By mail & electronically

H.E. Mr President Jean-Claude JUNCKER

European Commission Avenue de la Loi, 200
1049 – Brussels

Brussels, November 30, 2018

Cc:
Vice-President Andrus ANSIP
Vice-President Jyrki KATAINEN
Commissioner Elzbieta BIENKOWSKA
Commissioner Mariya GABRIEL
Commissioner Vera JOUROVA
Commissioner Julian KING

Dear President Juncker,

It is vitally important that the Commission helps Member States to address the terrorist threat – but the current Regulation on terrorist content online is targeting the wrong players.

As the alliance of cloud infrastructure service providers in Europe, we would like to highlight our serious concerns regarding the European Commission's Regulation to prevent the dissemination of terrorist content online. We are particularly concerned with the imposition of obligatory measures to proactively monitoring and filtering of content which is *asking cloud infrastructure providers to do the impossible*: snooping on all of their customers including large industrial concerns, governments and protected professionals (such as doctors and lawyers) and guessing - in each file - what could be terrorist content or not.

We urge the Commission to exclude cloud infrastructure providers from the scope of the Regulation.

Cloud infrastructure providers are not social media or video sharing platforms
The intended scope of the Regulation is online content sharing services such as social media and video sharing providers, and not infrastructure providers. CISPE members provide the underlying IT infrastructure. This is analogous to the power cables or water pipes in the ground that provide the essential but somewhat workmanlike services for a city and, more importantly, to its many buildings, businesses, public services and citizens.

It is not technically possible for cloud infrastructure providers to comply
While social media and video platforms may monitor the content made available by their users, it is technically not possible for cloud infrastructure providers to access the data and content that is controlled by their customers. The infrastructure providers have no general control and no access to what content is placed online, how content is made available to the public, and to whom it is made available. Most social media sites, video and other online content sharing services *do* have control down to the most granular piece of content that is made available by users on the platform: they have technical means to delete an individual comment and image, or target an individual. Cloud infrastructure providers cannot do this.

Cloud infrastructure service providers cannot even distinguish between what is "a piece of content" what is not "a piece of content". To take down a specific comment or image, for example, the infrastructure provider may need to take down an entire website or service, closing down access for related services and so affecting a large number of other innocent businesses or users. This is like asking the power company to turn off a single light bulb in a single apartment without shutting down power to the entire apartment block or city.

Imposing automated proactive measures to monitor and prevent uploads would mean 'snooping' on all content

It is unthinkable for the proposed law to result in the automated monitoring of the data of public institutions (e.g. national governments, hospitals, law enforcement bodies, the EU Commission or Parliament) and corporate bodies (e.g. lawyers, doctors, companies, banks, insurance) that use cloud infrastructure and do not typically make content publicly available. For many large industrial customers, who perhaps build trains, design aircraft or manage power plants, this could undermine the security of their operations and erode trust in the service. Indeed, if technical measures to prevent the upload of content were to be developed in the future, their application would contradict the Constitutions of a majority of Member States, since such proactive measures can be considered as hampering free speech.

The Regulation puts the SME community at risk

The Regulation would have a serious impact on all cloud infrastructure providers – not least as it is technically impossible to meet the requirements – including an immediate and notable impact on cloud infrastructure service providers that are SMEs. Such an effect would contradict ongoing strategy and efforts by EU institutions to support SMEs as the "backbone" of Europe's economy. SMEs could simply not afford the level of investment the Regulation will require if passed (and, once again, bearing in mind that effective implementation would not be technically possible). The Regulation creates huge barriers to enter the market that would be an issue for European SMEs.

Please make things right, don't rush in legal loopholes

We understand the tremendous pressure to deliver an agreement on this Regulation proposal adopted by the Commission in mid-September, ahead of the forthcoming elections. However, this means the proposed Regulation is being rushed through EU legislative procedures, with numerous attempts to plug legal loopholes resulting in ambiguous language being added.

We need clarity, not contradictory opinions or good intentions

Cloud infrastructure services providers require legal clarity in the form of binding provision, rather than ambiguous language and non-binding recitals, that (try to but not really) excludes cloud infrastructure providers from the scope of this Regulation. It should also be made clear that the regulation is targeting 'end-users' and not 'third parties' (In the context of cloud infrastructure, third parties refer to any customer of the cloud infrastructure provider, for instance a bank or government body).

On the eve of the elections with many prominent political contenders extolling the liberal values of the European Union, its vibrant democracy, individual liberties and freedom of speech, it cannot be that a Regulation at the Eleventh Hour brings to a halt some of the protections and freedoms created by the General Data Protection Regulation (GDPR) only six months ago, on a *malentendu*.

Together with our members, we remain available to work with your services to clarify the scope of the Regulation. We also reiterate our unwavering support for the EU's ambition to crack down on terrorist and other illegal content, and will continue to work diligently with law enforcement agencies.

Alban SCHMUTZ
CISPE, Chairman

Francisco MINGORANCE
CISPE, Secretary General

CISPE.cloud

Supporting organizations representing cloud infrastructure providers: