Ref. Ares(2023)781918 - 02/02/2023

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate D – Internal Security
**D.4 – Security in the Digital Age**

Brussels
HOME.D.4/

Michele Sciurba
sciurba@gmvv.eu

Dear Dr Sciurba, Dear Ms Schuster,

Thank you for your e-mail received on 22 December 2022 which was addressed to President Von Der Leyen and President Metsola concerning EU legislation to combat child sexual abuse online. They have asked us to respond on their behalf.

Taking action to combat child sexual abuse, offline and online, as well as guaranteeing the right to privacy and confidentiality of all users, are priorities for the Commission, as highlighted in the EU Strategy for a more effective fight against child sexual abuse (hereafter "the Strategy") adopted on 24 July 2020.

The Commission is well aware that the confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life guaranteed in the Charter of Fundamental Rights of the EU and Directive 2002/58/EC (the ePrivacy Directive). Mechanisms to detect child sexual abuse in communications interfere with these fundamental rights and that is the reason why the proposal for a regulation laying down rules to prevent and combat child sexual abuse (hereinafter, the 'Proposal') focusses first and foremost on prevention. It imposes on all providers of services at risk of misuse for the purpose of online child sexual abuse an obligation to assess such a risk and to take mitigating measures. It is only when these mitigating measures fail to reduce the risk of online child sexual abuse on a specific service sufficiently that a judge or independent administrative authority will be required to assess whether issuing a targeted detection order would be necessary and proportionate in the specific case. In other words, detection orders are a measure of last resort under the Proposal and they must be as limited as possible in time and scope, to ensure their compliance with requirements set by Article 52(1) of the EU Charter.

The involvement of a judge or independent administrative authority is meant precisely to ensure respect for the rights to privacy and data protection of users in the context of detection. This essential guarantee is compounded by a series of further safeguards that are triggered if a judicial or administrative detection order is issued. Amongst others, the Proposal ensures that, to detect online child sexual abuse, providers compulsorily have to use the list of indicators kept by the EU Centre only. This guarantees that the detection technology run on the service cannot collect any further knowledge or information besides the existence of a match between the content detected, on the one hand, and one of the indicators, on the other hand.

Moreover, the Proposal ensures that data protection authorities are involved at the stage of the assessment of detection technologies and at the stage of implementation of individual detection orders. The processing of personal data is governed by the General Data Protection Regulation (GDPR).

It is important to note that the Proposal establishes a decentralised EU Agency, the EU Centre to prevent and counter child sexual abuse, which is intended to act as a filter and identify any false-positives before they reach law enforcement. Such a filter is not present today: in the current situation, voluntary detection is performed by providers on their own initiative (rather than based on a judicial or independent administrative determination) and can lead to direct reports being sent to law enforcement.

Finally, the Proposal does not intend to undermine end-to-end encryption in the EU. On the contrary, it explicitly recognizes that the use of end-to-end encryption technologies is an important tool to guarantee the security and confidentiality of the communications of users, including those of children (Recital 26). Detection is not incompatible with end-to-end encryption. More importantly, the proposal caters for and encourages technological evolution, so that security and confidentiality of communications, as well as online child safety, are both increasingly protected. In this respect, it is important to note that, under the Proposal, orders can only be issued when available technologies exist to enable effective detection on the specific type of service concerned without entailing a disproportionate interference with the privacy of electronic communications. In other words, if there is an actual technical incompatibility between detection and a specific service, no detection order can be issued.

In conclusion, I assure you that the proposed legislation is aiming to ensure full respect of the rights to privacy and data protection of all users, including children, whose right to privacy is grossly violated in the images and videos depicting their abuse that circulate online. The proposed legislation pursues a balanced approach that is limited to what is strictly necessary and proportionate, in compliance with the ePrivacy Directive, the GDPR and the Charter of Fundamental Rights of the European Union and the case law of the European Court of Justice. The safeguards which are provided will ensure the full respect of all fundamental rights and case law, considering that child sexual abuse is a heinous crime that has serious life-long consequences for victims.

Yours faithfully,

[E-Signed]
Cathrin BAUER-BULST
Head of Unit