Subject: Enforcement of new GDPR rules

The fifth Internet Organised Crime Threat Assessment (IOCTA) issued by Europol on 18 September 2018 states that ‘Hacked companies would rather pay a smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by their competent authority’.

Europol also warns that, if such companies negotiate with cybercriminals, they ‘will only fund further attacks and other criminal activity’ and that the organisation at risk has no guarantee that ‘the attacker will not disclose or otherwise exploit the information’.

Is the Commission looking into this report issued by Europol?

Will the Commission take action to prevent the circumvention of General Data Protection Regulation (GDPR) rules through the criminal activity explained by Europol?

Answer given by Mr Avramopoulos on behalf of the European Commission
(5 March 2019)

The Commission is well aware of threat assessment reports by Europol, including the Internet Organised Crime Threat Assessment (IOCTA), which provide useful input to identify gaps, needs and set policy priorities. Based on surveys, these reports are addressed to law enforcement authorities. The IOCTA takes into account input from stakeholders such as private partners and academia. Looking at possible future criminal threats, stakeholders hypothetically indicated that ‘it may be that the hacked companies would rather pay’ a ransom for non-disclosure of a data breach than be subject to fines under the General Data Protection Regulation (GDPR).

The GDPR contributes to making companies more resilient against cyber-attacks and increases cybersecurity by preventing personal data breaches before they occur, including by requiring that appropriate technical and organisational measures be implemented. Such breaches must be promptly notified to data protection authorities in order to address them in an appropriate and timely manner, thus reducing possible damage. When deciding on administrative fines, such authorities shall take into account inter alia how the breach came to their knowledge and the degree of cooperation. The GDPR thus discourages cooperating with hackers.

Europol has been working on investigations, prevention and remediation on ransomware for some time and is a founding member of the ‘No More Ransom’ initiative, which informs about the dangers of ransomware and helps victims recover their data. Available in 35 languages, the platform gathers more than 130 public and private partners and contains more than 60 free decryption tools. Since its launch in 2016, more than 72 000 victims have been able to decrypt their affected devices thanks to these tools.