



# DIGITAL SERVICES ACT

**Webinar for National  
Regulatory and Competent  
Authorities**

24 January 2023

# Agenda

- Introduction to the Digital Services Act -> objectives and main building blocks, overview of the due diligence obligations
- Deep dive in DSA provisions: focus on responsibilities of Digital Services Coordinators and Competent Authorities



# I. Introduction to the DSA

# 2021 *This Is What Happens In An Internet Minute*



European  
Commission

# OBJECTIVES

One set of rules  
across the entire  
EU single market

Proportionate,  
asymmetric  
obligations

Exemptions for  
Small and Micro  
Enterprises



- 1.** To create a **safer digital space** in which the **fundamental rights** of all users of digital services are protected

- 2.** To establish a **level playing field** to foster **innovation, growth, and competitiveness**, both in the European Single Market and globally

Spread of illegal  
content, sale of non-  
complaint goods and  
services

Protecting fundamental  
rights online

Tackling societal  
concerns such as  
disinformation and child  
safety

## E-commerce Directive 2000/31

Rules for information society services providers



DECATHLON

SPIEGEL  
ONLINE



Conditional liability exemption -  
intermediary services

Mere  
conduits

Caching  
services

Hosting  
services

+ no general monitoring obligations



2000

SECTOR  
SPECIFIC  
LEGISLATION

## Digital Services Act Rules for intermediary services

Clarifies rules on conditional liability  
exemption and creates incentives for  
proactive measures

Due diligence obligations

Common framework for enforcement:  
Digital Services Coordinators + Commission

2022



European  
Commission



# Maintaining key principles - Liability in the DSA

## DSA harmonises liability exemptions

- Does **not attribute** liability for content
- Specifies self-standing **due diligence obligations** - **exemption** from liability unaffected
- Providers conducting **voluntary-own initiative investigations** still benefit from liability exemptions

## DSA is neutral

- Does **not define** what is illegal; illegality is defined by **national or EU law**
- Remains **technologically** neutral

## DSA is horizontal

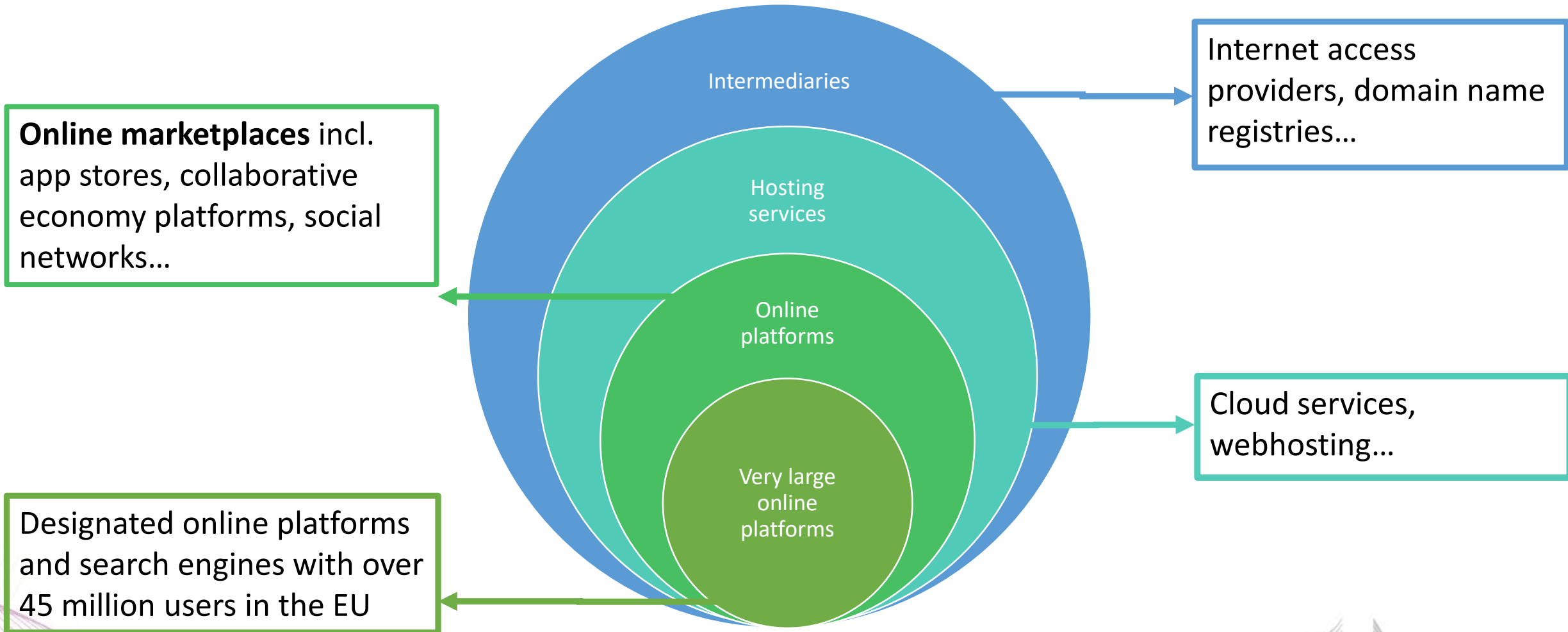
- All types of **illegal content**, civil and criminal liability



