- **Level of classification:** Classified – for official use only
- **From:** Permanent Representation of Germany to the EU, Brussels
- **To:** Federal Foreign Office
- **Copy to:** BMI (Federal Ministry of the Interior and Community), BMJ (Federal Ministry of Justice), BMWK (Federal Ministry for Economic Affairs and Climate Action), BMDV (Federal Ministry for Digital and Transport), BMFSFJ (Federal Ministry for Family Affairs, Senior Citizens, Women and Youth), BKAMT (Federal Chancellery), BMF (Federal Ministry of Finance)
- **Subject:** Meeting of the European Council's Law Enforcement Working Party (LEWP) (Police) on 19 and 20 January 2023
- **Re.:** Draft CSA Regulation
- **Purpose:** For information
- **Reference:** 350.80/4

1. Summary and assessment

In the first LEWP meeting chaired by the SE Presidency and addressing the CSA Regulation, the European Data Protection Supervisor (EDPS) opened with a brief presentation of the European Data Protection Board (EDPB)-EDPS Joint Opinion of 28 July 2022. He was clearly critical of the draft Regulation. The EDPS was often evasive in his responses to Member States' queries. He made no suggestions on how, to his mind, the Regulation could be organised in a legally compliant manner. Various MS and the COM in particular expressed their disappointment at the statements made by the EDPS. They had expected constructive solutions from the EDPS rather than sweeping criticism.

A round table discussion, initiated by the Chair, on encryption arrangements in the CSA Regulation revealed a divergence of opinion. While some Member States (MS) expressed a preference for a clear statement on the handling of encrypted content to be included in the enacting terms of the Regulation, most MS still had not adopted a definitive position on the matter. The Chair concluded that further discussion on the subject would be necessary. There was still no definitive position on whether and, where appropriate, under what conditions voluntary detection by service providers was expected to be allowed in future, in addition to mandatory detection orders. The Chair indicated that this area would also be subject to further discussion.

The fundamental positions adopted by the MS on audio communication within the scope of the CSA Regulation and on measures in publicly available services and interpersonal communication were also addressed. The meeting culminated in a discussion of Articles 12 to 16 of the draft Regulation.

II. Details

Agenda item 1: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

(1) EDPB-EDPS Joint Opinion 4/2022

The European Data Protection Supervisor (EDPS) gave a brief overview of the European Data Protection Board (EDPB)-EDPS Joint Opinion of 28 July 2022. The question arose

regarding the extent to which Europeans in future would be free in their use of the Internet. He questioned whether the strategy adopted was the right one. The COM proposal for a Regulation was, in his view, 'not entirely' compatible with European fundamental rights. The detection orders provided for in the draft Regulation were not sufficiently targeted and resulted in an 'unprecedented degree of legal uncertainty'. The EU Centre had to be separate from Europol in terms of its technical and organisational requirements.

FR voiced its opposition to the exclusion of grooming from the scope of the Regulation, as called for by the EDPS. With regard to paragraphs 47 et seq. of the EDPB-EDPS Joint Opinion, AT asked which 'less intrusive measures' the EDPS was proposing. The EDPS explained that he could not provide more specific details of such 'less intrusive measures'. In response to a question from FI, the EDPS explained that it made no difference whether a machine or a person was monitoring communication, as it was still an 'extraordinary intrusion into a person's privacy'. CZ cautioned against constantly 'going round in circles' and consequently losing sight of the objective of protecting children from sexual abuse. In the specific event of unknown material and grooming, awareness of the risk of errors was essential, but that did not mean that no action should be taken. The EDPS asserted that he could not 'agree' to the proposed Regulation, even if there were relatively low error rates in the detection of CSAM. SI took issue with the EDPS approach of focusing in a 'downright dangerous manner' exclusively on the protection of privacy and demanded that child protection take priority because children had to suffer the effects of sexual abuse for their entire lives. This phenomenon could not be tackled effectively without imposing legislative requirements on service providers, hence the intention to adopt the draft Regulation swiftly.

