EN
E-005634/2020
Answer given by Mr Hahn
on behalf of the European Commission
(8.4.2021)

IT security of the telecommunication infrastructure used by the Commission and the Executive Agencies (EAs) is assessed recurrently in line with the IT security policy (Commission Decision (EU, Euratom) 2017/46[1], its implementing rules and the corresponding IT security standards). This includes preventive security controls and cryptographic means for securing sensitive information in transit. For exchanging sensitive information, the Commission uses secure communication lines (e.g. the Trans European Services for Telematics between Administrations (TESTA) network). The security posture of other agencies and bodies is monitored by the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU)[2].

IT security standards apply to all telecommunication and information systems managed by the Commission. In particular, for encryption, the standard on 'Cryptography and Public Key Infrastructure' and the standard on 'Transport Layer Security (TLS)' apply.

Data produced by the Commission and the EAs are protected in accordance with the applicable policies and regulations, including Commission's information security policy, IT security policy and personal data protection regulation. Data is stored in the Commission-owned data centres or, in case those policies permit it, also in the sites operated by third party service providers. Cooperation with third service providers is managed and monitored through contractual agreements that specify the conditions to be respected when storing or processing data owned by the Commission or the EAs. One of those conditions is that storage/processing shall take place within the EU.

[1] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

[2] CERT-EU, in close liaison with the decentralised agencies, conducts regular vulnerability checks and alerts these entities about vulnerabilities and the necessity to patch them whenever required. It also proactively monitors the threat landscape for malicious exploitation technologies which support teleworking (e.g. videoconferencing, virtual private networks, etc.). As required, CERT-EU releases advisories and alerts to help the decentralised agencies secure these technologies or inform the related IT security risk management activities. In addition, it produces guidance, shares best practices and, when applicable, assists with the proper configuration of these technologies.