

# *EU's digital strategy and the role of the IT auditor*

-

## *Digital Services Act (DSA) and Responsible AI*

# Agenda

- 01 Introduction
- 02 EU digital initiatives
- 03 DSA
- 04 AI
- 05 Compliance story
- 06 Questions

**01**

# **Introduction**

# With you today



**Manon van Rietschoten**  
**RE RA**  
**Senior Manager, IT**  
**Assurance**  
**KPMG**



















**Angelica van Beemdelust**  
**Consultant, Responsible AI**  
**KPMG**



**02**

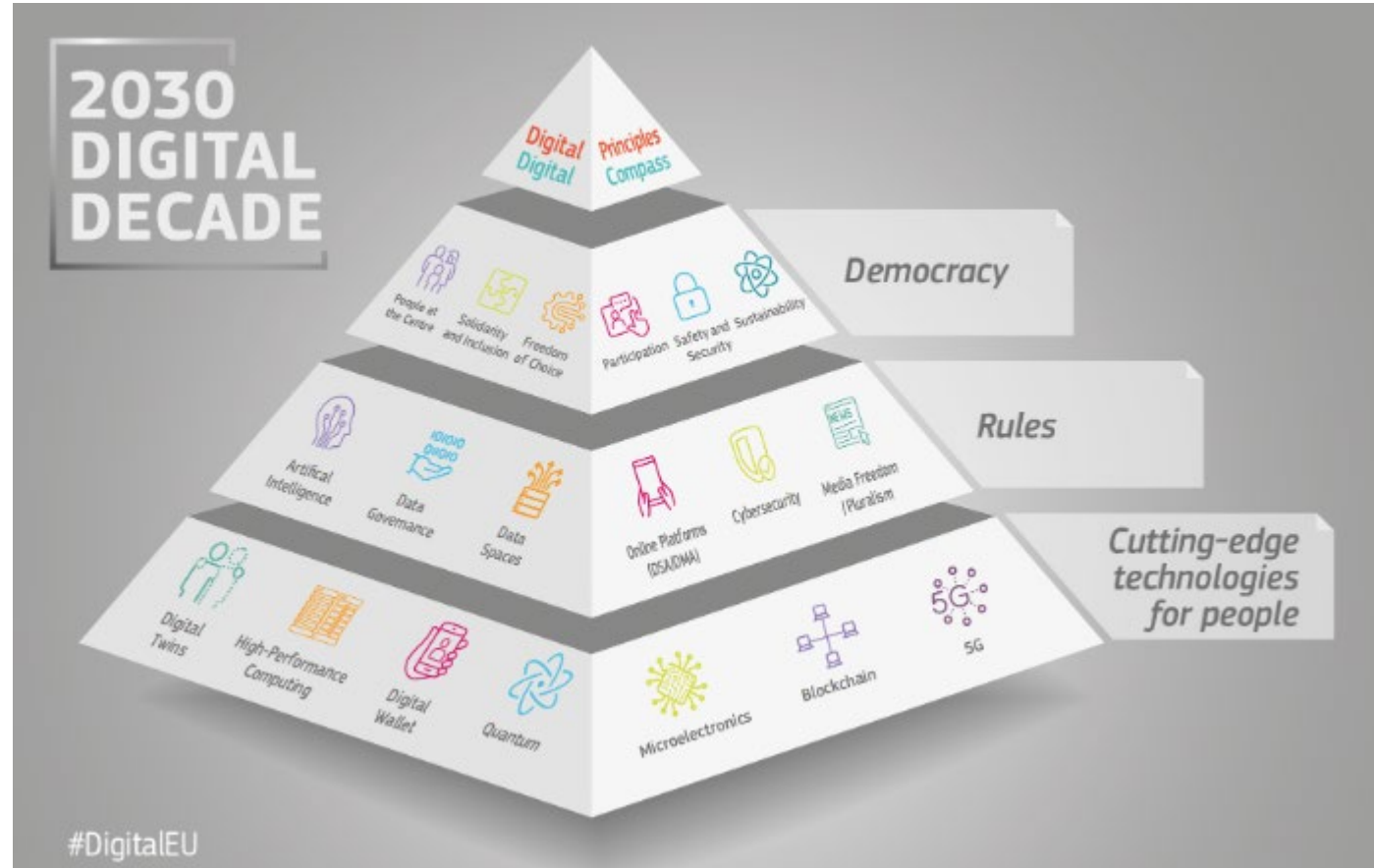
# **EU digital initiatives**

# Organisations take emerging technological opportunities to profit from

<b>3D printing</b>  <b>Ultimaker</b>	<b>Artificial Intelligence</b> 	<b>Cloud</b> 	<b>Sensors</b> 	<b>Advanced materials</b> <b>carbon3D</b>	<b>Platform business</b> 
<b>Robotics</b> 	<b>IoT</b> 	<b>Self-driving cars</b> 	<b>Augmented / Virtual reality</b> 	<b>Bio tech</b> 	<b>Blockchain</b> 
<b>Drones</b> 	<b>Big Data, Predictive &amp; Cognitive data analytics</b>	<b>Digital infrastructures</b> 	<b>Solar energy</b> 	<b>Quantified self</b> 	<b>Access over ownership</b> 

