

SELF-ASSESSMENT NETWORK IMPACT PROGRAM (SNIP)

PRIN PNRR 2022- n. P2022AK2HK

**BLUEPRINT GUIDELINES FOR STAKEHOLDERS TO ENSURE COMPLIANCE,
ACCOUNTABILITY AND USER PROTECTION UNDER THE DIGITAL SERVICES ACT**

These Blueprint Guidelines are developed within the framework of the SNIP – Self-Assessment Network Impact Program (PRIN PNRR 2022, n. P2022AK2HK).

They translate the obligations and governance logic of the Digital Services Act (Regulation (EU) 2022/2065) into policies and operational, scalable and proportionate measures, with particular attention to Small and Medium-Sized Enterprises (SMEs).

The document adopts a blueprint structure inspired by stakeholder-oriented governance models and articulates general and specific measures to support compliance, risk prevention, transparency, accountability and user empowerment in the digital environment.

These blueprint guidelines have been validated within relevant stakeholders. They constitute a complementary tool to raise awareness among SMEs and consumers, by providing recommendations on procedural safeguards, effective redress mechanisms, and resilience against manipulation and systemic risks within the framework of the EU Digital Services Act implementation.

These guidelines are not a restatement of the legal text. They are designed as a practical implementation framework supporting self-assessment, internal governance structuring and continuous compliance improvement.

Principles, targeted stakeholders, and categories of services.

All policies and operational measures should be grounded in the following principles.

<p>A. Risk Prevention and Integrity by Design Digital services should proactively prevent misuse, illegal content dissemination and structural vulnerabilities through proportionate governance, organisational workflows and technical safeguards. Risk prevention is not limited to very large platforms but represents a governance standard applicable, in proportionate form, to all providers.</p>
<p>B. Transparency and Procedural Fairness Users must be able to understand:</p> <ul style="list-style-type: none">• platform rules,• moderation logic,• enforcement consequences,• complaint and redress mechanisms. <p>Transparency is a structural precondition for accountability and trust-building.</p>
<p>C. Proportionality and SME-Sensitive Compliance Compliance mechanisms must be:</p> <ul style="list-style-type: none">• scalable,• resource-aware,• adaptable to organisational size and risk exposure. <p>The blueprint approach promotes functional compliance rather than formalistic replication of large-platform models.</p>
<p>D. User Empowerment and Effective Remedies Users must be placed in a position to:</p> <ul style="list-style-type: none">• understand their rights,• report illegal content,• challenge moderation decisions,• exercise redress mechanisms. <p>Empowered users reinforce systemic compliance and platform accountability.</p>

Target Stakeholders

The identification of target stakeholders follows a functional and regulatory-based approach, aligned with the categories of services defined under the Digital Services Act. Rather than focusing on the legal form or size of the provider alone, this document considers the role played by each stakeholder in the digital ecosystem, the degree of control exercised over content, goods or services, and the corresponding exposure to regulatory obligations.

Particular attention is devoted to Small and Medium-sized Enterprises (SMEs), start-ups and emerging digital service providers, which often operate across multiple regulatory categories simultaneously (e.g. hosting services combined with platform functionalities). The policies outlined herein are therefore designed to be modular and adaptable, allowing stakeholders to identify and apply only those measures relevant to their specific activities, risk profile and organisational capacity. This stakeholder-oriented approach supports proportionality, avoids one-size-fits-all compliance models, and reflects the DSA's underlying objective of ensuring a safe and trustworthy online environment without imposing undue burdens on smaller market actors.

<p>These policies are primarily addressed to:</p> <ol style="list-style-type: none">1. Intermediary service providers;2. Hosting service providers;3. Online platforms, including:<ul style="list-style-type: none">▪ social networks▪ content-sharing platforms▪ online marketplaces4. SMEs and start-ups operating digital services within the EU.
<p>Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are not the primary target, though several policies may also support compliance at higher regulatory threshold.</p>

Categories of Services and Applicable Obligations

For the purposes of these guidelines, reference is made to the following categories defined under the DSA:

- **Intermediary services** (Articles 3(g), 4–6 DSA);
- **Hosting services**, including cloud and web hosting providers (Article 3(g));
- **Online platforms**, meaning hosting services that disseminate information to the public (Article 3(i));
- **Online marketplaces**, subject to additional due diligence obligations (Article 3(k)).

General Measures common to all Digital Service Providers

- Establish documented internal compliance workflows.
- Map applicable DSA obligations according to service category.
- Maintain internal records of moderation decisions and enforcement actions.
- Define clear escalation and review procedures.
- Conduct periodic internal risk reviews.
- Integrate compliance responsibilities within management functions.

Specific Measures for Intermediary Services and Hosting Providers

1. Structured Notice-and-Action Mechanisms.

Providers should establish structured and accessible notice-and-action mechanisms that allow users to report illegal content in a clear and user-friendly manner. Reporting forms should be easily accessible from all relevant interfaces and designed to guide users in submitting sufficiently precise and substantiated notices.

