

NKL Associates s.r.o.

Independent Audit Report on XNXX.com

Independent practitioner's assurance report concerning
Regulation (EU) 2022/2065, the Digital Services Act (DSA)

Report date: 13 November 2025

Contents

Independent Assurance Report..... 3

- 1. Introduction..... 3
- 2. Objective and scope of the audit..... 3
- 3. Subject matter of the audit 4
- 4. Audit criteria 4
- 5. Level of assurance 5
- 6. Audit methodology 5
- 7. Limitations and Disclaimers 6
- 8. Stakeholder engagement and cooperation 6
- 9. Executive Summary 6

Appendix 1 – Conclusions and Test Procedures per Obligation..... 9

Appendix 2 – Details on Obligations Outside the Scope of the Audit Assessment 82

Appendix 3 – Template for the Audit Report Referred to in Article 6 of Delegated Act 85

Appendix 4 – Audit Risk Analysis 88

Independent Assurance Report on XNXX.com - NKL Associates s.r.o.

Prepared by:

CERTICOM s.r.o., Gorkého 10, 811 01
Bratislava – Old Town district
Slovak Republic

Certification body CERTICOM, Pod Donátom 907/5, 965 01
Žiar nad Hronom
Slovak Republic

Email: certicom@certicom.eu

(referred to in this report as “CERTICOM”, “we”, or “our”)

To: Management of NKL Associates s.r.o.

1. Introduction

We have been engaged by NKL Associates s.r.o. (“NKL”, or “provider”), a company registered in the Czech Republic, to perform a *reasonable assurance* engagement in accordance with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) and Commission Delegated Regulation (EU) 2023/6807 (“Delegated Regulation”), supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council (the Digital Services Act, “DSA”). These rules establish requirements for audits of very large online platforms (VLOPs) and very large online search engines.

The subject of this audit is the digital service XNXX.com (“platform”), operated by NKL. On 10 July 2024, the European Commission designated XNXX.com as a VLOP under Article 33 of the DSA. This designation triggered enhanced compliance obligations, effective from 13 November 2024.

In accordance with Article 37(1)(a) of the DSA, this audit evaluates whether the service provider complied, in all material respects, with the obligations applicable to VLOPs during the period from 13 November 2024 to 13 November 2025. The audit was conducted independently by CERTICOM in accordance with ISAE 3000 (Revised).

This report is intended for submission to the European Commission and competent national authorities pursuant to Article 42 of the DSA and will also be made publicly available. The tone and scope of this report reflect both the formal audit requirements and the importance of regulatory transparency and evidence-based assessment of the platform’s compliance with its obligations under the DSA.

2. Objective and scope of the audit

The objective of the audit was to assess whether NKL as the provider of XNXX.com, has established and implemented policies, processes, and controls that ensure its compliance with the applicable provisions of the DSA, particularly those arising from its designation as a VLOP.

The scope of the audit covered the following areas of the DSA:

- **Section 1 of Chapter III (Articles 11–15)** - provisions applicable to all providers of intermediary services,

- **Section 2 of Chapter III (Articles 16–18)** - additional provisions applicable to providers of hosting services, including online platforms,
- **Section 3 of Chapter III (Article 19–28)**: additional obligations applicable to online platforms,
- **Section 5 of Chapter III (Articles 34–42)**: Specific obligations for providers of VLOPs, including systemic risk management, crisis protocols, data access, and independent auditing.

The audit included both a design and operational effectiveness assessment of compliance measures, including systemic risk management, illegal content detection and response, recommender system functionality, advertising disclosures, and required transparency measures.

In addition, certain provisions within the articles listed above were determined to be not applicable to the provider. A complete list of such provisions, along with the rationale for their exclusion from the audit scope, is provided in Appendix 2 of this report.

3. Subject matter of the audit

XNXX.com is an adult content platform operated by NKL, which enables users - both anonymous and registered - to access audiovisual content uploaded by other users and content creators. The platform is freely accessible across all EU Member States and its Terms of Services (TOS) and key user-facing interfaces are available in multiple EU languages.

The audit covered the platform’s functionalities and compliance measures as implemented and operated during the period from 13 November 2024 to 13 November 2025. These included:

- Notice-and-action mechanisms for illegal content,
- Internal complaint handling and redress systems,
- Recommender systems and user control features,
- Moderation processes, both human and automated,
- Interface transparency and user information,
- Advertising transparency obligations,
- Risk assessments and mitigation plans,
- Transparency reporting obligations,
- Cooperation with national authorities and relevant bodies.

Given the nature of the audiovisual content hosted, specific attention was directed at the provider’s mechanisms for detecting and acting upon illegal content, in particular child sexual abuse material (CSAM) and on-consensual intimate imagery (NCII), as defined under Union law and applicable national provisions, as well as on the platform’s engagement with law enforcement and NGOs active in the field of online safety and child protection.

The provider does not engage in behavioural profiling for advertising purposes, nor does it employ complex algorithmic systems beyond basic geographical and popularity-based recommendation logic. User registration is optional, and privacy by design remains a core feature of the platform.

4. Audit criteria

The assessment criteria applied in the audit consisted of the following:

- The substantive obligations laid down in DSA,

- Interpretative notices and guidance issued by the European Commission and competent authorities,
- Requirements of the Commission Delegated Regulation,
- General principles of legality, accountability, transparency, and proportionality, in accordance with Recital 81 DSA and Article 3(2)(b) of the Delegated Regulation,
- Assurance engagement standards, notably ISAE 3000 (Revised).

Criteria were applied in accordance with the proportionality principle under Article 3(2)(b) of the Delegated Regulation, taking into account the provider's service characteristics and risk exposure.

5. Level of assurance

This report is the result of a reasonable assurance engagement, as defined in ISAE 3000 (Revived). The audit was designed to obtain a high level of assurance - though not absolute certainty - that XNXX.com complied, in all material respects, with the applicable obligations of the DSA for the audit period.

This means that based on the procedures performed and the evidence obtained, we provide a positive or negative conclusion on whether material misstatements or significant instances of non-compliance were identified.

Where measures were still being developed or adapted, these were reviewed against the criteria of legal adequacy and effective implementation. Such instances are reported in context and do not amount to non-compliance unless they fail to meet functional thresholds set by the DSA.

While the procedures were designed to identify material deficiencies, this engagement does not constitute a forensic examination, and the presence of undetected gaps cannot be ruled out. However, we applied professional diligence, maintained independence, and employed a methodology designed to capture material deficiencies.

6. Audit methodology

The audit methodology was based on the principles of risk-based assurance, applying both design evaluation and substantive testing across a range of DSA obligations. The audit was conducted between October 2025 and November 2025 and included the following procedures:

- structured interviews with content moderation team, compliance personnel, notice and complaint team, technical team and legal counsel,
- review of internal documentation, including moderation protocols, user complaint data, transparency report drafts,
- live demonstrations and guided process walkthroughs of moderation workflows and compliance procedures,
- ad-hoc sampling of moderation actions and internal review protocols, provider personnel provided procedural access and clarification as required, without affecting auditor independence,
- accessibility and interface checks,
- review of engagement with public authorities and child protection organizations.

Where systems and controls were found to be primarily manual or operated at limited scale, the audit approach remained aligned with the proportionality principle and focused on contextual evidence, design soundness, and observed responsiveness.

7. Limitations and Disclaimers

The audit was performed using methods designed to provide reasonable assurance but does not constitute a forensic examination or an absolute guarantee of compliance. The scope of testing was limited to the systems and procedures operational during the audit period and to the extent that access and cooperation by the provider were available.

Certain risks—particularly those related to real-time abuse, detection of manipulated content, or malicious user circumvention—are inherently difficult to assess in a retrospective audit. In such cases, evaluations were based on whether the provider demonstrated a good-faith, proportionate, and evolving response to these threats.

The findings and conclusions of this report are based on evidence obtained through audit procedures carried out independently and without influence by the service provider. The report has been prepared with the intent of regulatory transparency and accountability and reflects the state of DSA compliance as of 20 March 2025.

8. Stakeholder engagement and cooperation

Throughout the audit period, the provider demonstrated proactive engagement with relevant stakeholders, including public authorities, law enforcement bodies, and civil society organizations with expertise in child protection and online safety. The platform has actively participated in multi-stakeholder initiatives aimed at addressing the spread of illegal content, including CSAM and NCII.

This engagement is particularly visible in:

- ongoing partnerships with NGOs supporting victims of abuse,
- participation in working groups focused on protection of minors in online environments,
- development of internal training modules based on recommendations from external experts,
- active correspondence with competent authorities regarding incident response and transparency improvements.

The provider demonstrated active participation in multi-stakeholder efforts relevant to its DSA obligations. While such engagement does not itself confirm compliance, it indicates an ongoing commitment to regulatory cooperation and evolving practices in areas such as CSAM and NCII prevention.

9. Executive Summary

This executive summary presents the key findings and conclusions of the independent external audit performed in accordance with Article 37(1)(a) of the Digital Services Act (Regulation (EU) 2022/2065) and the requirements of Commission Delegated Regulation (EU) 2023/6807. The audit was conducted for NKL Associates s.r.o., provider of XNXX.com, a very large online platform (VLOP) designated by the European Commission on 10 July 2024. The audit covers the period from 13 November 2024 to 13 November 2025, corresponding to the first year of enhanced obligations under the DSA.

XNXX.com is an adult content platform offering access to audiovisual content uploaded by users, with optional registration and a strict emphasis on user privacy. The platform is accessible in all EU Member States and operates multilingual TOS. While user registration is optional, moderation and recommender systems are designed with simplicity and transparency in mind. Notably, XNXX.com does not engage

in behavioural advertising, and recommender systems are limited to basic indicators such as geography, popularity, and user history (with opt-out available).

The audit assessed the platform's compliance with obligations arising under Chapters III of the DSA, with particular focus on the following areas:

- Notice-and-action mechanisms for illegal content (Article 16),
- Internal complaint-handling systems (Article 20),
- Advertising transparency (Articles 26–27),
- Recommender systems and user control (Article 27),
- Systemic risk assessments (Article 34),
- Mitigation of systemic risks, including protection of minors (Article 35),
- Transparency reporting (Article 15, 24, 42),
- Cooperation with authorities and civil society (Article 37(1)(e)).

The methodology followed ISAE 3000 (Revised) standards and consisted of:

- structured interviews with key personnel,
- examination of internal policies, moderation manuals, and system documentation,
- walkthroughs and observation of moderation workflows,
- sampling of complaint and takedown cases (82 records across 6 EU language contexts),
- verification of transparency reports and user interface accessibility,
- review of language accessibility and communication with authorities.

The audit observed full cooperation from the provider. Access to required records and personnel was granted without undue limitation, and the information provided was sufficient for the audit purposes.