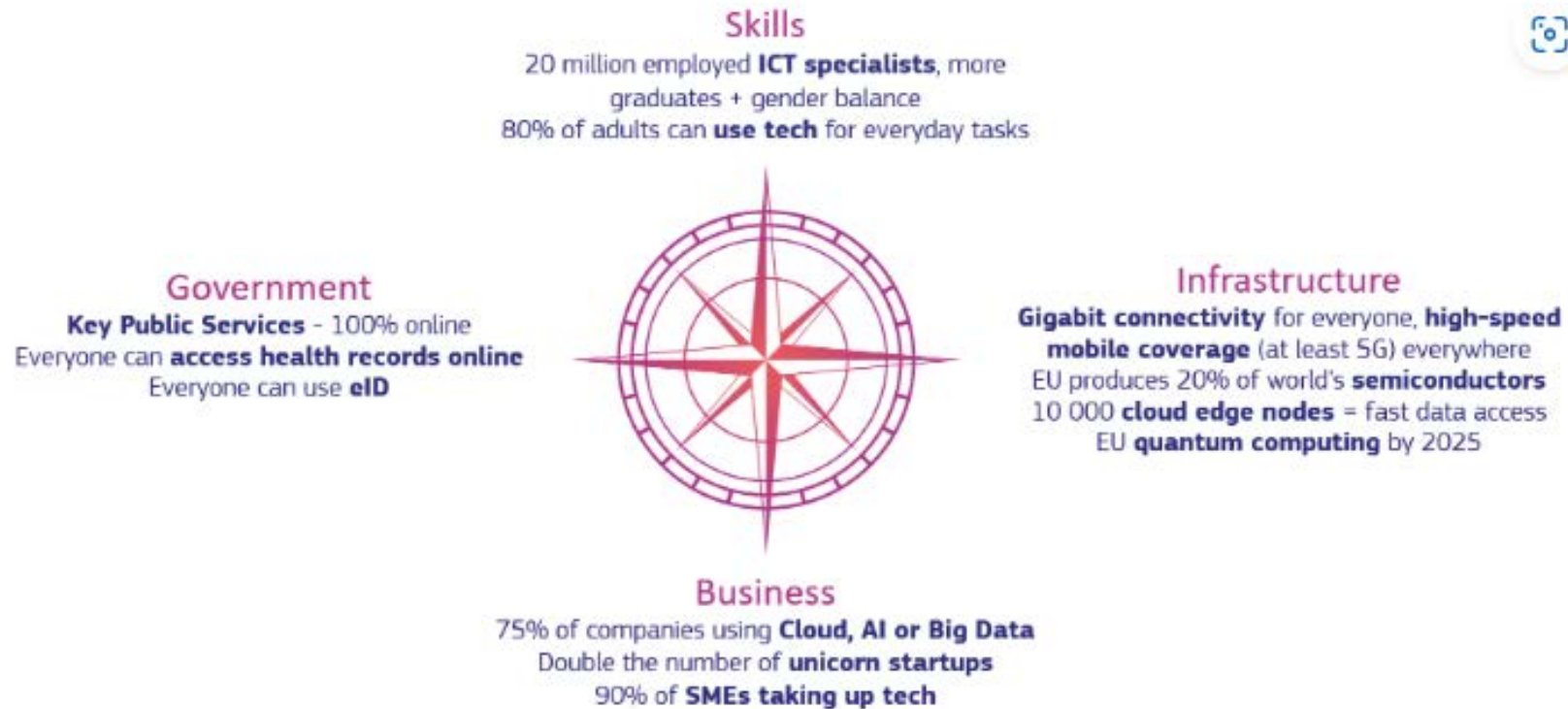


# Europe's digital decade (source EC)



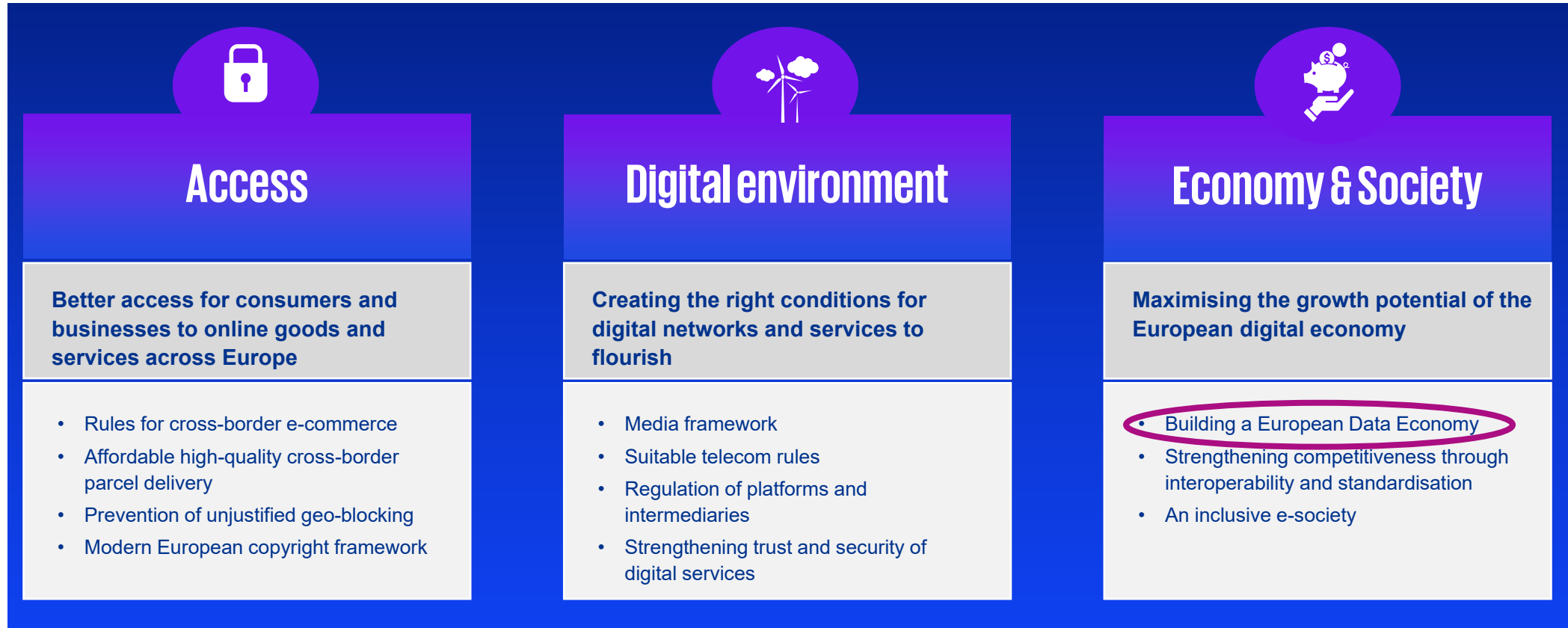
[Europe's Digital Decade | Shaping Europe's digital future \(europa.eu\)](https://europa.eu)