Internally, providers should distinguish between manifestly illegal content, which may allow for expedited intervention, and more complex cases requiring contextual legal assessment. While automated tools may support detection and prioritisation, effective human oversight must be ensured throughout the moderation process to safeguard proportionality and fundamental rights.

Providers should also define internal response timelines that are proportionate to their size, resources and risk exposure, ensuring that notices are handled diligently and without undue delay. Finally, all notices received and the corresponding actions taken should be systematically logged and documented in order to ensure accountability, enable internal quality control, and support potential audits or reviews.

Operational Measures	
1)	Implement a standardised and user-friendly notice-and-action form, accessible from all relevant interfaces.
2)	Establish internal workflows distinguishing between manifestly illegal content and content requiring contextual legal assessment.
3)	Ensure human oversight over automated content moderation tools.

- | |
|--|
| 4) Define internal response timelines that are proportionate to the provider's size and resources. |
| 5) Maintain internal records of notices received and actions taken for accountability purposes. |

Indicators
<ol style="list-style-type: none"> 1) Average response time to notices 2) Number of notices processed per reporting period 3) Ratio between automated and human-reviewed decisions 4) Embed safety and privacy features into the design of digital products and services to align their life-cycle of production with the principles of privacy and safety by design.
Do's and Don'ts
<ol style="list-style-type: none"> 1) Do ensure accessibility and transparency of reporting mechanisms. 2) Don't rely exclusively on automated systems without safeguards.

2. Transparent Terms and Conditions.

Providers should draft their Terms and Conditions using clear, plain and unambiguous language, so that users can easily understand their rights, obligations and the rules governing the service. In addition to the full legal text, providers should publish concise and accessible summaries that clearly explain content moderation policies, enforcement measures, and possible sanctions.

Internal practices and moderation workflows must be consistently aligned with the rules declared in the Terms and Conditions, ensuring coherence between what is communicated to users and what is implemented in practice. Finally, contractual clauses should be periodically reviewed and updated to reflect regulatory developments, operational changes, and emerging risks, thereby maintaining transparency and legal certainty over time.

Operational Measures
1) Draft Terms and Conditions using clear, plain and unambiguous language .
2) Provide concise summaries highlighting key elements such as content moderation, suspension, and termination rules.

3) Where relevant, make Terms and Conditions available in the official languages of the Member States in which the service operates.
4) Periodically review and update Terms and Conditions to reflect regulatory or operational changes.
Indicators
1) Availability of summaries
2) User feedback related to clarity of platform rules
Do's and Don'ts
1) Do apply legal design principles.
2) Don't introduce vague or discretionary clauses without justification.

3. Internal Complaint-Handling Systems

Platforms should establish internal complaint-handling systems that are functionally independent from the initial moderation decision-making process, ensuring impartiality and procedural fairness. Appeals should be reviewed by a different person or team than the one responsible for the original decision, thereby reinforcing objectivity and accountability.

Decisions adopted following a complaint should be clearly reasoned and communicated to users in an understandable manner, indicating the applicable rule and the rationale behind the outcome. Users should also be given the opportunity to submit additional contextual information or clarifications that may be relevant for reassessment.

To enhance internal quality control and consistency, platforms should systematically track decisions that are overturned during the appeal phase and analyse recurring errors or patterns. Finally, where applicable, users should be informed about the possibility of accessing certified out-of-court dispute settlement mechanisms, in accordance with the procedural safeguards established under the Digital Services Act.

Operational Measures
1) Establish an internal complaint-handling system separate from initial moderation decisions
2) Ensure decisions are reasoned, communicated clearly, and based on objective criteria.
3) Allow users to submit additional contextual information during appeals.
Indicators

1) Number of complaints received
2) Average resolution time
3) Percentage of decisions overturned
Do's and Don'ts
Do's
<ul style="list-style-type: none">• Do ensure that complaint-handling is functionally independent from initial moderation decisions.• Do provide clear and reasoned explanations for outcomes.• Do allow users to submit contextual information during the complaint process.• Do check the transparency platform (https://transparency.dsa.ec.europa.eu/) to assess your service respect to the overall enforcement mechanisms.
Don'ts
<ul style="list-style-type: none">• Don't design complaint procedures that are excessively complex or discouraging.• Don't rely on automated responses without human review safeguards.• Don't impose unreasonable time limits or procedural barriers on complainants.

4. Graduated Enforcement Framework.

Platforms should implement a graduated enforcement framework that applies measures proportionate to the nature, gravity and recurrence of the violation. Rather than relying exclusively on immediate suspension or termination, platforms should adopt a structured sequence of responses — such as warnings, temporary restrictions, reduced visibility measures or suspensions — calibrated to the seriousness of the conduct.

