



EUROPEAN COMMISSION  
SECRETARIAT-GENERAL

Deputy Secretary-General - Policy Coordination

Brussels,

**Subject: Encryption and law enforcement**

Excellency,

In the July 2020 Security Union Strategy, the Commission committed to explore and support balanced technical, operational and legal solutions to the challenges posed by encryption, which include how to maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism. In the Organised Crime Strategy adopted on 14 April 2021, the Commission has laid out its intention to: *“suggest a way forward in 2022 to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions that shall be based on a thorough mapping of how Member States deal with encryption together with a multi-stakeholder process to explore and assess the concrete options (legal, ethical and technical).”*

The Council resolution “Security through encryption and security despite encryption” of December 2020 also underlined *“the need to develop a regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communication could be further assessed”*.

Encryption is essential to the digital world, securing digital systems and transactions and also protecting a series of fundamental rights, including freedom of expression, privacy and data protection. However, the use of encryption also allows criminals to mask their identity and hides the content of their communications. Therefore, we would like to understand better the challenges encryption raises for law enforcement and judicial authorities, as well as the challenges the access to encrypted content may entail for fundamental rights and cybersecurity. Building on the work already undertaken by the Commission and its agencies, as well as the Member States, the Commission would like to explore further the current practices used by the Member States and understand where they may have identified deficiencies.



Therefore, the Commission plans to carry out a mapping of Member States' legal framework and case law that is applicable to law enforcement access to encrypted information, as well as Member States' operational practices and needs, with a view to identifying and focusing on areas where EU action could be relevant.

In order to launch this process, we would like to invite Member States to a meeting to discuss the objectives and methodology for the above-mentioned mapping exercise, as well as to explore how this process could be organised.

The meeting will be organised virtually and will take place on 25 May from 15:00 to 17:00, chaired by the Secretariat-General, with the participation of relevant Directors from DGs HOME, CNECT, JUST and the Joint Research Centre.

We expect the meeting to look at the topic of encryption and access by law enforcement and judicial authorities from two perspectives: of ensuring that EU and Member States' laws, including criminal laws, apply online as they do offline and can be enforced in practice; and of ensuring cybersecurity and fundamental rights, including freedom of expression privacy and data protection, as well as fair trial guarantees. We would appreciate your help in securing the participation of relevant actors from your Member State. Given the different angles to be addressed, the Commission proposes inclusion of all relevant expertise with participation from capitals as well as from your Permanent Representation. We would be grateful if you could send us up to three names of colleagues who will represent your Member State by 17 May 2021 to the email address [REDACTED]. You could also use this email address for any inquiries that you may have.

Participants will be sent a web link to join the meeting in due course.

Yours faithfully,

Elisabeth WERNER