# Goals Europe's digital decade (source EC)

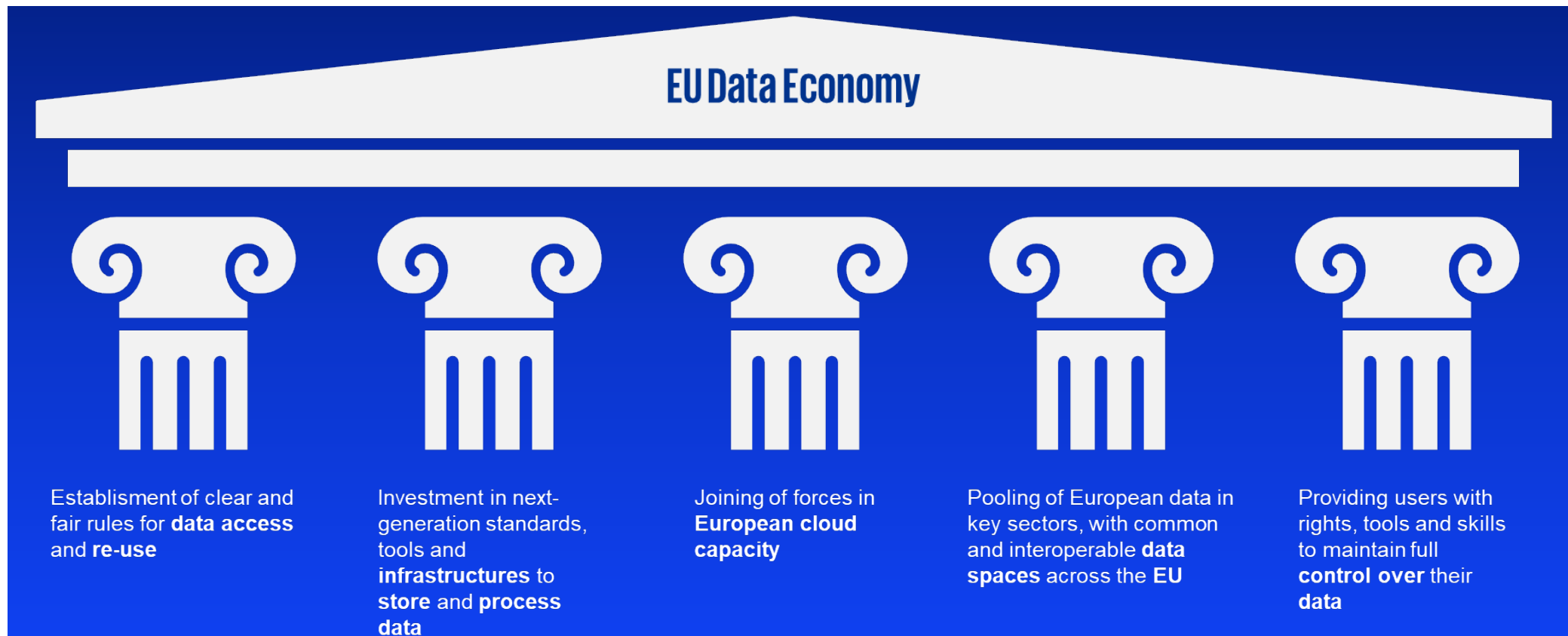




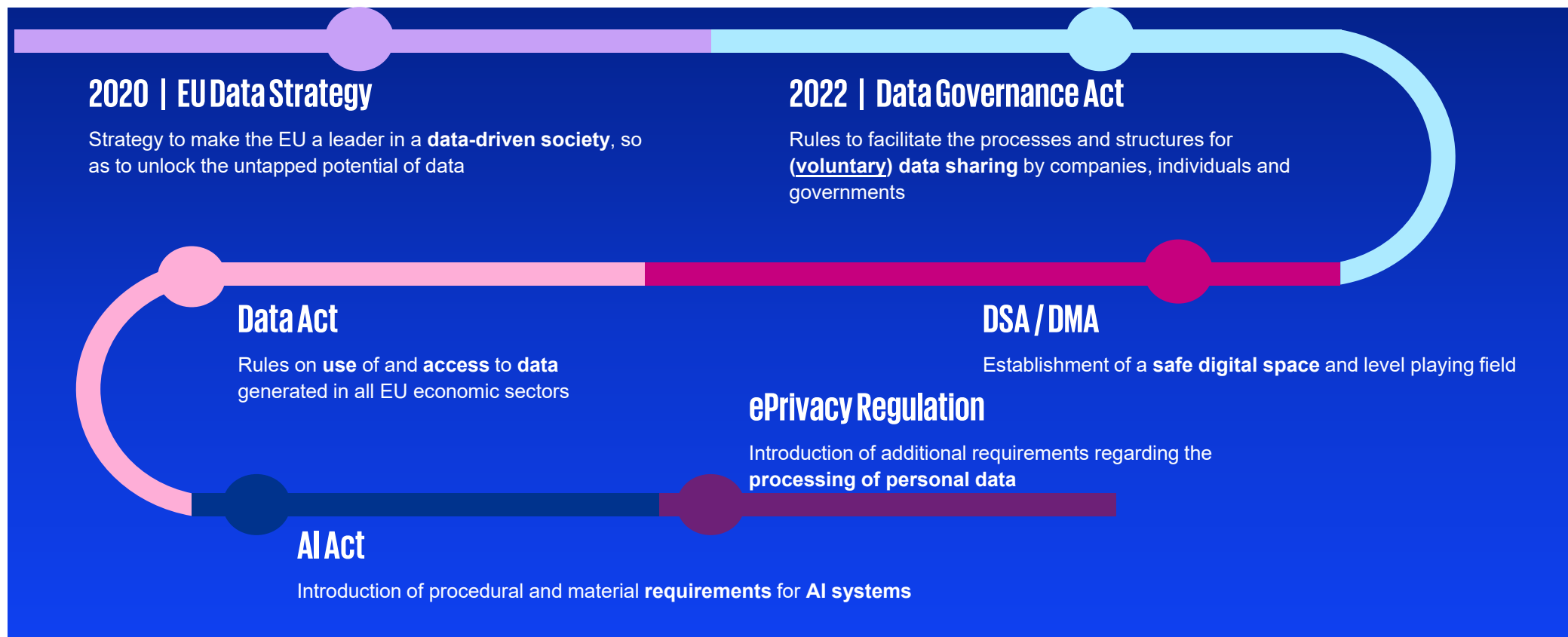
# Three pillars of the EU Digital Single Market; emphasis on establishing the EU Data Economy



# Five pillars of the EU Data Economy



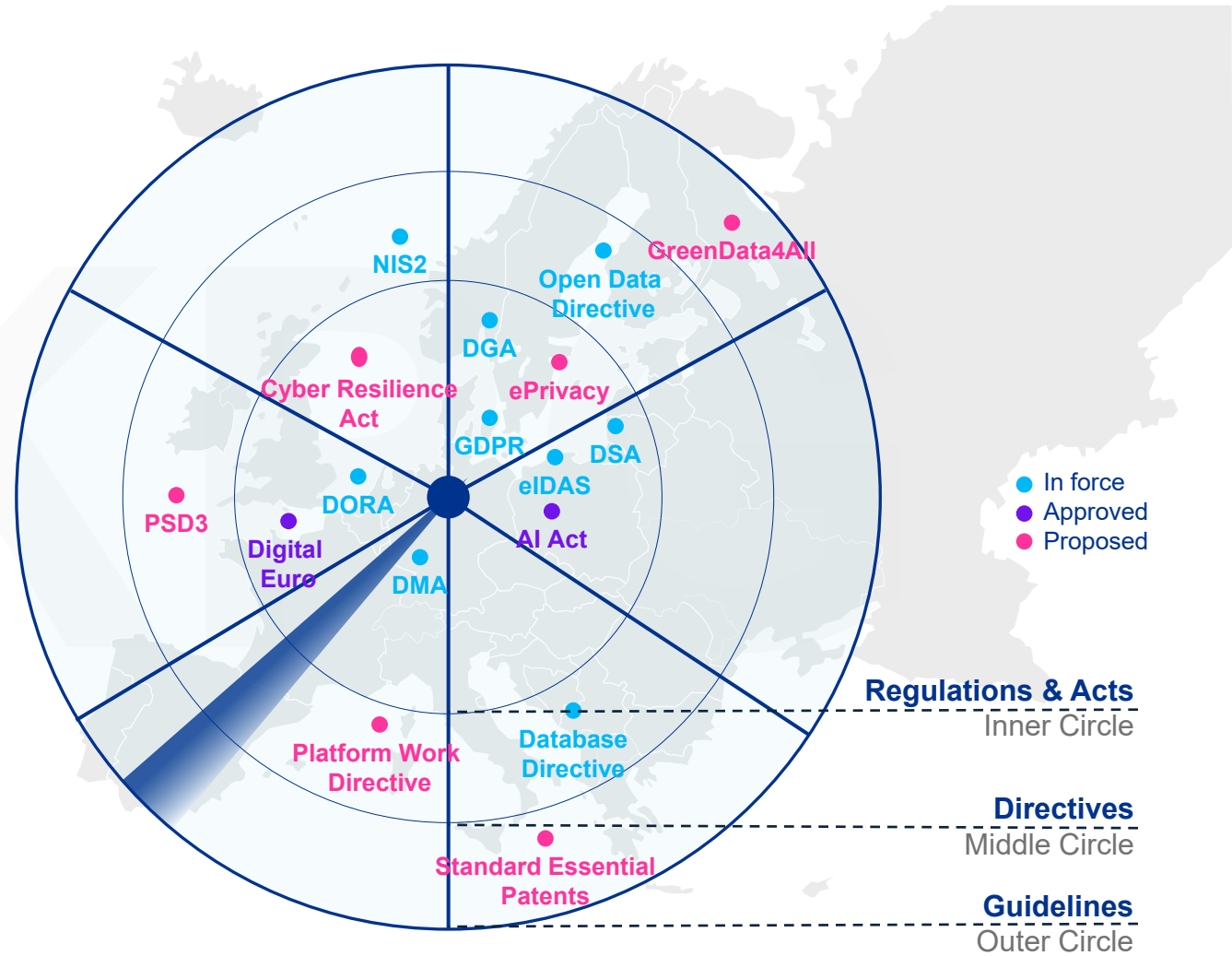
# Formation of the EU Data Economy



# Overview EU digital acts – Regulatory Horizon

“ In the coming years, the tech sector will become just as regulated as the financial sector ”

Martijn Snoep, Charmain ACM (Digital Service Coordinator for NL)



# Key points of attention data legislation (1 / 2)

	Data Act	Data Governance Act	ePrivacy Regulation	Digital Markets Act	Digital Services Act
1	<b>Right to data portability</b> extended to <b>non-personal data</b>	<b>Permission</b> under <b>DGA</b> does not serve as ' <b>consent</b> ' under <b>GDPR</b>	<b>Applicability</b> dependent on <b>technology</b> used, in lieu of nature of data	<b>Restricts</b> GDPR's <b>legal bases</b> for processing of personal data for certain activities from 6 to 4	<b>Traders</b> on marketplaces must be assessed on their <b>compliance</b> with <b>GDPR</b>
2	<b>Sensitive personal</b> data could become the object of data sharing	<b>Mixed datasets</b> are subject to GDPR obligations (including that of <b>controllers</b> and <b>processors</b> )	<b>Cookies</b> require <b>consent</b> that is <b>valid</b> under <b>GDPR</b>	Personal data <b>sourced</b> from <b>different</b> core <b>services</b> may (in principle) not be <b>combined</b>	<b>GDPR policies</b> of <b>traders</b> must be made available to end users
3	<b>Mixed datasets</b> will cause <b>overlay</b> and increased <b>complexity</b>	<b>Inconsistencies</b> between the GDPR and DGA might arise	Prohibition of <b>pre-ticked boxes</b>	<b>Consumer</b> (personal) <b>data</b> must be <b>portable</b> ('data portability')	<b>Marketplaces' interfaces</b> must <b>enable traders</b> to comply with <b>GDPR</b>
4	<b>GDPR prevails</b> in case of conflict	<b>GDPR prevails</b> in case of conflict	Prohibition of <b>cookie walls</b> (without explicit consent)	<b>Non-public (personal) data</b> generated from business and end users may not be used to <b>compete</b> with <b>business users</b>	<b>Marketplaces</b> must <b>enable traders</b> to publish their <b>GDPR policy</b>