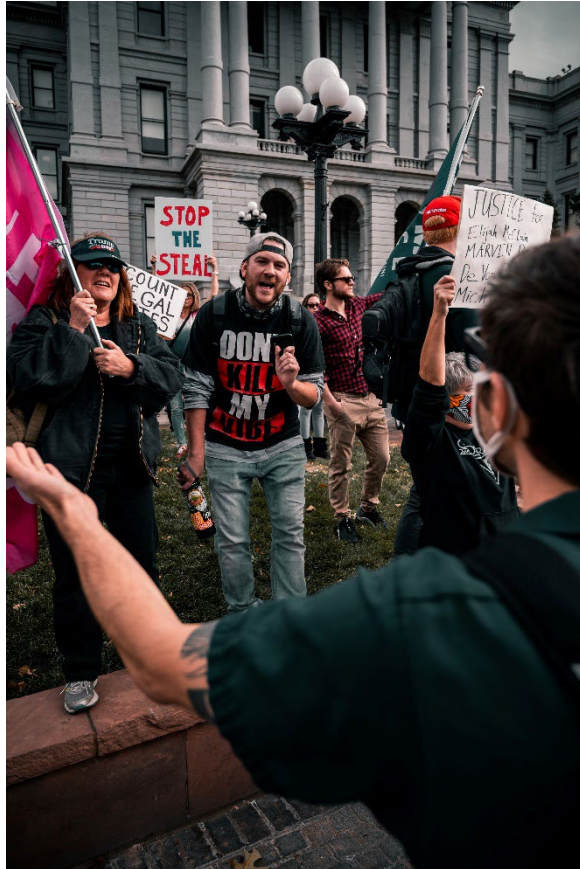
# Due diligence obligations & some highlights



# Asymmetric obligations I - Scope of the DSA



# Systemic risks materialize



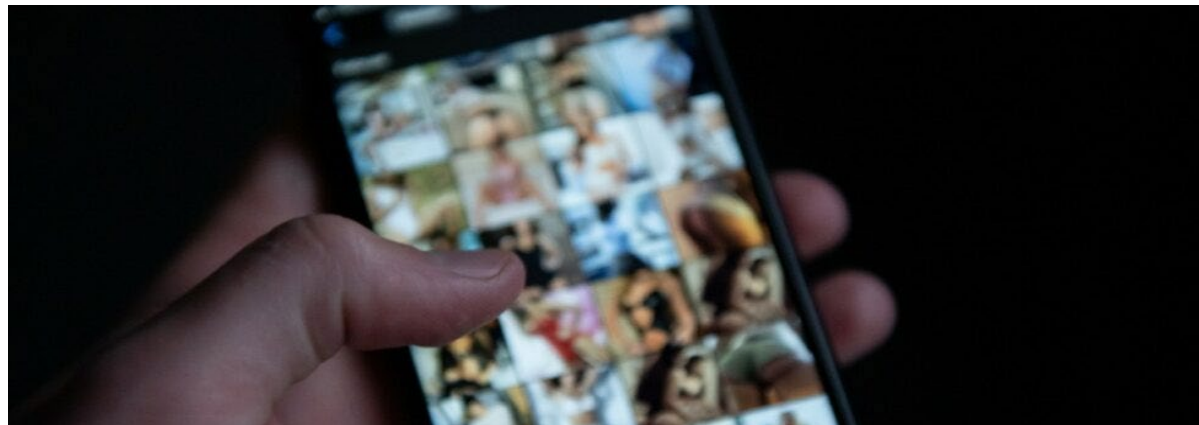
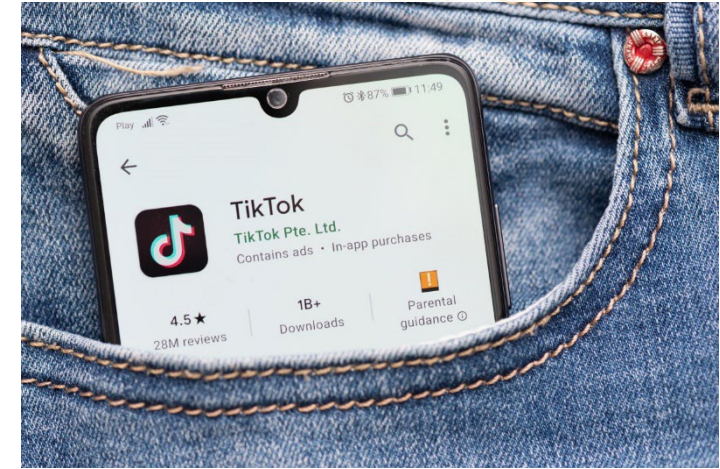
Capitol riots following the US election, 2021



