Council of the European Union

Brussels, 21 October 2020
(OR. en)

12143/20

LIMITE

JAI 851
COSI 156
CATS 73
ENFOPOL 256
COPEN 287
DATAPROTECT 106
CYBER 198
IXIM 107

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council Declaration on Encryption - Security through encryption and security despite encryption

Further to the informal VTC of the members of the Standing Committee on Operational Cooperation on Internal Security (COSI) on 23 September 2020, delegations will find in the Annex a Draft Council Declaration on Encryption.

The draft Declaration is based on the Presidency discussion paper submitted to COSI (10728/20) and the written contributions received by delegations (WK 11169/20). It also takes into account the joint paper of the COM services presented by DG Home and DG Just (10730/20), as well as the contribution of the EU CTC (7675/20).

Delegations are invited to submit to written comments and concrete drafting suggestions on the Draft Council Declaration set out in the Annex before 29 October 2020 (COB) to paul.gaitzsch@diplo.de; COSI.DE2020@bmi.bund.de and cosi@consilium.europa.eu

ANNEX

Draft Council Declaration on Encryption

Security through encryption and security despite encryption

1. Preamble: Security through encryption and security despite encryption

The European Union fully supports the development, implementation and use of strong encryption. Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society. At the same time, the European Union needs to preserve the ability of law enforcement and judicial authorities to exercise their lawful powers, both online and offline.

According to the European Council conclusions, 1-2 October 2020, EUCO 13/20 *the EU will leverage its tools and regulatory powers to help shape global rules and standards.* It was agreed to use funds under the Recovery and Resilience Facility to advance objectives such as *enhancing the EU's ability to protect itself against cyber threats, to provide for a secure communication environment, especially through quantum encryption, and to ensure access to data for judicial and law enforcement purposes.*

2. Current use/state of encryption

In today's world, encryption technology is increasingly used in all areas of public and private life. This is a means to protect governments, civil society, citizens and industry by ensuring the privacy and security of communications and personal data: all parties benefit from a high-performance encryption technology. Encryption has been identified by EU data protection authorities as an important tool contributing for instance to the protection of personal data transferred outside of the EU against (disproportionate) government access, which according to the Court of Justice is a legal requirement for data transfers[1]. Not only is the user data on electronic devices encrypted, but more and more communication channels are also secured by end-to-end (E2E) encryption. The majority of instant messaging apps on online platforms have equally implemented end-to-end encryption.

[1] Judgment of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

3. Challenges for ensuring public safety

The "digital life" is a source not only of great opportunities, but also of considerable challenges: the digitalisation of modern societies brings with it certain vulnerabilities and the potential for abuse in cyberspace. Thus criminals can make use of readily available, off-the-shelf encryption solutions conceived for legitimate purposes, including as part of their *modi operandi*[2].

At the same time law enforcement is increasingly dependent on access to electronic evidence to fight effectively terrorism, organised crime, child sexual abuse, particularly its online aspects or any cyber-enabled crime and bring criminals to justice.

In practice, there are instances where encryption application renders analysis of the content of communications in the framework of access to electronic evidence extremely challenging.

Independently of the technological environment of the day, it is therefore essential to preserve the powers of law enforcement and judicial authorities through lawful access to carry out their tasks, as prescribed and authorised by law. Such laws providing for the enforcement powers must always fully respect due process and other safeguards, as well as other freedoms and rights, in particular the right to respect for private life and communications and the right to the protection of personal data.

4. Creating a balance

The principle of security through encryption and security despite encryption must be upheld in its entirety. The European Union continues to support strong encryption. Encryption is an anchor of confidence in digitalisation and should be promoted and developed.

Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for law enforcement and judicial authorities to lawfully access relevant data for legitimate, clearly defined purposes of fighting serious crimes, in the digital world, are extremely important. Any actions taken have to balance these interests carefully.

[2] iOCTA 2020, p. 25

5. Joining forces with the tech industry

Moving forward, the European Union strives to establish an active discussion with the technology industry to ensure the continued implementation and use of strong encryption technology. Law enforcement and judicial authorities must be able to access data in a lawful and targeted manner, in full respect of fundamental rights and data protection regime, while upholding cybersecurity. Technical solutions for gaining access to encrypted data must match the principles of legality, necessity and proportionality.

Since there is no single way of achieving the set goals, governments and industry need to work together to create this balance.

6. Legal framework

There is a need for a regulatory framework that safeguards fundamental rights and the advantages of end-to-end encryption and which allows law enforcement and judicial authorities to carry out their tasks. Possible solutions may need the support of service providers in a transparent and lawful manner, as well as improving the technical and tactical skills which the law enforcement and judicial authorities need to face the challenges of digitisation at a global scale. In line with the principle of proportionality, such measures should be prioritised.

Developing technical tools aimed at supporting criminal proceedings, could also be considered. Such technical tools should be subject to the principles outlined in this declaration.

7. Innovative investigative capabilities

It is of a paramount importance that this matter is handled in a coordinated way at EU level in order to combine the efforts of all Member States and EU institutions and bodies to define and establish innovative approaches and best practice to respond to these challenges. Technical solutions anchored on the principles of necessity and proportionality should be developed in close consultation with service providers and the relevant authorities, while there should be no single prescribed technical solution to provide access to the encrypted data.