# Key points of attention data legislation (2 / 2)

	AI Act	EU Data Spaces	Wet hergebruik overheidsinformatie	Wet open overheid
1	Users/providers of AI systems, as resp. 'controllers'/processors' must comply with their respective <b>GDPR obligations</b> when using <b>AI systems</b>	Both <b>personal-</b> and <b>non-personal</b> data can be shared or granted access to	<b>GDPR</b> must be <b>adhered</b> to when applying <b>Who*</b>	<b>Restricts</b> the <b>legal bases</b> on which (government held) <b>sensitive personal data</b> may be <b>disclosed</b> (processed)
2	<b>DPIA</b> must be performed for <b>high-risk AI systems</b>	<b>Comply</b> and <b>operate</b> within the rules of the <b>GDPR</b>	(Personal) data may only be re-used if the re-use is <b>compatible</b> with the <b>initial purpose</b> for which the (personal) data was collected	<b>GDPR principles</b> (e.g. data minimization and transparency) must be <b>adhered</b> to when applying Woo
3	<b>Sensitive personal data</b> may also be processed to <b>de-bias algorithms</b>	<b>Secure</b> and <b>privacy-preserving</b>	The amended Who (in principle) <b>prohibits</b> the <b>re-use</b> of <b>personal data</b>	Any <b>disclosure</b> requires a <b>balancing of interest</b> between <b>disclosure</b> and data subject's <b>privacy</b>
4	GDPR's required <b>human oversight</b> extended to <b>providers</b> of AI systems	<b>Voluntary basis</b> for data sharing	The amended Who allows the <b>re-use</b> of <b>personal data</b> when adequately <b>anonymized</b>	Any <b>disclosure</b> requires a <b>GDPR</b> assessment of the <b>necessity</b> of the disclosure



## Overzicht Relevante Europese Wetgeving cybersecurity

- + Het doel van bijgaand overzicht van relevante Europese wetgeving betreffende cybersecurity, data en gerelateerde onderwerpen kan IT-auditors en andere belanghebbenden ondersteunen bij hun werkzaamheden. Dit overzicht beoogt een snelle en eenvoudige toegang te bieden tot de meest prominente wetgeving in dit domein, met nadruk op de connectie met NOREA- publicaties en hulpmiddelen.
- + Dit overzicht is bedoeld voor professionals die zich bezighouden met cybersecurity, data en gerelateerde onderwerpen, en die behoefte hebben aan een beknopt en praktisch overzicht van hierbij relevante Europese wetgeving
- + De achtergrond voor dit overzicht is de complexiteit van de Europese wetgeving, met meer dan 2000 wetten en richtlijnen, die het navigeren door dit landschap uitdagend maakt. De NOREA Kennisgroep cybersecurity heeft daarom een selectie gemaakt van de meest relevante wetgeving met betrekking tot cybersecurity, data en gerelateerde onderwerpen op basis van hun expertise

wetgeving	publicatie datum	in-werking datum	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
<b>Data protection</b>																			
GDPR	2016	2018																	
<b>Digital strategy</b>																			
NIS		2016																	
Cyber Security Act	2019	2024																	
Digital Service Act (DSA)	2022	2022																	
Data Governance Act		2022																	
CER	2022	2023																	
Cyber resilience Act	2022	2024																	
NIS2		2023																	
Data Act		2024																	
e-ID aka EIDAS 2.0	TBD	TBD																	
EIDAS	2014	TBD																	
AI Act		TBD																	
<b>Business, Economy, Euro</b>																			
PSD2	2015	2016																	
Digital Market Act (DMA)	2022	2022																	
CSRD	2022	2023																	
DORA	2022	2023																	
MICAR	2023	2024																	
PSD3	2023	TBD																	
FIDA	2023	TBD																	
RAAI		TBD																	

**inhoud**

Overzicht van de geselecteerde wetgeving:

- Wetten en richtlijnen met een beknopte beschrijving van hun doelstellingen en reikwijdte.
- Categorieën: cybersecurity, data, privacy, e-commerce, etc.

Koppelingen naar NOREA publicaties en hulpmiddelen:

- Verwijzingen naar relevante NOREA- studies, rapporten, brochures, tools en andere resources.

Informatie over updates:

- Dit is een "levend document" dat periodiek (minimaal 1x per jaar) wordt geactualiseerd door de Kennisgroep.

**gebruik**

Als referentiekader:

- Snelle toegang tot de meest relevante Europese wetgeving inzake cybersecurity, data en aanpalende onderwerpen.

Als startpunt voor verdere verdieping:

- De beschrijvingen en koppelingen in het overzicht leiden naar meer gedetailleerde informatie over de geselecteerde wetgeving.

Als bron voor NOREA publicaties en hulpmiddelen:

- Toegang tot relevante NOREA expertise en ondersteuning.

**over**

De NOREA Kennisgroep cybersecurity is een platform voor kennisdeling en samenwerking tussen professionals in het publieke en private domein. De Kennisgroep organiseert workshops, bijeenkomsten en trainingen, en publiceert studies en rapporten over actuele thema's inzake cybersecurity.

Disclaimer: Dit overzicht is een samenvatting van de wetgeving en kan niet worden gebruikt als juridisch advies. Raadpleeg altijd een expert voor de interpretatie en toepassing van wetgeving.

**03**

# **Digital Services Act - DSA**

# The need for regulation

## Amazon Gets Record \$888 Million EU Fine Over Data Violations

### How TikTok's algorithm 'exploits the vulnerability' of children

Kevin Rawlinson

Up to 1.4m children under 13 use app, watchdog finds - and experts say they are being flooded with harmful content to promote addiction

● **TikTok fined £12.7m for illegally processing children's data**



**Antitrust: Commission fines Microsoft for non-compliance with browser choice commitments**

### European Union fines Facebook parent Meta 390M euros for privacy violations

LONDON (AP) — European Union regulators on Wednesday hit Facebook parent Meta with hundreds of millions in fines for privacy violations and banned the company from forcing users in the 27-nation bloc to accept personalized ads based on their online activity.

Amazon faces \$1 bln lawsuit in UK for 'favouring its own products'



**The EU tells Twitter to hire more human content moderators amid concerns of rise of illegal content**

YouTube fined \$170m after collecting personal data of children under 13

YouTube is said to have touted its popularity with children while marketing itself to toymakers such as Mattel and Hasbro.

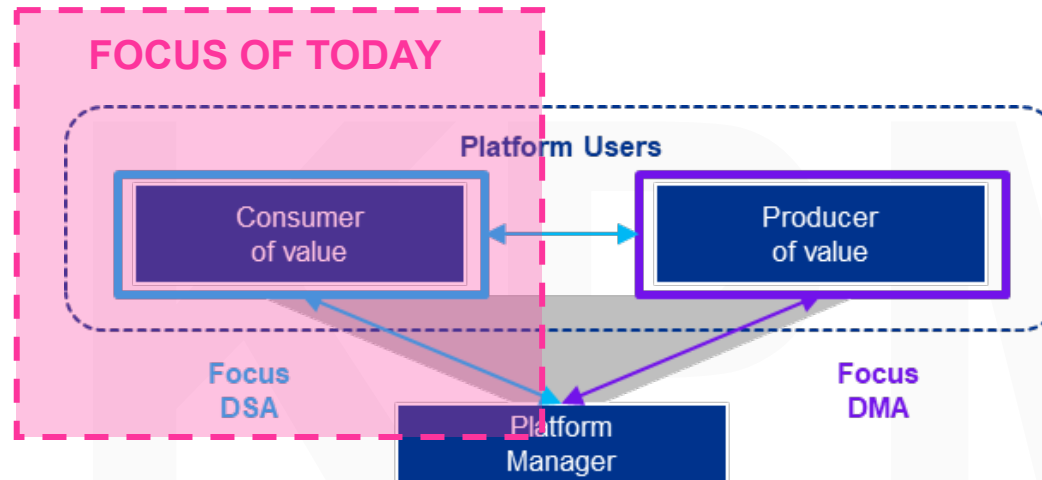
**Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising**



# 1. Digital Service Act (DSA) and Digital Markets Act (DMA)

The **Digital Services Act** (DSA) and the **Digital Market Act** (DMA) form a set of rules that apply across the whole EU. They have two main goals:

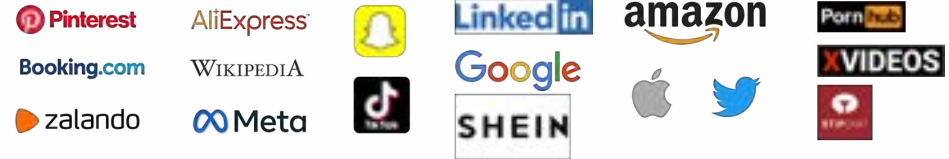
1. to create a **safer digital space** in which the fundamental rights of all users of digital services are protected;
2. to establish a **level playing field** to foster innovation, growth, and competitiveness, both in the European Single Market and globally.



