Background

• A step-change in the nature, scale and role that digital services play in our economy and society

• While the main principles of the E-commerce Directive (2000) remain valid, new rules are needed to address new challenges.

• Proliferation of sector-specific interventions in the EU (on terrorist content, copyright, audiovisual media services ...)

• Concerns from Member States and stakeholders => targeted actions have been rising leading to a patchwork of national laws.

• Announcement of DSA package by COM’s President led to three own initiative reports by the European Parliament, fleshing out areas of concern and calling for ambitious measures
Digital services today

AROUND 10,000 PLATFORMS IN THE EU

- Large: 8%
- Small: 13%
- Micro: 42%
- Medium: 37%

9,700 SMEs

European Commission
The current framework is 20 years old
unsafe products
terrorist offences
copyright infringements
scams
hate speech
illegal apartments
counterfeit products
Illicit drugs
harmful content
disinformation
Digital Services Act

• Ambitious reform for the EU to re-structure its own informational space & set global standards

• Ground rules for a truly competitive Single Market for digital services, with legal clarity and effective supervision of digital services

• Ensuring trust across Member States, and supporting cross-border cooperation of national authorities
Key questions

• Scope of the problems?
• How to consolidate the Single Market to nurture innovative scale-ups in Europe?
• How to ensure citizens’ safety online?
• What leavers for contestable markets where data-driven network effects are at the core of a « winner takes it all » environment?
• What does effective oversight look like for digital services? What capabilities, rules and cooperation mechanisms across the Single Market?
Stakeholder engagement – Open Public Consultation

• Opened from 2 June – 8 September 2020
• Almost 3000 contributions, including 14 Member States, 59 public authorities
• Submissions received also from non-EU citizens and stakeholders
• Broad convergence to keep the main principles of the e-Commerce Directive
• SMEs and innovation friendly environment crucial
Open Public Consultation - DNS

• Measures to tackle illegal content

• Measures to tackle potentially harmful content

• Question on usage of WHOIS information

• Cooperation of Member States/National Authorities
Some signposts for the ground-rules of the Internet

- **Preserve and enhance the fundamentals of the Single Market**: the ‘country of origin’ principle and the cooperation across MS
- **Fair balance of incentives and rules** for allowing digital businesses to scale and protecting freedom of expression:
- Liability principles and prohibition to impose general monitoring obligations are still valid
- Clear and robust rules for governing **responsibilities and transparency** of online platforms
Content moderation happens without proper transparency and accountability
Objectives in a nutshell

Modernise the rules to more effectively address illegal content and systemic risks in the online space

Clarify the rules on liability, giving companies legal certainty to take voluntary action in a diligent and proportionate manner under clear terms of service

Increase transparency, accountability and facilitate better oversight
### Liability provisions and content moderation

<table>
<thead>
<tr>
<th>It harmonises liability exemptions, not liability</th>
<th>It does not attribute liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>The contrary would mean to harmonise tort or criminal law</td>
<td></td>
</tr>
<tr>
<td>It is neutral</td>
<td>Does not define what is illegal</td>
</tr>
<tr>
<td>Illegality is defined by national or EU rules</td>
<td></td>
</tr>
<tr>
<td>It is horizontal</td>
<td>All types of illegal content, civil and criminal liability</td>
</tr>
<tr>
<td>Liability only for illegal content, not harmful content!</td>
<td></td>
</tr>
<tr>
<td>It applies to services, not to actors</td>
<td>Not “Facebook is an intermediary&quot;, but &quot;it provides intermediary services&quot;</td>
</tr>
<tr>
<td>A provider can provide many different services (mere conduit + caching + hosting)</td>
<td></td>
</tr>
</tbody>
</table>
Gradual mitigation

Online platforms – HSP - Caching – ISP – infrastructure...
**E-commerce Directive 2000/31**

Rules for information society services providers

**Digital Services Act**

Rules for intermediary services

- Clarifies rules on liability and creates incentives for proactive measures
- Due diligence obligations
- Common framework for enforcement: Digital Services Coordinators + Commission
Recital 27: “recalls that...”