Key Findings:

- **POSITIVE** - 39 obligations (60%) were assessed as fully compliant (“Positive”). The provider shows mature implementation across authority/user contact points (Arts. 11-12), clear and multilingual TOS with moderation disclosures and summaries (Arts. 14.1, 14(5)-14(6)), robust notice-and-action foundations incl. forms, fields, acknowledgments and timely processing (Arts. 16(1)-16(4), 16(6)), reason statements with required elements (Art. 17(3)-17(4)), trusted-flagger framework and prioritization (Art. 22(1)), case-by-case suspension assessment (Art. 23(3)), ad repository with search/API and one-year retention (Art. 39(1)), non-profiling recommender option (Art. 38), and a well-structured compliance function and governance (Arts. 41(1)-41(7)). Biannual transparency reporting cadence and publication timeliness were also met (Arts. 42(1)-42(4)).
- **POSITIVE WITH COMMENTS** - 25 obligations (≈38%) met the essential bar but have improvement headroom. Notable areas:
 - Transparency reporting: reports are detailed and biannual but should add machine-readable formats, legal vs. TOS bases for actions, and moderator training/QA detail (Art. 15); measure against misuse approach needs clearer documentation (Arts. 24(2), 24(3)).
 - User communications: decision notifications are strong for core flows but should be extended to comment/picture reports; standardize statements-of-reasons across all content types (Arts. 16(5); 17(1)-17(2); 20(1), 20(3)).
 - Documentation: formalize LEA notification playbooks incl. Member-State/Europol routing (Arts. 18(1)-18(2)), complaint-handling policy/SLAs (Art. 20.4), misuse policy for

unfounded notices/complaints and suspension parameters (Art. 23(4)), regulator-data access and algorithmic-explanation docs (Arts. 40(1), 40(3)), and training logs (Art. 41(3)).

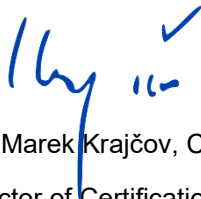
- Recommenders/ads: add parameter weighting rationale and improve ad transparency (payer vs. beneficiary; controls to modify targeting; label partner links) and reflect the split in the ad repository (Arts. 27(1). 27(2); 26(1); 39(2)-39(3)).
- Systemic risks/mitigation: annual assessments and controls are in place; next step is KPIs/metrics and (optionally) structured recommender testing; minors' safeguards are proportionate today but still rely on self-declaration - continue exploring privacy-preserving age assurance (Arts. 28(1); 34(1)-34(2); 35(1)).
- **NEGATIVE** - 1 obligation (2%) was assessed "Negative": Article 24(1). Transparency reports omit mandatory suspension breakdowns under Article 23 (manifestly illegal content vs. manifestly unfounded notices vs. manifestly unfounded complaints), due to backend categorization gaps. Remediation: add structured tagging, dashboards, and machine-readable outputs (recommended within 3 months).

The audit concludes that **NKL has, in all material respects, complied with its obligations under the DSA** for the audit period. No indications of deliberate or systemic non-compliance were observed. The provider has taken steps to operationalize DSA obligations in a proportionate and transparent manner, consistent with the platform's scale, service nature, and risk exposure.

The audit approach followed **a contextual and risk-based** interpretation in line with Article 3(2)(b) of the Delegated Regulation. Where partial or evolving compliance was observed, these instances were evaluated for legal adequacy and are not classified as non-compliance unless demonstrably falling below the minimum legal and functional adequacy requirements stipulated under the DSA.

We applied a contextual and proportional approach, reflecting the provider's operational scale and content sensitivity, in line with the Delegated Regulation. Areas of ongoing development have been documented and do not constitute material breaches, provided continued progress is maintained.

Bratislava, Slovakia 13 November 2025



Ing. Marek Krajčov, Company manager

Director of Certification body CERTICOM

Appendix 1 – Conclusions and Test Procedures per Obligation

The following table compiles the abbreviations and short names used throughout this annex:

API	Application Programming Interface
Board	European Board for Digital Services
CSAM	Child Sexual Abuse Material
ČTÚ	Czech Telecommunications Office
DSA	Digital Services Act (Regulation (EU) 2022/2065)
DSC	Digital Services Coordinator (national regulator under the DSA)
EC	European Commission
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HTML	HyperText Markup Language
IP	Internet Protocol
KPI	Key Performance Indicator
LEA	Law Enforcement Authority
NCII	Non-Consensual Intimate Imagery
TOS	Terms of Service
UI / UX	User Interface / User Experience
VLOP	Very Large Online Platform

Section 1 – Provisions Applicable to All Providers of Intermediary Services

Obligation: Article 11.1	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ An intermediary service contact was designated; ▪ The EU Member States' authorities, the EC and the Board were able to communicate directly by electronic means with the intermediary service contact. 	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Walkthrough of the provider's website confirmed that a dedicated contact point for competent authorities exists, accessible online via the following URL:
<https://info.xnxx.com/authority-contact>
2. The contact point is accessible through the "Information and Links" section (<https://info.xnxx.com/>). Users can reach the form via the following navigation path: *Information and Links* → *Support* → *Contact Us* → *Authorities Contact Us*. The form is accessible without login or prior registration.
3. Review of TOS (*Article 12. Notices to XNXX and/or NKL Associates*) confirmed explicit reference to the contact point for official EU authorities and the EC, stating:
NKL Associates has also established a single point of contact for direct communication with the European Board for Digital Services, the European Commission and the official authorities of the EU Member States. This point of contact is accessible via online form available at <https://info.xnxx.com/authority-contact>. You may use English or Czech language for communication with the point of contact.
4. Verified that this point of contact is referenced in the TOS (Article 4 and 12), which states that the provider has established a direct communication channel specifically for official authorities.
5. Review of the TOS confirmed that the link provided corresponds to the publicly available form on the website.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation: Article 11.2	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none">▪ The information necessary to identify and communicate with the single point of contact was made publicly available;▪ The information was published in an easily accessible location on the provider's interface;▪ The information was kept up to date.	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Performed an interface review of the XNXX platform and confirmed that the information identifying the single point of contact for competent authorities is clearly published through the dedicated online form located at: <https://info.xnxx.com/authority-contact>.
2. The contact point is accessible through the “Information and Links” section (<https://info.xnxx.com/>). Users can reach the form via the following navigation path: *Information and Links* → *Support* → *Contact Us* → *Authorities Contact Us*. The form is accessible without login or prior registration.
3. Examined the visibility and usability of the form interface, confirming that it is clearly titled “Authority Contact” and unambiguously designated for communication by official bodies. The form remains publicly accessible without the need for an account or authentication.
4. Checked that the TOS (*Article 12. Notices to XNXX and/or NKL Associates*) and the informational site info.xnxx.com are aligned, providing consistent references to the same URL and contact functionality. No discrepancies or inactive links were detected during the audit.
5. Confirmed that the contact point information was last updated in connection with the platform’s TOS amendments effective 17 February 2024, as disclosed in the document summary.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation: Article 11.3	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none">▪ The provider publicly specified the language or languages that can be used to communicate with the designated point of contact;▪ The languages included at least one official language of the Member State in which the provider has its main establishment or legal representative;▪ The specified languages included at least one widely understood language within the Union;▪ This information was made available alongside the contact information.	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Examined the form's layout and content. The form header explicitly states its purpose: "This email form is used to receive messages, requests or orders from the European Board for Digital Services, the European Commission and the competent authorities of EU Member States." The notice further specifies: "We only accept communication in Czech or English."
2. Reviewed TOS (Article 12. Notices to XNXX and/or NKL Associates), which reiterates that NKL Associates has established a direct communication channel for official authorities and that communications may be conducted in English or Czech.
3. Reviewed the structure and accessibility of the form interface and confirmed that it is designated explicitly for communications from public authorities. Confirmed that the contact point is accessible to any user without requiring prior registration.
4. Verified that this point of contact is referenced in the TOS (Article 12. Notice to XNXX and/or NKL Associated), which states that the provider has established a direct communication channel specifically for official authorities.
5. Confirmed that the same two languages (English and Czech) appear in the TOS and in the online form interface. The information is consistent across all user-facing and official documents.
6. Confirmed that Czech is the official language of the provider's Member State of establishment (Czech Republic), thereby satisfying the requirement for an official language of the establishment. English, being a widely understood language across the Union, fulfills the obligation to provide a common working language for cross-border communications.
7. Confirmed that the information on accepted languages is displayed directly within the authority-contact form, alongside the communication fields and file-upload feature, and that it is visible without navigation away from the contact page. No indications were found of outdated or inconsistent language information during the audit period.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation:	Audit criteria:	Materiality threshold:
Article 12.1	Throughout the period, in all material respects: <ul style="list-style-type: none">▪ A public point of contact was designated for recipients of the service;▪ The communication channel allowed for direct and rapid communication by electronic means;▪ The communication channel allowed for communication in a user-friendly manner▪ The provider offered at least one non-automated means of communication;▪ Recipients could choose among different means of communication.	N/A

Audit procedures, results and information relied upon:

1. Conducted a walkthrough of the provider’s website and confirmed that a designated point of contact for recipients exists, accessible through: <https://info.xnxx.com/contact>.
2. The contact point is accessible through the “Information and Links” section (<https://info.xnxx.com/>). Users can reach the form via the following navigation path: *Information and Links* → *Support* → *Contact Us* → *Contact Us*. The form is accessible without login or prior registration.
3. Reviewed the form structure and fields (topic selector, email, message body, optional device/log checkboxes, file attachment; CAPTCHA). The design enables one-step submission to the provider by email form (no ticketing account required). The mechanism supports direct electronic messaging. “Rapid” is supported by immediate submission; no UI barriers or account creation were observed.
4. Assessed clarity of labels and guidance text on the contact page, including (i) clear purpose statement (“This email form can be used to send a message to XNXX support”), (ii) topic drop-down, (iii) large message field, (iv) optional diagnostics checkboxes with info icons, and (v) “Send your message” CTA. Interface is simple and mobile-responsive (as shown in the screenshots), meeting “user-friendly” criteria.
5. Inspected TOS (*Article 12. Notice to XNXX and/or NKL Associated*) to confirm handling is “not solely on the basis of automated means,” indicating human review/processing is part of the workflow. Presence of human involvement is explicitly documented, satisfying the “non-automated means” element. Cross-checked that URLs referenced in the TOS match the live public pages reviewed (no dead links observed) - consistent linkage between policy and interface.
6. Reviewed the communication channels described in the TOS and confirmed multiple user-facing contact points:
 - General contact form: <https://info.xnxx.com/contact>;
 - Copyright infringement form: <https://info.xnxx.com/takedown>;
 - Abuse content form: <https://info.xnxx.com/takedown-amateur>.
7. The provider does not publicly state response-time targets or workflow steps (receipt, triage, escalation), which can limit user expectations management. Accepted languages for user communications are not explicitly stated on the user contact page (language clarity appears on the authority form, not on the user form). Aligning user-facing language disclosures with authority-facing disclosures would enhance transparency.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, there is an opportunity to improve transparency around response handling and language accessibility.

Recommendations on specific measures:

- Clarify publicly how user messages are handled (e.g., response timeline, responsible unit/person); enhance transparency by explicitly stating which languages are supported for user communication.

Recommended timeframe to implement specific measures:

Within 3–6 months from the audit conclusion.