Disinformation campaigns related to the war in Ukraine , 2022

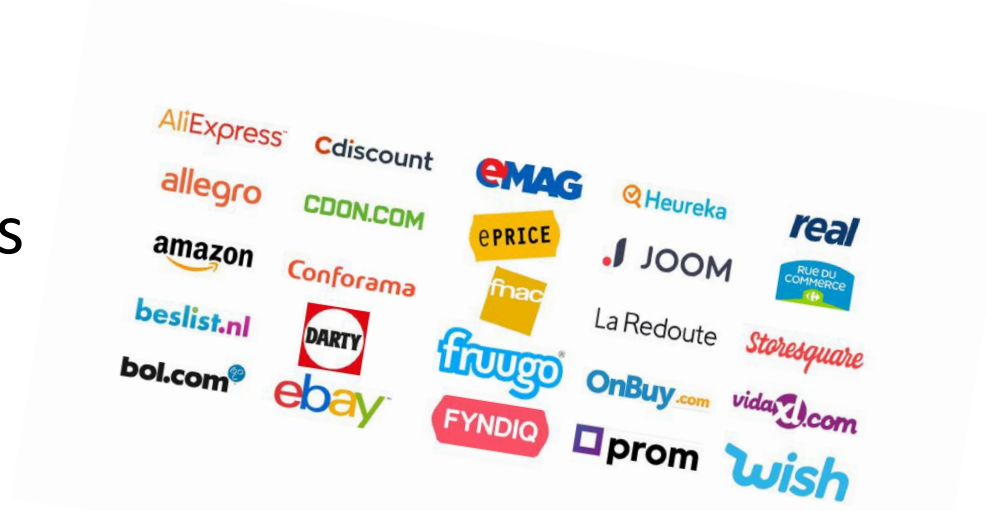
# Protection of children

- Important issue for co-legislators and COM
- Number of strengthened/new provisions
  - Easily understandable terms of service for children
  - Online platforms accessible to minors obliged to take appropriate and proportionate measures to ensure the privacy, safety and security of minors
  - Restriction (i.e. ban) of presentation of advertising to minors (based on profiling)
- VLOPs and VLOSEs: targeted assessment of negative effects of their services on minors and on respect of the rights of the child



# Obligations on online market-places

- Already very ambitious proposal, but both Council and EP called for further obligations
- Proportionality: SMicE exemption
- DSA introduces a number of strengthened obligations:
  - Better traceability of online sellers
  - Random checks of product compliance
  - Compliance by design
  - Right to information
- Not only tool – revision of GPSR close to finalization



