

From:

To:

EDPS-CABINET

CC:

CONSULT@edps.europa.eu>

Sent at:

01/02/23 17:11:01

Subject:

RE: Possible written questions following the today
Shadow Meeting on the CSA file?

Dear [REDACTED]

Attached please find The European Data Protection Supervisor's answers to the two questions that were raised by the shadows following the meeting on 14 December 2022.

My apologies for the delay.

We have also attached the Supervisor's opening statement during the meeting, for possible circulation.

Best regards,

[REDACTED]



[REDACTED]
Legal Officer – Policy and Consultation Unit

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

 [@EU_EDPS](https://twitter.com/EU_EDPS)  www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]
Sent: 16 January 2023 17:10
To: WIEWIOROWSKI Woiciech <woiciech.wiewiorowski@edps.europa.eu>
Cc: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Subject: RE: Possible written questions following the today Shadow Meeting on the CSA file?

Dear Mr Wiewiorowski,

in the framework of the below request, the LIBE Secretariat received the following two questions:

- *Do you consider it proportionate if non-EU entities, like NCMEC, exchange data with EU authorities? Is the GDPR legal basis for 'public interest' sufficient?*
- *Do you consider current reporting measures like WhatsApp has in place i.e. creating a "screenshot" of the last handful messages when a user complains about certain content, to be proportionate?*

Could you please provide us with a reply by Friday 27 January 2023 at the latest?

Thanks a lot in advance,



[REDACTED] mentary body

European Parliament

Directorate-General for Internal Policies of the Union
Directorate for Citizens' Rights and Constitutional Affairs
Secretariat of the Committee on Civil Liberties,

[REDACTED]
[REDACTED]
[REDACTED]

From: [REDACTED]
Sent: 1 [REDACTED] 2 21:18
To: WIEWIOROWSKI Woiciech <woiciech.wiewiorowski@edps.europa.eu>:
[REDACTED]
[REDACTED]
[REDACTED]

Cc: [REDACTED]
[REDACTED]
[REDACTED]

Subject: Possible written questions following the today Shadow Meeting on the CSA file?

Dear Mr Wiewiorowski,
dear all,

As you are aware, today some technical problems were experienced during the Shadows meeting and some Groups were not able to intervene. The Rapporteur, Mr Zarzalejos, would be grateful if you could accept to answer in written some additional questions from the Shadow Rapporteurs. They will be requested to send a maximum of two informal written questions each in order to address those topics that were not dealt with during today's meeting and to submit them to you, via the LIBE Secretariat, as soon as possible. It would be very much appreciated if you could accept and reply those additional questions by 16 January 2023.

Thanks a lot in advance for your cooperation.



entary body

European Parliament

Directorate-General for Internal Policies of the Union
Directorate for Citizens' Rights and Constitutional
Affairs
Secretariat of the Committee on Civil
Liberties,



Second CSA Shadow meeting

14 December 2022

EDPS Opening Statement

- Thank you for the invitation and for the opportunity to intervene in today's discussion. I very much recognise the importance of this file, of the need to fight child sexual abuse, and to create a safe environment for this to happen. I am myself father to two girls, of 8 and 15 years old, and I strongly defend the need to protect them. At the same time, we must be careful in avoiding putting in danger all other communications, on which extensive debate took place already.
- Because of the importance of this file, and its ability to affect all EU markets and jurisdictions, I am joined today by two colleagues from the EDPB, Luca Tosoni from the Norwegian supervisory authority and Gintare Pazereckaite from the Secretariat to the EDPB, as the Commission had requested a joint Opinion on the Proposal from EDPB and EDPS, recognising its particular importance for the for the protection of individuals' rights and freedoms with regard to the processing of personal data.
- In our Joint Opinion, while understanding the importance of the discussion, as said, the DPAs in the EU we have made clear that scanning of the content of interpersonal communications on the basis of "detection orders" (which, in practice, will be neither individually targeted nor limited to only a selection of service providers) will always be illegal under the Charter of Fundamental Rights (and probably under a number of national constitutional laws as well).
- Indiscriminate access to content also touches on the essence of the fundamental right to privacy (see the Court of Justice judgments in cases such as *Tele2 Sverige* and *Digital Rights Irelands*). When the essence of a fundamental right is affected, it is not possible to remedy it and ensure proportionality by adducing safeguards (substantive or procedural).
- The view of this legal situation, which is quite straightforward in light of the jurisprudence of the Court, is somewhat obscured by the fact that in the Proposal, the detection order comes in the guise of an individual targeted measure. However, the Proposal blurs procedurally the difference between the unknown criminal, the provider as a classical third party and the users of the services of the provider whose fundamental rights are interfered with by the measure. In my

opinion, this is a unique constellation in the law of state coercive measures, and all but typical for targeted measures.

