Council of the European Union

Brussels, 12 May 2021
(OR. en)

8519/21

LIMITE

JAI 545
COSI 97
CATS 36
ENFOPOL 191
COPEN 228
DATAPROTECT 128
CYBER 145
IXIM 86

NOTE

From:	Presidency
To:	Delegations
Subject:	Next steps on Encryption

Encryption is essential to the digital world, securing digital systems and transactions and protecting a series of fundamental rights, including freedom of expression, privacy, and data protection[1]. However, if used for criminal purposes, it masks the identity of criminals and hides the content of their communications.

Under the German Presidency of the Council of the European Union (Council), Member States adopted the **Council Conclusions on Internal Security and European Police Partnership**[2], recognising that encryption is an anchor of confidence in digitalisation and should be promoted and developed.

1 Commission Communication on the EU Security Union Strategy, COM(2020) 605 final, 24.7.2020; Commission Communication on the First Progress Report on the EU Security Union Strategy, COM(2020) 797 final, 9.12.2020.

2 13083/1/20 REV 1

Furthermore, through the **Council Resolution on Encryption**[3], the European Union (EU) reinforces the need for security through encryption and security despite encryption and fully supports the development, implementation and use of strong encryption. At the same time, the EU needs to ensure the ability of law enforcement and judicial authorities to exercise their lawful powers, both online and offline.

The Council also calls for an active discussion with the technology industry and the development of an appropriate regulatory framework that would allow national authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communications. Furthermore, the Council calls for the improvement of the coordination of the efforts of Member States and European Union institutions and bodies.

In December 2020, the German Presidency presented a document outlining a set of initial measures, as a **way forward on encryption**[4]**,** and a call for all Member States, Commission, and other EU institutions, to combine efforts to jointly develop targeted technical and operational solutions, built on the principles of legality, necessity and proportionality, in close consultation with service providers and relevant authorities.

Later, as announced in the **Counter-Terrorism Agenda**[5], the Commission has committed to working with the Member States to identify technical, operational and legal solutions to ensure lawful access to encrypted data while maintaining the effectiveness of encryption in protecting privacy and security of communications.

In the recently adopted **EU Strategy to tackle Organised Crime**[6], the Commission underlines, in line with the Council, the importance of ensuring lawful access to encrypted information, while maintaining the effectiveness of encryption in protecting privacy and security of communications. Furthermore, the Commission states that it will steer the process to analyse, with the relevant stakeholders, the existing capabilities and approaches for lawful and targeted access to encrypted information in criminal investigations and prosecutions.

---

3 13084/1/20 REV 1

4 13550/20

5 Commission Communication on A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM (2020) 795 final, 9.12.2020.

6 8085/21

Consequently, it is necessary to make law enforcement and the judicial autorithies fit for the digital age. Serious organised crime and terrorist attacks are planned, executed and concealed online, illegal substances and products are marketed, and criminals are finding subtle ways to launder profits unhindered by physical borders. Fast developing technologies amplify the scale of the problem.

Therefore, both the Council and the Commission acknowledge the need to review the effects arising from different relevant regulatory frameworks, to develop a further consistent regulatory framework across the EU that would allow competent authorities to continue to carry out their operational tasks.

It is underlined that the EU could leverage the strength of its single market to ensure that device manufacturers and service providers create technologies that meet the Member States' needs while preserving the benefits of encryption.

It is important to carefully balance the interests of protecting privacy, fundamental rights and security of communications through encryption, whilst upholding the ability of competent authorities in the area of security and criminal justice, to continue to access lawfully relevant data for legitimate, and clearly defined, purposes in fighting serious organised crime and terrorism in the future, across the physical and digital domains.

As stated in the **EU Strategy to tackle Organised Crime,** the Commission will suggest a way forward in 2022, based among other things on a mapping of how Member States deal with encryption to assess the concrete options from legal, ethical and technical perspectives.

Acknowledging the pertinence in obtaining a clear and comprehensive picture to assess the next steps on encryption, the Presidency, in close collaboration with the past German and incoming Slovenian Presidencies, considers that cooperation between the Commission and the COSI community is crucial for an integrated and holistic approach in this important process.

Noting the relevance of encryption to the activities of law enforcement and judicial authorities, reinforcing the European Area of Freedom, Security and Justice, and, at the same time, the preservation of fundamental rights of the citizens, the Presidency **calls on Member States to support and contribute to the Commission's efforts in the process of identifying options for the way forward on encryption**.

Recognising the Commission's role as a relevant stakeholder and a co-driver alongside the Member States, the Presidency **invites the Commission to regularly inform delegations about possible next steps on encryption.**