



Brussels, 10.1.2017
SWD(2017) 6 final

COMMISSION STAFF WORKING DOCUMENT

Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC ("the ePrivacy Regulation")

{COM(2017) 10 final}
{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}

EXECUTIVE SUMMARY

The ePrivacy Directive (2002/58/EC) sets forth rules guaranteeing the protection of privacy in the electronic communications sector. It aims to ensure that the protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life enshrined in Article 7 of the EU Charter of Fundamental Rights, is guaranteed.

The ePrivacy Directive requires providers of electronic communications services such as internet Access and fixed and mobile telephony to:

- (1) take appropriate measures safeguarding the security of electronic communications services (specific objective);
- (2) ensure confidentiality of communications and related traffic data in public networks (specific objective).

The Directive also provides protection for users and subscribers¹ of electronic communications services against unsolicited communications.

In 2015 the Commission considered it necessary to assess whether the rules of the ePrivacy Directive have achieved their main objectives, namely ensuring an adequate protection of privacy and confidentiality of communications in the EU, and whether these rules are still fit for purpose in the regulatory and technological context. The Regulatory Fitness and Performance (REFIT²) evaluation assessed the Directive against a number of indicators pursuant to the Better Regulation guidelines, namely: effectiveness, efficiency, relevance, coherence and EU added-value. The Commission also sought scope for simplification of the rules, whenever appropriate, without undermining the objectives of the ePrivacy Directive.

The evaluation covers the whole EU and the period from 2009 to 2016. The assessment is based on evidence gathered by a public consultation, a Eurobarometer, structured dialogues, external studies, monitoring reports, policy documents of the Commission and other relevant literature. Robust economic data to support the assessment have been difficult to find. Statistics and other quantitative data on the compliance costs stemming from the ePrivacy Directive either do not exist, or are not disclosed by the entities subject to the obligations. To corroborate the findings of the evaluation, the evaluation process has therefore built on the sources mentioned before.

Findings

The provisions of the Directive remain fully **relevant** to meet the objectives of ensuring privacy and confidentiality of communications but some of its rules are no longer fit for purpose in light of technological and market developments and changes in the legal framework. This is the case for the rules on security and notification of personal data breaches which are entirely mirrored in the General Data Protection Regulation adopted in April 2016,

¹ This ensures the application of the Directive not only to information related to natural persons but also to information related legal persons.

² COM(2012) 746, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Regulatory Fitness, 12.12.2012.

making them redundant. As regards confidentiality of communications, the rules have achieved their objectives vis-à-vis providers of electronic communication services, but have failed to ensure an adequate protection of citizens when they use 'Over-the-Top services' (e.g. voice over IP or instant messaging), given that the Directive does not apply to such services. This regulatory asymmetry has placed electronic communication service providers at a competitive disadvantage *vis-à-vis* these new players and led to varying degrees of protection according to the means of communications used.

Overall, the Directive appears to have provided an appropriate framework for protecting privacy and confidentiality of communications in the EU; but a series of issues were encountered with respect to its **effectiveness**.

The practical application and enforcement of the principles (e.g. confidentiality of communications and of terminal equipment) set forth in the Directive has proven to be challenging in a number of ways. A majority of Member States have established multiple authorities competent for the ePrivacy Directive, sometimes with overlapping competences, thereby creating confusion as to which body is responsible for enforcement. The evaluation also found that the application of the consent rules on the confidentiality of terminal equipment³, often referred to as the "cookie rule" and aimed at empowering individuals, has not been fully effective. Citizens are presented with requests to accept tracking cookies without understanding their meaning because of complex language and in some cases, are even exposed to cookies being set without their consent. Furthermore, the consent rule has been assessed as being over-inclusive, as it also applies to non-privacy intrusive practices such as first party analytic cookies, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. In the context of unsolicited commercial communications the sheer number of complaints from citizens indicates that the rules may not deliver its intended goals.

As regards the **efficiency**, it is necessary to acknowledge the difficulty to obtain reliable and representative quantitative data. The majority of stakeholders consulted were not able to estimate relevant figures for the provisions of the Directive such as for example the costs related to the requirement to set up security measures and the requirement to place cookie banners (to collect consent). According to the supporting study to this REFIT, it appears that the compliance costs would be around EUR 658 per business⁴.

The evaluation found no evidence of major inconsistencies between the Directive and the other relevant EU piece of legislation with which it interacts. However, a series of redundancies have been identified in particular with the General Data Protection Regulation (e.g. the security rule). Finally, the evaluation concludes that the ePrivacy has **EU added-value** as it imposes harmonised provisions on confidentiality of communications and traffic data which, in the light of an increasingly transnational electronic communications market, are becoming ever more important.

Lastly, based on the fact that the quantitative evidence remain scarce, the evaluation also shows that an effective system for monitoring the application of the Directive is currently lacking and should be put in place in the future.

³ These rules require users' consent for using technologies such as cookies to store or access information on smart devices.

⁴ SMART study 2016/080, Final Report, p 206.