



Brussels, 12.9.2018  
SWD(2018) 409 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**  
**on preventing the dissemination of terrorist content online**

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

## Executive Summary Sheet

Impact assessment on preventing the dissemination of terrorist content online

### A. Need for action

#### Why? What is the problem being addressed?

The proliferation of terrorist content online continues to be a strong and urgent societal and political concern. Despite a number of non-regulatory measures, online hosting services continue to be used for the dissemination of terrorist content.

#### What is this initiative expected to achieve?

This initiative aims to achieve greater trust in the online environment in the Digital Single Market by limiting the availability of terrorist content online, whilst ensuring a high level of security for EU citizens. Specifically, it aims to increase the effectiveness of measures to detect and remove terrorist content, while increasing transparency and accountability of hosting service providers. The measure also aims to improve the ability of relevant authorities to intervene against terrorist content online, and to safeguard against the risk of erroneous removal of legal content, and the appropriate protection of fundamental rights.

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

Most online platforms operate across borders and enable the access to content regardless of where the users or the providers of information are located. Member States have legislated in the field of removal of illegal content online, but the need to ensure public security at national level has to be balanced with the fundamental freedom of provision of services and freedom of establishment under single market rules.

A patchy framework of national rules is appearing or risks to increase, which would jeopardise an effective exercise of the freedom of establishment and the freedom to provider services in the EU, while also limiting the effectiveness of the fight against terrorist content online, as they would lead to increased compliance costs for businesses.

Member State action alone cannot effectively address the challenge of limiting availability of illegal content online, given the nature of the services in question, and the emerging fragmentation of the internal market.

### B. Solutions

#### What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

The Impact Assessment considered three options in addition to the baseline, reflecting a similar intervention logic with different degrees of intensity in terms of effectiveness and impact on fundamental rights. The building blocks for the options include:

Provisions to **harmonise the procedures for removal or disabling access to terrorist content** following a removal order from a national authority. To enable the procedures, harmonisation further includes a **common definition of terrorist content online** (different definitions considered under the three options), as well as clarity concerning **judicial redress** available to hosting service providers and content providers against removal orders (common to all options).

Provisions to ensure **transparent processes and reporting** to authorities and the Commission (similar across the options), would increase the accountability and trust in the content moderation process, and would support policy-makers and national authorities in combatting terrorist content, in addition to allowing users to better understand how hosting service providers apply their content management policies.

**Cooperation across national authorities and Europol** (to different intensities across options) would improve their ability to act collectively against terrorist content, avoiding duplication, and would reduce complexity and costs on hosting service providers in interacting with national authorities when offering their services cross-border.

In addition, provisions to ensure that, in those cases where companies are exposed to terrorist content, the hosting service providers put in place **appropriate and proportionate measures to proactively detect terrorist content** (different requirements across options).

**Safeguards** (common to all options) and provisions to ensure that measures taken to detect and remove terrorist content do not lead to erroneous removal of legal content and comply with fundamental rights.

Provisions **to ensure that measures are enforceable** (common to all options), including the establishment of legal representatives for non-EU companies, establishing points of contact and ensuring Member States have a coherent set of sanctions in place.

The report presents a combination of the measures assessed as most effective in tackling terrorist content online. It also presents an evaluation of the advantages of different building blocks in terms of effectiveness.

The Impact Assessment concludes that including measures such as a comprehensive definition of terrorist content, requirements to remove content flagged through removal orders within one hour, to assess referrals from both Europol and Member States, as well as requirements for hosting service providers exposed to terrorist content to take proactive measures to detect new terrorist content and prevent re-upload of known material, as well as a robust set of safeguards against erroneous removal of legal content and transparency obligations would be more effective in achieving the policy objectives.

#### **Who supports which option?**

Hosting service providers are generally supporting the baseline option, they consider the full effects of non-regulatory efforts should be evaluated first. If a legal instrument is adopted, they then support a targeted intervention on specific issues of particular public value.

Member States acknowledge the need for further supporting measures (i.e. continued development of the baseline) and support an intervention targeting terrorist content. Member States highlighted in particular the necessity to have a common definition of terrorist content, requirements for action upon referrals, proactive measures as well as transparency and measures facilitating that removed content is accessible for law enforcement purposes. The European Council called upon the Commission 'to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts.

Civil society representing digital rights and academia have shown support to the evolution of the baseline. They have advised caution on some components included in the regulatory options, in particular with regards proactive measures and effects on fundamental rights. Individuals shared these concerns in their responses to the public consultation; a representative sample of citizens responding to a dedicated Eurobarometer supported additional measures at EU level against illegal content online.

### **C. Costs and Benefits of the Preferred Option**

This Impact Assessment details costs and benefits for the measures included under each option. The assessment concludes that option 3 is most effective. The policy option would significantly contribute to achieving the policy objectives and bring most benefit in relation to the scale and scope of the problem. While the third option is expected to have the highest economic impact in relation to expected costs and additional administrative burden, it would also bring the highest benefits.

### **D. Follow up**

#### **When will the policy be reviewed?**

A detailed programme of monitoring the outputs, results and impacts of the legislation will be established in order to inform the evaluation. The monitoring will be based primarily on information from Member States gathered by the competent authorities during the course of their duties complemented by publicly available transparency reports. Other data, in particular on proactive measures, will be provided by hosting service providers as part of their reporting obligations. This monitoring will in all options be complemented by research to better understand the spread of illegal content online, as well as tracking the technological evolution concerning automated tools for illegal content removals.