SNIP Project - Final Conference

Policy and Recommendations under the Digital Services Act

From Legal Text to Operational Policies

- The Digital Services Act moves from previous reactive liability models to a **governance-based framework**, grounded in transparency, due diligence, risk prevention and accountability.
- About SMEs, : How do you translate complex regulatory obligations into day-to-day operational practices?
- Instead of reproducing the legal provisions of the DSA, we focused on “**functional compliance**”.

Functional compliance means the ability of a digital service provider to internalise regulatory objectives into:

- organisational processes;
- technical design choices;
- and decision-making workflows;

Workflow of policies:

- identifying stakeholder categories;
- defining policy objectives;
- translating DSA obligations and soft law instruments into practical scenarios;
- distinguishing between general and stakeholder-specific measures;
- and finally, defining indicators and do’s and don’ts for validation and monitoring.

The policies are:

- principle-based,
- scalable,
- proportionate,
- and implementable even by organisations with limited legal or technical resources.

The Core Policy Set for DSA Compliance

Policy 1 – Content Moderation and Notice-and-Action Mechanisms

- Content moderation is one of the pillars of the DSA but under the DSA, moderation is not simply about removing illegal content, it is about creating a **structured, accessible and accountable process**.

Policy 1 emphasises:

- user-friendly notice-and-action mechanisms;

- internal workflows distinguishing manifestly illegal content from context-dependent cases;

- human oversight over automated systems;

- documentation and traceability of decisions.

- For SMEs, this does not mean building complex AI systems. It means defining clear internal criteria and ensuring consistency in decision-making.

Policy 2 – Transparency of Terms and Conditions

- Transparency is a cornerstone of the DSA.
- However, transparency is not achieved through longer legal texts but through clarity.

Policy 2 promotes:

- plain-language drafting;
- summaries of key rules;
- coherence between written policies and actual practices;
- and periodic updates.

- This policy reduces information asymmetries and strengthens user trust.

Policy 3 – Internal Complaint Handling and Redress

- The DSA strengthens procedural safeguards for users.
- Internal complaint-handling mechanisms serve two functions:

- protecting users' rights;
- and acting as internal quality-control tools for providers.

- For SMEs, this can be implemented through:

- a separate review phase;
- reasoned decisions;
- and documented outcomes.

- Complaint mechanisms should not be discouraging or overly complex.
- They must be effective and accessible.

Policy 4 – Risk Prevention and Platform Integrity

- One of the most innovative aspects of the DSA is its shift towards **risk-based governance**.
- While systemic risk assessments are mandatory only for very large platforms, SMEs should adopt proportionate risk prevention practices.

- This includes:

- periodic internal reviews;
- identification of recurring abuse patterns;
- adaptation of platform features to emerging risks.

- Risk prevention should not be a one-off exercise. It should be iterative and integrated into ordinary governance.

Policy 5 – Marketplace Obligations and Trader Traceability

- Online marketplaces have specific obligations under the DSA.

- Traceability of traders is not only a compliance duty but a trust-building mechanism

Policy 5 focuses on:

- proportionate onboarding and verification;

- documentation of trader information;

- graduated enforcement in case of violations.

- Again, the key is proportionality.

Beyond Providers: A User-Centred Perspective

- A distinctive feature of policies is that it does not address only service providers.
- The DSA recognises that a safe digital environment also depends on **users' awareness and empowerment**.
- We therefore developed a dedicated section of user-centred policy guidelines.
- These guidelines are not meant to shift responsibility from platforms to users; rather, they aim to support informed participation.

- We structured them into:

- general guidelines for all users;

- and tailored measures for specific vulnerable groups.

General Users

- awareness of platform rules;
- responsible use of reporting mechanisms;
- exercise of redress rights.

- User empowerment reinforces transparency and accountability.

Vulnerable Users

- Particular attention was devoted to vulnerable users, including:
- consumers in online marketplaces;
- users with low digital literacy;
- content creators and small online sellers;
- and especially minors.

Protection of Minors and Vulnerable Users

- The DSA grants protection to minors.
- In this area, the European Commission has also adopted tailored guidelines under Article 28.

- Policies reflect this regulatory direction and promote:

- privacy-friendly default settings for minors;

- avoidance of profiling-based recommendations;

- age-appropriate explanations of risks and features;

- periodic review of design choices affecting vulnerable users.

Protection of minors is not a formal compliance requirement; It is an ongoing governance responsibility.

- Indicators to measure implementation, such as:

- availability of age-appropriate defaults;
- frequency of safety reviews;
- presence of profiling-based features affecting minors.

Learning from industry practices: the policies inspired by industry practices.

- Preventive and remedial mechanisms adopted by large platforms and abstracted them into scalable solutions for SMEs.

- Examples include:

- friction-based measures, such as confirmation prompts;
- sector-based risk signals;
- graduated enforcement systems;
- simplified transparency reporting;
- internal documentation and escalation pathways.

- The objective was not to replicate complex structures of large platforms but to extract functional principles adaptable to smaller actors.

Concluding Remarks

- The SNIP policy framework aims to bridge the gap between:

- regulatory complexity
and
- operational reality.

- It does so by:

- translating legal obligations into practical measures;
- integrating provider and user perspectives;
- focusing on SMEs;
- and embedding vulnerability awareness into digital governance.