- There are technologies that improve the availability, **efficiency, speed, reliability, capacity and security** of systems for the transmission and storage of data online.
- Providers of services establishing and **facilitating the underlying logical architecture** and proper functioning of the internet, including **technical auxiliary functions**, can also benefit from the exemptions from liability set out in this Regulation.
- Examples: WLAN, DNS, TLD name registries, certificate authorities, CDN, that enable or improve the functions of other providers of intermediary services.
- Voice over IP, messaging services and web-based e-mail services.
Intermediary services

- offering network infrastructure: Internet access providers, domain name registries, wifi hotspots...

Hosting services

- such as cloud infrastructure and webhosting services

Online platforms

- E.g. online marketplaces, app stores, or collaborative economy platforms or social media platforms

Very large online platforms

- Specific rules for platforms reaching 45 million users (10% of EU population)
## Due diligence obligations

<table>
<thead>
<tr>
<th>OBLIGATIONS</th>
<th>VERY LARGE PLATFORMS</th>
<th>ONLINE PLATFORMS</th>
<th>HOSTING SERVICES</th>
<th>ALL INTERMEDIARIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points of contact</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Legal representatives</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Terms and conditions</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Notice &amp; Action</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Statement of reasons</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Complaint handling</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Out of Court Dispute Settlement</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Trusted flaggers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Abusive behaviour</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Know Your Business Customer (KYBC)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reporting criminal offences</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Advertising transparency</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Additional transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Risk assessment and mitigation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Independent audits</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Recommender systems</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Enhanced advertising transparency</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data access and scrutiny</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Compliance officer</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Enhanced Transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
Proportionality towards SMEs

• Open public consultation: DSA should **avoid one-size-fits-all** approach
• Reflected in graduated duties according to the **societal role** of the company
• **Mitigation measures** in the proposal (Art. 13, 16; recital 26) while keeping certain level of **harmonisation**
• Smaller players should be the **biggest beneficiaries** of the DSA thanks to
  ✓ better **legal predictability**
  ✓ positive impact on **innovation, investments and competitiveness**
Transparency of content moderation

**Article 13**
- Basic transparency obligations for all online intermediaries and hosting services. Once per year
- Number of orders and, where applicable: notices, content removed through content moderation decision, number of complaints & decisions taken

**Article 23**
- Additional transparency obligations for **online platforms**
- Number of out-of-court disputes, suspensions of repeat offenders and notifiers; use of automated content moderation
- Monthly users

**Article 33**
- Widest transparency obligations for very large online platforms
- Report on risk assessment; mitigating measures; audit reports
Article 22 – *Traceability of traders*

**SCOPE**

- **Online marketplaces** – evolving concept
- **Traders** – as defined by Art 2(e) DSA and identified by Art. 6 Omnibus Directive
- **Consumers** – as defined by Art. 2(c) DSA
Risk based obligations on very large online platforms

Risk assessment (yearly)
Art 26
- Illegal content and activity
- Fundamental rights, freedom of expression, unjustified discrimination
- Intentional manipulation of their service (public health, electoral processes, protection of minors, etc)

Mitigation of risks:
Art 27
- Adapt services, terms and conditions
- Prevent advertising income to infringers
- Change moderation and recommender systems
- Codes of conduct
Accountability of very large online platforms

**Independent audit**
Art 28
- Annual independent audit covering **compliance with all obligations** and Codes of conduct

**Data access and scrutiny**
Art 31
- Digital Services Coordinators/COM
- To vetted researchers at the request of the Digital Services Coordinator

**Recommender systems**
Art 29
- Main parameters in ToS
- Include an option for users which is not based on profiling
Co-regulatory framework

**Codes of Conduct**
- Art 35
  - Codes of conduct to be supervised by the Commission and the Board
  - Can serve as compliance measures to fulfill the obligations under Article 27.