In doing so, platforms should clearly differentiate between negligent behaviour, isolated mistakes and intentional or repeated misconduct, ensuring that enforcement actions are tailored to the specific circumstances of each case. Consistency in enforcement should be documented and periodically reviewed in order to prevent discriminatory or uneven application of rules.

Finally, sanctions should never be opaque, discretionary or arbitrary. Users must be able to understand the reasons behind enforcement decisions and the criteria guiding their application, thereby reinforcing legal certainty, procedural fairness and trust in platform governance.

Operational Measures	
1)	Conduct periodic internal risk reviews focused on recurring illegal activities.
2)	Adapt platform features and moderation tools to emerging risks.
3)	Implement safeguards against fraud, impersonation, and deceptive practices.
Indicators	
1)	Frequency of internal risk reviews conducted
2)	Number of recurring or repeated abuse patterns identified
3)	Time elapsed between risk identification and mitigation action
4)	Reduction in repeated violations following preventive measures
Do's and Don'ts	
<p>Do's</p> <ul style="list-style-type: none"> • Do document identified risks and corresponding mitigation measures. • Do prioritise risks based on likelihood and potential impact. • Do adapt preventive measures over time in response to emerging misuse patterns. <p>Don'ts</p> <ul style="list-style-type: none"> • Don't treat risk prevention as a one-off or purely formal exercise. • Don't replicate complex VLOP risk assessment models without proportional adaptation. • Don't ignore low-level but recurring abuses that may indicate structural vulnerabilities. 	

5. Specific Measures for Online Marketplaces – Trader Traceability and Verification.

Online marketplaces should implement robust trader traceability and verification procedures prior to activating seller accounts. In particular, they should collect essential identification data from traders, including relevant contact details and, where applicable, VAT or tax identification numbers. Where such information is required by law, marketplaces should take reasonable steps to verify its accuracy before allowing the trader to operate on the platform.

Marketplaces should also maintain internal records documenting the onboarding process, including the information collected and any verification steps undertaken, in order to ensure accountability and facilitate cooperation with competent authorities where necessary.

In cases of non-compliance, marketplaces should apply a graduated enforcement approach, beginning with requests for clarification or corrective action and, where appropriate, escalating to temporary restrictions or suspension. Traders who repeatedly engage in serious or persistent violations should be suspended or removed from the platform, in order to safeguard consumers, preserve marketplace integrity and reduce exposure to regulatory and reputational risks.

Operational Measures	
1)	Implement trader onboarding and verification procedures.
2)	Require submission of essential identification information.
3)	Suspend or restrict traders engaging in repeated violations.
Indicators	
1)	Percentage of traders successfully verified at onboarding
2)	Number of trader-related violations detected per reporting period
3)	Average response time to trader non-compliance
4)	Rate of repeated violations by the same trader
Do's and Don'ts	
Do's	
<ul style="list-style-type: none"> • Do collect and verify essential trader identification information before activation. • Do apply graduated enforcement measures in case of non-compliance. • Do maintain internal records of trader verification and enforcement actions. 	
Don'ts	
<ul style="list-style-type: none"> • Don't allow anonymous or unverified traders to operate without safeguards. • Don't rely exclusively on user complaints to detect illegal products. • Don't delay enforcement actions in cases of repeated or serious violations. 	

Mapping Table: Policies, DSA Articles and Stakeholders.

Policy	Policy Title	Relevant DSA Articles	Primary Stakeholders	Secondary Stakeholders / Affected Actors
Policy 1	Content Moderation and Notice-and-Action Mechanisms	Arts. 14, 16, 17, 20	Hosting services; Online platforms	Users; Trusted flaggers; Authorities
Policy 2	Transparency of Terms and Conditions	Arts. 14, 15	All digital service providers	Users; Consumer organisations
Policy 3	Internal Complaint Handling and Redress	Arts. 17, 20, 21	Online platforms	Users; Out-of-court dispute bodies
Policy 4	Risk Prevention and Platform Integrity	Arts. 34–35 (by analogy for SMEs)	Online platforms; Hosting services	Authorities; Users
Policy 5	Marketplace Obligations and Trader Traceability	Arts. 22–24	Online marketplaces	Traders; Consumers; Market surveillance authorities

Preventive and Remedial Measures Inspired by Industry Practices.

This section indicates preventive and remedial measures inspired by practices developed by major digital platforms and adapts them to the operational reality of SMEs, in line with the proportionality principle underpinning the Digital Services Act. Rather than promoting complex or resource-intensive compliance models, the focus is placed on functional and scalable mechanisms that have proven effective in mitigating risks related to illegal content, abuse and misuse of digital services.

With regard to the detection and prevention of illegal content, providers are encouraged to combine user reporting tools with targeted keyword alerts and contextual human review. Risk signals — such as abnormal posting frequency, repeated complaints or anomalous transaction patterns — may be used to prioritise cases requiring closer scrutiny. In higher-risk situations, proportionate friction-based measures, including temporary posting limits or confirmation prompts, can reduce the likelihood of harm without amounting to general monitoring.

