



MAGNUS BRUNNER
MEMBER OF THE EUROPEAN COMMISSION

Brussels, 11/08/2025

Dear Mr Voge and Ms Lorenzo Perez,

Thank you for your letter regarding ProtectEU - the European Internal Security Strategy, addressed to both Executive Vice-President Virkkunen and myself. We appreciate the collective insight presented by the undersigned civil society organizations, companies, and cybersecurity experts.

The Commission agrees that encryption plays a fundamental role in ensuring robust cybersecurity and the effective protection of fundamental rights, including freedom of expression, privacy and data protection. Hence, I can confirm that the Commission will pursue efforts geared toward enabling a more secure digital realm, based on strong encryption mechanisms.

Moreover, the Commission would like to stress that the fundamental rights to privacy and confidentiality of electronic communications and the right to data protection are guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Directive 2002/58/EC ('ePrivacy Directive') ensures the protection of the right to confidentiality of electronic communications and the users' terminal equipment. In addition, Regulation (EU) 2016/679 ('GDPR') provides a comprehensive framework for the processing of personal data of individuals in the EU. Directive (EU) 2016/680 (LED) complements this framework by setting out the data protection rules applicable to law enforcement authorities processing personal data, such as accessing personal data stored in a user's device, for the purpose of prevention, investigation and prosecution of criminal offenses.

Encryption plays a fundamental role in achieving a strong cybersecurity and effective protection of fundamental rights, such as privacy and data protection. The GDPR and the LED explicitly mention encryption as an effective measure to guarantee the secure processing of personal data.



However, it is equally important not to prejudice the powers of competent authorities to safeguard national security and to prevent, investigate, detect and prosecute criminal offences, in accordance with the procedures, conditions and safeguards set forth by law. As the EU Charter of Fundamental Rights, the GDPR and the LED confirm, the rights to privacy and data protection are not absolute and can be subject to limitations to meet an objective of general interest, such as fighting crime, providing that these limitations are necessary and proportionate, provided for by law, and respect the essence of those rights.

Directive (EU) 2018/1722 ('EECC') in recital 97 states that the use of encryption and end-to-end encryption, where appropriate, should be promoted, and where necessary be mandatory. This use is in accordance with the principles of cybersecurity and privacy by default and by design. It must also be implemented without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences. Against that background, the Commission is committed to act to ensure that the EU and its Member States can protect their citizen in full respect of all fundamental rights.

As announced in the ProtectEU Strategy, and more recently, in the Roadmap for lawful and effective access to data for law enforcement, the Commission will task an expert group to provide support in preparing a Technology Roadmap on encryption. The group will identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, while safeguarding cybersecurity and fundamental rights. The group will include experts in law enforcement, cybersecurity, encryption, communication technologies, standardisation and fundamental rights, who will be selected following an open call.

Yours faithfully,



Magnus Brunner