# Intervention by the EDPS in the meeting of the Law Enforcement Working Party, Council, 19 January 2023

**Europa Building, Rue de la Loi 167, 1048 Brussels, meeting room S7 (7th floor)**

**19 January 2023, 14.30**

## Purpose of event

- **Presentation of EDPB/EDPS Joint Opinion 4/2022** on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse **by the EDPS (10 to 15 minutes)** and

- Exchange of views (answering to questions from delegations)

## Link to Strategy / Management Plan / Other relevant document/event:

***Case File:*** ***2022-1224 Invitation to the Council's Law Enforcement Working Party, Brussels, 19/01/2023***

***Joint Opinion:***
***https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf***

***Opinion on the temporary derogation:***
***https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en***

***Last briefing on CSAM:*** ***Briefing_Shadows CSAM***

## Speaking Points (Active)

### *Introduction*

- Thank you for the invitation and for the opportunity to present the joint EDPB-EDPS Opinion on this highly important topic.

The proposal to combat CSAM is particularly close to my heart, mainly for two reasons:

- On the one hand, I am a father of two minors, daughters. This legislative proposal has made it clear to me that we, as a society, obviously have a problem that we cannot close our eyes to and which urges us to act.
- On the other hand, the outcome of this legislative process will decisively determine how free and secure we Europeans will be in using communication technology in the future.

- As commendable as it is that the proposal has drawn the attention of Europe and the world to child sexual abuse and its depiction, the question remains whether the chosen strategy to combat it is the right one.
- The European Data Protection Board, i.e. the heads of the data protection supervisory authorities in Europe, together with the EDPS, gave a unanimous answer to this question and set it down in Joint Opinion 4/2022 of July last year. **In short, we do not believe that the approach chosen by the Commission is fully compatible with European fundamental rights,** and I will come to that in a minute.

*Disclaimer:*

- Please bear in mind that the EDPB-EDPS Joint Opinion is a consensual work of 31 independent supervisory authorities, focusing on high-level comments on the main issues within our specific data protection expertise.

*Relevant CJEU case law*

- When analysing the Proposal, the EDPS and EDPB took care to carefully consider the jurisprudence of the European Court of Justice. Since there have been no comparable encroachments on the confidentiality of communications so far, we had to orientate ourselves mainly on the Court's extensive case law on data retention.

- Two key words from that jurisprudence are "general and indiscriminate". According to the Court's jurisprudence, **general and indiscriminate retention** of traffic and location data, **even for combatting serious crime** is **not compatible** with Article 7 of the Charter of Fundamental Rights.

- Another important element in the Court's case law is that measures permitting public authorities to have access on a generalised basis to the **content of a communication** are more likely to affect the **essence** of the rights guaranteed in Articles 7 and 8 of the Charter.

- Both elements are highly relevant also with respect to measures for the detection of CSAM and solicitation of children, like the measures envisaged by the Proposal.

*Are detection orders targeted?*

- According to the Explantory Memorandum, the Commission's proposal aims to provide for a system of **"targeted" detection** orders. The EDPS and EDPB consider, however, that the proposed conditions for the issuance of a detection order will still lead to detection orders with a very broad scope in practice.

- Indeed, the **Proposal does not set clear 'limits, on the basis of objective and non-discriminatory factors'**, as the Court required in its data retention jurisprudence for traffic and location data[1]. Instead, the Proposal includes a number of general conditions for the issuance of a detection order, but those **conditions still leave a very broad margin of appreciation**, which would lead to considerable **uncertainty on how to balance the rights at stake in each individual case**.

[1] According to the CJEU, Member States could provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to
- the categories of persons concerned or
- using a geographical criterion,

for a period that is limited in time to what is strictly necessary, but which may be extended

- And while the Proposal also provides for a number of procedural safeguards, I must underline that **procedural safeguards can never fully replace substantive safeguards**.

- The Proposal envisages the involvement of independent authorities and national courts, who are expected to ensure that detection orders remain as targeted as possible. **Without clear and precise substantive obligations, however, the risk remains that detection orders remain very broad in practice.**

- Another aspect, which I consider as highly problematic, is that in the construction chosen by the Commission, **the provider's own risk management** (or even the provider's willingness or unwillingness to avoid a detection order) could ultimately be decisive for the decision on the encroachment on fundamental rights.

- Under the Proposal, the legislator would effectively delegate his task to regulate to a judge or other independent administrator, who shall be responsible not only to consider the totality of circumstances, but also to balance the interests involved. But as we are mostly dealing with the provider's risk management, the interests involved may not be clearer to the judge than to the legislator. The judge will probably not learn more about the individual children at risk or the individuals using the service. The balancing would have to be very abstract. It would actually be the balancing that would normally be required from the legislator.

- This is an unprecedented level of vagueness and legal uncertainty. While the Proposal certainly tries to make the detection orders look 'targeted', the conclusion of the EDPB and EDPS, however, is that the Proposal **fails to ensure a targeted approach**.