**Crisis Protocols**
- Art 37
  - Addressing crisis situations strictly limited to extraordinary circumstances affecting public security or public health
  - Limited in time, clear procedures and roles, safeguards and public reporting.
Transparency of online advertising

| Online Advertising transparency | For online platforms
|                               | Why am I seeing this ad?
|                               | Who is paying for the ad? |
| Additional online advertising transparency | For very large online platforms publicly available repository of all ads via API including:
|                               | Targeting criteria
|                               | Content of the ad
|                               | Time displayed
|                               | Total number of users reached |
| Code of conduct for online Advertising | Facilitate compliance with the obligations for online advertising transparency
|                               | Commission shall encourage and facilitate the drawing up of codes of conduct in a multi-stakeholder formation |
How can national authorities enforce their laws via providers established elsewhere?

Example: a Dutch court can ask **directly** to Airbnb to:

- **Remove the listing of a non-registered apartment**
  - Article 8: if under NL law, authorities can issue orders to act against illegal content
  - NL DSC should inform all other DSCs

- **Give information about an apartment owner**
  - Article 9: if under NL law, authorities can issue orders to provide information on users when necessary to enforce compliance of national rules by users
# Governance structure

<table>
<thead>
<tr>
<th><strong>Digital Services Coordinators</strong></th>
<th><strong>European Board for Digital Services</strong></th>
<th><strong>European Commission</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Independent authorities</td>
<td>• Ad-hoc independent advisory group</td>
<td>• Direct enforcement powers vis à vis very large online platforms for</td>
</tr>
<tr>
<td>• Direct supervision and enforcement (by default)</td>
<td>• Composed by DSCs</td>
<td>• specific obligations for very large online platforms (after DSC supervision)</td>
</tr>
<tr>
<td>• Coordination with other national competent authorities</td>
<td>• Chaired by COM, no vote</td>
<td>• all other obligations (if DSC failed to act)</td>
</tr>
<tr>
<td>• Coordination and cooperation at EU level with Board, COM and other DSCs</td>
<td>• Advising DSCs and COM, recommending actions</td>
<td>• Administrative support to the Board</td>
</tr>
<tr>
<td></td>
<td>• No binding acts, but need to take them into account</td>
<td>• Advises on cross-border disputes</td>
</tr>
<tr>
<td></td>
<td>• Cooperation with other EU bodies, agencies, offices on related matters</td>
<td>• Intervenes upon DSC request</td>
</tr>
</tbody>
</table>

In cases of breaches of DSA obligations = various sanctions and fines up to 6% of the provider’s turnover
What does the DSA bring for DNS?

- **Certainty** of being covered by the **EU legal framework** (rec. 27)

- **Proportionality** when tackling illegal content online: number of mitigation measures on SMicE + subsidiarity (rec. 26)

- **Harmonised framework**: clarification how the Member State can request to act against illegal content

- Overall **balanced solution** as far as infrastructural services providers are concerned
Questions?
Cyber threat landscape 2021

- Intensification of cyberattacks on **essential services**
- **Green transformation** requires secure cross-border grids, smart meters, avoiding unnecessary data storage duplication, patchable devices
- **IoT** proliferating: 25 bn connected objects by 2025 (GSMA)
- **Pandemic dependency** on digital → expands attack surface e.g. hospitals, vaccine distribution, disinformation
- **Geopolitical tensions**: authoritarian regimes weakening open, global Internet and hijack international bodies/ norm setting
The EU’s cybersecurity strategy for the digital decade
December 2020

- 26 strategic initiatives/ actions
- Smart digital investment: up to €4.5bn for cybersecurity 2021-27 (EU+MS+Industry)
- New regulation (eg NIS 2.0, IoT)
- New policies (Joint Cyber Unit, Security Operations Centres)
- Comprehensive
  - internal market
  - law enforcement
  - diplomacy
  - defence
<table>
<thead>
<tr>
<th><strong>Resilience, sovereignty, leadership</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure</strong></td>
</tr>
<tr>
<td>• Adopt NIS 2.0</td>
</tr>
<tr>
<td><strong>Cyber Shield</strong></td>
</tr>
<tr>
<td>• Develop Network of Security Operations Centres</td>
</tr>
<tr>
<td><strong>Ultra secure connectivity</strong></td>
</tr>
<tr>
<td>• Quantum enabled encryption</td>
</tr>
<tr>
<td><strong>5G networks</strong></td>
</tr>
<tr>
<td>• Complete implementation of Toolbox</td>
</tr>
<tr>
<td><strong>An Internet of Secure Things</strong></td>
</tr>
<tr>
<td>• Horizontal rules on IoT security</td>
</tr>
<tr>
<td><strong>Internet security</strong></td>
</tr>
<tr>
<td>• Develop DNS4EU</td>
</tr>
<tr>
<td><strong>Supply chain autonomy</strong></td>
</tr>
<tr>
<td>• Encourage EUR 4.5 bn investment across digital supply chain through Competence Centre and Network</td>
</tr>
<tr>
<td><strong>Skills</strong></td>
</tr>
<tr>
<td>• Eg investment in business resilience against cyber-enabled IP theft</td>
</tr>
</tbody>
</table>
Il Operational capacity: prevent, deter, respond