Responding to our questions regarding age verification, the EDPS felt that there were currently no reliable age identification service providers. He claimed that there was a 'risk of exclusion' or 'excessively intrusive age verification'. Without going into details, he suggested that, as appropriate, a 'parental control mechanism' could be activated. Otherwise the EDPS had 'no further suggestions'. COM was bewildered by the EDPS's comments and referred to the expert workshop on age verification conducted under the CZ Council Presidency. A number of tools facilitating satisfactory age verification were already commercially available.

The EDPS asserted that the matter 'might have to be revisited, because the related opinion was requested at very short notice'. He had no recommendations on how the draft Regulation could be organised lawfully. Various MS and in particular COM expressed their disappointment at the EDPS's failure to answer a number of questions or to propose any solutions.

COM pointed out that the detection order was a measure of last resort where 'mitigation measures' had been unsuccessful. Moreover, information could still be exchanged between the provider and the relevant authority. It was essential to ensure that the measures were implemented in a targeted manner. That was the specific objective sought by the EDPS. COM LS maintained that there were no relevant judgments thus far on this specific subject area. Data retention was an important reference framework, but there were further judgments by the CJEU which had to be taken into account for the purpose of legal analysis. For data retention purposes, illegal content was to be treated differently to metadata. The COM proposal provided for a number of safeguarding 'layers'. COM acknowledged that there were no solutions without legal risk but then conversely questioned how high the risk would be if nothing was done to protect children more effectively from sexual abuse.

ES, PT and FR requested that COM also forward its legal observations in writing. COM raised no fundamental objections but commented that this would still require internal approval. Responding to a request from IE and AT, the Council Legal Service (CLS) explained that its forthcoming written opinion was still delayed because it was currently without a Director General. There was a draft, but it still needed to be approved. It was not yet possible to confirm when the opinion would be communicated. AT suggested that the Chair also obtain an opinion from the Agency for Fundamental Rights (FRA). The Chair pointed out that this was not customary practice. Nevertheless, the FRA naturally reserved the right to express its own independent opinion.

(2) Encryption

The Chair conducted an ad hoc round table on the issue of encryption. Some MS were in favour of introducing a provision in the Regulation stating that encryption may not be compromised. There was also uncertainty among service providers about how encryption would impact detection orders.

CZ and IE expressed their opposition to an express prohibition in the Regulation, since that would completely stifle future technological development, and the legal instrument would have to be 'restarted' every time there was a new development.

FR requested that nothing be included in the text that could be regarded as a dilution or prohibition of encryption. SI likewise emphasised the significance of encryption.

We proceeded as directed. In that context, we stressed that a high level of data protection and a high degree of cybersecurity, including consistent and secure end-to-end encryption in electronic communication, were essential for the Federal Government. Against that background, we felt it was essential, in particular, to stipulate in the draft text that the use of technologies which would lead to an undermining, dilution, circumvention or modification of encryption was precluded.

PT warned that encryption could ultimately provide a safe harbour for paedophiles, and so great care would need to be taken. HR pointed out that encryption could have negative repercussions for the detection of CSA and advocated including provisions on encryption in the Regulation.

FI entered a scrutiny reservation but expressed support not only for a reference to encryption in a recital but also for its inclusion in the enacting terms of the Regulation.

RO did not claim to have a solution and mentioned encrypted communication issues encountered by the law enforcement authorities.

AT cited the opinion of its national parliament, which defined the parameters for safeguarding confidential communication on the Internet (in particular end-to-end encryption).

BG and MT entered a scrutiny reservation and notified their written opinions.

EE likewise entered a scrutiny reservation but also referred to the huge impact on the work of the law enforcement authorities (risk of hindering law enforcement) and the possible setting of a precedent for other areas.

NL referred to its written proposal on Article 10(3) of the draft Regulation (no technology precluding end-to-end encryption).

LU did not submit an opinion.

LV called for a provision on the integrity of encryption to be included in the Regulation, but the specific wording would need to be addressed.

IT entered a scrutiny reservation but advocated a technologically neutral solution. Although it was important to weigh up the benefits, encryption and privacy protection must not result in infringement of victims' rights.

