CISPE.cloud

CISPE highlights unintended impact of the EU Terrorist Content Online Regulation

Online businesses and public services could be shut down without warning, with dire consequences for European citizens and organisations

[Brussels: Wednesday, 13 November] Following an event on ‘Fighting Terrorist Propaganda Online’ today in the European Parliament, Alban Schmutz, Chair of the association of Cloud Infrastructure Service Providers in Europe (CISPE), warned that failing to remove cloud infrastructure providers from the scope of the final EU Terrorist Content Online Takedown Regulation could have serious unintended consequences for the industry, other businesses, and consumers.

The regulation, which targets the ‘takedown’ of terrorist content posted online within an hour, is now being finalised in trilogue negotiations between the European Commission, the European Parliament, and the Council. Despite recognition in some quarters that CISPE members were inadvertently included in the scope of the original Commission draft, which primarily targets online platforms, no clear commitment to addressing the issue has been agreed in trilogue negotiations so far.

Speaking after the event on ‘Fighting Terrorism Content Online’, Alban Schmutz said:
“Imagine how people, public services and businesses would be impacted if cloud infrastructure services were legally required to shut down access to whole online platforms on which they have come to rely.

Europe’s cloud infrastructure service providers are being asked to do the impossible. Unlike platforms, they cannot access the data and content controlled by our customer and have no general control or access to what specific content is placed online.”

Asking our members to remove a single piece of data posted to an online platform, therefore, is like asking a power company to turn off a single light bulb in an apartment without shutting down the entire apartment block or city.”

To provide examples of some of the potentially unforeseen impacts of including cloud infrastructure providers in the scope of the regulation, CISPE has produced a series of three short animated videos[1] that illustrate potential scenarios impacting their customers and the end-users.

Alban Schmutz added that he remains hopeful however that these scenarios can be avoided, saying: *“We are very grateful for the constructive discussions that we have had with representatives of the European Commission, European Parliament and some Member States throughout this process, including during today’s event. I believe that there is a recognition from many stakeholders in the negotiation that cloud infrastructure providers are the wrong target for this regulation.*

“Our industry, and those that are reliant upon the services we provide, now need the European Institutions to provide absolute clarity during the trilogue negotiations that this Regulation is not intended to include CISPE members.”

-More information-

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.

For more information, please contact:
Rory Douglas Home
rory.douglashome@heklacomms.com
+32 493791528

[1] https://cispe.cloud/wrongplayer/