**Joint Cyber Unit**
- Milestones and process to be set out Feb 2021

**Cybercrime**
- Complete Security Union agenda

**Cyberdiplomacy toolbox**
- Strengthen cyber deterrence posture and shared situational awareness
- Explore additional measures, and increase cooperation with international partners
- Review Implementing Guidelines

**Cyber Defence**
- Review the Cyber Defence Policy Framework to increase cyber defence cooperation and coordination
- Encourage Member States’ cyber defence capability development, notably through PESCO and EDF
### III Global and open cyberspace

#### EU leadership on international norms and standards
- Step-up EU engagement on international standardisation, i.e. ITU
- Take forward the Programme of Action to Advance Responsible State Behaviour in Cyberspace
- Promote the Budapest Convention and engage in multilateral discussions
- Promote and protect human rights and fundamental freedoms online

#### Cooperation with partners
- Strengthen and expand cyber dialogues with third countries, regional and international organisations
- Reinforce regular and structured exchanges with the multi-stakeholder community
- Form an informal EU Cyber Diplomacy Network with EU “cyber attachés” around the world to promote the EU vision of cyberspace

#### Strengthen global capacities to tackle cyber threats
- Develop an EU External Cyber Capacity Building Agenda
- Set-up an EU External Cyber Capacity Building Agenda Board
- Priorities on Western Balkans, EU’s neighborhood and partner countries experiencing a rapid digital development.
Thank you
Internet Security and Openness: Brief from the European Commission

ICANN Community Brief
26 February 2021
Internet Security and Openness in the EU 2020 Cybersecurity Strategy

1 - DNS and TCP/IP at the core of the Internet Infrastructure

2 - Security measures for Internet Critical Infrastructures

Internet Security and Openness within multistakeholder and multilateral fora
Main actions

Contingency Plan for extreme scenarios affecting DNS root system

Secure DNS Root System

Uptake of key internet standards (IPv6) and internet security standards and good practices for DNS

Secure & Autonomous DNS resolution

NIS2:
• Digital Infrastructure
• DNS and WHOIS

• Encourage DNS resolution diversification
• DN4EU

Security Critical Internet Infrastructure

Global Internet Standards
Resilience of the DNS root system

Goal:
- Guarantee that the Internet remains globally accessible in all circumstances

Instrument:
- Contingency plan dealing with extreme scenarios
- Mitigating risks affecting the integrity and availability of the global DNS root system

How:
- Work with the two EU DNS root server operators, Member States involved, ENISA and ICANN and the multi-stakeholder community
- Supported by EU funding
DNS4EU – how should it look like?

A public European resolver service

An alternative to existing services

State of art security and privacy features

Supported by EU funding (CEF 2 Programme)

Legal framework: EU and national based on the country of establishment.

Planned consultation and involvement of Member States and ENISA
Global internet standards

Uptake of Key internet Standards – IPV6

Implementation of standards with partner countries

Promote

Uptake of security standards and good practices for DNS, email and routing security

EU position in international standardization bodies

Accelerate
NIS2 Directive: DNS and domain name registration data

Critical role of DNS recognized: “upholding and preserving a reliable, resilient and secure DNS is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend.”

Importance of domain name registration data: “Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union.

Availability and accessibility of the data: “The availability and timely accessibility of these data [...] is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents.”
It is essential to have access to complete and accurate data.

