Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 01 March 2024

WK 3413/2024 INIT

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	Presidency
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Proposals for a refined approach

Delegations will find attached the presentation made by the Presidency at the Law Enforcement WP (Police) meeting of 1 March 2024 on the above-mentioned subject.

CSA Regulation

Proposals for a refined approach

INDEX

belgium24.eu

01 More targeted detection orders

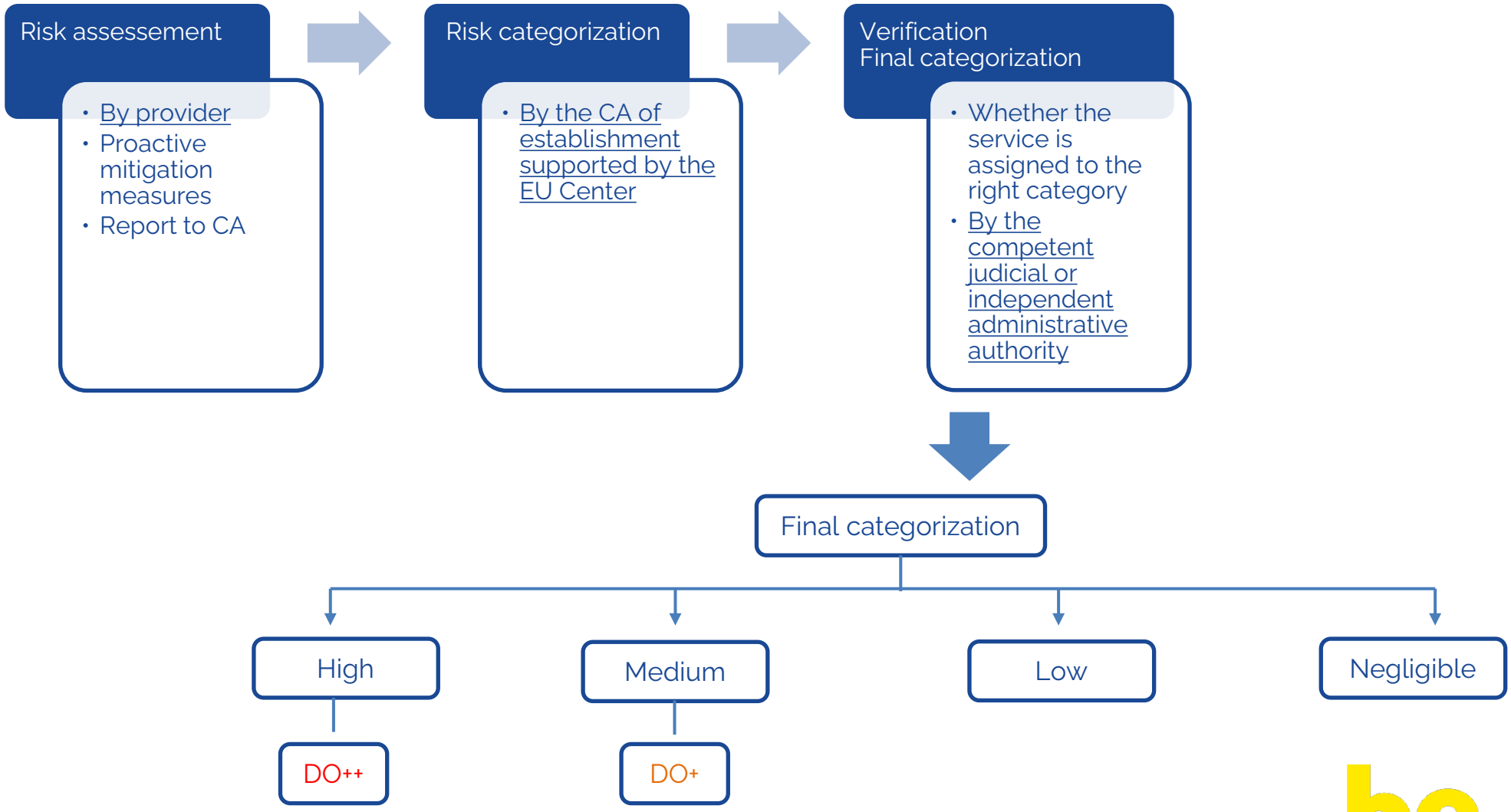
3 main steps

- Step 1 : Risk assessment/categorization
    - The service will be assigned to one of the 4 risk categories following an enhanced and objectified risk assessment
- Step 2 : Measures
    - Depending on the risk category of the service (Step 1), different measures are possible:

        - **Mitigation Measures** (obligatory / recommended)
        - **Penalties**
        - **Detection Orders** (standard / limited / none)
        - **Authorized detection orders requested by providers**
- Step 3 : Recategorization
    - The riskier the service, the more frequent the recategorization

belgium24.eu

Procedure



belgium24.eu

Risk categorization

- 4 categories of services…
  - High risk
  - Medium risk
  - Low risk
  - Negligible risk

- … Based on a set of parameters

  - Categories of parameters considered :
    - based on the category of services
    - based on the core architecture of the service
    - based on policies and safety by design functionalities in place
    - based on user tendencies and statistics
    - related to company policy on user safety

