

# The Regulatory Landscape Regarding New Technologies

**ERA Young European Lawyers Academy**

**24 June 2025**

Dr. Theresa Ehlen

Dr. Christina Möllnitz-Dimick



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.



# European Digital Strategy

Communication on 'Shaping Europe's Digital Future' published on 19 February 2020

## Key objectives set out by the European Commission (EC)

- Technology that works for people.
  - A fair and competitive economy, where companies of all sizes and in any sector can compete on equal terms.
  - An open, democratic and sustainable society.
- Strategy aims at **value-based digital transformation** which will benefit everyone and offer **new opportunities for the economy**.

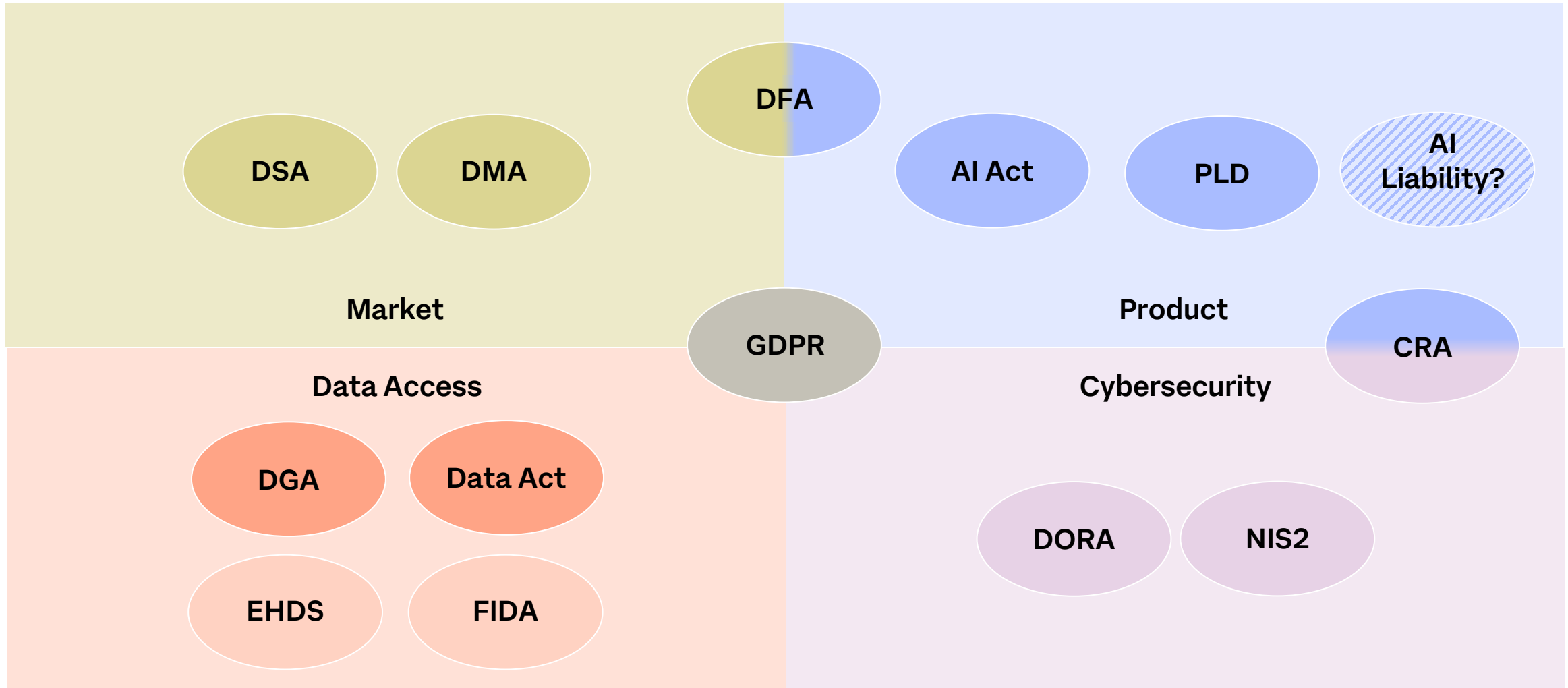
Creation of a legal framework for AI

European Data and Cyber Strategy

European Digital Platform and Service Package

Content and other

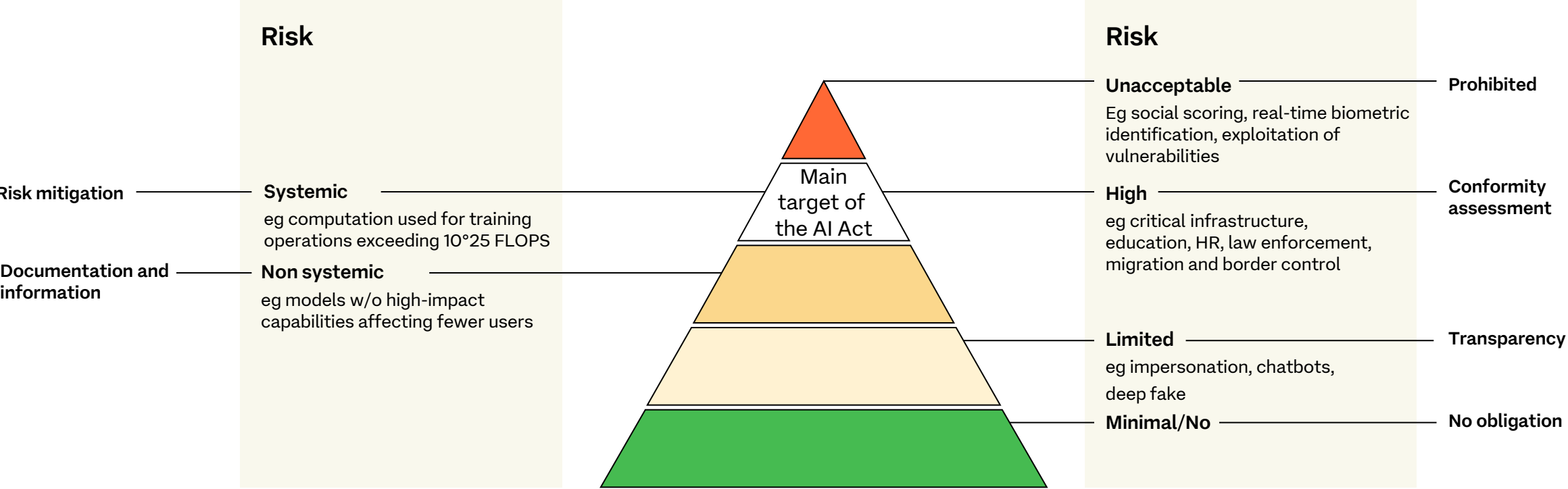
# EU Regulatory Landscape of Data & Tech



# AI Act

Harmonized rules on the development, use and distribution of AI systems. Safe AI systems that respect fundamental rights and Union values.

# AI Act



## GPAI model

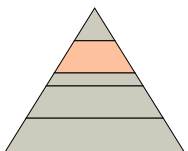
‘General-purpose AI model’ means an **AI model**, including where such an AI model is trained with a large amount of data using self-supervision at scale, that **displays significant generality** and is capable of competently performing a **wide range of distinct tasks** regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

## AI system

‘AI system’ means a **machine-based system** that is designed to operate with **varying levels of autonomy** and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

# High risk AI systems

What are high risk AI systems?



AI systems as safety components in critical infrastructure, such as road traffic, supply of water/gas/heating/electricity.

Biometric identification, categorisation and emotion recognition systems.

Education and vocational training.

Employment, workers management and access to self-employment.

Credit scoring and risk assessment and pricing of life/health insurance.

Essential public services, incl. healthcare and emergency services.

Law enforcement, migration, asylum and border control, administration of justice and democratic processes.

**Obligations: Providers of AI systems** must conduct a **conformity assessment** through which they certify themselves that the below obligations have been fulfilled. High-risk systems must then be **registered in an EU database**.

