercise). The impact assessment and the ongoing REFIT evaluation of the ePD are conducted broadly in parallel and will be closely coordinated in terms of timing and contents. Based on the previous and ongoing evaluations and consultation activities on the ePD, including the final results of the REFIT evaluation of the ePD, the work on future options may focus on the following possible areas:

- Reviewing the legal framework and adapting it the general data protection framework and in particular to ensure consistency with GDPR/other legal instruments and to ensure simplification of legislation
- Assessing the scope of the ePD in light of the new market and technological realities
- Ensuring effective and efficient protection against intrusions into confidentiality of communications and users' equipment
- Addressing fragmentation and inconsistent enforcement

B. Option Mapping

Baseline scenario – no EU policy change

The ePD, on the one hand, and the GDPR, and the future telecom regulatory framework on the other, may not be fully consistent, with consequences on legal certainty and regulatory inefficiencies, for example, as regards notification of data breaches. The provisions of the ePD (or the whole ePD), further to the evaluation and review exercise, may be considered as obsolete.

The Directive would continue to apply essentially to providers of publicly available electronic communications services and not to OTT service providers Voice over IP, instant messaging services or closed or private networks. This may lead to void of protection and uneven playing field.

Possible gaps and shortcomings identified in relations with the security and confidentiality of electronic communications will not be addressed. Personal data breach notification will be regulated both in the ePD, Electronic Communications Framework, and in GDPR, thus lack of coherence will not be tackled. Developments such as the increase use of direct marketing in social media, browser fingerprinting and other tracking technologies will not be addressed.

The implementation and interpretation of certain key provisions and concepts could remain fragmented and inconsistent across Member States. The competence to apply the national laws implementing the ePD will continue to be attributed to different type of national authorities or bodies and in some cases shared by multiple authorities in the same Member State, with possible resulting inefficiencies.

Options of improving implementation and enforcement of existing legislation or doing less/simplifying existing legislation

Options would include (1) launching infringement proceedings where relevant; (2) providing Commission guidance and (3) convening coordination meetings among national authorities. However, these options would not necessarily guarantee a substantial improvement of the present conditions as they would be based on a piecemeal approach and would not provide a comprehensive solution to the problems identified. The Commission's guidance may conflict with the requirement of independence of national data protection authorities and national regulatory authorities.

Improving implementation and enforcement of existing legislation may be hampered by the broad or ambiguous formulation of some of the provisions of the current ePD (especially from a technological point of view). There will be no creation of a level playing field and no coherence with the GDPR. Furthermore, the following problems will not be properly addressed: the wide exceptions provided for in the Directive, for example in the field of law enforcement, the existence of a diverse range of national authorities, the absence of a formal consistency mechanism or a proper coordination forum (like the Article 29 Working Party) including all authorities competent to enforce the ePD provisions.

In the evaluation and review exercise, the simplification of the current legal framework will be carefully assessed. Simplification is one of the objectives of the review, which will strive to eliminate and/or simplify all provisions which are no longer considered to be fit for purpose. It will also be considered whether, in light of the GDPR and the Electronic Communications Framework some of the ePD provisions have still a reason to exist.

Alternative policy approaches

The following preliminary options related to the main areas outlined above will be considered:

- Policy options concerning **simplification** of the legal framework and **consistency** with other legal instruments (in particular the GDPR) include repealing outdated or unnecessary provisions of the ePD or moving them to other legal instruments. The option of a total repeal of the Directive will also have to be considered, if it is established that none of the articles of the ePD have EU added value and/or are already covered by other legal instruments.
- Policy options concerning the **scope** of the Directive (the services to which it applies) include assessing the scope to encompass various categories services that are currently outside the definition of electronic communications services given by the Directive (such as OTTs) and/or to closed or private networks.
- Policy options in the area of protecting **confidentiality** of communications and terminal equipment include, but should not be limited to, improving safeguards for effective and efficient confidentiality of communications.
- On **fragmentation and enforcement**: options include legislative amendments addressing gaps in current harmonisation, detailed harmonisation of all substantive provisions as well as various ways of harmonising tasks and powers of competent authorities at national level and reinforcing cooperation.