<p>Obligation: Article 12.2</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider made publicly available the necessary information to identify and contact the single point of contact for service recipients ▪ The contact information was published in an easily accessible location on the provider’s interface; ▪ The information was kept up to date. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted a walkthrough of the provider’s website and confirmed that a designated point of contact for recipients exists, accessible through: https://info.xnxx.com/contact. The page is active, publicly reachable without registration, and its heading (“Contact Us”) clearly communicates its purpose to users. 2. The contact point is accessible through the “Information and Links” section (https://info.xnxx.com/). Users can reach the form via the following navigation path: <i>Information and Links</i> → <i>Support</i> → <i>Contact Us</i> → <i>Contact Us</i>. The contact entry point is located in a predictable section consistent with user-experience norms.” The form is accessible without login or prior registration. 3. All references (the URLs) remain accurate and functional. No outdated or broken links were detected, and the contact page structure is consistent with prior periods, indicating adequate maintenance of information currency. <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>		<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 14.1</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The TOS include clear information on any restrictions related to content provided by users, including types of prohibited content and the provider’s right to suspend or terminate access to the service; ▪ The TOS describe the principles, procedures, measures, and tools used to moderate content, including algorithmic systems and human intervention; ▪ The TOS reference the internal complaint-handling system available to users within the European Economic Area (EEA); ▪ The TOS must be drafted in language that is clear, intelligible, user-friendly, and unambiguous, ensuring 	<p>Materiality threshold: N/A</p>
--	---	--

	<p>that an average user can comprehend the key provisions;</p> <ul style="list-style-type: none"> ▪ The TOS must be published in an easily accessible and machine-readable format across all interfaces and available in the official languages of EU Member States where the service is offered. 	
--	--	--

Audit procedures, results and information relied upon:

1. The “Information and Links” section of the site includes a dedicated subsection titled “Legal Stuff”, which lists all core policy documents, including the Terms of Service, Privacy Policy, Repeat Infringers Policy, and Anti-Piracy Statement. The Terms of Service are directly available via <https://info.xnxx.com/legal/TOS> and this link is also consistently present in the footer of every XNXX webpage. The document reviewed was version-dated 17 February 2024. Both the summary and full versions were reviewed as part of the audit.
2. Upon examination of TOS (*Article 7. User Submissions* and *8. Content Moderation*), it was confirmed that the document provides clear information on content restrictions and enforcement procedures. It is explicitly prohibiting illegal and harmful content such as child sexual abuse material, non-consensual sexual acts, hate speech, terrorism-related content, and copyright infringement. In addition, the TOS clearly state the conditions under which user accounts may be suspended or terminated. Enforcement actions, including the use of warnings, removal of content, and account deletion, are described in legally grounded but understandable language.
3. With respect to content moderation the TOS (*8. Content Moderation*) provides a description of the moderation principles. It states that moderation on the XNXX platform is conducted through a layered system, combining automated detection technologies with human moderation. Automated systems are used for preliminary flagging of potentially illegal or policy-violating material, while human moderators carry out the final review and make the conclusive decision regarding removal or restriction. The TOS further mention cooperation with Trusted Flaggers and describe the procedures for “Notice and Action” and counter-notification mechanisms.
4. The audit also verified that the TOS include information about the internal complaint-handling system available to users in the EEA. Article 13.1. sets out a procedure through which users may contest moderation actions, such as content removal or account suspension, free of charge. Complaints can be submitted within six months of the contested decision, and the provider commits to handling these complaints “not solely on the basis of automated means.” The section also informs users of their right to escalate disputes through out-of-court settlement bodies, further evidencing compliance with Articles 14 and 20 of the DSA.
5. A linguistic assessment was performed on the English and Czech versions of the TOS to evaluate clarity and intelligibility. The TOS are organized into numbered chapters and subsections, each with descriptive headings and logical sequencing. The text, while formal and legally precise, remains readable for an average adult user. The inclusion of a simplified summary version enhances accessibility by explaining key provisions in more direct language.
6. In terms of accessibility and format, the TOS are available both as an HTML webpage and in PDF format, ensuring machine readability. A language selector enables users to view the TOS in all 24 official EU languages, in line with the platform’s operations across the Union. The same footer-based navigation is consistent across all interfaces, including the mobile version of the site, which demonstrates proper user access design.
7. The audit reviewed the update and version management practices. The version available during the audit period clearly indicates its effective date and reference to the DSA update cycle. A comparison between the summary and full versions revealed no discrepancies, and the moderation and redress procedures are described consistently in both. The document

therefore demonstrates an adequate process for maintaining legal and operational alignment with regulatory requirements.	
Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.	
Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A

Obligation: Article 14.2	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider has established procedures to define and track what constitutes a "significant change" to the TOS (TOS); ▪ The provider publishes the updated TOS in a prominent, publicly accessible location, clearly stating the effective date. ▪ The provider uses available and reasonable mechanisms to inform recipients of the service, considering its technical and user model limitations; ▪ Any key changes are made transparent through summaries or changelogs, when feasible. 	Materiality threshold: N/A
Audit procedures, results and information relied upon:		
<ol style="list-style-type: none"> 1. The audit confirmed that the provider has a formal internal process for monitoring and implementing TOS changes. The Legal and Compliance teams are jointly responsible for defining and tracking "significant changes," typically meaning modifications that materially affect user rights or moderation processes. 2. Inspection of https://info.xnxx.com/legal/TOS verified that the TOS are publicly available, clearly dated ("Last amended / Effective date: 17 February 2024"), and accessible via the footer of every XNXX page and through the "Legal Stuff" section of the information portal. The document is published in 24 EU languages and in both HTML and machine-readable PDF formats. 3. Given the platform's open-access model without individual notifications (e.g., email alerts or in-platform pop-ups) are not technically feasible. However, this limitation is mitigated by permanent visibility and accessibility of the TOS and version information. 4. Review of the section "Summary of Recent Changes" (<i>Article 16. General</i>) confirmed that the provider maintains a concise changelog summarizing recent updates and providing both effective and amendment dates, thereby ensuring transparency of modifications. 5. Found that the provider reasonably compensates for this by ensuring permanent, transparent, and machine-readable access to the latest TOS. 		
Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.		

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 14.4	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider applied restrictions under Article 14(1) diligently, objectively, and proportionately; ▪ The moderation and enforcement process incorporated safeguards for fundamental rights and legitimate interests of the affected parties; ▪ Decisions were based on verifiable facts, consistently applied, and subject to internal review; ▪ The provider ensured that its moderation agents were trained, supervised, and evaluated for compliance with the principles of fair enforcement. 	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. The audit team conducted interviews with Content Moderation and Notice & Complaint, teams to evaluate the governance structure supporting moderation decisions. The provider demonstrated a mixed human and automated workflow: automated detection tools flag potentially non-compliant material, while human moderators make the final decision on removal or restriction. Ticketing systems maintain an audit trail linking actions to case identifiers and responsible reviewers, supporting accountability.
2. The provider operates with written process description materials that set out the content moderation and notice-and-action workflow end-to-end. Moderation processes were found to be human led with automation limited to detection and prioritization. Enforcement actions (takedown, ghosting, strikes, and account suspension) follow a documented sequence, ensuring decisions are proportionate and reviewable. Ticketing systems maintain traceable logs linking every moderation decision to an assigned reviewer. Appeals and user notifications include reasoned statements, in line with Articles 17-20 DSA.
3. In parallel, the provider has drafted a Content Moderation Guideline intended to formalize roles, decision criteria, escalation logic, and automation boundaries across XNXX (governance model, compliance oversight, toolset, record-keeping, and training). While this document is still being developed, its structure demonstrates the planned consolidation of procedures into a single internal standard to improve consistency and audit readiness.
4. No evidence was found of arbitrary or discriminatory enforcement, nor of procedural deficiencies affecting the diligence or fairness of decisions.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider's moderation and enforcement framework is effective, transparent, and rights-respecting, with only minor opportunities for improvement relating to formal documentation.

Recommendations on specific measures: <ul style="list-style-type: none"> ▪ Finalize and implement the <i>Content Moderation Guideline</i> to consolidate all moderation procedures into a single approved internal standard. 	Recommended timeframe to implement specific measures: Within 6 months from the audit conclusion.
--	--

<p>Obligation: Article 14.5</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider made publicly available a concise summary of the TOS; ▪ The summary was written in clear, unambiguous language that is understandable by a reasonably well-informed user; ▪ The summary included information on remedies and redress mechanisms available to users; ▪ The summary was available in a machine-readable format (e.g. HTML, structured PDF) and easily accessible via the provider’s interface. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. The audit team accessed the publicly available TOS through the “Legal Stuff” section on the XNXX information portal at https://info.xnxx.com/legal/TOS. Both the full and summary versions were reviewed. 2. The summary version presents a concise overview of every chapter contained in the full TOS. Each section includes explanatory text written in plain English and direct hyperlinks to relevant features such as contact forms, parental-control tools, reporting mechanisms, providing clear navigation to supporting policies. 3. The summary also contains a dedicated paragraph outlining the internal complaint-handling system available to users within the EEA and the external dispute-resolution options, including arbitration and out-of-court mechanisms. These points correspond directly to the full TOS. 4. The summary employs plain, intelligible, unambiguous language. Legal terminology is simplified or accompanied by short explanations; section headers are descriptive, and sentences are short and structured for readability. 5. Accessibility testing confirmed that the summary is available in both HTML and PDF versions. Both are machine-readable and easily accessible via a stable footer link on every page of the website. <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>	

Obligation: Article 14.6	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider published TOS in the official language of each EU Member State where the service was offered; 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. A walkthrough of the provider’s information portal at https://info.xnxx.com/legal/TOS confirmed that the TOS are available in 24 official EU languages. 2. The webpage provides a language-selection drop-down menu displayed at the top of the TOS interface. Each language option is labelled both with the official language name and the corresponding country flag. Selecting a language automatically loads the relevant translation without redirection or loss of functionality. The multilingual format applies consistently to both the summary and the full version of the TOS. Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.		
Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A	