EL emphasised that the police's 'hands were tied' without access to encryption. LT likewise stressed the importance of having access to encrypted data (even outside the CSA framework).

DK pointed out that it had received no instruction on the matter of encryption and could only comment generally that both legal guarantees and 'flexible procedures' were important. In DK, there was a national system governing blocking orders that was to be continued even after the CSA Regulation entered into force.

CY maintained that breaking open encryption was imperative for combatting CSA as well as other criminal activities. A provision to that effect was needed in the operative part of the Regulation. Any solution would have to be carefully weighed and be consistent with CJEU case-law.

PL argued that the nature of the encryption must not be called into question. That said, privacy protection was not an unconditional right. The safeguarding of children's rights was of paramount importance, but measures always had to be proportionate. Further discussion was necessary in this regard. PL submitted a written opinion.

HU entered a scrutiny reservation. It stated, however, that child protection was an 'absolute priority' and, therefore, collaboration with the service providers was vital.

BE likewise entered a scrutiny reservation. In its view, it could be concluded for the time being that authorities were expected to have access to data and had to process it quickly, effectively and securely.

ES claimed that access to encrypted material was essential for combatting crime. Like CZ and IE, ES recommended that the Regulation should also take account of future technological developments; it would be useful if the Regulation could simply mention the subject generally.

SK noted that those internal discussions were still ongoing. Encryption was an important aspect in the protection of fundamental and human rights. However, it was also clear that this must not be allowed to impede the prosecution of CSA offences.

COM highlighted that technological neutrality was a cornerstone of its proposal for a Regulation. Excluding end-to-end encryption from the scope of the Regulation would result in significant loopholes, and service providers must not be allowed to circumvent their obligations under the CSA Regulation by introducing encryption. Providing an exemption for certain services was dangerous, and an exemption from detection obligations would render the proposal disproportionate and ineffective. In those circumstances, there would no longer be a 'level playing field' among service providers.

The Chair concluded that the issue of encryption was of great importance to the delegations and pointed to the precedent that would be created by a provision in the CSA Regulation. While some MS preferred there to be a clear statement in the operative part of the Regulation, most MS had not taken up a definitive position in that regard. The Chair pointed out that recital 26 of the draft Regulation specifically contains statements on encryption. 'Impunity in the field of encryption' must be prevented. The Chair would also discuss access by law enforcement authorities (LEAs) to confidential communication in other bodies and address the subject in the informal JHA Council, in COSI and in the COPEN Working Party.

(3) Voluntary detection measures even after entry into force of the CSA Regulation?

The Chair pointed out that some MS were in favour of continued voluntary detection by the service providers following implementation of the CSA Regulation. For this purpose, either the derogation on e-privacy could be extended or continued, or a separate provision could be included in the CSA Regulation. The Chair questioned whether the relevant options should be assessed further.

IE, CZ, FI and FR advocated the continuation of voluntary detection measures by the service providers. In that regard, FR highlighted that the hosting service providers needed a clear legal basis.

We, like AT, PL, NL, IT and RO, expressed our support at least for assessing whether and, as necessary, under what conditions voluntary detection by the service providers was to be permitted in future. From the proportionality perspective, this could potentially be a less stringent measure than a detection order ('hierarchical relationship'). In that situation, a clear legal basis for the voluntary detection had to be created, given that the temporary derogation from the e-Privacy Directive had expired. From a technical and legal perspective, preference was to be given to an independent provision in the CSA Regulation. The fundamental legal issues would still need to be discussed in detail.

By contrast, COM was sceptical about permitting continued voluntary detection after expiry of the temporary derogation on e-privacy. The draft CSA Regulation provided exclusively for the legal instrument of the detection order. According to COM, there was no longer any scope in the CSA Regulation for voluntary detection measures by the service providers. The notion of the two instruments existing in parallel was conceivable only on a 'purely hypothetical basis'.

The Chair concluded that there was sufficient MS support for an assessment of whether and, as appropriate, the conditions under which (legal basis) voluntary detection by the service providers was to be permitted in future. The subject would therefore be revisited.

