EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 4 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

{COM(2017) 10 final}
{SWD(2017) 3 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

A. Need for action

What is the problem and why is it a problem?

The Impact Assessment has been carried out in parallel to the ex post evaluation of the ePrivacy Directive (ePD) under the Regulatory Fitness and Performance Programme (REFIT).

The overall conclusion is that the ePD objectives are still relevant.

The REFIT evaluation has led to the identification of three main sets of problems:

- Citizens' private life when communicating online is not sufficiently and effectively protected;
- Citizens are not effectively protected against unsolicited marketing;
- Businesses face obstacles created by fragmented legislation and differing legal interpretations across Member States as well as unclear and outdated provisions.

The REFIT evaluation concluded also that there is scope for simplification, specifically with regard to the existence of some outdated or unnecessary provisions and the rules on enforcement.

This is also supported by a REFIT Platform opinion which recommends strengthening the protection of citizen's private life through an alignment of the ePrivacy Directive with the General Data Protection Regulation, that exceptions to the 'consent' rule for cookies are added and that the Commission addresses national implementation problems.

What should be achieved?

The specific objectives of the review are to:

1. Ensure effective confidentiality of electronic communications;
2. Ensure effective protection against unsolicited commercial communications;
3. Enhancing harmonisation and simplifying/updating the legal framework.

What is the added value of action at the EU level?

As electronic communications, especially those based on Internet protocols, have a global reach, the dimension of the problem goes well beyond the territory of single Member States. National rules on confidentiality of communications differ widely on scope and content. Whilst it is therefore possible for Member States to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of common EU rules and would create restrictions on cross-border flows of personal data related to the use of electronic communications services to other Member States that do not meet the same data protection standards.

The upcoming revision of the ePrivacy Directive is deemed to comply with both subsidiarity and proportionality by preserving the harmonization approach and cooperation mechanism, while allowing Member States to take national derogatory measures for specific legitimate purposes.

B. Solutions

What are the various options to achieve the objectives? Is there a preferred option or not? If not why?

The options are grouped according to their level of growing ambition (i.e. option 1 is the least ambitious and option 4 is the most ambitious) in relation to the achieving of the above objectives (privacy and simplification). Option 5 considers the repeal of the ePD.

1. **Option 1: Non-legislative ("soft law") measures**: it includes guidance provided by the Commission, encouragement of self-regulatory initiatives and other soft-law measures

2. **Option 2: Limited reinforcement of privacy/confidentiality and harmonisation**: provides for a minimum reinforcement of privacy/confidentiality rights (by clarifying the scope of the ePrivacy instrument covers OTTs, publicly available Wi-Fi and IoT devices) and protection against unsolicited calls (clarifying the current rules and imposing a standard prefix) and simplification (repeal of security provisions, reinforcing cooperation in cross-border cases)

3. **Option 3: Measured reinforcement of privacy/confidentiality and harmonisation**: provides for a more significant reinforcement of privacy/confidentiality rights (extension of the scope, enhanced transparency of privacy settings, greater transparency, reinforcing enforcement powers) protection against unsolicited communications (introducing opt-in for marketing calls) and simplification (broadening the exceptions, further repealing of unnecessary provisions and streamlining enforcement by entrusting powers to the authorities responsible for enforcement of the GDPR and extending the GDPR consistency mechanism).

4. **Option 4: Far reaching reinforcement of privacy/confidentiality and harmonisation:** provides for more far-reaching measures in addition to Option 3, such as a general prohibition of "cookie walls", the repeal of the exception of previous business relationship for email and SMS marketing, additional repeals and Commission's implementing powers.

5. **Option 5: Repeal of the ePD**: provides for the repeal of the ePD and ensuing applicability of the GDPR, including the enforcement system, for protecting confidentiality of personal data relating to electronic communications; the generalised application of an opt-out system for unsolicited communications and application of the GDPR consistency mechanism.

What are the different stakeholders? Who support which option?

- **Citizens** rights are affected by the level of protection of the confidentiality of their communications. They would favour options reinforcing their rights, such as Option 2, 3 and 4.
- **National authorities and the EDPS** would support options leading to greater and more consistent privacy protection such as Options 2, 3 and 4.
- **Electronic communications providers** are the main addressees of the ePD obligations. They would strongly favour Option 5. As a second best, they might accept options 2 and 3 that ensure that competing OTTs become subject to the same rules.
- **Over-the-Top** providers would also favour Option 1 and 5, as they would normally prefer not to be subject to more stringent regulatory requirements. Option 3 would be the most acceptable after these two, given the margin of flexibility that it ensures.
- **Website publishers and OBA operators** would clearly prefer Option 5 for the same reasons of ECS and OTTs.
- **Browsers providers** would be subject to specific responsibilities under Option 3. They would therefore not support Option 3 and 4.
- **SMEs** would generally support Option 1 and 5. If they are ECS, they would support Option 2 and 3 for the level playing field with OTTs If they are OTTs, they would prefer options 1 and 5, with Option 3 being the most acceptable after these.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise of main ones)?

The preferred option is Option 3. The main benefits are:

- Enhancing protection of confidentiality by means of a technologically neutral definition, enhanced user's control and transparency requirements and more effective enforcement.
- Enhancing protection against unsolicited communications, thanks to the introduction of the opt-in for marketing calls, the introduction of a prefix and the consequent banning of anonymous marketing calls and the enchanced possibilities to block calls from unwanted numbers.
- Simplification through harmonisation and clarification of the regulatory environment, thanks to the reduction in the margin of manoeuvre left to Member States, the repeal of outdated provisions and the broadening of the exceptions to the consent rules.

What are the costs of the preferred option (if any, otherwise of main ones)?

The preferred option is expected to deliver savings as a result of additional harmonisation and simplification. For instance, savings of up to 70% of costs related to eprivacy have been calculated through a centralised management of privacy choices once for all websites and applications.

At the level of specific categories of stakeholders, **OTT players** would have to incur some costs for reviding the legality of their business models. However, such costs are not expected to be significant. **Website publishers** may incur some small adaptation costs. **Browsers and providers of similar applications enabling access to the Internet** would have to incur significant costs for ensuring that users are presented with the appropriate choices regarding their privacy settings. **Marketers** would incur some costs following the introduction of opt-in for marketing calls.

Will there be significant impacts on national budgets and administration?

The main impacts on national budgets and administration would derive from the implementation of the consistency mechanism and the possible need to re-allocate enforcement competences to DPAs only. The impact is not considered to be major, as the synergies with already existing EU coordination bodies (e.g. in the field of data protection) might be exploited.

Will there be other significant impacts?

No

Proportionality?

The preferred option include balanced measures, all deemed necessary to achieve the objectives at stake without imposing excessive burden on the relevant stakeholders. Moreover, the measures are flexibly designed, to allow for the necessary exceptions, and technologically neutral to minimise distortion on competition and ensure a level playing field.

D. Follow up

When will the policy be reviewed?

Continuous monitoring will be ensured, inter alia, through a reporting from Member States to the Commission and from the Commission to the European Parliament, the Council and the Economic and Social Committee.