Obligation: Article 15	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider has published a transparency report at least once per year in a machine-readable and easily accessible format; ▪ The report includes the number and type of government orders received pursuant to Articles 9 and 10 DSA, categorized by illegal content type and issuing Member State, with relevant response times; ▪ The report includes the number and categorization of notices submitted under Article 16, including whether actions taken were based on law or TOS, and whether notices were submitted by trusted flaggers; ▪ The provider has provided a meaningful and comprehensible overview of own-initiative moderation efforts, including the use of automated tools, measures taken, and categorization of actions; ▪ The report includes statistics and outcomes from the internal complaint-handling system in accordance with Article 20 DSA; ▪ The provider has disclosed any use of automated content moderation tools, including their purpose, accuracy indicators, error rates (if available), and applicable safeguards. 	Materiality threshold: N/A
----------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Reviewed transparency reports published by the provider for:
 - July – December 2024 (first reporting period); and
 - January - June 2025 (second reporting period).
2. Confirmed both reports are publicly available in PDF format, accessible via official channels. Confirmed publication frequency exceeds DSA requirements: The provider issues biannual reports, fulfilling and surpassing the Article 15(1) obligation of an annual report
3. Verified that the provider issues transparency reports on a semi-annual basis, exceeding the minimum annual requirement set out in Article 15(1) DSA. Confirmed that reports are downloadable from corporate channels and accessible to the public.
4. The audit verified that no removal orders under Article 9 DSA were received during either reporting period. The provider disclosed one information orders under Article 10 in the first report and 2 in second report and reported an average response time of 96 days.
5. Both reports provided data on notices submitted via user reporting mechanisms, including content categories such as CSAM, non-consensual content, hate speech, and copyright violations. Actions taken (e.g., removal, rejection) were also reported along with resolution times. Importantly, the report confirmed that no notices were submitted by trusted flaggers in first period. In second period there were 2 notices submitted by trusted flaggers.
6. The reports provide the provider's explanation of proactive content moderation measures. It includes descriptions of (i) the use of automated tools for pre-flagging, (ii) the escalation process to human moderators, and (iii) moderation measures such as content removal, downranking, de-indexing, and account restrictions.
7. The reports categorize these measures by content type and provide a basic matrix on content visibility impacts.
8. Both reports contain relevant data on internal complaint-handling systems. They outline the number of complaints received, reasons for submission, decisions taken, reversal rates, and median resolution times. This is in line with Article 15 and Article 20 requirements.
9. Both reports describe the general use of automated tools in content moderation, particularly for triage and detection. They include further detail on the purposes of these tools, notes the involvement of human reviewers for sensitive content (e.g. CSAM, revenge porn), and briefly mentions moderator escalation processes. Both reports provide error rates, accuracy indicators, and the methodology for evaluating the performance of these tools.
10. Assessed the accessibility and clarity of the report. Verified that the report is well-structured, written in legally and technically accessible language, includes sections for lay users, and is made available in a machine-readable format.

Conclusion:

Positive with comment – The provider has established a biannual reporting cycle, which demonstrates proactive engagement with regulatory obligations. The reports provide detailed disclosures in line with Article 15 requirements.

However, despite this progress, several deficiencies remain:

- While the reports are made publicly available in downloadable PDF format, they are not published in structured machine-readable formats (such as XML or JSON);
- The reports detail content moderation actions, but do not clarify whether these actions were grounded in national/EU law or the provider's TOS.
- The reports refer to the existence of human moderators but do not provide sufficient detail on moderator training programs, oversight mechanisms, or quality assurance processes.

This limits the ability of stakeholders to assess the robustness and fairness of the provider's content governance systems.

Recommendations on specific measures:

- Publish transparency reports in structured machine-readable formats: Reports should be made available not only in PDF, but also in machine-readable formats such as XML or JSON, consistent with anticipated Commission Implementing Regulation (EU) 2024/2835¹, which mandates the use of standardised templates and formats. This will facilitate data interoperability, enable third-party analysis, and increase transparency for regulators and the public.
- Distinguish legal vs. policy-based enforcement actions: All content moderation actions, including those following user notices, should specify whether they were taken based on national or EU law, or the provider's TOSs.
- Provide more detailed information on moderator training and oversight: Include a qualitative and, where possible, quantitative overview of (i) training modules, (ii) decision-making criteria for human moderators, (iii) escalation channels (iv) mechanisms for quality assurance and consistency.

Recommended timeframe to implement specific measures:

To address the identified gaps in transparency reporting, it is recommended that the provider implements the proposed corrective measures within the next 3 (three) months. This will ensure alignment with the upcoming standardized reporting format, the harmonized annual cycle starting 1 January 2026, and the obligation to publish reports in machine-readable form no later than two months after the reporting period ends.

¹ Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council

Section 2 – Additional provisions applicable to providers of hosting services, including online platforms

<p>Obligation: Article 16.1</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider has a clearly defined process for assigning responsibility for the handling of notices submitted; ▪ There is an accessible, user-friendly mechanism for the electronic submission of notices; ▪ The reporting mechanism is visible and functional across all user interfaces (e.g. desktop, mobile web, app). 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Based on the process description obtained from notice and action team, and interface verification, it was confirmed that user can report content by: <ul style="list-style-type: none"> • the “Abuse Reporting Form” for non-copyright issues such as CSAM, non-consensual material, terrorism, or harassment; • a dedicated “Copyright Infringement Form”, • an in-content “Report” (flag) button is available directly below each content item (video, images, comments, galleries). 2. Each form is accessible online without login credentials and allows submission exclusively by electronic means. All include fields corresponding exactly to the four elements required by Article 16(2) DSA. Confirmation of receipt is generated automatically on-screen and by email. 3. The TOS (sections 3, 4, 8, 12, 13) explicitly define the notice-and-action process, the responsibilities of the providers as host, and the rights of users. The document confirms that moderation decisions are taken exclusively by trained human moderators and that no algorithmic or fully automated tools determine removal outcomes. 4. During testing on multiple browsers (desktop - Firefox, Safari; mobile - iOS Safari, Android Chrome), the “Report” flag appeared consistently beneath each video beside engagement metrics. Selecting the flag opened a form with button categories, a text field for description, and contact information entry. Submission produced an on-screen acknowledgment and, subsequently, an email confirmation. Tests confirmed that reporting was possible without user registration, CAPTCHA barriers, or software dependencies, thus meeting the accessibility expectation. 5. Moderation responsibilities are distributed among dedicated human teams (Content Moderation and Notice&Complaint teams) as confirmed by the internal organizational chart and interviews with relevant teams. <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>	

<p>Obligation: Article 16.2</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The reporting form enables submission of (a) a reasoned explanation, (b) an exact electronic location of the content, (c) reporter identification details, (d) a good faith declaration. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Platform’s interface verification confirmed that each of the forms explicitly contains four mandatory fields reflecting Article 16(2): <ul style="list-style-type: none"> • a sufficiently substantiated explanation of why the content is considered illegal or non-compliant, • the exact electronic location of the content (e.g. specific URLs), • the name and email address of the notifier, • a statement confirming the notifier’s good faith belief that the information is accurate and complete. 2. Reviewed the TOS (<i>Article 8. Content Moderation</i>) lists , verbatim, the four elements of information a reporter must include when submitting a notice via either the abuse form or the reporting button. The TOS explain that incomplete submissions “may not be valid or may be delayed in processing,” confirming that field validation is enforced. The provision also establishes that confirmation of receipt is sent “without undue delay” to the reporter’s email. 3. The auditor navigated the XNXX platform on multiple browsers (desktop - Safari and Firefox; mobile - iOS Safari and Android Chrome) and accessed both the “<i>Report</i>” button and the <i>Abuse Reporting Form</i>. For each submission channel: <ul style="list-style-type: none"> ▪ The form provides a large free-text field titled “Describe the reason” where users can explain why the content is illegal. Text entry was unrestricted, allowing full contextual descriptions. ▪ A mandatory URL field is pre-filled when accessed from an in-content “Report” button and remains editable; in the standalone form, the field must be manually filled. Attempts to submit without a valid URL produce an error prompt. ▪ Both name and email address are compulsory. The form rejects empty or malformed entries and automatically associates the email address with confirmation and subsequent correspondence.; ▪ At the bottom of the form, a checkbox labelled “I confirm that the information is accurate and provided in good faith” must be ticked before the “Submit” button activates. 4. Upon submission, the user is redirected to a confirmation screen displaying “Received. If your claims are correct, the videos will be taken down soon,” and simultaneously receives an acknowledgment email. No accessibility barriers or device-specific issues were observed; both forms functioned without login and were compatible with standard browsers. <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>	

<p>Obligation: Article 16.4</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider, without undue delay, send a confirmation of receipt to the individual or entity that submitted a notice, provided that electronic contact details were supplied. 	<p>Materiality threshold: N/A</p>
--	---	--

Audit procedures, results and information relied upon:

1. The internal process description describes in detail the confirmation mechanism applicable to each notice channel:
 - For both the Abuse Reporting Form and the Copyright Infringement Form, two forms of acknowledgment are generated simultaneously:
 - On-screen confirmation immediately after submission, displaying the message: *“Received. If your claims are correct, the videos and galleries will be taken down soon.”*
 - Automatic email confirmation sent from content@xnxx.com to the email address entered in the form. The email explicitly acknowledges receipt of the report and includes a reference (URL) to the reported content.
 - For notices submitted through the in-content “Report” button, confirmation is likewise issued automatically via email, originating from report@xnxx.com, and referencing the specific video.
2. The TOS (*Article 8. Content Moderation*) reiterates that: *“If you entered your email address into the reporting form, NKL Associates will, without undue delay, send you a confirmation of receipt to your email”*. This statement confirms both the timing (“without undue delay”) and conditionality (“if email address is provided”) of the confirmation process, precisely mirroring the requirement of Article 16(4) DSA. The TOS further clarify that the notice remains pending for review only after confirmation has been sent, ensuring that acknowledgments form an integral part of the workflow.
3. The auditor performed functional testing of the reporting interfaces on desktop and mobile browsers. When submitting a test report through the “Report” button beneath a sample video, an immediate on-screen confirmation appeared, followed by an automatic acknowledgment email within seconds, confirming receipt and reproducing the reported video’s URL. Similarly, when using the “Abuse Reporting Form,” the system displayed the same acknowledgment page and delivered an email. Both messages included the reported content link, confirming that the platform ties acknowledgments to the specific submission and notifies the user electronically without manual moderation. No significant delay was observed between submission and receipt confirmation, and no failed transmissions were detected in the testing samples.
4. According to the moderation workflow detailed during interview with Content Moderation and Notice & Complaint teams, the platform’s backend automatically generates a ticket once a report is submitted. Each acknowledgment includes a timestamp and is stored in the platform’s ticketing logs, providing a verifiable audit trail. The system design thus guarantees that confirmation of receipt is issued automatically and cannot be overridden by human moderators.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 16.5	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The notifier is informed of the provider’s decision without undue delay; ▪ The notification includes accessible and intelligible information on redress options; ▪ If the provider has decided on a restriction, the provider documents the implementation of that restriction in a traceable manner. 	Materiality threshold: A performance materiality threshold of 5 % was applied for this obligation.
------------------------------------	--	--

Audit procedures, results and information relied upon:

1. Based on internal process description and interview provided with Content Moderation and Notice & Complaint team, the provider operates several parallel notice mechanisms that differ in complexity and feedback functionality.
2. For videos and for notices submitted through the Abuse Reporting Form or the Copyright Infringement Form, the process is comprehensive and closely aligned with the DSA’s intent. Once a notice is reviewed, the notifier receives a reasoned decision explaining the outcome (whether the content has been removed, rejected, or otherwise restricted) and, crucially, is informed about how to contest that decision. Decision notifications contain clear, intelligible instructions and direct links to an appeal form or to the internal complaint-handling mechanism, in line with Articles 16(5) and 20 DSA.