### *Types of detection orders*

- Now I would like to briefly address the three types of detection measures that can be ordered, for

    - known CSAM,



4

- unknown CSAM, and
- grooming.

- In all three types of detection orders, the technologies currently available rely on the automated processing of content data of all affected users. **Given the general conditions for the issuance of a detection order under the Proposal, there is a real risk of general and indiscriminate monitoring for all three types of detection orders.**

- In addition, the EDPS and EDPB consider that the measures envisaged for the detection of unknown child sexual abuse material ('CSAM') and solicitation of children ('grooming') in interpersonal communications are particularly problematic due to their intrusiveness, their probabilistic nature and the error rates associated with such technologies.

- But the fact that the Joint Opinion labels new CSAM and grooming detection as "particularly problematic", should not be interpreted to infer that detection of known material as proposed could be lawful.

- Indeed, the EDPB and EDPS consider that the interference created by the detection orders as proposed would be incompatible with the requirements imposed by the EU Charter of fundamental rights.

### *The role of the EU Centre*

- Before concluding, I would like to briefly reflect upon the role of the EU Centre. The Proposal aims to move, at least in part, the task of dealing with immanent errors of the technology from the providers to the EU Centre. As an old-school administrator, I think this is a good thing.

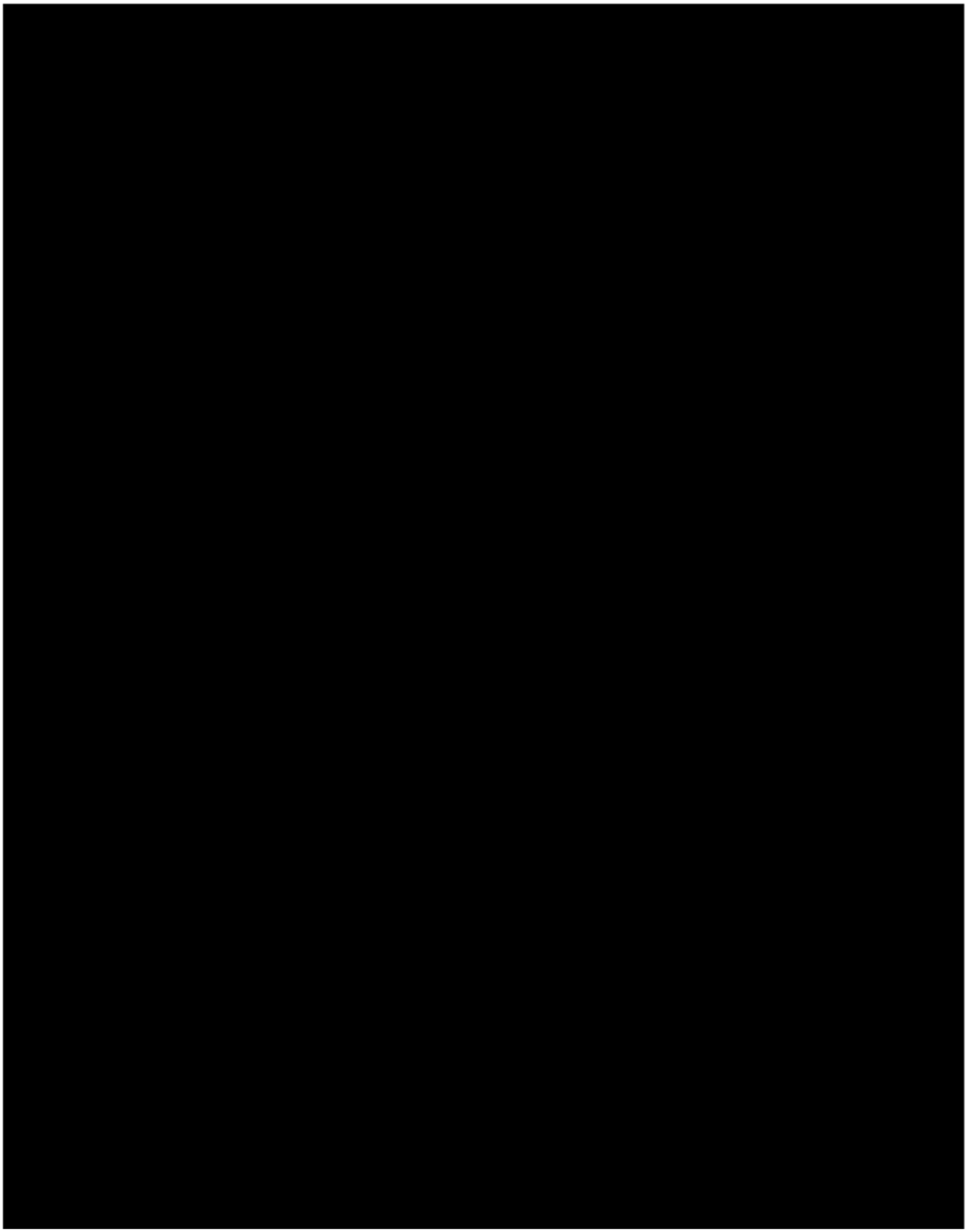
- Moreover, manual sifting of content data is a very significant intrusion into the privacy of communications, that should be executed only by trustworthy staff without a particular interest in the matter and with the necessary knowledge, neutrality and supervision. I do not see such conditions fulfilled by the providers. However, if we install such a neutral, civil authority

to handle false positives and make sure they do not reach law enforcement, then we should also aim at the necessary organisational and technical separation of the centre from Europol.