Enforcement should follow a graduated and transparent logic. Platforms are encouraged to adopt proportionate responses — ranging from warnings and temporary restrictions to suspension — while clearly distinguishing between isolated mistakes and intentional or repeated misconduct. Enforcement decisions should be systematically communicated and linked to specific rule violations, thereby enhancing legal certainty and procedural fairness.

Preventive governance should also include user education and contextual guidance. Clear community guidelines, FAQs and pre-action warnings can reduce inadvertent violations and foster responsible participation. Nudging techniques may steer users toward compliant behaviour, provided they are transparent and non-coercive.

To safeguard platform integrity, providers should adopt measures to detect coordinated or inauthentic behaviour, including automated activity or abusive reporting campaigns. Temporary feature restrictions or rate-limiting mechanisms may be applied where credible abuse signals emerge, and cooperation with competent authorities should be ensured when legally required.

Finally, transparency plays a central role in strengthening accountability and trust. Even SMEs can contribute to a transparent governance culture by maintaining internal moderation logs and publishing simplified transparency summaries, including aggregate data on notices, removals and appeals. Such proportionate transparency practices reinforce user confidence while supporting anticipatory compliance and reducing long-term enforcement risks.

Table of preventive and remedial measures inspired by industry practices

Section	Measure Type	Key Objective	Concrete Tools / Mechanisms	Preventive or Remedial Nature	Relevance for SMEs
7.1 Proactive Content Moderation Systems	Governance & Technical Moderation	Prevent dissemination of illegal or harmful content	AI-assisted detection tools; keyword filters; risk-based monitoring; escalation protocols	Primarily Preventive (with remedial follow-up)	Scalable solutions adaptable to SME resources; modular AI support reduces manual burden
7.2 Notice-and-Action Enhancement Mechanisms	Procedural Safeguards	Ensure efficient and transparent handling of user reports	Structured reporting forms; tracking systems; internal deadlines; feedback notifications	Remedial , with preventive impact through deterrence	Standardised templates reduce administrative costs and improve compliance
7.3 Internal Complaint and Redress Systems	Accountability & Due Process	Safeguard user rights and correct moderation errors	Independent review channels; documented reasoning; appeal workflows; audit trails	Primarily Remedial	Strengthens trust and reduces litigation risk for SMEs

Section	Measure Type	Key Objective	Concrete Tools / Mechanisms	Preventive or Remedial Nature	Relevance for SMEs
7.4 Transparency and User Empowerment Measures	Transparency & Information Governance	Increase user awareness and regulatory alignment	Plain-language T&Cs; transparency reports; algorithmic explanation summaries	Both Preventive and Remedial	Enhances credibility without requiring complex infrastructure
7.5 Trader Traceability and Marketplace Safeguards	Economic Governance & Consumer Protection	Prevent fraudulent or unsafe commercial activity	Identity verification; KYC-lite systems; suspension protocols; cooperation with authorities	Primarily Preventive , with remedial enforcement	Risk-based verification avoids disproportionate compliance burdens

I. Sector-Specific Applications.

This section translates the preventive and remedial measures analysed in the previous section into sector-specific applications, reflecting the diverse operational realities of different types of digital services. While the underlying compliance objectives remain consistent, the manner in which risks manifest and mitigation measures are implemented varies significantly across content-sharing platforms, online marketplaces and hosting services. Drawing on industry practices observed among large stakeholders, this section illustrates how such measures can be contextualised and simplified for SMEs, ensuring relevance, proportionality and practical applicability within specific service models.

Sector specific application
<p>Social Media and Content-Sharing Platforms: Platforms relying on user-generated content should prioritise notice-and-action mechanisms, graduated enforcement and user education tools</p>
<p>Online Marketplaces: Marketplaces should focus on trader verification, product monitoring and cooperation with consumer protection authorities.</p>
<p>Hosting and Cloud Services: Hosting providers should emphasise cooperation mechanisms and procedural clarity upon receipt of notices.</p>
<p>Context-Specific Friction Measures: Digital service providers may introduce context-specific friction mechanisms tailored to the characteristics of their sector in order to prevent high-risk behaviours without unduly restricting legitimate use. Such measures, widely adopted by large platforms, include confirmation steps, temporary limitations or contextual warnings activated in predefined risk scenarios. For SMEs, these mechanisms can be implemented through simple interface adjustments or procedural checks triggered only in clearly defined contexts (e.g. first-time sellers, newly created accounts, high-risk product categories).</p>
<p>Sector-Based Risk Signalling: Large stakeholders rely on sector-specific risk indicators to prioritise moderation and enforcement resources. This measure encourages SMEs to define basic risk signals linked to their sector of operation, allowing targeted and proportionate interventions. Examples include unusual posting frequency in content platforms, abnormal transaction patterns in marketplaces, or repeated abuse reports linked to specific service features.</p>
<p>Differentiated Enforcement by Service Function: This measure promotes the differentiation of enforcement responses based on the functional role of the service component involved, rather than applying uniform sanctions across the entire platform. For example, SMEs operating hybrid services may restrict specific functionalities (e.g. commenting, selling, messaging) instead of imposing full account suspensions, thereby aligning enforcement with proportionality principles.</p>
<p>Do's and Don'ts</p>
<p>Do's</p> <ul style="list-style-type: none"> • Do adapt preventive and remedial measures to the specific risks and functionalities of each service sector. • Do apply context-specific friction and enforcement mechanisms only where higher risks are reasonably identified.