- … and how services score on those parameters
  - Multiple scoring methods possible (binary, multi-class, sampling)

belgium24.eu

Risk mitigation and detection orders

- Depending on the risk category of the service :
  - Risk mitigation measures
    - obligatory
      - With sanctions (?)
      - Without sanctions (?)
    - recommended
  - (authorized) detection orders
    - standard
    - limited

Parameters	DO ++ Standard detection orders (issued by a judicial or independent administrative authority)	DO + Limited detection orders (issued by a judicial or independent administrative authority
Maximum duration	Up to 24 months	Up to 6 months
Public or private	Public and private content	Public information
Services using E2EE	Including services using E2EE	Excluding services using E2EE
Technologies used	All technologies	Only low error rate technologies
Suspect based detection	Suspect based detection	(if requested by MS) suspect based detection

belgium24.eu

Risk mitigation and detection orders

- Services categorised as "high risk" :
  obligatory risk mitigation measures
  + a standard detection order (up to 24 months)
  + services using E2EE
  + additional step : suspect based detection

- Services categorised as "medium risk" :
  obligatory risk mitigation measures
  + a limited detection order (up to 6 months)
  + (potentially) additional step : suspect based detection

- Services categorised as "low risk" :
  list of recommended mitigation measures.

- Services categorised as "negligible risk" :
  no list of recommended mitigation measures but should take voluntary mitigation measures based on their risk assessment.

belgium24.eu

Suspect based detection

- Additional step for services categorized as “high risk” (and also "medium risk" if considered by delegations)

- While the “category based detection order” focuses on the **content**, the “suspect based detection” focuses on the **person**

- *A person of interest could be defined as a user who has already shared CSAM or attempted to groom a child. This would be automatically detected but not known to anyone (including the provider), until a certain number of hits is reached on the sharing of possible CSAM or attempted grooming (1 hit for known CSAM ; 2 hits for unknown CSAM/grooming).*

- Only then the person of interest would be detected and reported to the EU Centre

- Error rate will exponentially decrease

belgium24.eu

RISK CATEGORISATION (STEP 1)	LEVEL OF DETECTION ORDER (DO)	SUSPECT DETECTION TO CREATE A LIST OF POTENTIAL OFFENDERS (PERSON TARGETING)	AUTHORIZATION OF PROVIDERS (AOP) (STEP 2)	FREQUENCY OF (RE)CATEGORISATION (STEP 3)
Risk + + High	DO + + - Including services using E2EE - (e.g.) Up to 24 months - Intrusive technologies	Detect potential suspects -> creation of a list of potential offenders/ persons of interest.	AOP	Very frequent (e.g.) 6 months
Risk + Medium	DO + - Excluding services using E2EE - (e.g.) Up to 6 months - Less intrusive technologies	*If deemed necessary* : Detect potential suspects -> creation of a list of potential offenders/ persons of interest.	AOP	Quite frequent (e.g.) 12 months
Risk - Low	None	No suspect-based detection	None	Frequent (e.g.) 18 months
Risk - - Negligible	None	No suspect-based detection	None	Rare (e.g.) 3 years

02 Protecting cyber security and encrypted data

Protecting cyber security and encrypted data

- Different concerns from Member States:
  - Some have privacy concerns about breaking into E2EE data and cybersecurity concerns about “backdoors” to E2EE
  - Some consider that excluding services using E2EE would make the regulation less effective and that solutions to address privacy and cybersecurity concerns can be found
- BEPCY proposes a compromise:
  - Only a standard DO (so only high-risk services) could be applied to services using E2EE, provided that service providers
    - are not obliged to create access to end-to-end encrypted data
    - technologies used for detection are vetted regarding effectiveness, impact on fundamental rights and risks to cyber security
  - Adding further safeguards to protect cyber security

belgium24.eu

03 Questions to delegations

- **1.** Do you support the idea of developing a risk categorization for (parts of) services of providers and classifying them into four categories, and do you have suggestions regarding the methodology and the parameters to be applied?

- 2. Do you support the approach that risk mitigation measures and detection orders should be linked to the risk categorization?

- 3. Do you support the establishment of two different kinds of detection orders depending on the risk level of a service?

- 4. Do you agree that there should be a possibility for providers of hosting services and of interpersonal communications services, under certain conditions, to request to the co-ordinating authority, on their own initiative, the authorization to detect (parts of) their service, based on a detection order issued by a competent judicial or independent administrative authority?

- 5. Do you agree to include high-risk services using E2EE in the scope of standard detection orders, under the condition that a detection order should not create any obligation that would require a provider to create access to end-to-end encrypted data and that the technologies used for detection are vetted with regard to their effectiveness, their impact on fundamental rights and risks to cyber security?

belgium24.eu

- 6. Do you support the addition of further safeguards to protect cyber security in the operative part of the text and the recitals as suggested by the Presidency?

belgium24.eu

- 7. Do you have any additional remarks that the Presidency should consider when further developing the concept and working on consequential changes to other parts of the proposed regulation, including on the EU Centre, resulting from the new approach related to more targeted detection orders and protecting cyber security and encrypted data?

THANK YOU FOR YOUR ATTENTION

belgium24.eu


be
EU
belgium24.eu