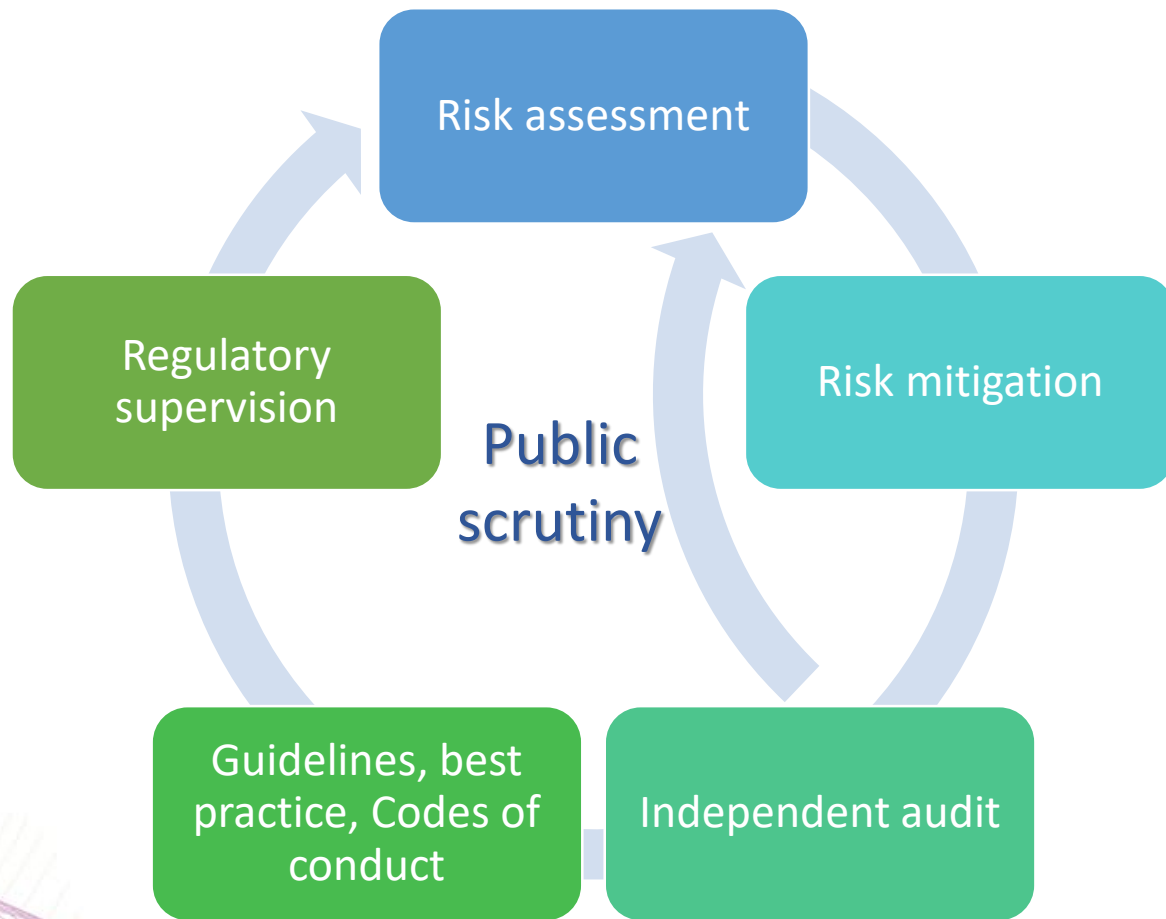
# Online advertising



- Bans for targeted advertising on online platforms that exploit users' vulnerabilities
- User-facing transparency
- Further obligations for Very Large Online Platforms and Very Large Search Engines: their advertising systems must be adapted to mitigate societal risks



# Supervised risk management



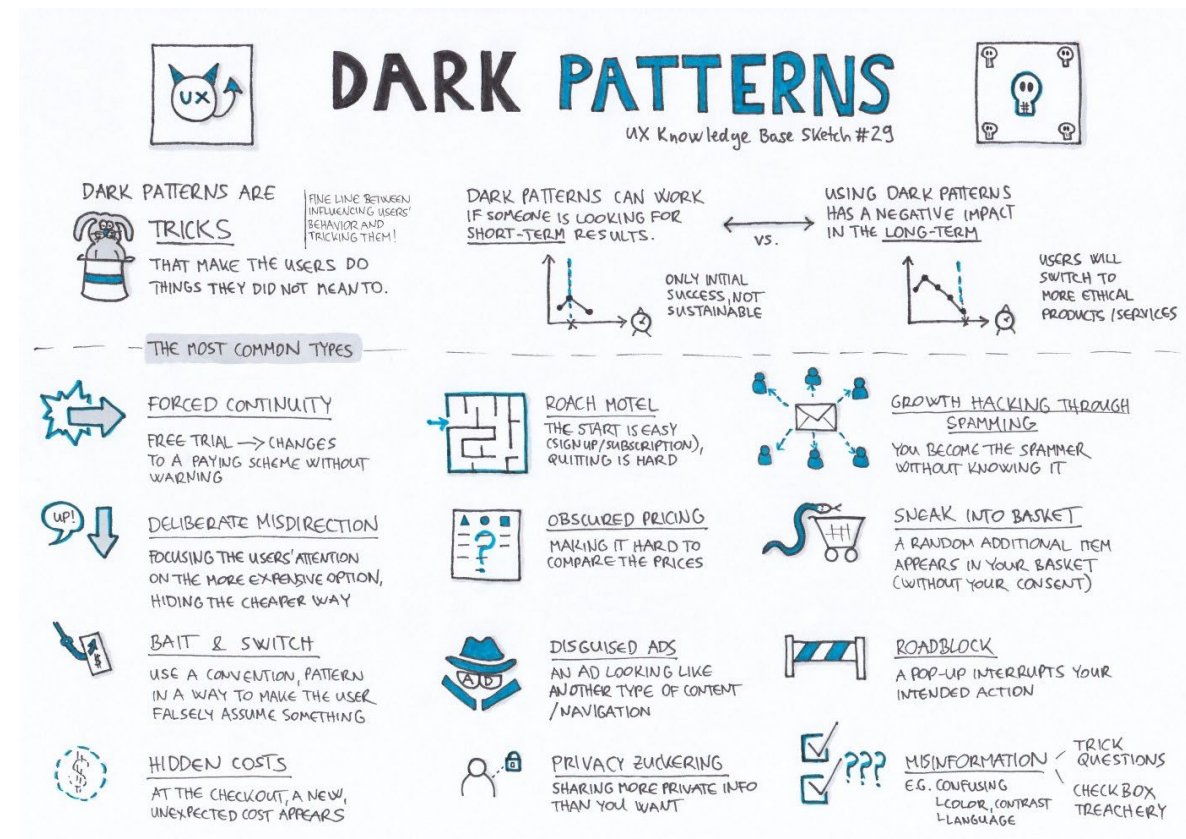
- Places societal risks and interests **at the top of the priorities** in the design of a platforms' systems
- A **dynamic** approach to identify and address **societal risks as they emerge**:
  - **Dissemination of illegal content**
  - **Negative effects on fundamental rights**
  - **Negative effects on electoral processes, civic discourse, public security**
  - **Negative effects on public health, minors, mental and physical well-being, gender-based violence**
- Covers the **core design of a service**, from its T&C, to its algorithmic systems and optimisation choices