This workflow is supported by a ticketing system that automatically records every moderation decision, including timestamps, the specific URL concerned, the moderator identifier, and the action taken. In cases involving serious violations (e.g. CSAM or non-consensual sexual material), the system also notes whether the case has been referred to law-enforcement authorities. These records provide a complete and verifiable audit trail of each restriction imposed, satisfying the traceability element of Article 16(5).
3. Also, the audit identified two categories where the post-decision communication process remains incomplete:
 - Users may report comments via a “Report” button next to each comment. After submission, reporters receive an automatic acknowledgment email confirming that their report was received. However, the system does not send any follow-up message informing them of the outcome or of any redress options. The moderation decision is internal to the platform and not communicated back to the notifier.
 - A similar situation applies to the Privacy Takedown Form and the Takedown Amateur Form used to report illegal or privacy-infringing pictures. Reporters are sent an immediate confirmation of receipt, but no decision notification or information on possible appeals is issued later.
4. In both cases, the moderation process itself is logged internally and the underlying decisions are recorded in the moderation dashboard, ensuring full traceability. The gap lies solely in user communication: notifiers are not informed of the outcome or of available redress mechanisms. During the interview, the IT team confirmed that they are aware of this shortfall and that work on resolving the issue is in progress. They plan to finalize this work by the end of this year.

5. These findings were corroborated through system demonstrations and testing.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The systems for communicating moderation decisions, providing redress information, and documenting restriction actions are robust and fully functional for the core reporting mechanisms. The absence of decision feedback for reports on comments and pictures constitutes a limited shortfall; however, given the existence of traceable internal documentation and the ongoing remediation efforts planned for completion by the end of the year, this does not amount to material non-compliance. The provider is encouraged to implement the planned improvements.

Recommendations on specific measures:

- Extend the decision-notification functionality to the comment and picture reporting mechanisms so that users who submit these notices receive an email detailing the outcome and providing information about available redress or appeals.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 2 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 16.6	<p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ All received notices are processed; ▪ Decisions on notices are made in a timely, diligent, non-arbitrary, and objective manner; ▪ Where automated means are used in decision-making, such use is explicitly disclosed to the notifier; ▪ The decision-making process is documented in a comprehensible and transparent manner. 	<p>A performance materiality threshold of 5 % was applied for this obligation.</p>
Audit procedures, results and information relied upon:		
<p>1. The process review defines a unified ticket-based moderation system in which every submitted notice automatically generates a case (“ticket”) visible in the moderators’ dashboard. The dashboard lists all pending cases chronologically, with priority sorting for trusted flagger submissions. Each ticket includes:</p> <ul style="list-style-type: none"> • the reported content’s preview and URL, • the text of the notice, • the notifier’s contact details, • the assigned moderator, and • a timestamp of receipt. <p>No notice can be deleted or archived without resolution status (“safe,” “harmful,” or “deleted”). This structure ensures that all received notices are processed; unprocessed cases remain active in the queue until closed.</p> <p>2. The moderation workflow describes how moderators evaluate each report:</p> <ul style="list-style-type: none"> • Review the video preview and accompanying report text. • Classify the notice under one of several categories (e.g., <i>copyright</i>, <i>consent</i>, <i>age verification</i>, <i>harassment</i>). 		

<ul style="list-style-type: none"> • Take one of two actions: mark content as safe (report rejected), or mark content as harmful (report upheld → content removed). • Record the reason using a drop-down list of predefined options. <p>3. When more information is needed, moderators may contact the reporter or the uploader through an integrated messaging tool; all correspondence is logged in the same ticket. If no reply is received within the specified period (generally 48 hours for user clarification), the system escalates the case or triggers automatic closure according to predefined severity rules.</p> <p>These controls demonstrate that decisions are not arbitrary, as every action must be justified by a selected reason category and timestamped by the responsible moderator.</p> <p>4. The process description and internal dashboards confirm that notices are reviewed chronologically and that trusted flagger submissions appear at the top of the queue, ensuring priority handling. Ordinary notices are processed within standard response times (48-72 hours), and severe cases (CSAM, rape, terrorism) are reviewed immediately upon receipt.</p> <p>5. The TOS (<i>Article 8. Content Moderation</i>) further stipulate that “<i>NKL Associates processes all notice in a timely, diligent, non-arbitrary, and objective manner</i>” and that the reported content remains hidden from public view pending a decision. These statements are supported by the documentation of transparency reports reviewed during the prior audit cycle, which record total notices received, processed, and average time-to-decision metrics.</p> <p>6. Moderators rely on structured classification and predefined “reason codes” that reduce subjective variation. Additionally, peer review and escalation protocols apply when a moderator is uncertain. For example, cases involving potential criminal offences are escalated to senior reviewers. All escalations are traceable within the internal audit trail, which records the moderator’s ID, time, and decision type.</p> <p>7. Both the TOS (<i>Article 8. Content Moderation</i>) and internal documentation explicitly state that XNXX does not employ algorithmic or fully automated decision-making for determining whether to remove or retain reported content. The human moderator always makes the final decision. Because automation does not influence substantive outcomes, no disclosure to notifiers is required, but the TOS nonetheless transparently notes the use of automated detection tools to assist moderators.</p> <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 17.1, 17.2</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Affected users receive a clear and specific statement of reasons for restrictions imposed, including (i) removal or demotion of content; (ii) suspension or termination of service or account; (iii) restrictions on monetization; ▪ The information is provided where contact details are known; 	<p>Materiality threshold: A performance materiality threshold of 5 % was applied for this obligation.</p>
--	---	--

	<ul style="list-style-type: none"> ▪ The statement is issued no later than the moment the restriction is imposed; ▪ Excludes deceptive high-volume commercial content. 	
--	--	--

Audit procedures, results and information relied upon:

1. Reviewed the TOS (specifically *Articles 8. Content Moderation* and *Article 13. Internal Complaint-Handling System, Dispute Resolution, Agreement to Arbitrate, Class Action Waiver, Venue and Forum*), which outline moderation measures and user rights. The TOS confirms that users whose content is removed, or access is restricted are entitled to be informed of the rationale and may appeal through the internal complaint-handling system where applicable.
2. Interviewed platform Notice & Complaint and IT teams responsible to describe the processes. The provider has implemented structured mechanisms for issuing justifications when restrictions are applied to content or user accounts. These mechanisms include:
 - template-based emails generated via the moderation backend,
 - ticketing system updates visible for users via link in email,
 - use of predefined content classification tags linked to violation categories,
 - escalation procedures for sensitive cases (e.g., CSAM, non-consensual content).
3. After each notice is resolved, the system automatically sends an email from to the reporter and to the uploader (if applicable). The message contains:
 - the final decision (“video deleted,” “report rejected,” “account deleted,” etc.),
 - the reason category selected by the moderator (e.g., “non-consensual content,” “copyright violation,” “terrorist material”),
 - a direct link to the affected content,
 - information about the internal appeal mechanism and complaint link.
4. Verified that statements of reasons are automatically generated and communicated at the time a moderation decision is made. Upon completion of the review, the system sends an automatic email to both:
 - the reporting party (informing them of the decision outcome), and
 - the affected uploader or account holder (informing them of the restriction and rationale).

The email is issued at the moment the restriction is imposed.
5. Where contact details are known, notifications are issued automatically via the user’s registered email address. For reports submitted anonymously or without valid contact information (e.g., external notifiers), no direct communication is possible; however, system logs confirm the generation of internal statements stored for compliance and transparency reporting.
6. For reports concerning images and comments, users receive email acknowledgments and moderation outcomes; however, these communications lack the same structured statement format and tracking visibility found in the video moderation process.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the audit noted procedural inconsistency in the way statements of reasons are generated for images and comments. While affected users receive acknowledgment and decision notifications, these communications are not issued through the same structured statement-of-reasons template or tracked in the unified

moderation ticketing system used for video content. The difference does not constitute material non-compliance but represents a gap in uniformity and user experience across content types.

Recommendations on specific measures:

- Standardize the statement-of-reasons template and transmission process across all moderation categories (videos, images, comments).

Recommended timeframe to implement specific measures:
The identified measures should be implemented within 6 months.

<p>Obligation: Article 17.3, 17.4</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Each statement of reason contains: <ul style="list-style-type: none"> – Type of restriction and its scope (e.g., removal, demotion, account suspension); – Facts and circumstances that led to the decision; – Whether a user report (Article 16) or proactive detection was involved; – Whether automation was used, and if so, its role; – Legal or contractual basis for the decision; – Redress mechanisms (complaint-handling, dispute resolution, legal remedies); ▪ The language used is clear, comprehensible, and actionable. 	<p>Materiality threshold: A performance materiality threshold of 5 % was applied for this obligation.</p>
--	---	--

Audit procedures, results and information relied upon:

1. The statements of reasons included the type and scope of the restriction imposed, such as removal of a video, demotion or limitation of visibility, temporary or permanent suspension of an account, or restrictions on monetization. The system uses structured categories enabling moderators to select the precise action taken
2. The statements also included the factual circumstances leading to the decision. Moderators worked within a structured interface that required them to identify the specific type of violation detected, such as non-consensual behavior, age-related concerns, privacy violations, copyright infringements, or other ToS breaches. These selected categories were reflected in the reasoning communicated to users. Where additional communication unfolded during a moderation process (e.g., clarification requested from reporters or uploaders), that information contributed to the final reasoning.
3. The system distinguished whether a case originated from a user report, a trusted flagger, or moderator-driven review. This information was included in the statement received by affected users. The Notice & Action documentation (screenshots) shows a flag marking the source of each report, ensuring accuracy in reasoning.
4. Each statement provided information on available redress mechanisms, including the internal complaint-handling system and the option for out-of-court dispute settlement. The notification emails included direct links enabling users to appeal decisions electronically, submit explanations, or upload supporting evidence. These options made the redress pathways clear and actionable.

<p>5. The language used in the statements of reasons was found to be clear, accessible, and user-oriented. Emails included direct references to the content concerned, used straightforward explanation categories, and avoided technical jargon. Users were provided with concrete next steps, including how to appeal or request a review.</p> <p>6. The platform is connected to the DSA Transparency Database, and records of all restrictions are automatically transmitted to the database. This means that each statement of reasons issued to users corresponded with a database entry containing:</p> <ul style="list-style-type: none"> • the type of action, • the category of violation, • the basis for the decision, • whether a user report triggered the measure, • the role of automation (where applicable), and • a concise summary of the reasoning. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 18.1</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider had established internal procedures for identifying and escalating information that may indicate criminal threats to life or safety; ▪ The provider ensured that such information, when identified, was promptly reported to the appropriate law enforcement or judicial authorities of the relevant EU Member States; ▪ The reporting process included transmission of all relevant and available information necessary to support investigation or intervention. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. <i>Article 4. Terrorism and Physical Harm Violence</i> of the revised TOS is explicitly prohibits any content promoting terrorism or physical harm and affirms that such content is removed and reported to law enforcement in accordance with applicable laws. 2. Interviewed responsible personnel and confirmed the existence of an established internal content moderation process including the obligation of reporting illegal content to authorities. 3. Assessed the design of relevant processes to determine whether they align with the requirements of Article 18(1). 4. Examined documentation of the content moderation process and verified that the provider uses a designated internal classification to flag content that is undoubtedly illegal. 5. Verified that flagged content in this category is manually uploaded to a shared law enforcement server (LEA). 		

