Dear Sir or Madam,

I am contacting you to express my deepest concerns about the envisioned Council Resolution on Encryption[1] that has been published by the Austrian media broadcaster ORF on 3 November 2020.[2]

The draft resolution is to **call for technical solutions that would allow national authorities to break effective and secure end-to-end encryption on private communications** via messaging services. National governments have been asked to submit their input by noon on Thursday, November 12. Subsequently, the Presidency intends to present the text to the Standing Committee on Operational Cooperation on Internal Security (COSI) for endorsement on **November 19, in view of further submission to COREPER II on November 25, followed by adoption by the Council via written procedure.**

There is no such thing as a "balanced" way of breaching the security of online communications. On the contrary, it is technically impossible to grant access to securely encrypted communications solely for "lawful" purposes. As soon as messaging services allow for the decryption of private communications, for instance by implementing backdoors or providing master keys, the security of communications will be broken once and for all – and not only for the 'legitimate' purposes envisioned by the national governments. **Once secure encryption is broken, it will open the door to mass espionage by foreign intelligence services and hacker groups.** Anyone who sacrifices secure encryption in order allow for eavesdropping will destroy the protection of personal secrets, business secrets, and state secrets. As encryption evidently ensures the effective exercise and protection of the freedoms of expression and opinion, any breaching of encryption can have detrimentaleffects on these fundamental rights[3].

As such, contrary to what is argued by the Presidency, **there is no middle-way between upholding "fundamental rights and the digital security of governments, industry and society" and breaking secure end-to-end encryption.**

Therefore, I call on your responsibility as a representative of the public services to **uphold and protect the fundamental right to privacy as well as the security of our digital communications infrastructure** by safeguarding our private communications from interference by third-parties and national authorities and to reject the proposed resolution.

Yours sincerely,

References:

[1] Council of the European Union: "Draft Resolution on Encryption - Security through encryption and security despite encryption", 06 November 2020, availavble at: https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf.

[2] Moechel, Erich: "Auf den Terroranschlag folgt EU-Verschlüsselungsverbot", ORF-Online, 08 November 2020, available at: https://fm4.orf.at/stories/3008930.

[3] Davide Kaye: "Report of the UN-Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye", presented to the United Nations Human Rights Council, Twenty-Ninth Session on 22 May 2015, available at: https://www.undocs.org/A/HRC/29/32.