Brussels, September 21, 2020

Dear representatives of the Council of the EU, the European Parliament and the European Commission,

Firstly, we hope that you and your families are in good health and coping with the challenging circumstances. The undersigned organisations are writing to you ahead of the fourth 'trilogue' meeting on the **Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online.** We have followed the Regulation closely since its initial proposal in September 2018 and fully support the objective of the EU institutions to counter terrorism and incitement to violence. Throughout the process we have provided input to ensure that the legislation meets its objectives while at the same time safeguarding fundamental rights and a productive business environment. Based on the latest state of negotiations[1], we would like to draw your attention to the following core concerns:

1) Clear scope of the Regulation

The scope of the Regulation should be restricted to companies relevant for the Regulation's objective. These are platforms that facilitate dissemination of content to the public at the direct request of the content provider and have the ability to remove discrete pieces of content. Accordingly, it should exclude cloud services, DNS services, and internet access providers, as it is technically impossible for these service providers to remove pieces of content. Equally, services that facilitate interpersonal communication and exchange of information within a limited group of people (private messaging, email services, videoconferences, etc.) should be excluded, in order to protect users from interference with private communications. We consider the draft compromise set out in Section 14 of the above mentioned document to be a good basis for further discussion, and stress that additional clarifications remain necessary.

2) Targeted and clear definition of terrorist content

We have previously argued that the definition of terrorist content should clearly and explicitly exclude content published for journalistic, educational, research, artistic or other lawful purposes. To ensure consistency and clarity, the definition should be based on the exclusive list of terrorist offences mentioned in Articles 3 and 4 of Directive (EU) 2017/541[2] and target content that is shared with the intent to cause such offences to be committed. A clear and targeted definition is crucial to avoid overbroad restriction of lawful content. This was also one of the issues raised by three UN Special Rapporteurs in their position on the draft Regulation[3].

[1] https://www.politico.eu/wp-content/uploads/2020/03/SKM_C45820030612100.pdf
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541
[3] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234

3) Competent authorities

It is of utmost importance that competent authorities empowered to issue legally binding removal orders are designated as independent from the government. Independence of competent authorities is a fundamental pillar of societies governed by the rule of law, and essential to safeguarding fundamental rights. We would also recommend that Member States appoint one single competent authority. This would enable service providers to authenticate removal orders and execute them efficiently. We have supported the European Parliament's position on this issue.

4) Removal orders and the one-hour deadline

We recommend that removal orders should be issued by competent authorities in the Member State in which the service provider is established. A competent authority in another Member State should notify the competent authority of the Member State in which the service provider is established and request a removal order to be issued. Moreover, we have previously argued[4] that the one-hour deadline should be replaced with more flexible wording. Laws that impose heavy penalties, if short and fixed turnaround times are not met, will have troubling implications for free expression and will lead to overblocking. The Regulation should also take into account the capabilities and characteristics of the many different types of service providers covered by the Regulation. This would avoid imposing disproportionately burdensome obligations on SMEs and start-ups which would face significant technical and financial obstacles to implementing a 1-hour response capability. The Regulation should not force companies to prioritise speed of removal where decisions require more careful consideration.

5) Proactive measures

We have expressed serious concerns about the draft provisions on proactive measures. This is because of the risk that they result in widespread mandatory use of filtering technologies. While automated tools play an important role in online content moderation at scale, they cannot be relied on[5] to understand the context in which content is shared. This means they capture legitimate content shared by e.g. journalists and human rights defenders[6]. Therefore, indiscriminate use of these tools could have potentially serious consequences for free expression and access to information. Moreover, it is important to stress that proactive measures should be compatible with the 'E-Commerce Directive'[7] and the prohibition on general monitoring obligations for hosting service providers.

---

[4] https://cdt.org/wp-content/uploads/2019/04/2019-04-15-Joint-Letter-TerReg-plenary-17-4.pdf
[5] https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf
[6] https://www.witness.org/witness-and-partners-push-back-against-eu-regulation-that-threatens-online-free-expression/
[7] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

6) Law enforcement disclosure

Companies are committed to assisting law enforcement, pursuant to due process and appropriate oversight. We are concerned that new referral obligations impede existing practices, in particular for companies that already voluntarily refer information where there are imminent threats to life. It also puts service providers in an untenable position of assessing information for criminal evidentiary value. Finally, the text is at odds with the European Commission's 'e-Evidence' proposals[8]. These are intended to create a harmonised, efficient and fundamental rights-protective framework for law enforcement authorities to obtain electronic data from service providers. The Regulation should be amended to ensure that companies are not required to disclose user data without appropriate judicial oversight.

We thank you for considering these points and remain at your disposal for any questions or comments you may have.

Yours sincerely,

Allied For Startups
Bitkom
BVDW e.V. - German Association for the Digital Economy
CCIA - Computer and Communications Industry Association
Center for Democracy & Technology
Confederation of Industry of the Czech Republic
DIGITALEUROPE
Digital Infrastructure association NL (DINL)
eco - Association of the Internet Industries
EDiMA
EuroISPA - European Internet Services Providers Association
Finnish Federation for Communications and Teleinformatics FiCom
ISFE - Interactive Software Federation of Europe
NLdigital
Polish Confederation Lewiatan
Startup Poland
Technology Ireland
ZIPSEE - Cyfrowa Polska

[8] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108(COD)&l=en
https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0107(COD)&l=en


ALLIED
FOR
STARTUPS


bitkom


BVDW


Computer & Communications
Industry Association
Tech Advocacy Since 1972


CENTER FOR
DEMOCRACY
& TECHNOLOGY


CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC


DIGITALEUROPE


Digital Infrastructure
Association Netherlands


eco


EDiMA


EuroISPA


FiCom
FINNISH FEDERATION FOR
COMMUNICATIONS AND
TELEINFORMATICS FiCom ry


EUROPE'S
VIDEO GAMES
INDUSTRY


NL digital


LEWIATAN


STARTUP
POLAND


Technology
Ireland
Ibec


CYFROWA
POLSKA