Alternative policy instruments

It is unlikely that a non-legislative instrument, such as a recommendation, a communication, or self/co regulation could be used to achieve the existing objectives of the ePD as they would not be legally binding. Only legislative instruments (regulation, directive or a combination of the two) can provide a suitable solution. However, in certain areas non-legislative instruments may play a crucial role to complement the legislative provisions and ensure their consistent and effective application in the market.

Alternative/differentiated scope

In principle, anyone who provides the services covered by the ePD will have to abide by the same rules because of fundamental rights protection. Fundamental rights should be respected in all situations and exemptions or derogations are generally not envisaged. Certain procedural or administrative requirements may be scaled according to the risk posed by operators in specific situations. This aspect will be further examined in the context of the impact assessment, with particular regard to the impacts on SMEs and micro-enterprises.

Options that take account of new technological developments

Taking account of new technological developments is one of the core objectives of this initiative. Therefore, policy options would be designed to reflect these developments. Examples include the possible extension of the scope of the ePD to online platforms providing OTT communication services of services regarded as substitutable by consumers such as OTTs or to closed or private networks or the review of Article 5(3) with a view to making it consistent with modern tracking technologies (see e.g. device fingerprinting techniques or WIFI

tracking).

As a general rule, the review aims to be technologically neutral, which means that it does not intend to impose, or discriminate in favour of, the use of a particular type of technology, but ensure that the same service or function is regulated in an equivalent manner, irrespective of the technical means by which it is delivered.

Preliminary proportionality check

In line with the principle of proportionality, in reviewing the ePD, the Commission will make sure that neither the content nor the form of Union action goes beyond what is necessary to meet the objectives of the Treaties. Particular attention will be devoted to ensuring that the policy approach and its intensity match the identified problem/objective. Moreover, for each field involved, the REFIT evaluation and review will look into whether there is scope for streamlining and simplification of procedures thereby reducing or in any event not augmenting the administrative burden.

C. Data Collection and Better Regulation Instruments

Data collection

Existing evidence base

On 4 November 2010, the Commission set out a strategy to strengthen EU data protection rules. In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. All the information gathered throughout the EU data protection reform process[1] will be taken into account. In addition, in 2015, the Commission concluded a specific study on the ePD (SMART 2013/0071) launched by DG CNECT in 2014. The study's objective was to assess its transposition, effectiveness and compatibility with the proposed General Data Protection Regulation. The study was finalised in April 2015 and provides important evidence for the evaluation exercise: https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data. The Study covered the following provisions of the ePD: Articles 1 and 3 on scope, Article 5 on confidentiality, Article 5(3) on confidentiality of terminal equipment, Article 6 on traffic data, Article 9 on location data and Article 13 on unsolicited communications.

Data gathering

Additional information and data is needed on the implementation of the Directive in some particular areas, for instance those which were not directly covered by the Study on the ePD. These include, in particular, provisions on security measures, directories, itemised billing, calling line identification. Some additional data may be needed with regard to the economic effects of the current rules, including costs on businesses and operators.

In the context of both the REFIT evaluation and impact assessment, evidence will be gathered through stakeholder consultations (see below) and the following study:

1. Study aimed at collecting further information for the REFIT evaluation and assessment of options.
2. Eurobarometer survey.
3. Individual meetings-workshops with categories of stakeholders, including public administrations, business and civil rights associations.

Consultation approach

Public consultation

A public consultation on the evaluation and review of the ePD took place between April-July 2016.

The public consultation included backward and forward-looking questions on the need for the ePD on the relationship and compatibility with the GDPR, simplification and continuing need for ePD provisions, delimitation of the scope, accessing data stored in users' equipment, online tracking, unsolicited communications and institutional and enforcement aspects.

Other information gathering activities

Consultation on the initiative also include the following activities with the aim to gather additional information and stakeholder views: (1) academic workshops, (2) targeted workshop with key stakeholders, (3) outreach to the European Parliament, (4) cooperation with the Joint Research Centre (**JRC**), the European Union Agency for Network and Information Security (**ENISA)** the Body of European Regulators of Electronic Communications (**BEREC**) and EUROPOL, (5) online or otherwise direct engagement with stakeholders.

Will an Implementation plan be established?

Yes

[1] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

D. Information on the Impact Assessment Process

- The REFIT evaluation started in the first half of 2016. The results of the public consultation and the past and planned studies are crucial for the evaluation.
- The IA work started in the first half of 2016. It builds on the results of the public consultation and of the planned and past studies.
- The Inter-Service Group was set up in February 2016 with DG CNECT, JUST, HOME, ENER, MOVE, DIGIT, FISMA, COMM, EAC, EMPL, ENV, REGIO, TRADE, GROW, COMP, ESTAT, RTD, SANTE, TAXUD, JRC, the Legal Service, the EPSC and the SG participating.

E. Preliminary Assessment of Expected Impacts

Likely economic impacts

The review is likely to affect providers of electronic communications, OTTs, app providers, as well as manufacturers of ICTs used in the electronic communications sectors. Strengthening the rights of individuals by way of additional legal requirements or safeguards is in general expected to generate costs for industry, either in terms of implementation or as a loss of economic opportunities. Simplification or added flexibility should instead result in economic benefits. Moreover, higher privacy and personal data protection may nurture further trust and thus lead to more widespread use of ICT with overall positive results for market and users.

Likely social impacts

By legislating on the confidentiality and security of electronic communications, the review of the ePD is bound to have a clear social impact. Respect for confidentiality of communications is an essential pre-condition for exercising other fundamental rights having a significant social component, such as human dignity, personal data protection, freedom of thought, conscience and religion, freedom of expression, the freedom of association and non-discrimination.

Likely environmental impacts

No specific or major impact on the environment is expected.

Likely impacts on simplification and/or administrative burden

Simplification and administrative burden on relevant operators will be looked at in each option in all the policy fields. Improving the current procedural requirements (e.g. on cooperation between the Member States) may reduce the administrative burden for them.

Likely impacts on SMEs

Under the new initiative, SMEs should continue to be able to provide their services freely throughout Europe and benefit from enhanced legal certainty. If rules on privacy and confidentiality are simplified, especially in the field of online tracking, this may have a positive impact on small Internet companies.

Likely impacts on competitiveness and innovation

Extending the scope of the ePD to online platforms providing OTT communication services may help to establish a level playing field in the market for electronic communications services. Moreover, the simplification of certain requirements may spur competitiveness of European industry.

As explained above, the ePD aims to be technologically neutral. Consequently, it should not unduly interfere with future technological innovation. Some stakeholders claim that strict privacy rules may have an effect on innovation, e.g. inhibiting the development of certain technologies which are considered as privacy intrusive while others state that regulatory constraints may encourage creative solutions and eventually create competitive advantages for market players that can provide privacy friendly solutions to common challenges. Thus, if properly crafted it may result in economic benefits. Furthermore, privacy protection may increase trust and users acceptance ICT.

Likely impacts on public administrations

If the level of regulation changes in one or more fields covered by the ePD, this would directly affect the tasks of the national regulators. As the objective of the initiatives is to clarify and simplify the legal framework, this would in general facilitate the tasks and work of the public administrations in Member States, including the regulators. Public administrations may be affected if the review of the ePD revisits the allocation of competence at national level. Apart from the above, this Directive does not impose any substantive obligation upon public administrations which will be out of the substantive scope of the legal instrument.

Likely impacts on third countries, international trade or investment

The options are unlikely to significantly affect international trade or investment other than the benefits (cost saving, easier legal environment) that would derive from a revised instrument.