# Zoom on specific types of risks and issues

revenge  
porn



accessibility



# Data access

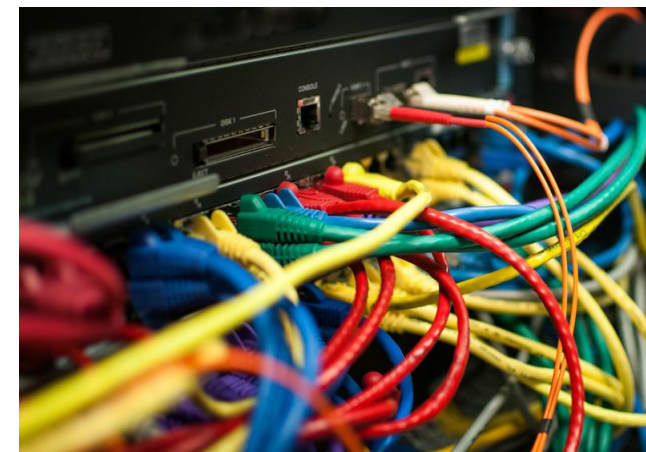
- For Digital Services Coordinators and the Commission

➔ data necessary to monitor and assess compliance with the DSA

- For vetted researchers to support their public interest mission

➔ data for research that contributes to the identification and understanding of systemic risks

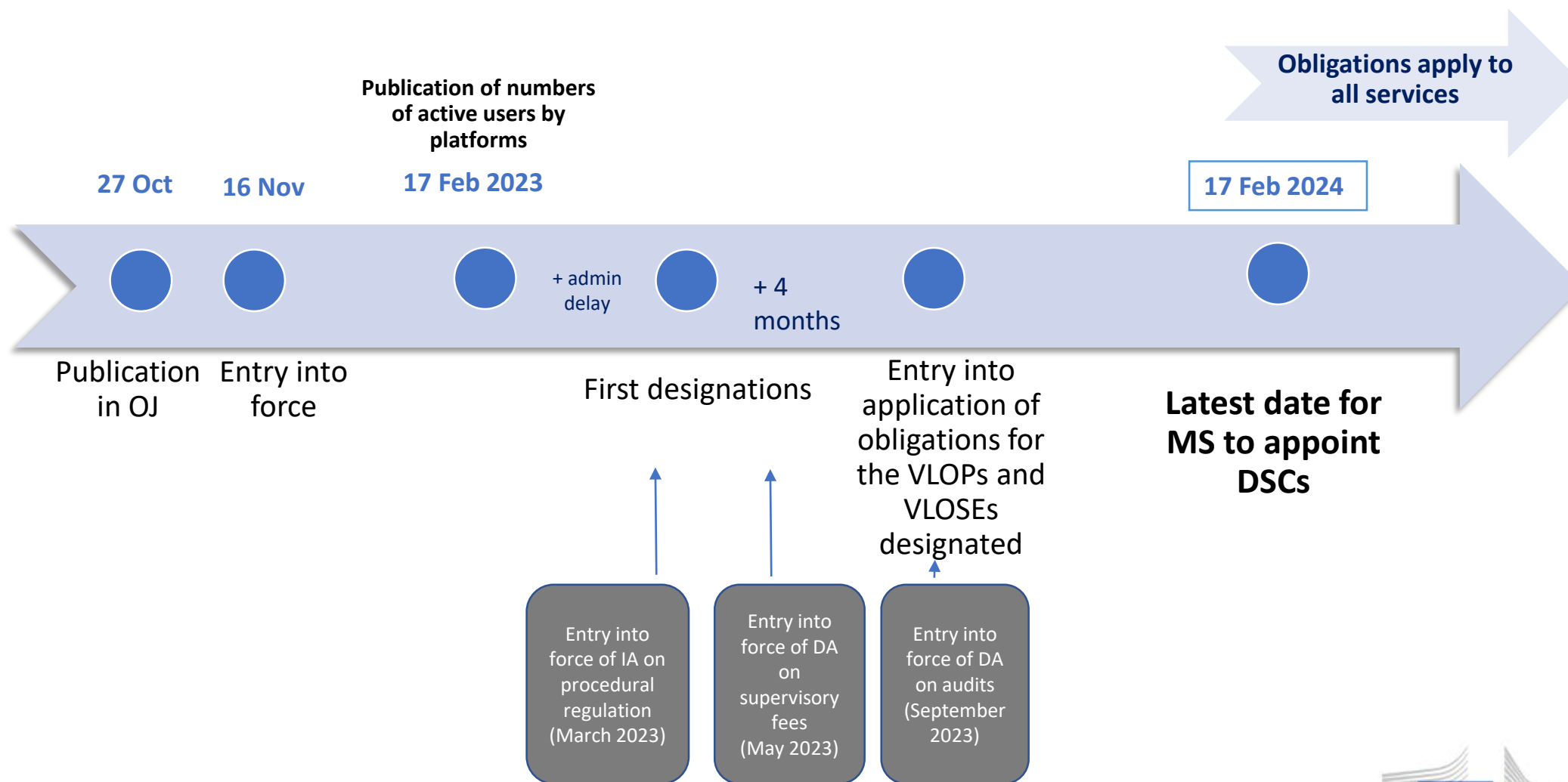
- Vetted researchers awarded by DSC of establishment of the VLOP or VLOSE
- Direct requests to the VLOP or VLOSE by researchers that fulfil certain criteria for publicly available data



