European Council agrees new far-reaching terrorist content Regulation: technically impossible for cloud infrastructure providers to implement

Brussels, 06/12/2018 **– CISPE, the alliance of Cloud Infrastructure Services Providers in Europe, describes the European Council's proposal as "technically unworkable and targeting the wrong actors". CISPE is urging the European Parliament to clarify the proposed rules and to make them fit for purpose and consistent with the GDPR privacy protections enacted barely six months ago.**

The Regulation will obligate cloud infrastructure providers to proactively scan, filter and remove data, covering all enterprise and government data running across cloud infrastructure services. CISPE maintains this cannot be the intention of the legislator and so this needs to be clarified in the Regulation, which targets the wrong players. It is technically impossible for cloud infrastructure to deliver what is requested.

"CISPE companies already co-operate fully with the authorities in fighting terrorist content," says Alban Schmutz, CISPE Chairman and VP Strategic Development & Public Affairs, OVH. "The rules adopted today are designed for online content sharing services like social media and content sharing platforms that can access, monitor data and content made available by their end-users. Even if the automated proactive measures (Article 6) contemplated in the Regulation were to be developed in the future, they would require cloud infrastructure providers to proactively 'snoop' on all customers - imposing blanket scanning, filtering and data removal obligations".

CISPE urges European legislators to clarify the scope of the Regulation to include rules that are clear, workable and proportionate, and do not put the entire cloud infrastructure sector in Europe at risk.

Contact: to speak to CISPE or a member please email cispe@europa-insights.com or call +32 2 502 65 80

Notes to Editors: Unlike the filtering 'hashing recognition' technology used by social, video, image or audio sharing platforms, which creates a digital fingerprint of content that must be already identified (and made available to the public at least once) so the same content is not re-uploaded in another platform, cloud infrastructure providers are **not technically able** to use such technology since they do not have visibility or access over the content.

About CISPE: The association is open to all companies, no matter where they are headquartered, provided they declare that at least one of their cloud infrastructure services meets the requirements of the CISPE Data Protection

Code of Conduct. The CISPE Code of Conduct already has more than 100 services declared, provided by 30+ cloud enterprises headquartered in more than 15 EU Member States and used by millions of businesses across Europe.

CISPE Executive Board https://cispe.cloud/board-of-directors/

Cloud Computing Services declared under CISPE Code of Conduct https://cispe.cloud/publicregister/