- Do use sector-based risk signals to **prioritise human review** without engaging in general monitoring.
- Do differentiate enforcement actions based on the **service function involved**, in line with proportionality.
- Do periodically reassess sector-specific measures in light of emerging risks or changes in service design.

Don'ts

- Don't apply uniform compliance measures across different service types without contextual assessment.
- Don't replicate complex sectoral solutions developed by large platforms without proportional simplification.
- Don't rely exclusively on automated signals to justify enforcement actions.
- Don't introduce sector-specific restrictions that are opaque or insufficiently explained to users.
- Don't overlook low-intensity but recurring sector-specific abuses that may indicate structural vulnerabilities.

II. Governance, Accountability and Internal Controls

This section focuses on the organisational and governance dimension of DSA compliance, which plays a central role in the compliance strategies of major digital platforms. Large stakeholders typically rely on dedicated teams, internal escalation processes and formal accountability structures to implement preventive and remedial measures effectively. For SMEs, equivalent outcomes must be achieved through lighter, function-based governance arrangements, clear allocation of responsibilities and basic internal controls. This section therefore abstracts governance practices observed in larger platforms into minimal yet robust organisational safeguards, suitable for smaller providers and aligned with the DSA's emphasis on process-based accountability.

Measures
<p>Allocation of Responsibilities: SMEs should formally allocate DSA-related responsibilities, even where a single individual covers multiple roles.</p>
<p>Training and Awareness: Periodic internal training supports consistent application of policies and reduces error rates.</p>
<p>Internal Escalation and Decision Review Pathways: Major platforms rely on structured internal escalation mechanisms to handle complex or high-impact decisions. This measure adapts such practices by encouraging SMEs to define simple escalation pathways for sensitive moderation, enforcement or risk-related decisions. Escalation may involve a second reviewer, a senior staff member or an external advisor, without requiring formal committees or dedicated departments.</p>
<p>Documentation and Traceability of Key Decisions: Systematic documentation of moderation and enforcement decisions is a core governance practice among large platforms. This measure encourages SMEs to maintain lightweight documentation enabling traceability and accountability. Basic decision logs, structured spreadsheets or ticketing systems may suffice, provided they allow reconstruction of the rationale and actions taken.</p>
<p>Periodic Internal Compliance Self-Assessment: Large stakeholders routinely conduct internal audits and compliance reviews. This measure adapts such practices by promoting periodic self-assessment exercises focused on key DSA obligations. For SMEs, self-assessments can take the form of short internal reviews or checklists conducted annually or following significant service changes</p>
Do's and Don'ts
<p>Do's</p> <ul style="list-style-type: none"> • Do clearly allocate internal responsibilities for DSA-related compliance, even in small teams. • Do establish simple and documented escalation pathways for complex or high-impact decisions. • Do maintain lightweight but reliable documentation of key moderation, enforcement and risk-related decisions. • Do conduct periodic internal self-assessments to verify the effectiveness of governance measures. • Do update internal procedures following incidents, audits or regulatory developments.

<p>Don'ts</p> <ul style="list-style-type: none"> • Don't concentrate all compliance-related decisions in a single role without safeguards. • Don't rely on informal or undocumented practices for high-impact decisions. • Don't treat governance measures as static or purely formal requirements. • Don't postpone corrective actions once governance gaps are identified. • Don't introduce governance structures that are disproportionate to the size and risk profile of the organisation.
--

Detailed Preventive Measures Catalogue

This section provides a **systematic catalogue of preventive measures** observed in large digital platforms and abstracted into proportionate, SME-applicable policies. Measures are grouped by functional objective and may be combined according to the scale and risk profile of the service.