Risk management system

Data and data governance

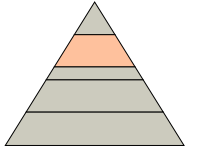
Technical documentation

Record-keeping

Transparency

Human oversight

Accuracy, robustness and security



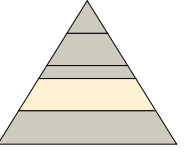
# Key obligations for high-risk AI systems

## Key obligations imposed on operators along the value chain regarding high-risk AI systems

	Providers	Importers	Distributors	Deployers
Compliance with technical requirements for the system development	✓	✗	✗	✗
Carrying out registration procedure and self-assessment	✓	✗	✗	✗ (for exceptions see*)
Preparation of technical documentation	✓	✗	✗	✗
Preparation of quality and risk management systems	✓	✗	✗	✗
Verification of the AI system's conformity with the AI Act	✓	✓	✓	✗
Carrying out corrective actions in case of non-compliance of the AI system	✓	✗	✓	✗
Suspend the use of the AI system when risks to health, safety and fundamental rights of natural persons have been identified	✓	✓	✓	✓
Notification obligations vis-à-vis the supervisory authorities	✓	✓	✓	✓

\* Except for (1) public bodies which must comply with registration obligations, and (2) deployers that are bodies governed by public law or private operators providing public services and **deployers of high-risk systems for creditworthiness evaluation/establishing credit score of natural persons, and risk assessment and pricing in relation to life and health insurance in banking and insurance**, which all must conduct a **fundamental rights impact assessment**.

# Transparency-related risks



## Requirements for AI systems with specific transparency risks

### Provider

AI systems intended to

1.  
interact with people, or

2.  
to generate audio, images,  
video or text content

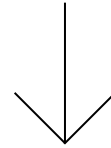
(e.g. chatbots for communication with customers/employees)

### Deployer

AI systems intended to

1.  
Emotion recognition  
systems, or

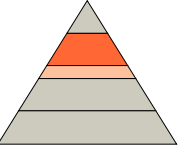
2.  
deep fakes



**Transparency obligations**  
(notification, labelling)



# General-purpose AI models



Providers of general-purpose AI (GPAI) models are subject to the AI Act since GPAI models can be incorporated into GPAI systems to generate audio, images, video or text

## Tiered approach

1.

### Obligations for all GPAI models

- Documentation and information-sharing.
- Complying with EU copyright law.
- Publishing summaries about the content used in training.
- Voluntary Codes of Conduct.

2.

### Additional obligations for GPAI models with “systemic risk”

- Assessing and mitigating systemic risks.
- Reporting of serious incidents assessing systemic risks.
- Ensuring an adequate level of cybersecurity.

## GPAI models with “systemic risk”

Most powerful models = presumed to be of systemic risk if it has reached a certain threshold of computational resources used in training (currently: greater than  $10^{25}$  FLOPS).

Commission can amend thresholds and include other criteria considering technological developments via delegated acts.

# Digital Services Act (DSA)

What is illegal offline must be illegal online. Broad regulation of providers of digital services with staggered obligations

# Goals



## Three key goals of the DSA:

1. Better protect consumers and their fundamental rights online
2. Establish a powerful transparency and a clear accountability framework for online platforms
3. Foster innovation, growth and competitiveness within the single market



## For users

- Better protection of fundamental rights
- More choice, lower prices
- Less exposure to illegal content



## For business users of digital services

- More choice, lower prices
- Access to EU-wide markets through platforms
- Level-playing field against providers of illegal content



## For providers of digital services

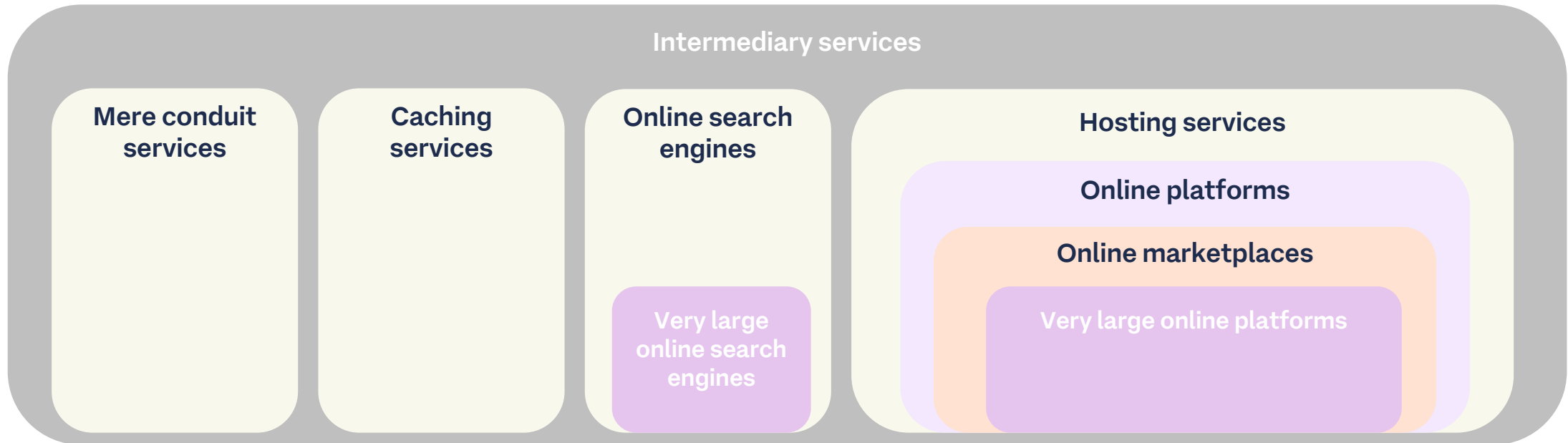
- Legal certainty and harmonisation of rules
- Tailored asymmetric obligations
- Easier to start-up and scale-up in Europe