- In fact, this Proposal creates an illusion of legality by introducing numerous procedural "safeguards" which, however, do not fundamentally change the substance, i.e. that it would amount to a generalised access to the content of inter-personal communications of most, if not all, users.
- I admit that the current situation for victims of child sexual abuse requires urgent action. Still, I am convinced that, in order to be successful, this action should not overplay the potential technological solutions, and must not violate the fundamental rights of citizens protected under the Charter and numerous national constitutions.
- Let me also say at the outset that there might be viable measures that would not amount to indiscriminate and generalised access to content to communications which may be worth exploring.



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

Answers by the EDPS
to questions received following the
Shadow Meeting on 14 December 2022
regarding the Proposal for a Regulation laying down rules to
prevent and combat child sexual abuse

1. Question: Do you consider it proportionate if non-EU entities, like NCMEC, exchange data with EU authorities? Is the GDPR legal basis for 'public interest' sufficient?

It is our understanding that some provisions of the Proposal may be construed as to authorizing that EU authorities would exchange personal data with private entities in third countries, such as NCMEC.

The Proposal provides in Article 54 that the EU Centre may 'cooperate' with partner organisations, defined as organisations and networks with information and expertise on matters related to the prevention and combating of online child sexual abuse, including civil society organisations and semi-public organisations. Recital 69 provides two examples for such partner organisations, the US National Centre for Missing and Exploited Children and the International Association of Internet Hotlines ('INHOPE') network of hotlines for reporting child sexual abuse material.

According to Article 51(2)(n) of the Proposal, the EU Centre would be allowed to process personal data as strictly necessary for the purposes of cooperating with Europol and partner organisations in accordance with Articles 53 and 54, including on tasks related to the identification of victims.

However, it is the EDPS's assessment that, as currently drafted, Article 51(2)(n) is not drafted in a sufficiently precise manner to constitute a valid legal basis for the processing of personal data. At the very least, categories of personal data would need to be listed, alongside precise purposes for their processing. As a general rule, such processing could only be permissible in so far it is necessary and proportionate. To the extent international transfers of data would be envisaged, this should be spelled out in the Proposal.

As concerns the example of victim identification provided in the Proposal, I recall that according to Article 48(3) subparagraph 2 of the Proposal the EU Centre would forward cases of confirmed child sexual abuse to Europol for further analysis, if the Centre is

unable to establish a competence of a national law enforcement authority¹, so that Europol would undertake efforts to identify the victim and establish a national law enforcement competence. Recital 71 considers Europol's mandate and its experience in identifying competent national authorities in unclear situation and its database of criminal intelligence which can contribute to identifying links to investigations in other Member States decisive for establishing a close cooperation between the EU Centre and Europol. I can therefore not see a reason for the EU Centre to cooperate with private entities in third countries in order to identify a victim for establishing the competence of an EU law enforcement authority.

I further recall that Article 20 of the Proposal would provide a right to information for the victim regarding any instances where the dissemination of known child sexual abuse material depicting them is reported to the EU Centre pursuant to Article 12, to be exercised at the Coordinating Authority which would then involve the EU Centre. As the EU Centre would only report on instances reported to the EU Centre, there would be no need for international transfers either.

2. Question: Do you consider current reporting measures like WhatsApp has in place i.e. creating a "screenshot" of the last handful messages when a user complains about certain content, to be proportionate?

The reporting functionality enables the recipient to report criminal content of the communication to WhatsApp, which then, after reviewing and confirming child exploitation imagery is concerned, forwards relevant content to NCMEC in accordance with US law².

I note that in the case of WhatsApp, there are always the last five messages sent to the complainant (or a user group) forwarded to WhatsApp. The reporting user has no influence on this mechanism. Whether this constitutes a privacy-friendly design would be for the competent supervisory authority to review. But as a principle, such low-threshold reporting opportunities seem to be a good practice, by far less intrusive than general and indiscriminate monitoring of the communications of all users. We should not forget that a recipient could also make a screenshot of a message and report the message directly to the police, which would be a comparable scenario.

¹ Cf. also recital 71 and Article 45(2)(c) of the Proposal.

² <https://faq.whatsapp.com/5704021823023684>