Measures
<p>Friction-Based Preventive Measures:</p> <p>Friction-based measures introduce minimal procedural steps aimed at preventing unlawful or harmful behaviour without restricting legitimate use.</p> <p>Examples include: - confirmation prompts before publishing content in high-risk categories; - cooling-off periods for repeated submissions; - visibility warnings indicating potential rule violations.</p> <p>These measures are particularly effective for SMEs as they are low-cost, easy to implement and consistent with freedom of expression safeguards.</p>
<p>Early Warning and Risk Signaling Tools:</p> <p>Risk signaling tools allow providers to prioritise human review without engaging in general monitoring.</p> <p>Preventive practices include: - keyword alerts linked to known illegal goods or services; - thresholds for abnormal posting or transaction frequency; - user reputation indicators based on past compliance.</p> <p>Such tools support diligence obligations under Articles 14 and 16 DSA.</p>
<p>User Education and Awareness Measures:</p>

<p>Preventive compliance is strengthened through user education mechanisms such as:</p> <ul style="list-style-type: none"> - contextual reminders of platform rules; - accessible community guidelines; - onboarding tutorials explaining acceptable use. <p>Education-based prevention reduces enforcement costs and supports systemic risk mitigation. To this end, to invite the user to consult the EU Commission DSA Transparency Platform could be extremely useful.</p>
<p>Platform Integrity and Abuse Prevention:</p> <p>To preserve platform integrity, SMEs may adopt: - rate limiting and temporary feature restrictions;</p> <ul style="list-style-type: none"> - detection of coordinated or automated behaviour; - safeguards against impersonation and fraudulent activity. <p>These measures are proportionate responses to abuse patterns commonly identified by large platforms.</p>

Remedial Measures Catalogue

This section outlines **remedial actions** available to service providers following the detection of illegal content or rule violations. Remedial measures should be applied progressively and documented.

Measures
<p>Content-Level Remedies:</p> <p>Remedies targeting specific content include: - removal or disabling of access to illegal content; - reduction of visibility or distribution; - labelling or warning notices where appropriate.</p>
<p>Account-Level Remedies:</p> <p>Account-based remedies address repeated or severe violations: - formal warnings; - temporary account restrictions; - suspension or termination in cases of persistent non-compliance.</p> <p>Graduated enforcement supports fairness and proportionality.</p>
<p>Transaction-Level Remedies (Marketplaces):</p> <p>Online marketplaces may implement: - suspension of specific product listings; - temporary freezing of transactions; - delisting of traders in case of serious violations.</p>
<p>Cooperation and Escalation Measures:</p> <p>Where required, providers should cooperate with: - Digital Services Coordinators; - law enforcement authorities; - trusted flaggers and consumer protection bodies.</p>

User-Centred Policy Guidelines under the Digital Services Act.

An awareness programme for users and consumers.

The Digital Services Act explicitly recognises that the effectiveness of digital regulation depends not only on the obligations imposed on service providers, but also on the ability of users and consumers to understand, exercise and effectively rely on their rights.

In this perspective, user-oriented policies play a complementary role to provider-facing compliance measures, contributing to risk prevention, trust-building and the protection of fundamental rights.

This section sets out policy guidelines addressed to users and specific categories of users, taking into account structural vulnerabilities, asymmetries of information and power imbalances that characterise digital environments. These guidelines are not intended to shift responsibility from service providers to users, but to support informed, autonomous and safer participation online, in line with the objectives of the DSA.

General Guidelines for Users and Consumers

I Awareness of Platform Rules and Content Moderation Practices.

The objective of this policy is to enable users to understand how platforms regulate content, enforce their rules and adopt moderation decisions. In order to participate responsibly and exercise their rights effectively, users should familiarise themselves with the platform's Terms and Conditions, community standards and content moderation policies. Particular attention should be paid to rules concerning prohibited content, possible sanctions and available appeal mechanisms. Where platforms provide summaries or explanatory materials, users are encouraged to consult them to gain a clearer and more accessible understanding of the applicable rules.

This awareness is essential in light of the transparency obligations established under the Digital Services Act, which aim to reduce information asymmetries between providers and users. A better understanding of platform governance strengthens procedural fairness, fosters responsible participation and helps prevent misunderstandings related to moderation and enforcement decisions.

Do's and Don'ts

Do's

- Do read summaries and key sections of platform Terms and Conditions.
- Do pay attention to explanations provided with moderation decisions.
- Do consult transparency resources made available by platforms.

Don'ts

- Don't assume that platform rules are identical across services.
- Don't rely solely on informal user interpretations of platform policies.
- Don't ignore updates or changes to platform rules.

II Use of Notice-and-Action and Reporting Mechanisms.

The objective of this policy is to empower users to report illegal or harmful content effectively and responsibly. Users are encouraged to make active use of notice-and-action mechanisms whenever they reasonably believe that specific content may be unlawful or in breach of applicable rules. Reports should be as precise and substantiated as possible, clearly indicating the reasons for concern and providing relevant contextual information to facilitate an informed assessment by the platform.

At the same time, users should refrain from engaging in abusive, bad-faith or coordinated reporting practices, which may undermine procedural fairness and distort moderation processes.

User reporting constitutes a core component of the enforcement architecture established under the Digital Services Act and contributes to more targeted, proportionate and effective moderation decisions.

