Stellungnahme zur Initiative der Europäischen Kommission für eine Verlängerung der Ausnahmeregelung zur Datenschutzrichtlinie für elektronische Kommunikation

The German Digital Opportunities Foundation welcomes the European Commission's initiative to extend the existing temporary derogation from specific provisions of Directive 2002/58/EC to open up the possibility for combating child sexual abuse after August 3, 2024 for further two years. The current report of the European Commission[1] on the implementation of Regulation (EU) 2021/1232 on the temporary derogations reveals "that voluntary reporting contributed significantly to the protection of a large number of children" (see page 33). With regard to decisions of the European Parliament and the European Council on the duration of the designated extension we highly encourage all European legislative bodies to strive for a solution in the upcoming trilogue that opens up an appropriate window of opportunity to ensure a long-term regulation aimed to protect children from sexual abuse online.

The EC's report mentioned above shows that in 2022 8.9 million corresponding content items or accounts were identified by providers (see page 7-8). Given that 6.6 million of the reports in 2022 were submitted by Meta their announcement in December 2023[2] of implementing end-to-end encryption by default gives rise to the assumption that the number of reports then will decrease significantly although child sexual abuse will at least stay on the same level or even increase more.

The designated extension of the temporary derogation until August 3, 2026 will provide the opportunity to address more thoroughly so far highly discordant issues of the European Commission's proposal to combat and prevent child sexual abuse online. This time should be used efficiently to overcome seemingly insuperable positions, e.g. regards detection in encrypted environments or privacy preserving age verification. The draft regulation proposed by the EC combines measures to prevent and combat child sexual abuse while balancing fundamental rights of children as well as all users. Efforts to strive for measures and policies, which are commonly accepted are worthwhile.

Many MS and other stakeholders refuse detection in encrypted digital environments due to the assumption that this might open a backdoor which might be unlawfully exploited by criminals or unauthorized persons. Against this backdrop it seems obvious to invest in research and development to address these legitimate concerns and find better solutions. For example, a locked backdoor in an encrypted service, which could be opened only for a single purpose with a special key that is kept safe from unwarranted usage, e.g. through different players to store the key and to permit controlled usage which shall be logged for transparency reasons. Concerns in regard of potential breaches to such a backdoor should be addressed appropriately but not prevent us from striving for solutions to keep children safe also in encrypted environments.

Age assurance is the silver bullet to create safe spaces online for children and to allow respective freedoms for adults. Knowledge of the age range a user belongs to is essential to provide them with age-appropriate functionalities and settings and where applicable, with precautionary measures and support. In such a secure environment, the need for issuing a detection order would be significantly reduced. Nevertheless, the known methods of age verification are often devalued due to their intrusiveness through the collection of biometric and/or personal data, a potentially inaccurate age

[1] European Commission (2023): Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of numberindependent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. 19.12.2023. COM(2023) 797 final. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2023:797:FIN (11.01.2023)

[2] Meta (2023): Launching Default End-to-End Encryption on Messenger. 6.12.2023. https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ (11.01.2023)

estimation or their possible circumvention through a false self-declaration of age. It therefore seems necessary and obvious to further develop tools that fulfil essential requirements such as guaranteeing the anonymity of the user and preventing their Internet activities or history from being linked to a specific person.

Assuming such tools can be brought to market maturity within the next two years, this would create conditions for a future-proof regulation to combat child sexual abuse online.