## For society at large

- Greater democratic control and oversight over systemic platforms
- Mitigation of systemic risks, such as manipulation or disinformation

# Services in scope



## Intermediary services

- information society service that is offered to users located in the Union
- irrespective of the place of establishment of the service itself

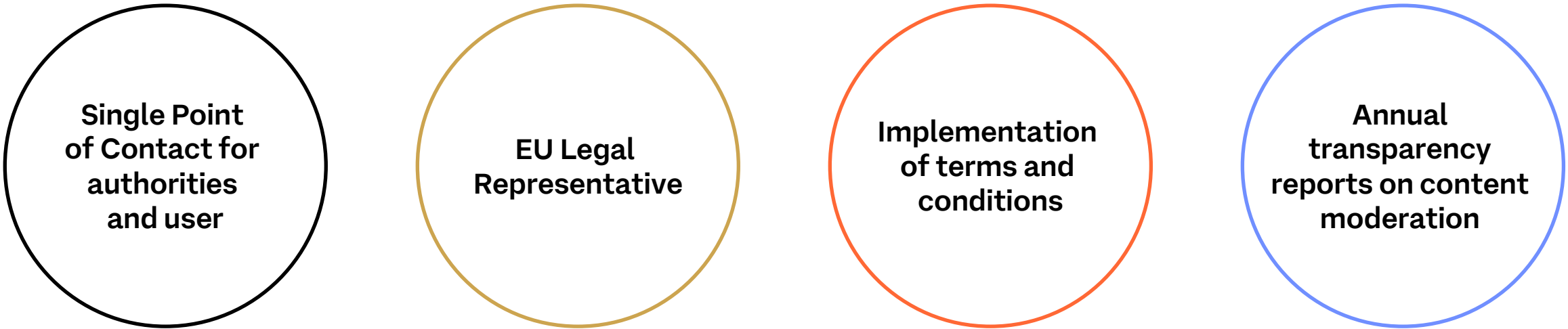


## Online platforms

- hosting service that stores and disseminates information to the public
- examples: social networks, content-sharing platforms, app stores, online marketplaces, and online travel and accommodation platforms

# Baseline obligations

A series of '**baseline**' obligations apply to all intermediaries providing 'mere conduit', 'caching' and 'hosting' services (e.g. ISPs and domain name registrars):