6. For defined specific content automated process is in place to inform LEA about the content.
7. Majority of the process is intentionally non-automated, requiring a content moderator to review the flagged material and initiate the upload to the law enforcement server, reducing the risk of wrongful reporting.
8. Inspected that the following data is provided to law enforcement: the illegal content file, IP address of the uploader, and all related metadata.
9. While the reporting process exists, we did not identify a formalized internal policy or framework explicitly detailing the procedure for informing the *EU Member States concerned of its suspicion*.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The platform has a human-led workflow in place for assessing and reporting content that may pose a threat to life or safety. Moderators manually escalate content classified to LEA server. However, the absence of a formalized internal document clearly describing the process of informing the *EU Member States concerned of its suspicion* represents a documentation gap that should be addressed.

Recommendations on specific measures:

Develop and formalize a comprehensive internal guidance document (e.g. Notice Lifecycle and Moderation Framework) detailing (i) notification of suspicions of criminal offenses, including escalation pathways to *EU Member States concerned* when identifiable.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 18.2	<p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider had a procedure in place for notifying the authorities of the Member State of its establishment or informing Europol or both, if the relevant Member State could not be identified with reasonable certainty. 	N/A

Audit procedures, results and information relied upon:

1. Reviewed the TOS, particularly Chapter 4 “Terrorism and Physical Harm Violence”, which explicitly prohibits any content promoting terrorism or physical harm and affirms that such content is removed and reported to law enforcement in accordance with applicable laws.
2. Assessed the design of relevant processes to determine whether they align with the requirements of Article 18(1).
3. Examined documentation of the content moderation process and verified that the provider uses a designated internal classification to flag content that is undoubtedly illegal.
4. Verified that flagged content in this category is manually uploaded to a shared law enforcement server (LEA).
5. For defined specific content automated process is in place to inform LEA about the content.
6. Majority of the process is intentionally non-automated, requiring a content moderator to review the flagged material and initiate the upload to the law enforcement server, reducing the risk of wrongful reporting.

7. Inspected that the following data is provided to law enforcement: the illegal content file, IP address of the uploader, and all related metadata.
8. While the reporting process exists, we did not identify a formalized internal policy or framework explicitly detailing the procedure for informing the *Member State of establishment* or *Europol* when the relevant Member State cannot be determined.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The escalation of undoubtedly illegal content to an international LEA server functionally enables access by relevant law enforcement bodies, including those of the Member State of establishment. However, no internal documentation was identified that formalizes procedures for *cases where the Member State concerned cannot be identified with reasonable certainty*. This presents a minor documentation deficiency that should be addressed.

Recommendations on specific measures:

Develop and formalize a comprehensive internal guidance document (e.g. Notice Lifecycle and Moderation Framework) detailing (i) notification of suspicions of criminal offenses, including procedures when the *Member State concerned cannot be identified with reasonable certainty*, and the requirement to inform the *Member State of establishment* and/or *Europol*.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Section 3 – Additional provisions applicable to providers of online platforms

<p>Obligation: Article 20.1.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider has implemented an internal complaint-handling system; ▪ Access is granted to both users and notifiers to lodge complaints against decisions relating to content; ▪ Allows for the submission of complaints related to decisions taken by the platform regarding illegal content or violations of its TOS, including content removal, restriction of visibility or access, account suspension or termination, restrictions on the ability to monetize content; ▪ Operates electronically and without cost to the complainant. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed Article 13. <i>Internal Complaint-Handling System, Dispute Resolution, Agreement to Arbitrate, Class Action Waiver, Venue and Forum</i> of the TOS, which outlines the internal complaint-handling mechanism. The ToS establish an internal complaint-handling mechanism accessible to all service recipients affected by moderation decisions. Users can lodge complaints electronically and free of charge within six months of being notified of a decision (such as content removal, account suspension, visibility restriction, or monetization disablement). Complaints can be submitted via (i) the user account interface, or (ii) a designated link emailed automatically to the user following a moderation decision. All complaints are reviewed by qualified human moderators, under supervision and not solely based on automated means. The commits to handle complaints timely, diligently, non-discriminatory, and non-arbitrarily. Where appropriate, decisions are reversed, and the user receives a reasoned response, including information on out-of-court settlement and redress options. Access is also extended to recipients located in the EEA, with the option to refer unresolved matters to certified dispute settlement bodies in accordance with Article 21 DSA. 2. The process description review verified that the ticketing system integrates a complaint-handling interface allowing affected users to appeal moderation outcomes. After a moderation decision (content removal, reinstatement, or account action), users receive a reasoned decision via email. The system enables users to “Appeal this decision” directly via the online interface, opening a form that allows submission of an explanatory statement and supporting evidence. The appeal is handled electronically within the same ticket-tracking system, and users can monitor case status (“pending,” “in review,” “closed,” etc.). 3. Complaint mechanisms are free of charge and accessible electronically through the XNXX platform. No login requirement applies to initial notice submissions; however, appeals and complaints regarding moderation outcomes require authentication (ensuring linkage to the affected account or notice). 4. Confirmed through navigation of the web interface that users receive the “reasoned decision” email upon moderation outcomes, consistent with DSA Article 20(5) expectations. Confirmed that both users and notifiers (reporters) can file appeals via the ticketing system. 5. Users reporting via comment or picture-specific forms receive acknowledgment but do not have integrated appeal functionality in the ticketing system; however, they may seek redress through the “point of contact for users” available via https://info.xnxx.com/contact. 		

<p>Conclusion:</p> <p>Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, users reporting comments or pictures through mechanisms cannot file appeals via the automated ticketing system; instead, they may seek redress via other available channels, such as the point of contact for users. This limitation does not materially affect compliance, as an alternative complaint path remains operational and publicly available.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> Extend the integrated electronic appeal functionality (currently available for videos and abuse reports) to cover all content types, including images and comments. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 2 months.</p>

<p>Obligation:</p> <p>Article 20.2.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> The provider ensures that users and notifiers have access to the internal complaint-handling system for at least six months following the communication of a decision covered under Article 20.1.; The six-month accessibility period starts from the day the user is informed of the provider’s decision regarding content removal, service restriction, account suspension/termination, or monetization restriction. 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> The reviewed TOS (<i>Article 13. Internal Complaint-Handling System, Dispute Resolution, Agreement to Arbitrate, Class Action Waiver, Venue and Forum</i>) explicitly establishes that “recipients shall have the right to lodge such complaints for 6 months from the date they are informed of the relevant decision.” The TOS specify that this applies to all moderation-related decisions and further confirm that complaints can be submitted electronically and free of charge via the user account interface or via the designated link emailed to the recipient at the time the decision is communicated. Interviews were conducted with the Content Moderation and IT teams. It was confirmed that although the system does not automatically block access after six months, it remains active for the entire six-month period starting from the date the decision email is sent. The communication is verifiably electronic, through an automated email confirmation that contains the decision link and complaint-submission interface. Based on this mechanism, users are able to initiate a complaint or appeal within six months from receiving the decision. 	
<p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects</p>	
<p>Recommendations on specific measures:</p> <p>N/A</p>	<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>

<p>Obligation: Article 20.3.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The internal complaint-handling system is easy to access and user-friendly across interfaces; ▪ The system enables and facilitates the submission of sufficiently precise and adequately substantiated complaints. 	<p>Materiality threshold: N/A</p>
---	--	--

Audit procedures, results and information relied upon:

1. The reviewed TOS (*Article 13. Internal Complaint-Handling System, Dispute Resolution, Agreement to Arbitrate, Class Action Waiver, Venue and Forum*) explicitly establishes that “recipients shall have the right to lodge such complaints for 6 months from the date they are informed of the relevant decision.” states that XNXX provides an electronic, free-of-charge internal complaint-handling system accessible via the user account interface, and a dedicated link included in the decision notification email following moderation actions. Complaints can be submitted directly in response to moderation decisions covering content removal, visibility restriction, account suspension, or monetization limitation.
2. Verified that the complaint-handling interface is integrated into the same electronic ticketing system used for content moderation and notice review. The system automatically associates the complaint with the relevant case (ticket ID, URL) and allows users to track their complaint status through the dashboard (“pending,” “in review,” “closed”), fulfilling the “user-friendly” and “sufficiently precise” criteria.
3. The complaint interface functions across all major browsers (Safari, Firefox, Chrome) on both desktop and mobile, without registration fees or third-party software. All interactions are electronic and supported by automated confirmations at submission and resolution stages.
4. For videos the complaint-handling system is fully integrated and compliant with Article 20(3) DSA.
5. For pictures and comments reports are submitted via standalone forms (“Notice mechanism for pictures” and “Notice mechanism for comments”). These forms collect sufficient information (URL, description, user identity, bona fide statement). Reporters receive email acknowledgment but no direct appeal or complaint option within the same ticketing interface. Users may, however, request reconsideration through the “Point of Contact for Users” at <https://info.xnxx.com/contact>. While this alternative ensures functional accessibility, it is less user-friendly and lacks integration with the primary complaint-tracking system used for video reports.
6. All complaint submission channels request structured, case-specific input. This structured design ensures that complaints are sufficiently precise and adequately substantiated for meaningful review by moderators.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, users reporting comments or pictures through mechanisms cannot file appeals via the automated ticketing system; instead, they may seek redress via other available channels, such as the point of contact for users. This limitation does not materially affect compliance, as an alternative complaint path remains operational and publicly available.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Extend the integrated electronic appeal functionality (currently available for videos and abuse reports) to 	<p>Recommended timeframe to implement specific measures: The identified measures should be implemented within 2 months.</p>
---	--

cover all content types, including images and comments.	
---	--

Obligation:	Audit criteria:	Materiality threshold:
Article 20.4.	Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Complaints are handled in a timely, non-discriminatory, diligent, and non-arbitrary manner; ▪ If a complaint contains sufficient grounds, the provider reverses its initial decision without undue delay. 	A performance materiality threshold of 12.5% was applied.

Audit procedures, results and information relied upon:

1. The Notice & Complaint team provided a real-time walkthrough of how complaints are received, assessed, and resolved using the internal ticketing interface. Due to company limitations on direct system access for external auditors, a shadowing method was used to validate procedures. During the demonstration, it was confirmed that all complaints are routed to human moderators, and that no automated decisions are applied at this stage. The system flags incoming complaints and assigns them based on predefined categories (e.g. content type, severity, prior user history).
2. The moderator demonstrated how complaint tickets include:
 - The original moderation decision;
 - The user’s appeal message or clarification;
 - Attached metadata (e.g. timestamps, user IDs, enforcement logs);
 - Action buttons to reverse or uphold decisions.