- Applies to **Digital Service Providers**
- Protect **consumers (recipients of the service)**
- Obligations on content moderation, recommender systems, risk management and transparency
- **Scope of DSA includes online intermediaries and platforms**
- **Audit obligation** to very large online platforms and search engines (VLOP / VLOSE) on all Chapter 3 obligations.

- Applies to **Gatekeepers**, which are digital service providers with a very dominant position.
- Level playing field: fairness towards **Business Users**
- Obligations on fairness of recommender systems and freedom of users to access data that helps them to circumvent the dominant platform
- **Audit obligation (Art. 15)** solely on the completeness and accuracy of the profiling description

# The Digital Services Act explained (DSA)



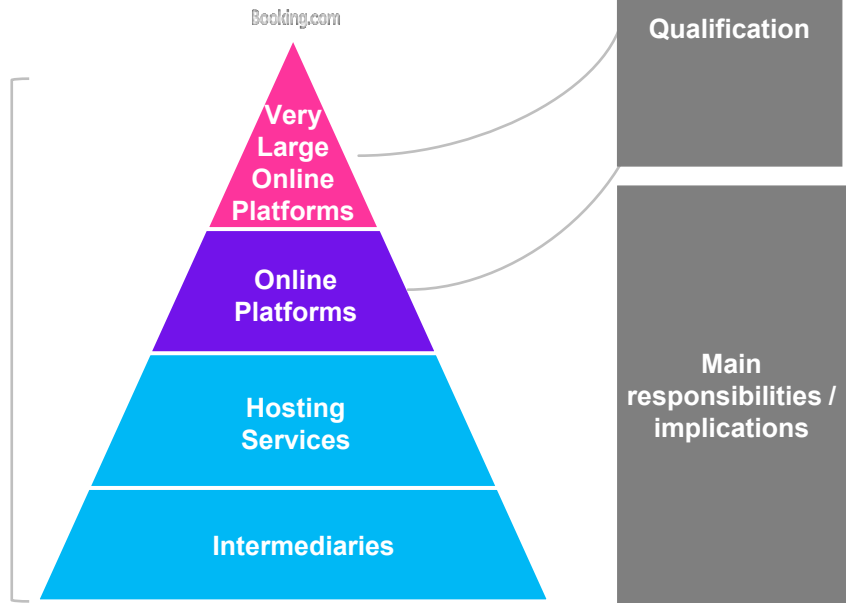
Penalties impose fines up to:

**6%** of global turnover

Temporary **suspend** services

Require **immediate** actions

Digital Services Act (DSA)



**Online Platforms ("OP")**

**Online platforms** are defined in the DSA as providers of hosting services that publicly disseminate users' information.

The EC expressly states that i.e. online marketplaces, travel websites and collaborative economy platforms qualify as online platforms.

- DSA impact for OPs is predominantly expected in the following areas:
- I. Content moderation and decision-making
  - II. Algorithms, recommender systems transparency
  - III. Trusted flaggers, illegal content & KYBC
  - IV. Reporting and transparency
  - V. Platform design
  - VI. Advertising (transparency)

**Very Large Online Platforms ("VLOP")**

**Online platforms** with >45 million monthly EU users.

The EC holds the right to scrutinize and determine user numbers themselves, and to allocate VLOPs based on this calculation.

- In addition to Online Platforms additional obligations include:
- I. Systemic risk assessment
  - II. Crisis response systems
  - III. Independent audit
  - IV. Recommender systems based on non-profiling
  - V. And other regulations concerning transparency

# DSA articles

I  
(Legislative act)

## REGULATIONS

**REGULATION (EU) 2022/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
**of 19 October 2022**  
**on a Single Market for Digital Services and amending Directive 2000/11/EC (Digital Services Act)**  
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,

Having regard to the opinion of the Committee of the Regions <sup>(2)</sup>,

Acting in accordance with the ordinary legislative procedure <sup>(3)</sup>,

Whereas

(1) Information society services and especially intermediary services have become an important part of the Union's economy and the daily life of Union citizens. Twenty years after the adoption of the existing legal framework applicable to such services laid down in Directive 2000/11/EC of the European Parliament and of the Council <sup>(4)</sup>, new and innovative business models and services, such as online social networks and online platforms allowing consumers to conclude distance contracts with traders, have altered business users and consumers to interact and access information and engage in transactions in novel ways. A majority of Union citizens now uses those services on a daily basis. Moreover, the digital transformation and increased use of those services has also resulted in new risks and challenges for individual recipients of the relevant services, companies and society as a whole.

(2) Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation, imposing, in particular, diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online discrimination or other societal risks. These diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty on the Functioning of the European Union (TFEU), comprises an area without internal frontiers in which the free movement of goods and services and burdens of establishment are ensured, taking into account the inherently cross-border nature of the internet, which is generally used to provide those services. The conditions for the provision of intermediary services

<sup>(1)</sup> OJ C 386, 16.7.2022, p. 76.

<sup>(2)</sup> OJ E 448, 29.10.2022, p. 47.

<sup>(3)</sup> Position of the European Parliament of 3 July 2022 (not yet published in the Official Journal) and decision of the Council of 9 October 2022.

<sup>(4)</sup> Directive 2000/11/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 13.7.2000, p. 1).

