FINLAND

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

We have serious concerns on the possible negative impact that CSA-proposal might have on the confidentiality of communications, including on the use of end-to-end encryption in electronic communication services. So far, this has remained unclear. Considering the importance of encryption to confidentiality of communications (respect for private or family life), freedom of speech, high level of data protection as well as cybersecurity, this Regulation's impact on end-to-end encryption should not remain unsatisfactorily ambiguous.

In the digital world, encryption of communication is central, as it secures digital systems on the one hand and protects privacy and personal data of the users on the other. Finland draws attention to the fact that the proposal's restrictions on strong encryption of electronic communications must not endanger cyber security or the security of communication and information systems. We are concerned about the impacts of the proposal on the use of strong encryption, which is an essential tool to guarantee trust in the online environment. In particular, we are worried that this proposal might lead to undermining the security of communication systems and services, and any backdoors for justified purposes could potentially be abused by malicious third parties.

We consider that more information should be obtained about the technical and organizational means behind the detection order during the negotiations. We encourage the Presidency/Commission to provide more information about measures and technologies that would not undermine use of encryption and would not jeopardize security of information services and systems, but that would help fight CSAM online. Finland believes that service providers must also have responsibilities in creating a safer online environment, and we would emphasis to place the responsibility on the providers.

Finland still has several reservations regarding Article 7 of the proposal. The proposal should be examined in more detail in relation to the Charter of Fundamental Rights of the EU in the negotiations. While existing case law of the ECJ does not include cases where the challenged legislation would be identical with the proposed regulation, there is already a series of judgments of relevance, as regards the general requirements applied to limiting fundamental rights under Article 52 of the Charter, including strict necessity and proportionality of the limitations on the relevant rights. See, in particular, Grand Chamber judgment of 8 April 2014, Digital Rights Ireland, in joined cases Joined Cases C- 293/12 and C- 594/12, and Grand Chamber judgment 21 December 2016, Tele2 Sverige AB, in Joined Cases C-203/15 and C-698/15 , as well as judgment of 6 October 2020, La Quadrature du Net and Others, C- 511/18, C- 512/18 and C- 520/18. Depending on the impact of the regulation on the confidentiality of communications, it seems there is also an apparent conflict with the Finnish Constitution.

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

Yes, FI supports exploring measures that could allow voluntary detection measures also in the future. The need for which the Temporary Regulation was drafted has not disappeared, and if the basis for voluntary detection measures is repealed, this would lead to the inconsistent requirements and processing in the EU, based on each member state's national legislation – exactly the reason why the Temporary Regulation exists.

FI is in favour of including the provisions of the Temporary Regulation to the CSA proposal – for example in connection with art. 4 risk mitigation measures. Voluntary measures could be implemented e.g. in cases, where the risk assessment indicates that there is a need for such detection. Also provision of voluntary measures should fully comply with the general requirements for limitation of fundamental rights, thus not only providing for a legal basis of processing but setting out the rules under which the voluntary measures may be taken.

The impacts of both voluntary and mandatory detection processes being in place at the same time must still be assessed. However, as the detection order is meant to be used only as the last resort, this should not lead to significant legal uncertainty – less intrusive measures must be exhausted before detection order could be issued. Also the aim of protecting children would support allowing voluntary measures to be implemented without waiting for the possibly lengthy process of issuing the detection order. Voluntary processing should be taken into account as a part of risk assessment and risk mitigation measures. Voluntary measures should not be as intrusive as mandatory detection measures.

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

The definitions of criminal offences should not be extended in substance in this Regulation from those defined in Directive 2011/93. We would therefore exclude amending to CSAM definition to audio communications in this Regulation.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

FI supports the approach of the proposal that various service providers would assess their services and the risks related to their use, and that the service providers are encouraged to address these identified risks. These mitigation measures should be the primary measure to intervene in case of high risk services.

Firstly, we welcome that number-based services have been excluded from the scope of interpersonal communications. However, we still have reservations regarding the scope of Article 7 and its impact on the privacy and confidentiality of communications. The proposed regulation (Article 7) concludes that the detection order should be limited to what is "strictly necessary". Nevertheless, taking into consideration the vagueness of the key terms in Article 7 (e.g. "significant risk") and still open questions about technology, it remains unclear that the application of Article 7 together with Article 10 would not de facto result in a general monitoring obligation of private communications. In this respect, we have serious doubts regarding some elements of the detection order. These particularly relate to detecting new CSAM and solicitation of children. First, while it is clear that the proposed legislation has a legitimate aim, it is not clear how it is ensured that the means included in the proposed legislation for detecting new CSAM and solicitation of children is proportionate to the aim pursued. Also, we have some questions as to whether the detection order, in all respects, necessarily constitute an effective means to prevent CSAM. For instance, has the Commission analysed in the impact assessment, whether and to what extent there could be risks that criminals increasingly would start using other means not targeted by the Regulation, as knowledge of the new legislation spreads? It is also unclear to us to what extent other available measures that interfere less with fundamental rights have been taken into account in the impact assessment of the proposal.

While FI supports the goal of improving the protection of children against these particularly heinous crimes, the proposed regulation raises some unprecedented questions about general monitoring of confidential communications whose effect are not limited to this proposal. These questions should be very carefully and thoroughly scrutinized and the obligations imposed under this regulation have to be targeted both in text and in practice, ie. when these rules are actually applied.