Single Point  
of Contact for  
authorities  
and user

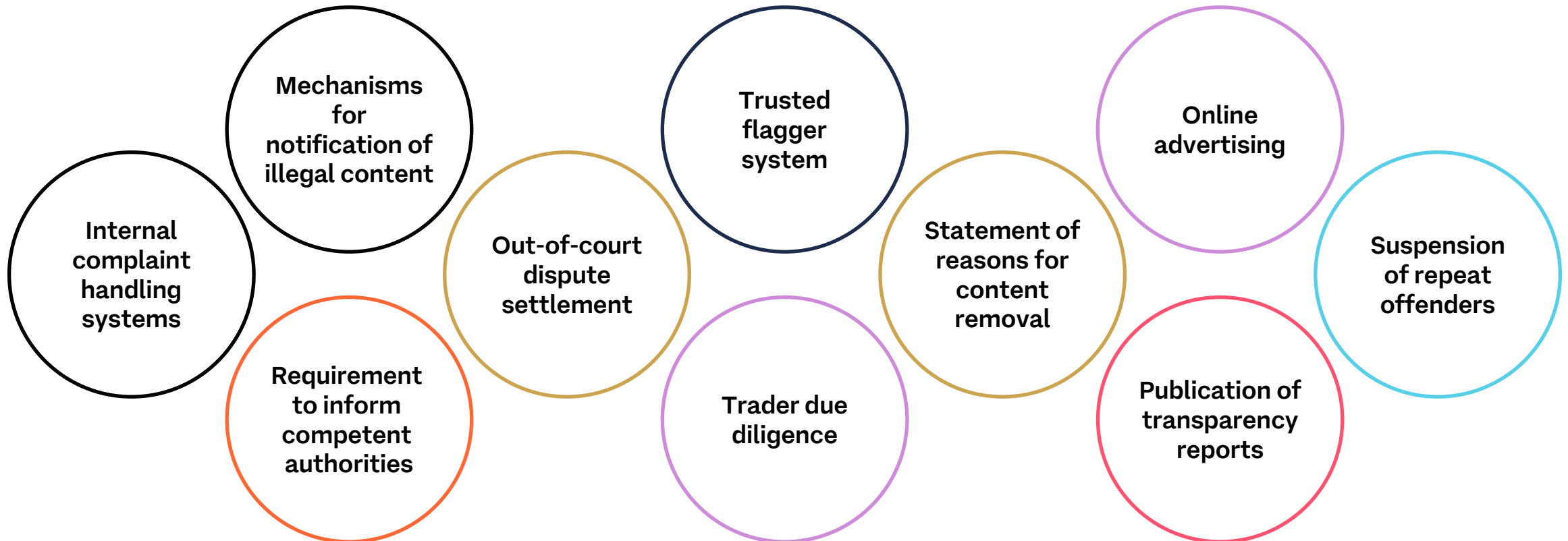
EU Legal  
Representative

Implementation  
of terms and  
conditions

Annual  
transparency  
reports on content  
moderation


# Obligations for all online platforms

Additional obligations apply to all online platforms, other than micro and small enterprises:



# Obligations for very large online platforms

The DSA imposes additional ‘top-up’ compliance, accountability and risk management obligations on **‘very large online platforms’** (VLOP) – defined as online platforms which provide their services to at least **45 million monthly active recipients** in the EU and which are designated as VLOP by the EU Commission:



Positive duty  
to identify and  
mitigate  
‘systemic  
risks’

Annual  
independent  
audit

Provide access  
to data to  
monitor  
compliance  
with DSA

Compliance  
officers

Enhanced  
transparency  
reporting  
obligations

# Designated VLOPs and search engines (May 2025)



\* In late May, the Commission de-designated Stripchat as a VLOP due to consistently low EU user numbers over the past year.



# Digital Markets Act (DMA)

Creating a novel competition law in the digital sector.

‘Gatekeepers’, digital companies above certain thresholds, require special regulation to keep markets contestable and fair.

# Overview of the Digital Markets Act

Entered into force on 1 November 2022, designation of gatekeepers by September 2023 and compliance required by March 2024

## Core Platform Service (CPS)

- Online intermediation services
- Online search engines
- Online social networking services
- Video-sharing platform services
- Number-independent interpersonal-communication services
- Operating systems
- Web browsers
- Virtual assistants
- Cloud computing services
- Online advertising services

### 1. Significant impact on the EU internal market

Presumed if the undertaking:

- provides the same CPS in at least three Member States; and
- EU turnover of at least €7.5bn in each of the last three financial years or market capitalisation / equivalent fair market value of at least €75bn in the last financial year.

### 2. CPS is an important gateway for business users to reach end users

Presumed if at least:

- 45m monthly active end users established/located in the EU; and
- 10,000 yearly active business users established in the EU.

### 3. Enjoy (or will foreseeably enjoy) an entrenched and durable position

Presumed if:

criteria in (2) above met in each of the previous three financial years.

### Requirements

General obligations vs obligations susceptible of being further specified

- Data use and access
- Tying/bundling
- Interoperability
- Self-preferencing
- Consumer switching/choice
- Transparency

- FRAND access
- Reporting & monitoring
- Merger notification requirements

# Data Act

Improving access, exchange and use of data for public and private stakeholders.