Registries and registrars struggle to find a clear ground to reply to requests to access.

Currently the vast majority of data are not available and access requests remain unanswered.

There is little to no uniform practices to address access requests.

A legal framework that ensures that the domain name registration data are accurate, complete and accessible to legitimate access seekers.
Main elements

- EU Member States will have to transpose the Directive into national law.

- Obligations concern TLD registries and entity providing registration services for the TLD.
  - Collect and maintain accurate and complete domain name registration data.
  - Contain relevant information to identify/contact holders and contact points.
  - Publish non-personal data without undue delay.
  - Ensure all requests to access domain name registration data receive a reply without undue delay.
  - Provide access to specific personal data upon duly justified requests by legitimate access seekers.

[EC can adopt guidelines]
Thank you
REVISION OF THE NIS DIRECTIVE

DG CNECT, unit H2
Proposal for a revision of the NIS Directive

- It is a revision of the first NIS Directive from 2016.
- It is a Commission proposal.
- Legislative process has just started.
- Directive as legal instrument.
EU legislative process

- European Commission
  - Proposal
  - Negotiations with CO-LEGISLATORS (European Parliament and Council (27 Member States))
  - Adoption
  - Law
Three main pillars of the proposal for NIS 2

**MEMBER STATE CAPABILITIES**
- National authorities (such as CSIRTs and cybersecurity authorities)
- National frameworks (such as on CVD and crisis management)

**RISK MANAGEMENT & REPORTING**
- Essential and important entities to take security measures
- Entities to notify significant incidents and cyber threats

**COOPERATION AND INFO EXCHANGE**
- European fora (Cooperation Group and CSIRTs network)
- European frameworks on CVD and crisis management
- Biennial ENISA cybersecurity report
RISK MANAGEMENT & REPORTING
## Two regulatory regimes

<table>
<thead>
<tr>
<th>Essential entities</th>
<th>Important entities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Mostly scope of NIS1</td>
</tr>
<tr>
<td><strong>Security requirements</strong></td>
<td>Risk-based security obligations, including accountability of top management</td>
</tr>
<tr>
<td><strong>Reporting obligations</strong></td>
<td>Significant incidents and significant cyber-threats</td>
</tr>
<tr>
<td><strong>Supervision</strong></td>
<td>Ex-ante + ex-post</td>
</tr>
<tr>
<td><strong>Sanctions</strong></td>
<td>Minimum list of administrative sanctions, including fines.</td>
</tr>
<tr>
<td><strong>Jurisdiction</strong></td>
<td>General rule: MS where the service is provided</td>
</tr>
</tbody>
</table>
## Scope: sectors covered

<table>
<thead>
<tr>
<th>Essential entities</th>
<th>Important entities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy</strong> (electricity, district heating, oil, gas and hydrogen)</td>
<td>Postal and courier services</td>
</tr>
<tr>
<td><strong>Transport</strong> (air, rail, water, road)</td>
<td>Waste management</td>
</tr>
<tr>
<td>Banking</td>
<td>Chemicals (manufacture, production, distribution)</td>
</tr>
<tr>
<td>Financial market infrastructures</td>
<td>Food (production, processing, distribution)</td>
</tr>
<tr>
<td><strong>Health</strong> (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)</td>
<td>Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)</td>
</tr>
<tr>
<td>Drinking water</td>
<td>Digital providers (search engines, online market places and social networks)</td>
</tr>
<tr>
<td><strong>Waste water</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Digital Infrastructure</strong> (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)</td>
<td></td>
</tr>
<tr>
<td><strong>Public administrations</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Space</strong></td>
<td></td>
</tr>
</tbody>
</table>
Size as a clear-cut benchmark and proxy for importance.

Scope: all companies, which are medium-sized or larger.

Exceptions: electronic communications, trust services, TLD registries, DNS service providers and public administration.

In certain cases, Member States will be in a position to add operators below the size threshold.
Obligations for entities

- Risk management measures
  (including incident handling, business continuity, supply chain security etc.)

- Report significant incidents and significant cyber threats
  (three stage process, first report within 24 hours)
Thank you for your attention!