Do's and Don'ts

Do's

- Do use reporting tools to flag content you reasonably believe to be illegal.
- Do provide clear and factual information when submitting a notice.
- Do retain confirmation or reference numbers for submitted reports.

Don'ts

- Don't engage in mass or coordinated reporting campaigns.

- Don't submit notices in bad faith or for retaliatory purposes.
- Don't expect immediate removal without assessment.

III Exercise of Redress and Appeal Rights

The objective of this policy is to ensure that users are able to effectively challenge moderation decisions that affect their content or accounts. When content is removed, visibility is reduced, or accounts are restricted or suspended, users should make use of the internal complaint-handling systems made available by the platform. Appeals should be clearly reasoned and focus on the factual context of the case, as well as on the specific platform rules that are considered relevant to the decision.

Where applicable, users may also access certified out-of-court dispute settlement mechanisms, in accordance with the procedural guarantees provided under the Digital Services Act.

The procedural safeguards introduced by the DSA can only function effectively if users are adequately informed about their rights and are willing to exercise them. Active engagement with appeal and redress mechanisms contributes to greater accountability, consistency and fairness in platform governance.

Do's and Don'ts

Do's

- Do use internal complaint-handling systems where available.
- Do explain the context and reasons for your appeal clearly.
- Do respect procedural timelines and platform guidance.

Don'ts

- Don't submit repetitive or abusive appeals.
- Don't assume appeals are automatic reversals of decisions.
- Don't disregard out-of-court dispute resolution options where offered.

Guidelines for Specific Categories of Vulnerable Users.

I. Consumers in Online Marketplaces – Informed and Safe Online Consumption

The objective of this policy is to protect consumers from fraud, unsafe products and misleading commercial practices in online marketplaces. While platforms are subject to specific traceability and transparency obligations, consumers themselves play a crucial preventive role in ensuring safe transactions.

Before concluding a purchase, consumers should carefully verify trader information, examine product descriptions and consult available reviews. Particular caution should be exercised in the presence of unusually low prices, time-limited offers designed to create artificial urgency, or pressure-based sales tactics that may signal fraudulent or misleading behaviour.

Where irregularities arise, consumers should promptly make use of available complaint, refund and reporting mechanisms provided by the platform.

Although marketplace obligations under the Digital Services Act aim to enhance traceability and transparency, informed and vigilant consumer behaviour remains a fundamental element in preventing harm and strengthening trust in digital commerce.

Do's and Don'ts
<p>Do's</p> <ul style="list-style-type: none">• Do verify trader identity and product information before purchase.• Do use secure payment systems and official platform channels.• Do report suspicious listings or traders promptly. <p>Don'ts</p> <ul style="list-style-type: none">• Don't rely exclusively on promotional claims or ratings.• Don't complete transactions outside the platform where protections apply.• Don't ignore warning signs such as pressure-based sales tactics.

II. Users with Low Digital Literacy or Increased Exposure to Manipulation.

The objective of this policy is to mitigate the risks associated with dark patterns, misleading interface design and behavioural manipulation in digital environments. Such practices may influence user

decisions in subtle or non-transparent ways, particularly affecting individuals with lower digital literacy or heightened vulnerability.

Users should therefore approach default settings, consent prompts and interface features that encourage rapid, repeated or impulsive actions with particular caution. It is advisable to periodically review privacy settings, content recommendation preferences and notification configurations in order to maintain meaningful control over one's digital experience. Where uncertainty arises regarding the implications of certain design choices, users should consult explanatory materials provided by the platform or seek independent guidance.

Although the Digital Services Act addresses deceptive practices primarily through transparency and fairness obligations, informed and attentive user behaviour significantly enhances the Regulation's protective effect, especially for minors and other vulnerable users.

Do's and Don'ts
Do's <ul style="list-style-type: none">• Do take time to review default settings and consent requests.• Do seek clarification through help centres or trusted sources.• Do question interfaces that encourage rushed decisions.
Don'ts <ul style="list-style-type: none">• Don't accept permissions or settings without understanding them.• Don't assume design choices are always neutral.• Don't hesitate to disengage from confusing or coercive interactions.

III. Content Creators, Prosumers and Small Online Sellers.

Responsible Participation and Economic Activity Online.

The objective of this policy is to support users who operate in hybrid roles within digital environments, acting not only as consumers but also as content creators, sellers or service providers. These dual roles increase exposure to platform governance decisions and potential legal risks, making enhanced awareness and procedural preparedness essential.

Creators and online sellers should therefore familiarise themselves with platform monetisation rules, visibility criteria and enforcement mechanisms, in order to understand how content is ranked, promoted or restricted. Particular attention should be paid to compliance with applicable consumer

protection, advertising and intellectual property rules, as breaches may result not only in platform sanctions but also in legal liability.

In addition, users engaged in economic or content-related activities should systematically document relevant interactions, communications and decisions that may become significant in the event of disputes or enforcement actions. Such documentation strengthens procedural safeguards and contributes to more transparent and accountable digital participation within the framework established by the Digital Services Act.