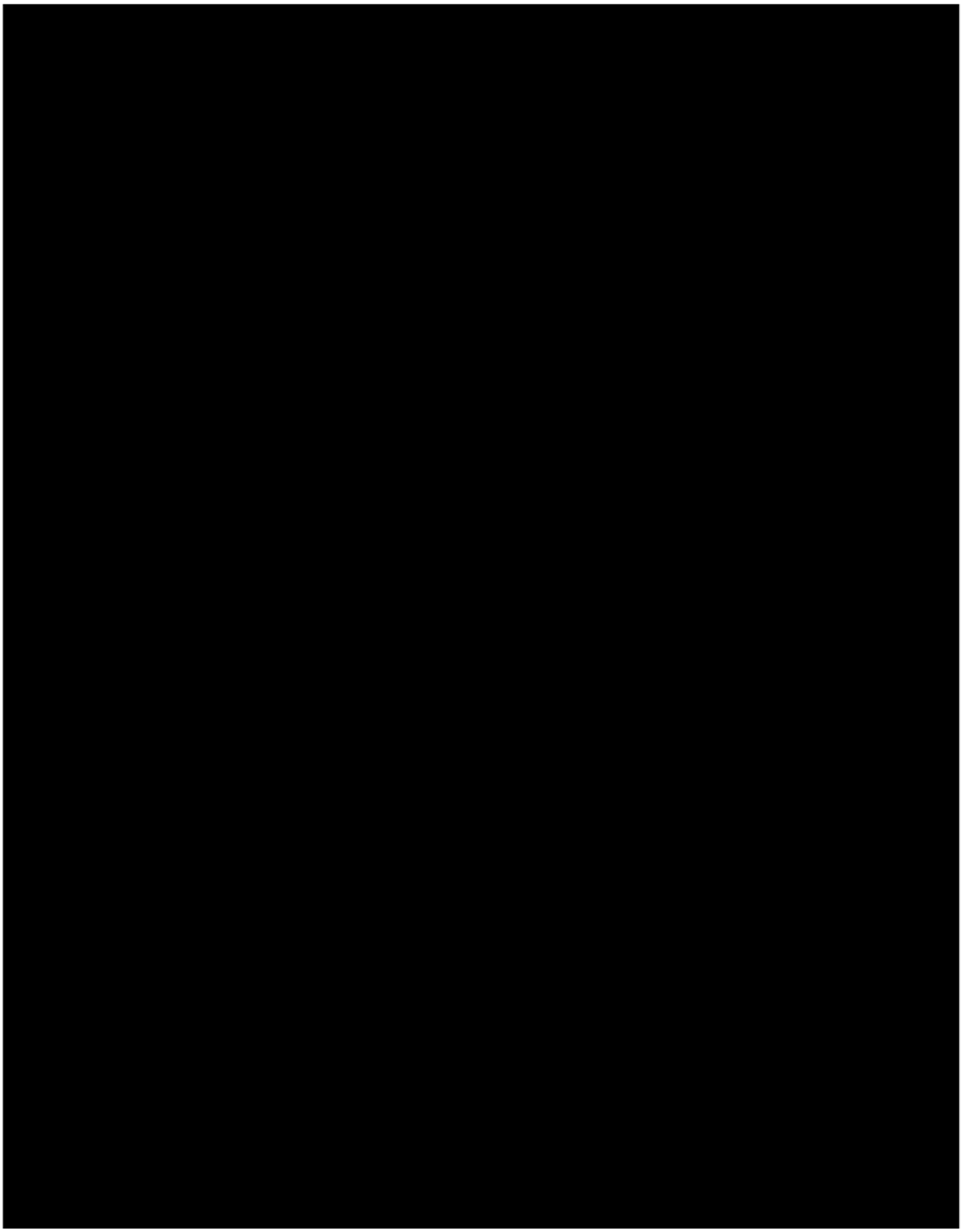
- This concludes my introductory remarks. I am happy to elaborate on aspects in response to your questions.

[redacted]

[redacted]



[3] para. 94.



[redacted]

[redacted]

## Case officer / contact point

[redacted]

[redacted]

## Background

The Presidency has communicated to P&C on 10 January 2023, that the focus of the meeting will be laid on detection orders, as their shape will also determine the tasks of the EU Centre and Europol. The Presidency has mentioned during a preparatory meeting the following questions they find worth exploring:

- No specific crime
- More intrusive than traffic data (or subscriber data)
- Relation between detection order and prohibition of general monitoring DSA
- would it be a solution if the proposal stated clearly that it is not meant to undermine E2E encryption?
- automated analysis, recital 177 of La Quadrature du Net judgment in particular