DIGITAL SERVICES ACT

EUROJUST Regional Meeting

24/05/2023
OVERVIEW AND STATE OF PLAY
Central ideas for the DSA

- **Maintaining key principles** from the eCommerce-Directive, upgrading them where necessary

- **Asymmetric due diligence obligations** to account for different sizes and risk profiles in the ecosystem of digital services

- **Procedure** over substantive rules

- **Strengthening fundamental rights** by providing more safety online and protection freedom of expression.
General regulatory framework for digital intermediaries

- Horizontal regulatory framework for all online intermediaries
  - Subset of «information society services» (ECD remains valid as general framework for ISS)
  - Not only «platforms» (mere conduit, pure hosting, caching as well)
  - Not only big players or cross-border services (but graduated obligations)

- **Maximum harmonisation** but
  - National legislation pursuing different objectives/subject matter
  - National measures implementing the national institutional structure (DSC)
  - National and EU legal basis for orders (no legal basis in DSA)

- **Lex specialis** principle for other platform-related EU legislation
Asymmetric **due diligence obligations**

<table>
<thead>
<tr>
<th>Very large online platforms</th>
<th>Online platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Risk management, crisis response &amp; audits</td>
<td>- Internal &amp; out of court complaint systems*</td>
</tr>
<tr>
<td>- Recommender systems: choices</td>
<td>- Trusted flaggers*</td>
</tr>
<tr>
<td>- Ad repositories</td>
<td>- Limiting misuse*</td>
</tr>
<tr>
<td>- Data access for researchers and supervisory authorities</td>
<td>- Obligations for marketplaces (KYBC, information to users, random checks)</td>
</tr>
<tr>
<td>- Compliance officer</td>
<td>- Advertising transparency and bans on certain targeted ads*</td>
</tr>
<tr>
<td>- Further transparency reporting</td>
<td>- Transparency of recommender systems*</td>
</tr>
</tbody>
</table>

* Not applicable to SMicE, unless VLOP

<table>
<thead>
<tr>
<th>Hosting services</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Notice &amp; action</td>
</tr>
<tr>
<td>- Information to notice-providers</td>
</tr>
<tr>
<td>- Information to content provider</td>
</tr>
<tr>
<td>- Suspicious criminal evidence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>All intermediaries</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Points of contact &amp; legal representatives</td>
</tr>
<tr>
<td>- Clear terms and conditions &amp; diligent, objective, proportionate enforcement</td>
</tr>
<tr>
<td>- Transparency reporting</td>
</tr>
</tbody>
</table>
First implementation steps DSA

Publication of number of active users by platforms
17 Febr. 2023

First designations
Entry into application of obligations for the VLOPs and VLOSEs designated, including the submission of their first risk assessment

Latest date for MS to appoint DSCs
17 Febr. 2024

1 year after designation

+ 4 months

Obligations apply to all services

The designated platform receive the audit report from the independent auditor

2nd risk assessment

+ 3 months

The designated platform publishes all risk management and audit reports online (1st cycle)

VLOPS: First risk management yearly cycle

VLOPS: Second risk management yearly cycle
Enforcement state of play

• First batch of VLOP/VLOSE designation on 25 April 2023
  ➢ Alibaba, Amazon, Apple AppStore, Booking.com, Facebook, Instagram, LinkedIn, Google Play/Maps/Shopping, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, and Bing, Google Search

• Understanding Member States’ set-up of Digital Services Coordinators

• Implementing regulation, implementing and delegated acts

• DG CONNECT reorganisation

• European Centre for Algorithmic Transparency (ECAT)
THE DSA AND INTELLECTUAL PROPERTY
In a nutshell

- DSA is not an IPR enforcement tool – it is general and horizontal
- But it includes a **full toolbox which can be very useful** for the enforcement of IPR
- These measures would apply **without prejudice to existing IPR rules**
N&A procedures

Trusted flaggers

Standards for notices, also by trusted flaggers via APIs

Repeat infringer policy

General rules on transparency

KYBC obligations

Risk mitigation measures by very large online platforms

Codes of conduct

Removal and information orders

European Commission
How can national authorities enforce their laws via providers established elsewhere?

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

- **Remove the listing of a counterfeit product**
  - Article 9: under NL law, authorities can issue orders to act against illegal content
  - NL DSC should inform all other DSCs

- **Give information about a user (for instance selling counterfeit goods)**
  - Article 10: under NL law, authorities can issue orders to provide information on users when necessary to enforce compliance of national rules by users
Highlights of the negotiations

- Notice provider can benefit from redress mechanisms
- Rightholders can become trusted flaggers
- Search engines clearly in scope
- Possibility of specific monitoring, in accordance with CJEU case-law
- No strict deadlines for N&A
- KYBC limited to online marketplaces – but broad definition
Thank you!

@ec.europa.eu