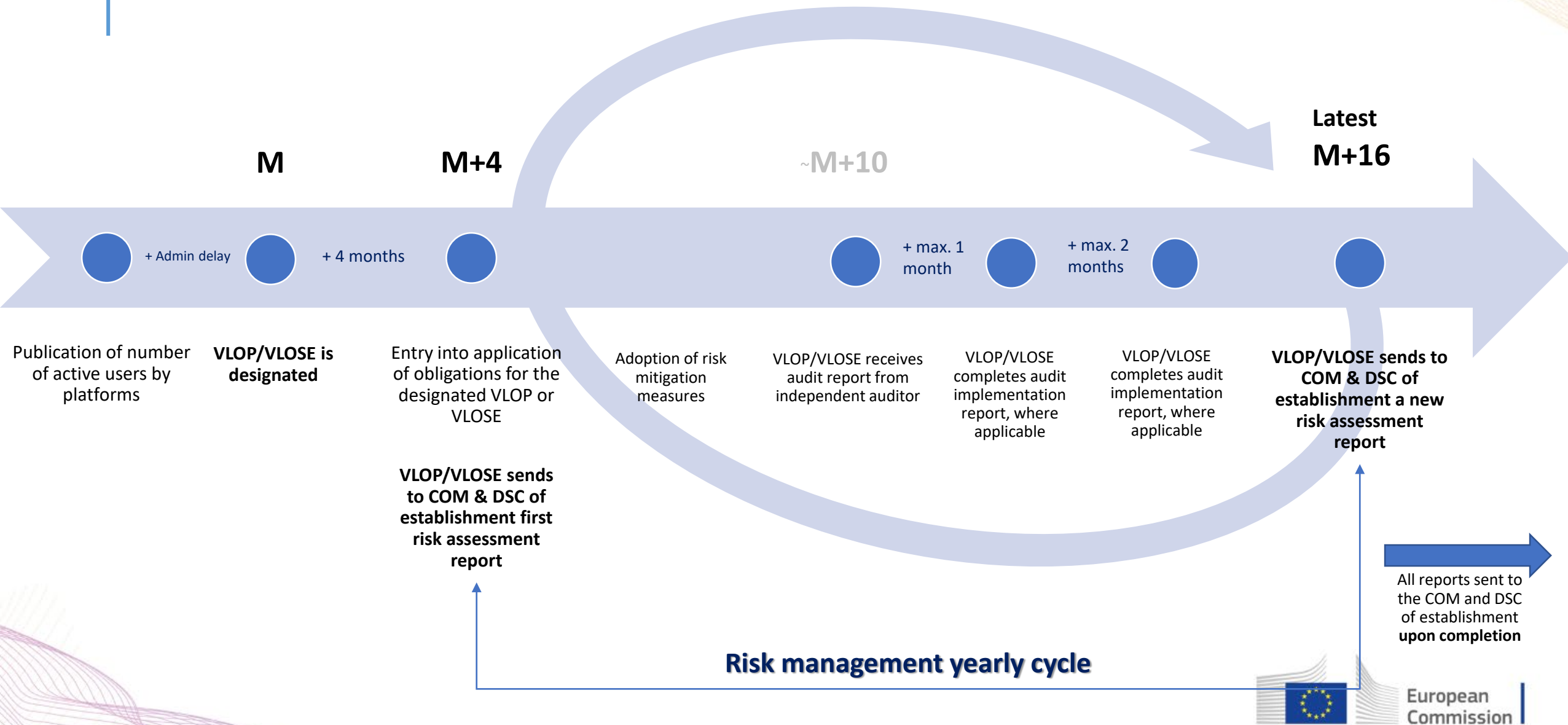


# Timeline and next steps

# Timeline and main milestones



# What the planning could look like for a VLOP/VLOSE



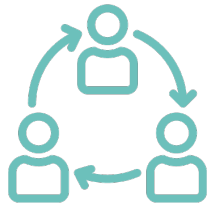
***Any questions or comments?***



## II. Role of national authorities in DSA governance



# Governance of supervising digital services



## Digital Services Coordinator (National level)

- Independent authorities
- Direct supervision and enforcement
- Coordination and exchanges with other national **competent authorities**



## European Board for Digital Services

- Ad-hoc independent advisory group
- Composed by national Digital Services Coordinators
- Chaired by the Commission
- Advises DSCs and COM, issues recommendations



## European Commission

- Direct/primary enforcement powers vis-à-vis VLOPs/VLOSEs
- Advises on cross border disputes
- Intervenes following DSC requests