# Data Act

## Key aspects

- **Companies which manufacture/offer connected products and/or related services (including software)**
  - Obligation for companies to grant users (B2C), third parties (B2B) or the public sector (B2G) access to data: fair, transparent and non-discriminatory regulation (standards) of access to data.
  - Data access by design (connected products shall be designed to enable user accessing product data).
- **Provider of data processing services (incl. SaaS)**
  - Obligation for cloud service providers to allow users to easily switch cloud services and to improve portability between cloud providers.
  - Obligation to limit switching charges.

## Need-to-know/Risk management

- **Supervisory powers**
  - Each Member State must designate a competent authority responsible for application and enforcement and, if applicable, nominate a data coordinator.
  - Where personal data is concerned the relevant Data Protection Authority under GDPR is responsible.
- **Fines:** Data Act refers to GDPR fines, up to 4 percent of global annual turnover.
- **Enforcement in Member States** (class/collective actions and private litigation).

# European Cybersecurity Law

# NIS2 Directive

## Key aspects

- **Scope:** Applies (mainly) to **medium** and large **entities** in **specific critical sectors**, eg **digital infrastructure (incl. SaaS)**
- **Governance**
  - Management bodies must approve cybersecurity risk-management measures and oversee its implementation.
  - Management liability for potential infringement by entity.
- **Cybersecurity risk-management measures**
  - Take appropriate and proportionate TOMs, state-of-the-art.
- **Reporting obligations**
  - Entities are required to notify significant incidents within a given time frame.

## Need-to-know/Risk management

- **Supervisory powers**
  - The designated national authority can carry out, eg, on-site inspections or Ad hoc audits.
  - Essential entities: Any person at C-Level can be temporarily prohibited from exercising management functions.
- **Fines**
  - Essential entities: up to 2 percent of global annual turnover.
  - Important entities: up to 1,4 percent of global annual turnover.
- **Three-step reporting obligations for significant incidents**

1. Early warning within **24 hours** of becoming aware of incident.

2. Incident notification within in **72 hours** of becoming aware of incident (+ notification of competent DPA).

3. Final report **one month** after incident notification.

# Cyber Resilience Act

## Key aspects

- **Scope:** All wired and wireless products connected to the internet and **software** that are placed on the EU market. **SaaS is generally excluded** from the scope.
- **Obligations for manufacturers**
  - Essential cybersecurity requirements.
  - Vulnerability handling process
  - Conformity assessment: Non-critical products | Critical products | High-risk AI products.
  - Information/Transparency obligations.
- **Due diligence obligations for importers/distributors**
  - **Importers** must ensure compliance with cybersecurity requirements and CE marking, while **distributors** must verify the CE marking and the fulfilment of obligations by manufacturers and importers.

## Need-to-know/Risk management

- **Supervisory powers:** The designated national authority can, eg, conduct an evaluation of a product; request access to data and documentation; bring non-compliance to an end and eliminate the risk, incl. an order to withdraw products from the market.
- **Fines:** Up to 2.5 percent of global annual turnover.
- **Reporting obligations**
  - Manufacturers: to the **European Union Agency for Cybersecurity** and national authorities within **24 hours** of becoming aware of any actively exploited vulnerability and **to users** without undue delay.
  - Importers and Distributors: To the manufacturer without **undue delay**.

# Thank you!



**Dr. Theresa Ehlen**

Partner, Global Transactions  
Düsseldorf

E [theresa.ehlen@freshfields.com](mailto:theresa.ehlen@freshfields.com)



**Dr. Christina Möllnitz-Dimick**

Associate, Dispute Resolution  
Munich

E [christina.moellnitz@freshfields.com](mailto:christina.moellnitz@freshfields.com)

This material is provided by Freshfields, an international legal practice. We operate across the globe through multiple firms. For more information about our organisation, please see <https://www.freshfields.com/en-gb/footer/legal-notice/>.

Freshfields LLP is a limited liability partnership registered in England and Wales (registered number OC334789). It is authorised and regulated by the Solicitors Regulation Authority (SRA no. 484861).

This material is for general information only. It is not intended to provide legal advice on which you may rely. If you require specific legal advice, you should consult a suitably qualified lawyer.

© 2025 Freshfields LLP, all rights reserved

[www.freshfields.com](http://www.freshfields.com)

DS205221