Do's and Don'ts
<p>Do's</p> <ul style="list-style-type: none"> • Do understand platform monetisation, visibility and enforcement rules. • Do keep records of transactions, communications and moderation decisions. • Do comply with consumer protection and advertising obligations. <p>Don'ts</p> <ul style="list-style-type: none"> • Don't rely on informal practices inconsistent with platform rules. • Don't ignore repeated warnings or enforcement signals. • Don't assume platform hosting removes legal responsibilities.

IV. Children as Vulnerable Users.

This policy reflects the enhanced level of protection that the Digital Services Act grants to minors and other vulnerable users, acknowledging their greater exposure to online risks and power imbalances in digital environments. The Regulation promotes preventive design choices, privacy-friendly default settings and proportionate risk mitigation measures tailored to specific vulnerabilities. For SMEs, compliance in this area should primarily be achieved through responsible design and governance decisions rather than complex age-verification or profiling systems. The objective is to mitigate risks through safety by design, transparency and precaution, avoiding platform practices that could disproportionately expose minors or vulnerable users to harm. Relevant provisions include Articles 28 and 34 DSA.

Operational Measures
1) Apply privacy-friendly default settings for minors.
2) Avoid profiling-based recommendations where minors are involved.

3) Provide age-appropriate explanations of platform risks and features.
Indicators
<ol style="list-style-type: none"> 1) Availability of child- and age-appropriate default settings 2) Number of reports or complaints involving minors or vulnerable users 3) Presence of profiling-based recommendation features affecting minors 4) Frequency of reviews of features potentially impacting minors' safety 5) User feedback related to safety and accessibility for vulnerable groups
Do's and Don'ts
<p>Do's</p> <ul style="list-style-type: none"> • Do apply privacy-friendly and safety-oriented default settings for minors. • Do minimise exposure of minors to potentially harmful content or interactions. • Do provide age-appropriate explanations of platform features and risks. • Do periodically review design choices that may disproportionately affect vulnerable users. <p>Don'ts</p> <ul style="list-style-type: none"> • Don't rely on profiling-based recommendation systems for minors unless strictly necessary and justified. • Don't design interfaces that nudge minors towards excessive use or risky behaviour. • Don't collect or process personal data of minors beyond what is strictly necessary for service provision. • Don't treat the protection of minors as a purely formal requirement rather than an ongoing governance responsibility.

Key recommendations provided by EU
<ul style="list-style-type: none"> • Setting minors' accounts to private by default so their personal information, data, and social media content is hidden from those they aren't connected with to reduce the risk of unsolicited contact by strangers. • Modifying the platforms' recommender systems to lower the risk of children encountering harmful content or getting stuck in rabbit holes of specific content, including by advising platforms to prioritise explicit signals from children over behavioural signals as well as empowering children to be more in control of their feeds.

- **Empowering children to be able to block and mute any user** and ensuring they can't be added to groups without their explicit consent, which could help prevent cyberbullying.
- **Prohibiting accounts from downloading or taking screenshots of content posted by minors** to prevent the unwanted distribution of sexualised or intimate content and sexual extortion.
- **Disabling by default features that contribute to excessive use**, like communication "streaks," ephemeral content, "read receipts," autoplay, or push notifications, as well as removing persuasive design features aimed predominantly at engagement and putting safeguards around AI chatbots integrated into online platforms.
- **Ensuring that children's lack of commercial literacy is not exploited** and that they are not exposed to commercial practices that may be manipulative, lead to unwanted spending or addictive behaviours, including certain virtual currencies or loot-boxes.
- **Introducing measures to improve moderation and reporting tools**, requiring prompt feedback, and minimum requirements for parental control tools¹.

Conclusions

These Blueprint Guidelines operationalise the governance architecture of the EU Regulation 2022/2065 on Digital Services Act through a structured, stakeholder-oriented and proportionate framework.

They are designed to:

- Support SMEs and non-VLOP providers in achieving sustainable compliance.
- Promote transparency, procedural fairness and accountability.
- Strengthen platform integrity.
- Empower users as active participants in digital governance.

By integrating preventive governance, structured moderation workflows and user-centred safeguards, digital service providers contribute to a safer, more trustworthy and rights-respecting online environment in line with the European digital regulatory strategy.

¹ <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>.

These guidelines are part of the deliverable D6 “Policy and recommendations report”, SNIP - Self-assessment Network Impact Program, COD.MUR: P2022AK2HK, CUP J53D23018800001.

Suggested citation: J. Fortuna, D. Amram, A. Davola, D. Foà, A. Polisenò, C. Sganga, *Blueprint guidelines for stakeholders to ensure compliance, accountability and user protection under the Digital Services Act*, available at www.lider-lab.it/snip.

Licence: CC.BY. 4.0.