# Principles of DSA governance

- Ensuring appropriate **supervisory and coordination** function at national level
  - Digital Services Coordinator (DSCs) and other Competent Authorities
- Ensuring **cooperative and consistent enforcement** cross-border
  - European Board for Digital Services (Board)
- Ensuring **strong EU oversight**
  - Primary role of Commission in supervision of VLOPs/VLOSEs, in cooperation with national layer

# National institutional level – DSCs and CAs

- Mapping of tasks around three functions
  - Administrative tasks laid down in Chapter II and III
  - Coordination
  - Supervision and enforcement pursuant to Chapter IV (*DSCs and CAs*)
- Flexibility in allocation of **supervisory and enforcement** competences BUT...
  - Clear coordination function at national level (Digital Services Coordinator)
  - Common independence requirements and harmonised powers for both DSCs and CAs
  - DSC default authority for all tasks if not established otherwise
  - Professional secrecy obligations to be respected

# Powers of DSC and division of powers with CA

- Administrative tasks
- National coordination
- Cross-border coordination
- European coordination
- Supervision and enforcement

# DSC - Administrative tasks I.

- Receiving and transmitting orders (Articles 9 and 10) – DSC of issuing MS
- Receiving notification of legal representative (Article 13(4)) – DSC of establishment of the legal representative
- Certification of out of court dispute settlement bodies and related tasks (Article 21) – DSC of establishment of the OOC
- Awarding trusted flaggers status and related tasks (Article 22) – DSC of establishment of the applicant

# DSC - Administrative tasks II.

- Requesting info on number of users/informing COM on number of users (Article 24 and 33) – DSC of establishment of intermediaries
- Co-operation of the DSC-COO in case of VLOP's designation (Article 33) – MS of establishment or request by DSC-COO
- Vetting of data access requests (Article 40(8)) – DSC of establishment of VLOP (+ pre-assessment and transmission by DSC of affiliation of researcher)
- Requests for access to data (Article 40(1) and (4)) – DSC of establishment of VLOP

# Coordination tasks of DSC – national coordination

- With other Competent Authorities and other authorities
  - **Consultation/exchange** of info with CA and other national authorities (Art. 49(2)), including law enforcement, consumer protection/market surveillance etc., where relevant for performing their respective tasks (e.g. information on on-going investigation, recital 112)
  - **Involvement of relevant CAs / receiving information** from CAs (in particular Art. 53 - complaints, Art. 55 - Annual report, Art. 57 and 58 - Cross-border cooperation requests)
  - **Coordination of national positions** in the Board (Art. 62(1))
  - **Coordination access** to the information sharing system (Art. 85(1))

# Coordination tasks – cross-border coordination I.

- Notification of **initiation of proceedings** against third country providers without legal representative in Union (Article 56(7))
- **Mutual assistance** (Article 57)
  - DSC-COO: info on opening, intention to take a decision, request of info to COD
  - DSC-COD: reply to COO's requests (eventually exercising investigatory powers or involving CAs)

# Coordination tasks – cross-border coordination II.

- **Cross-border cooperation** (Article 58)
  - DSC-COD: to trigger cooperation request
  - DSC-COO: to reply to cooperation request
- **Joint investigations** (Article 60)
  - DSC-COO: to invite to joint investigation; to coordinate activities: to provide preliminary position
  - DSC-COD: to cooperate in the joint investigation (eventually exercising investigatory powers or involving CAs)

# Coordination tasks – European coordination I.

- **Participation in the Board (Art. 62)**
  - Right of initiative; decision making; working groups
  - DSC to appoint other delegates from CAs if provided under national law
- Coordinating provision of **expertise and capabilities** (Art. 64)
- Request to COM to assess **systemic issues** (any DSC) – Art. 65

# Coordination tasks – European coordination II.

- **Involvement in COM investigations re VLOP/VLOSE (Art. 66-72) and blocking orders (Art. 82 in conjunction with Art. 51(3))**
  - **DSC-COO**
    - receiving information on investigations and preliminary findings
    - to request blocking orders
  - **All DSCs**
    - to be notified on opening and enhanced supervision
    - to reply/cooperate to COM requests

# Supervision and enforcement by DSC and CAs

- By default, **DSC is responsible** for every ISS/issue covered by DSA, unless other CA **is explicitly appointed** for specific tasks/sectors
- Exercise of **investigatory and decision making powers** (autonomously for DSC/CAs in COO, or on the basis of coordination at DSC/cross-border/European level), including Art. 51 and 69
  - Power to request information, to carry out or request judicial orders, to carry out inspections (incl. upon request of COM), to interview and take statements
  - Power to adopt binding commitments, cease and desist order, positive remedies, sanctions/penalties, interim measures (either directly or through courts)
- **Request blocking orders**, including upon COM request (Art. 82/Art. 51(3))



# Use cases

# Designation (1)

## CASE

An online platform with allegedly **more than 45 million users** is provided by a provider established in a Member State.

The provider **fails to publish the number of users** of that platform or the reported number of users appears abnormally low.