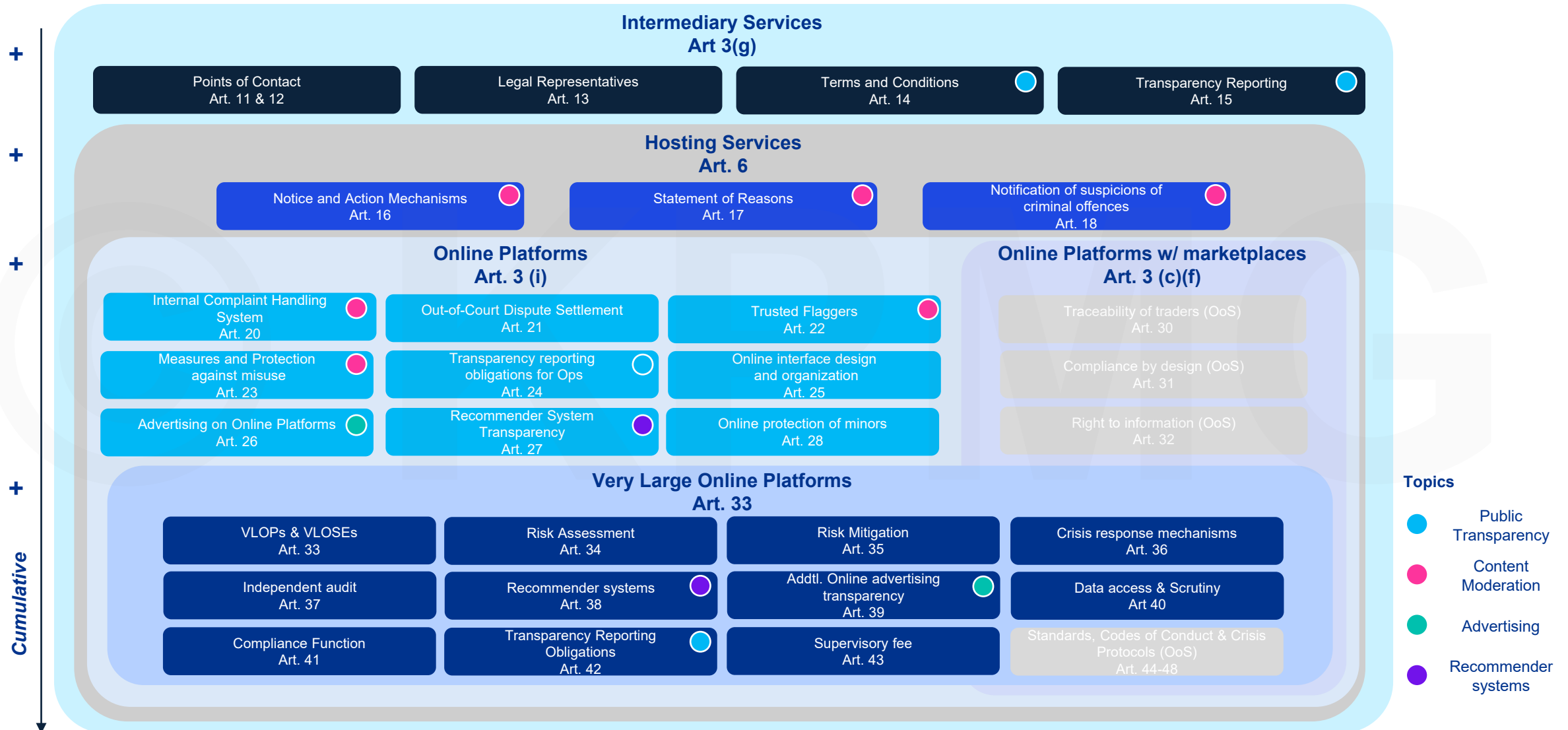


# DSA articles



Article	Description
11	Points of Contact for Member States' authorities, the Commission and the Board.
12	Points of contact for recipients of the service
13	Legal representatives
14	Terms and conditions
15, 24, 42	Transparency reporting
16	Notice and action mechanisms
17	Statement of reasons
18	Notification of suspicions of criminal offenses
20	Internal complaint handling system
21	Out-of-court dispute settlement
22	Trusted flaggers
23	Measures and protection against misuse
25	Online interface design and organisation
26, 39	Advertising on online platforms
27, 38	Recommender systems
28	Online protection of minors
30	Traceability of traders
31	Compliance by design
32	Right to information
34	Risk assessment
35	Risk mitigation
36	Crisis response mechanism
37	Independent audit
40	Data access and scrutiny
41	Compliance function
45, 46, 47	Codes of Conduct
48	Crisis protocol

# Structure and topics of the DSA (and scope of Audit)



# European Contact Group (ECG)

**Represents the six largest international professional services networks in Europe. The ECG mission is to contribute constructively to European legislation and policy debates to maintain confidence in the profession and large networks in Europe**

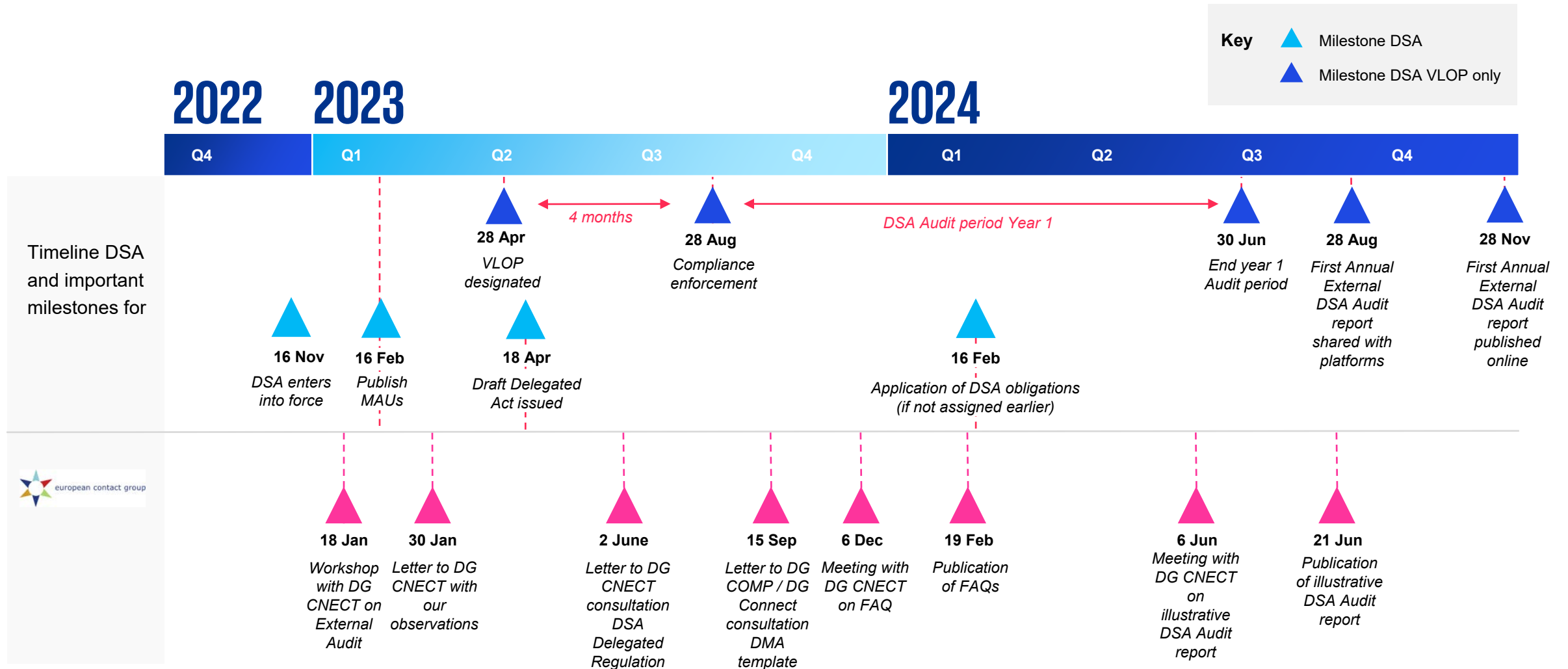


## Topics that have been discussed:

- The use of Assurance standards (i.e. ISAE 3000)
- The use of Audit Criteria and Benchmarks
- The Audit of Codes of Conducts
- The Audit period
- The Audit Risk Assessment
- The Audit conclusions and overall opinion
- The Audit Report template

*Several meetings have been held with the European Commission to challenge the Delegated Act and to confirm a common understanding of its interpretation.*

# What we have done so far



# Challenges



Collaborate to work on illustrative Audit reports and FAQs



We are no lawyers – Interpretation of ambiguous terms / obligations remains a challenge



Reasonable assurance in year 1 is challenging for both the platforms and the auditors



Various conversations with the DG CNECT (4 meetings held) and open to connect further



Mixed skillset in team is pivotal (Tech Law, AI Assurance, Tech Assurance and Privacy)



More to come (AI Act, ePrivacy Regulation, EU COPD, EU CoC Hate Speech, etc)

# Delegated Regulations vs ISAE 3000 standard



- Reasonable assurance in year 1
- Delegated Regulation on Auditing the DSA
- Differences between ISAE 3000 and Delegated Regulation

## Audit opinion

### Article 8

#### Audit opinion, audit conclusions and recommendations

- The audit report shall include the audit conclusions that the auditing organisation has reached on the audited provider's compliance with each of the audited obligations and commitments. The audit conclusions shall be either:
  - 'positive', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has complied with an audited obligation or commitment;
  - 'positive with comments', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has complied with an audited obligation or commitment, but:
    - the auditing organisation includes remarks on the benchmarks provided by the audited provider pursuant to Article 5(1), point (a); or
    - the auditing organisation recommends improvements that do not have a substantive effect on its conclusion.
  - 'negative', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has not complied with an audited obligation or commitment.

## Reporting template

### ANNEX I - Template for the audit report referred to in Article 4

#### Table of contents

SECTION A: General information	
1. Audited service:	.....
2. Audited provider:	.....
3. Address of the audited provider:	.....
4. Point of contact of the audited provider:	.....
5. Scope of the audit:	
a. Does the audit report include an assessment of compliance with all the obligations and commitments referred to in Article 37(1) of Regulation (EU) 2022/2065 applicable to the audited provider? Yes/No	
i. Compliance with Regulation (EU) 2022/2065	
Obligation set out in Chapter III of Regulation (EU) 2022/2065:	
Audited obligation	Period covered
Indicate the precise obligation audited	(DD/M/YYYY)
Insert as many lines as necessary	(DD/M/YYYY)
ii. Compliance with codes of conduct and crisis protocols	
Commitments undertaken pursuant to codes of conduct referred to in Articles 45 and 46 of Regulation (EU) 2022/2065 and crisis protocols referred to in Article 48 of Regulation (EU) 2022/2065:	
Audited commitment	Period covered
Specify the code of conduct or crisis protocol and the	(DD/M/YYYY)

## Disclosure requirements

4. Providers of very large online platforms or of very large online search engines shall transmit to the Digital Services Coordinator of establishment and the Commission, without undue delay upon completion, and make publicly available at the latest three months after the receipt of each audit report pursuant to Article 37(4):

- a report setting out the results of the risk assessment pursuant to Article 34;

- (b) the specific mitigation measures put in place pursuant to Article 35(1);

- (c) the audit report provided for in Article 37(4);

- (d) the audit implementation report provided for in Article 37(6);

- (e) where applicable, information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures.