Reviewers must enter a justification and select a resolution outcome (e.g. content reinstated, account restored, complaint rejected) before closing the case
3. The moderator presented case handling data from the current workday, as well as recent examples from prior weeks. Although direct sampling of complaint logs was not permitted, multiple cases were shown covering both reversals and rejections. In each instance:
 - Timeliness of resolution ranged from under 1 day to approximately 5 days;
 - Decision rationales were clearly documented;
 - Notifications sent to users were shown, confirming reasoned communication and redress options.
4. The moderator explained how complaints flagged as complex or high-risk (e.g. involving legal content, impersonation, or rights disputes) are escalated to senior team members for additional review, based on internal (but undocumented) criteria.
5. Although the procedures appear consistently applied in practice, the audit noted the absence of a formal internal document. Decision standards, escalation thresholds, and expected turnaround times are known to staff but remain informal.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the lack of formal documentation of complaint-handling criteria (e.g. what defines timeliness or diligence) limits auditability and may lead to inconsistent application in the future as teams scale or change.

<p>Recommendations on specific measures: Develop and adopt a written Complaint Handling Policy, which should:</p> <ul style="list-style-type: none"> ▪ Provide expected resolution times and escalation rules by case type; ▪ Include guidance on when and how to reverse enforcement decisions; ▪ Be embedded into training for all complaint reviewers. 	<p>Recommended timeframe to implement specific measures: The identified measures should be implemented within 6 months.</p>
---	--

<p>Obligation: Article 20.5.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Complainants are informed of the provider's reasoned decision without undue delay; ▪ The decision notification includes <ul style="list-style-type: none"> – a clear explanation of the outcome, – reference to the out-of-court dispute settlement mechanism (Article 21 DSA); – other available redress options or escalation channels. 	<p>Materiality threshold: N/A</p>
---	---	--

Audit procedures, results and information relied upon:

1. Reviewed communication templates used by provider for notifying users of the outcome of internal complaints. These templates are filled in from the internal ticketing system and include placeholders for (i) moderator rationale for decision, (ii) complaint reference, (iii) a hyperlink to further redress information and out-of-court dispute settlement, (iv) contact email for follow-up queries.
2. Sampled complaint resolution emails sent to users during the audit period. The samples included both accepted and rejected complaints across various violation types (e.g., content takedowns, account restrictions, monetization issues). In each sampled case, the notification included a reasoned explanation, written in accessible language. The explanation typically addressed:
 - The substance of the complaint;
 - The basis for the provider's final decision;
 - Whether the original decision was upheld or reversed.
3. Verified inclusion of redress information in 100% of the sampled communications. The notifications consistently included a brief statement explaining the user's right to challenge the decision externally and a fallback contact (e.g., content@XNXX.com) for further inquiry.
4. Assessed timeliness of notifications by comparing internal timestamps for complaint closure and user notification dispatch. The notifications were sent within 48 hours of the complaint decision.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 20.6.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ All decisions on complaints submitted via the internal complaint-handling system are made under the supervision of appropriately qualified personnel; ▪ No decision is made solely by automated means; 	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Performed interviews with members of the notice and complaint team, who are responsible for receiving and responding to user reports and notices. It was confirmed that no reports were received from trusted flaggers during the examination period, and that no dedicated process exists to flag or prioritise such notices. The team acknowledged that, while general notices are resolved within 24 hours, no dedicated input channel or technical label exists to distinguish trusted flagger reports from general user notices.
2. Shadowed the complaint-handling and moderation process by observing live sessions with moderators. It was observed that moderators consistently followed internal procedures, exercised individual judgment, and in complex cases, engaged in peer consultation or escalation to senior personnel.
3. Inspected that all designated personnel had completed onboarding modules, including general moderation principles, platform-specific policy guidance, redress and reversal decision-making criteria.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 21.1.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ User and notice submitters were informed of their right to access a certified out-of-court dispute settlement body (once available); ▪ This information was easily accessible, clearly presented, and user-friendly on the platform's interface; ▪ The provider did not impede users' right to seek judicial redress at any stage. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. A review of the TOS confirmed that the document includes a specific reference to users' and notice submitters' right to access a certified out-of-court dispute-settlement body once available under the DSA. The clause is drafted in clear, comprehensible language.
2. Inspection of Section 13 ("Complaints and Dispute Resolution") of the TOS at <https://info.xnxx.com/legal/TOS> confirmed that the document explicitly states users' entitlement to submit complaints through the internal complaint-handling system and to access a certified out-of-court dispute settlement body, once designated in accordance with the DSA framework. The section further clarifies that users retain the right to pursue judicial redress independently of this process.
3. The information is presented in a dedicated, clearly titled subsection, written in plain English, and available through the same "Legal Stuff" menu accessible via the footer of every XNXX webpage. The text is displayed in all 24 official EU languages, ensuring accessibility for users.
4. Testing of the interface confirmed that the relevant information can be reached in two clicks or fewer from the main page. The layout and readability of the dispute-resolution section were found to be user-friendly, and no language or design barriers were identified.
5. Both transparency reports state, that during reporting period no submissions or disputes were received from any certified out-of-court settlement body

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation: Article 22.1,	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none">▪ Trusted flagger notices are given priority over other types of user reports;▪ Trusted flagger notices are processed and decided upon without undue delay (for the purposes of this audit, a benchmark of ≤ 48 hours was applied to assess timeliness);▪ The provider maintains dedicated technical and organizational processes to distinguish and track such notices.	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. The audit confirmed that the provider has implemented a structured framework for managing trusted flaggers reports. The document outlines a formal onboarding and verification process.
2. Inspection of the public webpage <https://info.xnxx.com/trusted-flaggers> verified that a dedicated section for Trusted Flaggers is available under the "Information and Links" domain. The page describes the DSA concept of trusted flaggers, explains the application and verification process, and explicitly states that their notices are given priority and

<p>handled diligently. The page is written in clear and accessible language, ensuring transparency and user comprehension.</p> <ol style="list-style-type: none"> 3. Examination of the “<i>Notice and Action Process Description</i>” document demonstrated that the platform uses a separate workflow for trusted flagger notices. Such notices are automatically tagged as “TF” and routed to a distinct moderation queue, guaranteeing higher prioritisation compared with ordinary user reports. 4. The same process documentation confirms that trusted flagger notices are processed by trained human moderators with the assistance of automated detection tools. Moderators are required to provide a reasoned decision via the internal ticketing system, and the TF dashboard enables each flagger to track submission status in real time. 5. Review of the XNXX 2nd Transparency Report (January – June 2025) confirmed that the provider received two trusted flagger notices during the reporting period. The transparency report also demonstrates that trusted flaggers notices are reviewed exclusively by human moderators and not by automated means. While the provider shows clear prioritisation, the measured response time (median ≈ 74 hours) slightly exceeds the 48-hour internal benchmark adopted for this audit. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. While compliance with the “without undue delay” standard is achieved, the median response time slightly exceeded the benchmark applied for this audit, suggesting an opportunity for improvement in processing speed and monitoring.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> • Define and formalise an internal KPI for trusted flagger notice handling (e.g., ≤ 48 hours) as an internal target 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>

<p>Obligation:</p> <p>Article 23.1., 23.2.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider has defined a process that enables suspension of users who frequently and manifestly provide illegal content; ▪ The provider has defined a process to identify and suspend users who frequently submit manifestly unfounded notices or complaints through Article 16 (notice and action) and Article 20 (internal complaint-handling) mechanisms; ▪ The process includes a warning system before service suspension is applied; ▪ The warning clearly states the reason for suspension and potential consequences; ▪ Suspensions are issued for a reasonable period; 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed the TOS (specifically <i>Article 8. Content Moderation</i> and <i>Article 7. User Submissions</i>), which define the rules governing illegal content, the detection process, and the enforcement actions applied to user accounts. The TOS establish a repeat infringer policy whereby users who upload illegal content receive “strikes,” and after the accumulation of three strikes, the user’s account is deleted and access to the Website is 		

terminated. This demonstrates the existence of a structured process for suspending users who frequently and manifestly provide illegal content.

2. Notice & Complaints and Content Moderation teams were interviewed. It was confirmed, that upon receiving a takedown notice, the provider suspends visibility of the content and informs both the reporter and uploader. The uploader may be contacted during review to provide observations, which forms the practical warning step before more serious enforcement actions such as “strikes” or suspension are applied.
3. Reviewed the “Repeat Infringers Policy”, which specifies that:
 - First and second violations result in “strikes,”
 - Content moderators may delete a strike if the user shows it was an accidental or isolated mistake,
 - After three strikes, the user’s account is permanently terminated. The staged escalation and moderation review constitute a warning-based system.
4. Verified the TOS requirement that users are notified of reasons for moderation decisions, including removal of content, temporary disabling, and account-level actions. EEA users receive a statement of reasons and have the right to complain internally, confirming that each warning includes the reason for the enforcement action and its consequences, as required.
5. Confirmed that suspensions and account deletions are limited to what is proportionate to the violation type. The platform applies immediate and permanent bans only for the most serious categories, such as CSAM, NCII, terrorism and violent extremist content. For all other illegal content types, penalties follow the progressive “strike” model, ensuring that suspensions occur only after repeated and manifest violations, demonstrating reasonableness and proportionality.
6. While the provider has the authority to sanction repeated submission of manifestly unfounded notices or complaints, interviews revealed that the platform applies these measures cautiously and with flexibility. Moderators confirmed that:
 - Abuse of reporting tools does occur, most commonly between competing content uploaders attempting to disrupt competitors’ content visibility;
 - However, the provider is reluctant to block reporters, as doing so may deter legitimate notices involving illegal content;
 - Misuse designations are therefore applied only in clear and repeated cases, and typically not for complaints, because a complaint may still relate to a legitimate disagreement or misunderstanding;
 - The repeat infringer policy remains the most effective and consistently used enforcement tool across both illegal content and misuse-related conduct.
7. Established that although the provider has informal internal criteria for identifying manifestly unfounded notices (e.g., repeated baseless reports, false allegations, or misuse in competitive disputes), these practices are not yet documented in a standalone misuse policy. Moderators rely on shared experience, internal communication, and supervisory guidance, which supports operational consistency but reduces formal auditability.
8. Confirmed that enforcement actions for misuse are preceded by a warning explaining the justification and potential consequences.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the audit note that the provider intentionally applies misuse-related sanctions less strictly to avoid discouraging users from filing legitimate notices, especially regarding illegal content. This risk-aware approach is operationally

reasonable but is currently based on informal practices and team-level guidelines rather than a documented policy framework.

Recommendations on specific measures:

- Formally document the full approach to addressing manifestly unfounded notices and complaints, including definitions of misuse, escalation thresholds, the warning process, the conditions for temporary suspension, documentation guidelines for moderators, safeguards ensuring that legitimate reporters are not deterred.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 12 months.