# Designation (2)

## ACTION 1

[Article 24(3)]

DSC-COO **requests the online platform to comply** with the obligation to publish its online active users on its online interface or to provide additional information (possible sanction)

*Question: how is the Member State planning to identify the providers that failed to publish their number of users? Will it consider any review of suspect low reporting?*

The Member State has **reasons to consider** that the online platform meets the threshold of 45 million users in the EU [Article 24(4)]

The DSC-COO **informs the Commission**

# Complaint (1)

## CASE

Academic lodging a complaint to the DSC-COD against an online platform established in a Member State for a breach of the DSA

## ACTION 1 - necessary [Article 53]

DSC-COD



Assessment of the complaint



the complaint is relevant



Complaint transmitted to  
the DSC-COO

# Complaint (2)

**ACTION 1a – optional: complaint affecting recipients in the MS of destination (e.g. undue limitation of freedom of expression of MS-COD recipients)**

[Article 58]

DSC-  
COD

→ Request to DSC-COO for cross-border cooperation...  
(explicit request with assessment of impacts)

COO to assess within 2 months, either

- Request of info to COD (Article 57)
- Launch joint investigation (Article 59)

...or request to COM (if  
VLOP/VLOSE, systemic,  
seriously affecting), see  
next slide



COO Assessment communicated to COD  
DSC, Board, COM



Board disagrees with COO assessment



COM to settle the dispute

# Complaint (3)

## ACTION 2

[Article 65(2)]

The DSC-COO receives the complaint (with opinion) request and assesses it

*Question: which criteria for requests?*

A VLOP/VLOSE online platform has **systematically infringed** a provision of the Regulation in a manner that **seriously** affects collective interest of recipients

Request to the Commission to assess (duly reasoned ex article 65(3))

COM opens or rejects

No systematic infringement,  
no seriously affecting

VLOP/VLOSE (incl.  
COM rejects)

DSC-COO to  
assess,  
eventually  
open and  
inform  
COM/DSCs

No VLOP/VLOSE

# Joint investigation

## **ACTION 3**

[Article 66(3)]

The Commission receives the request from the DSC-COO



The Commission **requests the support** of the COO and COD DSCs and requests to join a joint investigation, e.g.:

- COO/COM to request info on algorithm used by VLOP
- COD to provide input to algorithm to COD-related content
- COM (incl. JRC) to test algorithm
- Common analysis



COM to adopt preliminary findings and sent to  
DSC-COO and Board (all DSCs)



# Engagement and cooperation with the European bodies and authorities

# Cooperation with EU bodies and authorities I.

- A possibility for the **Board to cooperate with other Union bodies, offices and agencies** (Art. 62(5))
- Field of expertise (rec. 134) – open list, link with tasks performed
  - equality, including gender equality, and non-discrimination,
  - data protection,
  - electronic communications,
  - audiovisual services,
  - detection and investigation of frauds against the Union budget as regards custom duties,
  - consumer protection,
  - or competition law
- Results of cooperation to be made publicly available

# Cooperation with EU bodies and authorities II.

- A possibility for the Commission to engage EU bodies in drawing up, testing and supervising the **crisis protocols** (Art. 48(3))
- Within development of **European expertise and capabilities** (Art. 64(3)), the COM might ask for a support in respect of VLOPs and VLOSEs oversight:
- *The Commission may ask the DSCs, the Board and **other Union bodies, offices and agencies with relevant expertise** to support the assessment of systemic and emerging issues (...).*
  - See also Annex I Draft Delegated Regulation on the fees (5<sup>th</sup> tiret) in case of agreements signed with the relevant bodies



# Discussion: how to ensure cooperation in practice

# Information sharing system (ISS, art. 85)

- COM working on a common and interoperable information sharing principle with the following approach and open questions/views
- ISS to be used for official requests between COM/DSCs but also for other less formal information sharing (and possibly a collaborative space), including for operational tasks (e.g. investigations), partially substituting email exchanges
- Options:
  - Option 1) MS has its own internal system and also use the ISS (with some interoperability requirements)
  - Option 2) The MS uses the ISS also internally in the DSC.
  - Option 3) Besides option 2, MS may also be able to use the system for official requests between the DSC and relevant competent authorities

# Information sharing system (ISS). Questions

- What options would be more helpful/feasible in view of **internal organisation**?
- **Access control/security:**
  - Need to ensure strict control on access to the system, as sensitive information will be channelled but will be necessary that relevant people in the case/task team are included (need-to-know basis).
  - How to ensure that more general, regulatory communications (i.e. in the context of participation within the Board) and specific investigatory communications are clearly separated and subject to potentially very different confidentiality requirements and internal audience? Do regulators have access to secure communications (i.e. TESTA network)?
- **Roles:** Do MS envisage to have different roles in the system (e.g. registrar –with full access rights-, normal user, director/head –user that approves actions within the DSC)? If so, how many? Assigning rights to other users in the DSC should be left to an official in the MS?

***Any questions, comments or suggestions?***

***Thank you for your attention!***