5. Where a provider of very large online platform or of very large online search engine considers that the publication of information pursuant to paragraph 4 might result in the disclosure of confidential information of that provider or of the recipients of the service, cause significant vulnerabilities for the security of its service, undermine public security or harm recipients, the provider may remove such information from the publicly available reports. In that case, the provider shall transmit the complete reports to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of the reasons for removing the information from the publicly available reports.



# Audit opinions DSA / ISA 3000

## Article 8

### *Audit opinion, audit conclusions and recommendations*

1. The audit report shall include the audit conclusions that the auditing organisation has reached on the audited provider's compliance with each of the audited obligations and commitments. The audit conclusions shall be either:
  - (a) 'positive', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has complied with an audited obligation or commitment;
  - (b) 'positive with comments', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has complied with an audited obligation or commitment, but:
    - (i) the auditing organisation recommends improvements that do not have a substantive effect on its conclusion;
    - (ii) the auditing organisation indicates that it has applied audit criteria pursuant to Article 10(2), point (a), which are different from the benchmarks for compliance communicated by the audited provider pursuant to Article 5(1), point (a).
  - (c) 'negative', where the auditing organisation concludes with a reasonable level of assurance that the audited provider has not complied with an audited obligation or commitment.

Audit opinions pursuant to paragraphs 4 and 5 shall be either:

- (a) 'positive' if the auditing organisation has reached a 'positive' audit conclusion for all of the audited obligations or commitments;
- (b) 'positive with comments' if the auditing organisation has reached at least one audit conclusion that is 'positive with comments' for an audited obligation or commitment and has not reached a 'negative' audit conclusion for any of the audited obligations or commitments;
- (c) 'negative' if the auditing organisation reached a 'negative' audit conclusion for at least one audited obligation or commitment.

# Template DSA reporting

**ANNEX I - Template for the audit report referred to in Article 4**

Table of contents

<b>SECTION A: General information</b>	
1. Audited service:	.....
2. Audited provider:	.....
3. Address of the audited provider:	.....
4. Point of contact of the audited provider:	.....
5. Scope of the audit:	
a. Does the audit report include an assessment of compliance with all the obligations and commitments referred to in Article 37(1) of Regulation (EU) 2022/2065 applicable to the audited provider? Yes/No	
<b>i. Compliance with Regulation (EU) 2022/2065</b>	
<b>Obligations set out in Chapter III of Regulation (EU) 2022/2065:</b>	
<b>Audited obligation</b>	<b>Period covered</b>
<i>Indicate the precise obligation audited</i>	<i>(DD/MM/YYYY)</i>
<i>Insert as many lines as necessary</i>	<i>to</i>
	<i>(DD/MM/YYYY)</i>
<b>ii. Compliance with codes of conduct and crisis protocols</b>	
<b>Commitments undertaken pursuant to codes of conduct referred to in Articles 45 and 46 of Regulation (EU) 2022/2065 and crisis protocols referred to in Article 48 of Regulation (EU) 2022/2065:</b>	
<b>Audited commitment</b>	<b>Period covered</b>
<i>Specify the code of conduct or crisis protocol and the</i>	<i>(DD/MM/YYYY)</i>

<b>SECTION C: Summary of the main findings</b>			
1. Summary of the main findings drawn from the audit (pursuant to paragraph 37(4), point (e) of Regulation (EU) 2022/2065)			
.....			
<b>SECTION C.1 : Compliance with Regulation (EU) 2022/2065</b>			
1. Audit opinion for compliance with the audited obligations referred to in Article 37(1), point (a) of Regulation (EU) 2022/2065:			
<input type="checkbox"/> Positive <input type="checkbox"/> Positive with comments <input type="checkbox"/> Negative			
2. Audit conclusion for each audited obligation:			
<b>Audited obligations</b>	<b>Audit conclusions</b>		
Indicate the precise obligation audited <i>Insert as many lines as necessary</i>	<input type="checkbox"/> Positive	<input type="checkbox"/> Positive with comments	<input type="checkbox"/> Negative
<b>SECTION C.2 : Compliance with voluntary commitments in codes of conduct and crisis protocols</b>			
<i>Repeat section C.2 for each audited code of conduct and crisis protocol referred to in Article 37(1), point (b) of Regulation (EU) 2022/2065:</i>			
1. Audit opinion for compliance with the commitments made under specify the code of conduct or crisis protocol covered by the audit:			
<input type="checkbox"/> Positive <input type="checkbox"/> Positive with comments			

# Main Challenges Delegated Act vs ISAE 3000A

- **Audit opinion**
- **Audit report form**
- **Exceptions noted**
- **Public reporting including disclosures (including mentioning audit team members)**
- **Reporting timelines**
- **Lack of industry framework**
- **At the time of the start: Draft status of delegate act**

**04**

**AI**

# Pillars of Responsible AI

Using 5 pillars to ensure client AI systems are **fit for purpose**, **ethical** and **compliant** with rules & regulations.

## RELIABILITY

*AI should do what it is intended to do*

— How do we define reliability and which level is sufficient?

## RESILIENCE

*AI should not only function now, but also in the future*

— How deep/far should explainability go?

## EXPLAINABILITY

*AI must provide results that can be comprehensible and transparent*

— To whom should the explanation be understandable and how can you measure this?

## ACCOUNTABILITY

*AI must have an owner which can be addressed*

— What is the right criterion for fairness?

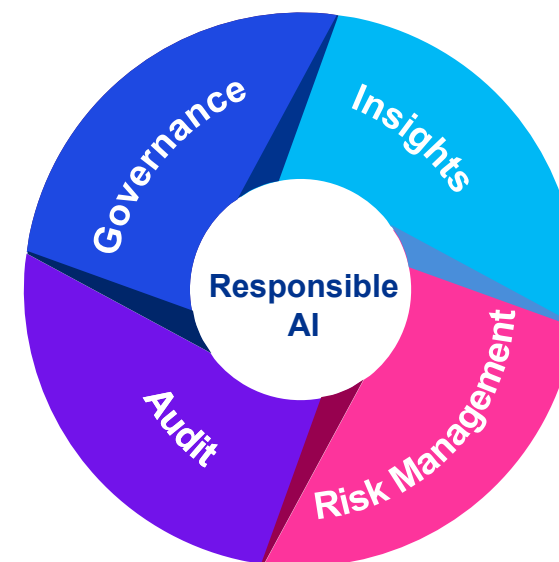
## FAIRNESS

*AI must be fair, non-discriminatory and in line with human rights*

— Which security standards apply to an AI System?

— What are the (legal) requirements regarding accountability?

— ....



# Pillars of Responsible AI for the DSA

The DSA tackles specific parts of these pillars: **Reliability**, **Explainability**, and **Fairness**.

## RELIABILITY

*AI should do what it is intended to do*

## RESILIENCE

*AI should not only function now, but also in the future*

## EXPLAINABILITY

*AI must provide results that can be comprehensible and transparent*

## ACCOUNTABILITY

*AI must have an owner which can be addressed*

## FAIRNESS

*AI must be fair, non-discriminatory and in line with human rights*

The DSA achieves these goals through **transparency**.

Most notable articles:

15

**Content moderation**

26

**Advertiser systems**

27

**Recommender systems**

# Algorithmic systems in the DSA

The DSA puts several obligations specifically on your platform's algorithmic systems, specifically *automated means for the purpose of content moderation (CM)*, *advertising systems* and *recommender systems*.

## Summarized Obligations on algorithmic systems

### Automated means of content moderation

In a half-yearly report on content moderation (CM), providers should include:

- Reporting on all means of content moderation at the provider's own initiative. This includes a comprehensive overview of automated tools used for CM.
- Representative indicators of reliability and error rates for each of the automated tools

### Advertising systems

- Real-time transparency on advertisements, including information on the main parameters used.
- Transparency on advertisements through a public, searchable repository
- Ad targeting cannot be based on special categories of personal data (art 9(1) GDPR)
- No ad targeting based on profiling for minors

### Recommender systems

Platforms should be transparent about:

- Why information or offerings are recommended to users. This means an explanation of the most important parameters and criteria used
- Options for the recipient to influence or change the main parameters where appropriate
- VLOPs should provide options for recommendations that are not based on profiling



# Compliance through Process and Data Flow Control

## Processes and methodologies support a compliant way of working

Examples include

### Recommender System transparency

Standardized methodology to identify and monitor the main characteristics that attribute the recommendations of the algorithmic system.

### Test Data

Guidelines on evaluation and reporting on test data, incl. data quality requirements and evaluation of statistical biases in test data.