(4) Audio communication under the CSA Regulation, measures in publicly available services and interpersonal communication

The Chair asked the MS for their positions on audio communication under the CSA Regulation and about measures in publicly available services and interpersonal communication.

FR and CZ entered a scrutiny reservation concerning audio communication. CZ felt that further safeguards were necessary. As instructed, we – supported by NL – submitted that audio communication should be excluded from the scope of Article 7 of the draft Regulation. According to PT, audio communication should still be covered by the Regulation, as PT definition covered all content irrespective of the media form involved. COM emphasised that audio communication was gaining in importance, also in the CSAM field.

The Chair observed that one difference between the TCO Regulation and the CSA Regulation was that terrorist content as a rule was intended to be distributed publicly whereas CSAM as a rule was shared privately. As instructed, we submitted that the scrutiny reservation related, in particular, to interpersonal communication services and personal cloud storage. IT commented that the protection of minor users had to be weighed against data protection. NL expressed support for proportionate detection measures in connection with known CSAM in interpersonal communication services; in the case of unknown (new) CSAM and grooming, doubts were expressed with regard to proportionality. HR – supported by ES, PL, CZ, PT and HU – advocated detection orders in interpersonal communication services; there was no unconditional right to privacy, CSAM was often shared by means of interpersonal communication services. ES pointed to the duty to protect children and young people, as laid down in various documents of EU and international law; the CSA Regulation must not fall short of those standards.

CLS stated that, when assessing the legality of detection orders, a distinction had to be made between publicly accessible areas and interpersonal communication. With regard to publicly accessible areas, case-law on similar circumstances provided guidance (CJEU, judgment of 3 October 2019 in Case C-18/18 and CJEU, judgment of 26 April 2022 in Case C-401/19). According to those judgments, there was a very low legal risk regarding detection in public services. There were fewer established judgments concerning interpersonal communication. Decisions in these areas related very specifically to the data concerned; they were consequently less well suited as a basis for drawing conclusions in relation to the CSA Regulation. It could be inferred, to the extent possible, that the intended purpose (combatting serious criminal offences) was of major importance. Furthermore, the Court of Justice had, in the past, delivered significantly more restrictive judgments on content data than on metadata. CLS announced that there would be a written report (date of publication not known). For the time being, it was established that, in the light of the case-law thus far, there were legal risks in relation to interpersonal communication services.

COM highlighted that two thirds of current CSAM reports originated in interpersonal communication services. COM had opted to draw a distinction between the different types of content because that allowed for a graduated approach. For measures that applied generally

and without distinction, the CJEU made the distinction between the purpose of combatting serious criminal offences and the protection of public safety. However, the CSA Regulation provided for specific, temporary and targeted measures. Unlike in the case of 'offences offline', data was needed not simply to identify the offender; by contrast, in the case of CSAM, the content data itself constituted the criminal offence. In view of the duty to protect children and young people, a high legal risk was likewise established in failing to adopt appropriate measures for combatting CSAM. FR, HU and IE requested written communication of the legal positions.

(5) Article 12 et seqq. of the draft Regulation

With regard to Article 12: The Chair considered the prospect of transferring the duty to report information from the user to the recipient authority. DK entered a scrutiny reservation on that proposal; it advocated extending the time period set out in Article 12(2) and direct reporting to national authorities. We likewise entered a scrutiny reservation; LEAs should not be overburdened, and duplication of reporting and information channels should be prevented. According to COM, responsibility for receiving reports predominantly lay with the national authorities; they were also responsible for suspending the obligation to report information. However, information was obviously to be provided by the service provider to the user concerned. PL welcomed amendments to Article 12, in particular the extension of the suspension of the requirement to provide information in paragraph 2. A transfer to the law enforcement authorities of the duty to provide information was to be assessed with particular regard to the high number of reports expected.