### Evaluation and monitoring

Standard process for design and implementation of evaluation and monitoring. Including guidelines on choice of parameters, and design of monitoring controls.

## Controls to ensure compliance and accuracy

### Process Controls

Monitoring controls on key risks of (the processes around) algorithmic systems.

### Data reliability controls

Ensuring data integrity accuracy and completeness throughout the dataflows.

### IT General Controls

Identity and access management, Change management, Continuity management.

## Core inventories and references provide a foundation to compliance functions, management and auditors

### User Profiles

Description of available properties per user, including classification into categories of personal data under GDPR

### Data flows

Descriptions of dataflows per system, including flows to and from the providers other services and third-party services

### Definitions and classifications of illegal content

Including definitions and classifications of content incompatible with the T&Cs

### Inventory of algorithmic systems

Including their purpose and responsible divisions/units

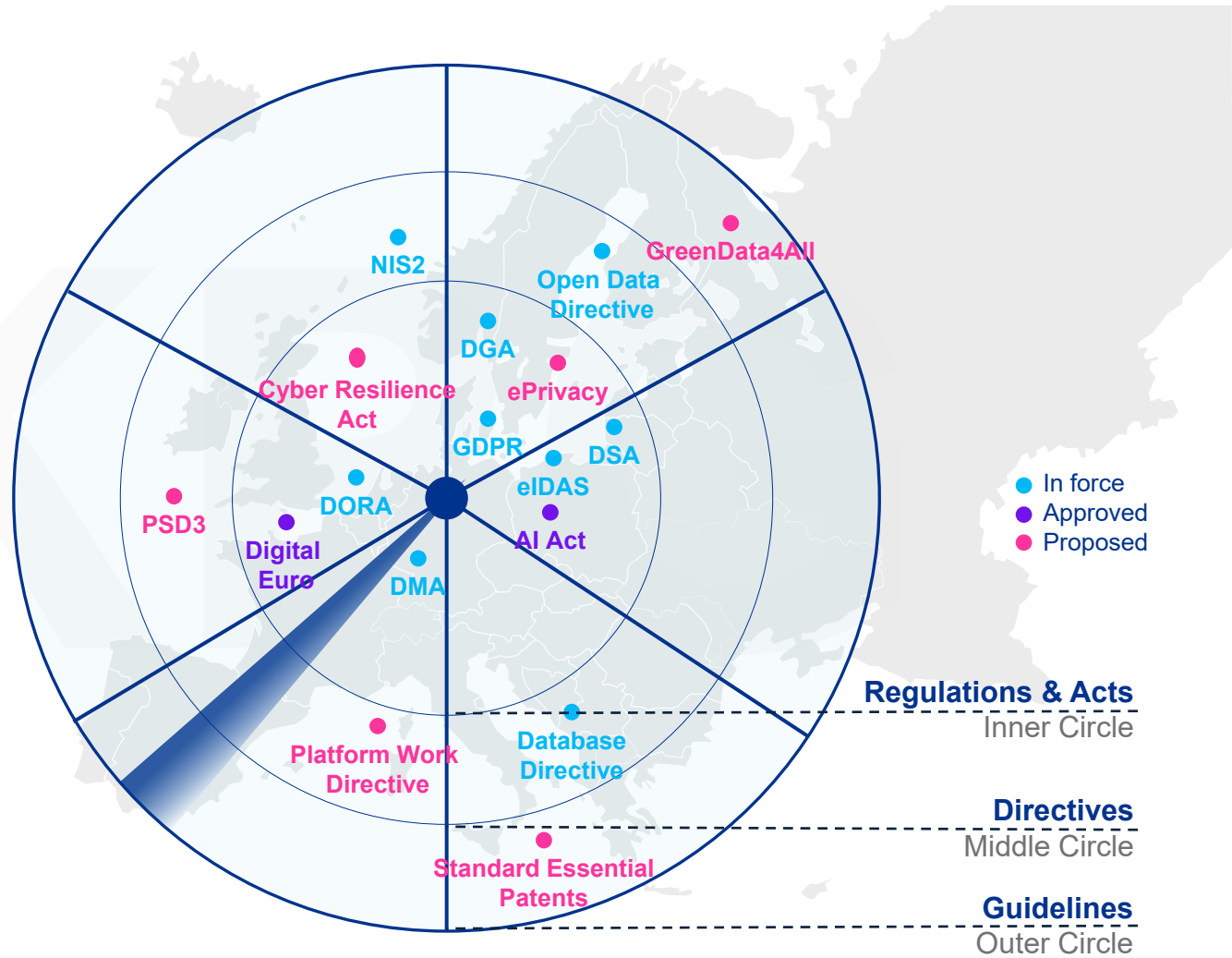
**05**

# **Compliance story**

# Overview EU digital acts – Regulatory Horizon

“ In the coming years, the tech sector will become just as regulated as the financial sector ”

Martijn Snoep, Charmain ACM (Digital Service Coordinator for NL)



# What we see in the Tech sector: from one-off programmes to 'reusable compliance capabilities'

## Common focus of DSA compliance projects

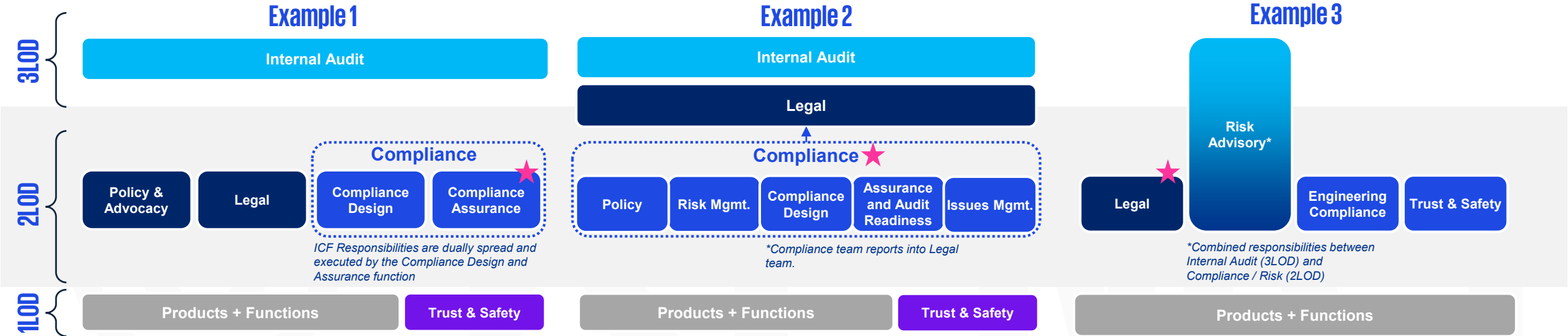
- Focus on a single Regulation
- Program - based
- One time (Plan-Do)
- Minimal Compliance
- Support from Advisors
- New compliance function solely for DSA



## Required situation:

- Continuous (Plan–Do-Check-Act)
- Demonstrable and controlled compliance
- With all applicable (T&S related) regulations (globally)
- Embedded in BAU organization
- Continuous cost reduction for compliance by automation (automated controls, A.I., D&A and GRC solutions)

# Example Compliance Operating Models at VLOPS



- Considerations**
- Trust & Safety plays a key role in managing Regulatory Reporting and conducting Systemic Risk Assessments; operational alignment and data-driven Compliance strategy
  - Compliance Assurance is Independent from Compliance Design
  - DSA Head of Compliance Function is Independent from the Compliance implementation efforts
- Clear hierarchy between Legal and Compliance
  - Pillars follow the risk and compliance lifecycle; facilitates clear handoffs across teams
  - DSA Head of Compliance Function is Independent from the operational Compliance pillars and the business, but is involved in Compliance Design
- Nimble and flexible blended approach for 2<sup>nd</sup> and 3<sup>rd</sup> LoD within the Risk Advisory team
  - Dedicated Engineering Compliance expertise
  - DSA Head of Compliance Function is Independent from the Business, but is involved in Compliance Design
- ★ DSA Head of Compliance sits here

**06**

# **Questions**







[kpmg.com/socialmedia](https://kpmg.com/socialmedia)

## Contacts KPMG:

Angelica van Beemdelust

[Vanbeemdelust.angelica@kpmg.nl](mailto:Vanbeemdelust.angelica@kpmg.nl)

Manon van Rietschoten

[Vanrietschoten.manon@kpmg.nl](mailto:Vanrietschoten.manon@kpmg.nl)

© 2024 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

**Document Classification: KPMG Confidential**