COM stated that the establishment of an independent EU Centre, operating as a strong European partner subject to high standards under EU law, was in direct contrast to the previous dependency on private stakeholders based outside the EU. EP's request in the negotiations for the 'interim Regulation' was therefore acted upon. Where duplicated reports by providers (to the National Centre for Missing and Exploited Children (NCMEC) and the proposed EU Centre) could not be avoided, measures would have to be introduced to ensure that LEAs did not receive duplicated reports. In that case, the EU Centre would have to merge reports if necessary following assessment of false positives. FR asked how duplications were to be prevented in MS which received reports directly from NCMEC. COM explained that NCMEC currently did not send the reports to the MS but made them available online so that MS could access them. That practice was also permitted under the CSA Regulation.

With regard to Article 13: BE was in favour of a stronger involvement for reporting hotlines (e.g. as trusted flaggers), in particular to assess the urgency of reports. IT and PT welcomed the amendment to Article 13(1)(f). NL asked whether Article 13(1)(c) also covered audio recordings. HR, PL, IT, RO and HU supported the existing wording of Article 13(1)(c). Service providers could not assess which data was 'relevant'; only the law enforcement authorities could do that. COM commented that recourse was had to Article 13 (in conjunction with Annex III) to ensure that all reports were 'actionable'. This was not currently the case for all NCMEC reports. Article 13(1)(h) referred to parallel reports to the NCMEC. Article 13(1)(j) and Article 48 included a reference to the urgency of reports. Annex III point 8 made provision for indicating the origin of reports. Annex III point 3 gave details of the scope of Article 13(1)(c). Accordingly, in the event of a report of audio communication, accompanying images, audio or video material, as applicable, were also to be forwarded.

With regard to Article 14: FR, IE, CY, PL and BE expressed support for the deletion of 'under the jurisdiction of [that] Member State' from Article 14(1). The phrase was obsolete in the light of Article 14(1)(a). PT pointed out that appointment of the competent national authority had to be left as before to the MS. FR called for a reduction in the time period in Article 14(2) to one hour, in alignment with the TCO Regulation: Annex IV was unworkable in practice.

The Chair proposed a significant shortening of paragraph 3(a). BE and HR were in favour of the complete deletion of the above provision. As directed, we submitted that the provision in paragraph 3(a) appeared to be barely workable in relation to domestic situations. Redress could be found, as appropriate, in Article 15(1); that position was supported by IE. Several MS referred to problems in relations between national authorities which complicated the implementation of paragraph 3(a) in its current version. As instructed, we submitted, in relation to paragraph 5, that information concerning the non-execution of the removal order should be forwarded directly to the Coordinating Authority. The Chair commented that, in this context and as appropriate, there was also a need to make changes in paragraph 7. The Chair would send a compromise text to that effect which would streamline the processes involved. IT asked whether the EU Centre should not also be included in paragraph 6. COM stated that the administrative authorities had to be informed of every stage of the procedure; the EU Centre was the last to be informed under paragraph 7.

With regard to Article 14a: IE welcomed Article 14a as a whole, although it expressed doubts regarding Article 14a(4). The recipient in this context should be the competent authority in the requesting MS; IE was therefore in favour of deleting paragraph 4; as a result, providers obtained more extensive rights than with national orders. DK and EE voiced concerns about Article 14a in relation to individual national constitutions. We commented on Article 14a as instructed. COM expressed doubts about the introduction of Article 14a; inasmuch as the MS were striving to transfer the provision from the TCO Regulation into the CSA Regulation, Article 14a would have to be adapted. The Chair announced a revision of Article 14a.

With regard to Article 15: DK and PT considered that the time period in Article 15(4) was too short; the term 'necessary' in the first sentence of paragraph 4 needed to be qualified.

The Chair explained with regard to Article 16 that blocking orders were activated for URLs. In that context, it was, as a rule, only possible to block entire websites. Here, it was important to preserve the constitutional balance; Article 16 gave rise to a further set of issues. At the same time, the blocking of content was a very important measure for tackling content hosted in third countries. Established and effective systems for blocking content were operational in DK and FR. This article would be discussed further at the next meeting.

Agenda item 2: AOB

COM announced an infographic on child abuse. To that end, it would be asking the MS to nominate the competent national authorities.