<p>Obligation: Article 23.3.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider performs a case-by-case assessment before suspending any user under Articles 23.1 or 23.2; ▪ The assessment is conducted promptly, diligently, and objectively; ▪ The provider considers all relevant facts and circumstances, including (i) absolute number of violations or unfounded complaints, (ii) relative proportion compared to total activity, (iii) severity of misuse, including the nature and potential harm, (iv) intent of the user, where it can be identified. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed TOS (specifically <i>Article 8. Content Moderation</i> and <i>Article 7. User Submissions</i>) and internal moderation guidelines, which demonstrate that enforcement actions are not applied automatically. Moderation actions require a manual human review, and enforcement outcomes are applied through a structured, individual case evaluation. This confirms that suspensions are based on case-by-case assessments rather than automated triggers. 2. Interviewed the Notice & Complaints and Content Moderation teams. Moderators confirmed that each enforcement case is reviewed by a human moderator or senior reviewer. They verify whether repeated reporting or repeated uploads represent a pattern, whether actions appear accidental, or competitive, and whether prior warnings were acknowledged. These interviews confirm that assessments are performed promptly and diligently using all available information in the ticketing system. 3. Reviewed the “Repeat Infringers Policy.” The policy indicates that strikes are not applied automatically; moderators may remove strikes where the user demonstrates that conduct was not intentional or was due to misunderstanding. This demonstrates evaluation of intent, severity, and mitigating circumstances prior to suspension. The system therefore considers both the absolute number and proportion of violations compared to typical user behavior. 4. Verified moderation workflow evidence from interviews showing that: <ul style="list-style-type: none"> • enforcement decisions require moderator consensus or escalation to senior moderation leads in complex cases, • competitive misuse is specifically checked for before action is taken (e.g., where uploaders misuse reporting tools against competitors), 		

<ul style="list-style-type: none"> • moderators assess whether the misuse is isolated or systematic. <p>5. Observed that misuse-related enforcement (Article 23.2) is applied cautiously, consistent with interview statements:</p> <ul style="list-style-type: none"> • The provider avoids suspending users unless misuse is clear and repeated, • This is designed to avoid chilling effects on legitimate notices, • Warnings are used as the first step, providing space for explanation. <p>6. The audit confirmed that no automated suspension mechanisms exist. All suspensions are manually imposed, ensuring that each case necessarily undergoes a case-by-case assessment.</p> <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 23.4.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider’s TOS clearly and in detail describe the policy regarding misuse under Articles 23.1 and 23.2; ▪ The Terms include examples of misuse (e.g. repeated illegal content or unfounded complaints); ▪ The Terms describes the factors considered in determining misuse (e.g., volume, intent, severity); ▪ The Terms states the duration and nature of suspensions that may be imposed. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed TOS (<i>Articles 7. User Submissions and 8. Content Moderation</i>), which provide a structured policy addressing repeated illegal content under Article 23.1. The TOS describe the repeat infringer “strike” system, including the escalation pathway and consequences (content removal, warning, and eventual account deletion after three violations). This satisfies the requirement for a documented misuse framework relating to repeated illegal content. 2. Reviewed the TOS for Article 23.2 compliance (misuse of notice and complaint mechanisms). The TOS do not contain: <ul style="list-style-type: none"> • any reference to “frequent” or “repeated” violations as criteria for enforcement beyond the illegal-content strike system; • any policy on misuse of notice and complaint-handling mechanisms (e.g., false reports, bad-faith reporting, repeated manifestly unfounded notices); • any examples or definitions describing what behaviour would qualify as misuse under Article 23.2 or trigger warnings or suspensions; 		

<ul style="list-style-type: none"> any explanation of suspension durations, proportionality considerations, or case-by-case review factors for misuse-related enforcement; any description of users' rights or remedies in the event of suspension or enforcement for misuse under Article 23.2. <p>This means that, although the TOS provide clarity regarding Article 23.1, they do not address the misuse scenarios required under Article 23.2.</p> <p>3. The TOS give several examples of illegal content (e.g., CSAM, NCII, terrorism, serious safety threats), including the consequences such content triggers (immediate permanent ban). These examples reaffirm compliance with Article 23.1 regarding repeated illegal content.</p> <p>Conclusion:</p> <p>Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the TOS do not clearly or fully document the misuse policy required under Article 23.4, particularly regarding repeated unfounded notices or complaints, factors for assessing misuse, examples of prohibited behaviour, and the nature and duration of suspensions for misuse.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> Revise the TOS to define misuse under Article 23, include clear examples (e.g., false complaints), specify enforcement criteria and durations, and explain user rights and suspension procedures. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>

<p>Obligation:</p> <p>Article 24.1.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects, the provider includes in its biannual transparency reports:</p> <ul style="list-style-type: none"> The number of disputes submitted to out-of-court dispute settlement bodies under Article 21, their outcomes, median time to resolution, and the implementation rate of outcomes; Number of suspensions imposed under Article 23, distinguishing between manifestly illegal content, manifestly unfounded notices, and manifestly unfounded complaints. 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

Audit procedures, results and information relied upon:

1. The audit team reviewed both transparency reports:
 - July – December 2024 (first reporting period); and
 - January - June 2025 (second reporting period).
2. Both reports states that no disputes were submitted to the provider by certified dispute settlement bodies.
3. Across both reports, the provider only reports account terminations for posting manifestly illegal content, such as underage material, rape, and zoophilia. These data appear under the section “Measures against platform misuse” but correspond only to Article 23.1 actions (illegal content). The reports do not contain:
 4. the number of suspensions imposed for manifestly unfounded notices;
 5. the number of suspensions imposed for manifestly unfounded complaints;
 6. any temporary suspension counts;
 7. an Article 23-aligned categorisation or breakdown.
8. During interviews, staff confirmed that the backend systems do not currently track suspensions according to the distinctions required by Article 23 and Article 24.1. Moderation teams indicated that the platform cannot extract or reconstruct this data for reporting because the database was not designed to classify enforcement actions in DSA-compliant categories. As a result, the transparency reports omit mandatory information regarding Article 23 suspensions.
9. The compliance team attributed the missing breakdown to technical limitations in the provider enforcement database and data retrieval infrastructure. Also, it indicated that work is underway to implement these features for future reporting cycles.

Conclusion:

Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While transparency reports were published and included some required data, they lacked the mandated suspension breakdown.

Recommendations on specific measures:

- Implement structured reporting fields to log suspension types by category (illegal content, unfounded notices, unfounded complaints);
- Enhance moderation and enforcement systems to support tagging and categorization of enforcement actions;
- Automate suspension logging and integrate tracking dashboards for future audits.

Recommended timeframe to implement specific measures:

The above changes should be implemented within 3 months.

<p>Obligation: Article 24.2.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Publishes, at least every six months, for each online platform, the average number of monthly active recipients of the service in the Union; ▪ Ensures the data reflects a six-month average; 	<p>Materiality threshold: N/A</p>
---	---	--

	<ul style="list-style-type: none"> ▪ Makes this information publicly accessible via the online interface (available to anyone without prior clearance or qualification). 	
--	---	--

Audit procedures, results and information relied upon:

1. Verified that the provider published the number of average monthly active recipients for the EU on the following dates:
 - February 17, 2023: 160 million
 - August 17, 2023: 160 million
 - March 26, 2024: 105 million
 - August 17, 2024: 77 million
 - February 17, 2025: 46 million
 - August 8, 2025: 44 million
2. All publications appeared on the XNXX Information Portal (<https://info.xnxx.com>) confirmed the existence of a dedicated “Mandatory Information / Reports” section. Confirmed that figures were posted at six-month intervals (except March 2024), as required, and were visible and accessible at the time of the audit.
3. Reviewed explanatory text published on the providers information page. It states that:
 - Early numbers (160M) were overestimated, using maximum assumptions to avoid underreporting.
 - Later figures (e.g. 46M in August 2025) reflect a revised estimation, adjusted after the platform developed new ways to estimate incognito traffic, which represents up to 40% of sessions.
 - The platform itself describes the published numbers as “largely estimated rather than calculated”.
4. No formal documentation or transparent methodology was published alongside the figures.
5. The audit team was not granted access to internal datasets, logs, or the algorithm used for calculating user averages. Instead, conclusions relied solely on verbal representations and information posted by the provider.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the lack of verifiable methodology, reliance on estimation over calculation, and absence of documentation limit the transparency and auditability of the reported figures.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Replace “estimated” figures with systematically calculated values based on verifiable internal data; ▪ Document and retain the methodology used, including treatment of private/incognito sessions. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>
--	---

<p>Obligation:</p> <p>Article 24.3.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p>	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

	<ul style="list-style-type: none"> ▪ Is prepared to supply the EC or the DSC with updated information on average monthly active recipients, upon request and without undue delay; ▪ Is able to substantiate the figure and explain the methodology used for its calculation; ▪ Does not transmit any personal data when fulfilling these obligations. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Performed interviews with the Compliance Officer to assess preparedness to respond to regulatory requests for updated average recipient data. Confirmed that no formal requests were received from the EC or any DSC during the examination period. Inquired about internal readiness to respond to such a request. 2. The provider stated that they are able to retrieve traffic data and provide an updated number. However, the audit team was not granted access to internal data sources or supporting technical methodology and was, therefore, unable to verify whether the provider could substantiate the published figure if requested. <p>Conclusion:</p> <p>Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, due to the lack of documented calculation methodology, it remains unclear whether the provider can fully substantiate its figures in accordance with the DSA's expectations.</p>		
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Develop and document a clear methodology for calculating average monthly active recipients, including treatment of incognito and non-logged-in traffic. 		<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>

<p>Obligation:</p> <p>Article 24.5.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Submits to the EC, without undue delay, all decisions and statements of reasons referred to in Article 17.1. DSA; ▪ Ensures these decisions are transmitted to a publicly accessible machine-readable database managed by the EC; ▪ Confirms that such submissions do not contain personal data. 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. The Provider regularly publishes statements of reasons on a designated website https://transparency.dsa.ec.europa.eu/, where the statements are publicly accessible. 2. Based on samples and also template of statements of reasons was confirmed that no these reports do not contain personal data. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 25.1.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider did not design, organise or operate the online interfaces in a way that deceives or manipulates the recipients or otherwise materially distorts or impairs the ability to make free and informed decisions ▪ The platform's choices and actions are presented neutrally and symmetrically; ▪ Users are not subject to repeated prompts or pop-ups that coerce decision-making; ▪ Cancellation of services is not significantly more difficult than registration. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Reviewed the presence and frequency of pop-up windows and system prompts. Verified that user choices (age verification, category selection, cookie preferences) were not repeatedly requested or imposed after a choice was already made. The audit does not indicate any structures or workflows that would impair or distort users' ability to make autonomous and informed decisions.
2. The key user actions observed, such as reporting content, submitting notices, appealing moderation decisions, accessing account controls, and navigating to complaint-handling or contact points, are presented through straightforward, single-click pathways. The interfaces described (Report button, Abuse Reporting Form, Copyright Form, appeal submissions via ticketing system) do not condition access on unrelated actions, nor do they require unnecessary steps that could be interpreted as coercive.
3. Navigation elements on the platform (e.g., content player, reporting button, footer navigation, and content removal section) follow a logically structured layout. Options appear in standard UI positions and are not visually or functionally obscured. No asymmetric presentation of choices (e.g., emphasizing "cancel" over "confirm" or vice versa) was identified in the materials provided.
4. The documentation does not describe the use of repeated prompts, "nagging," forced continuity mechanisms, or intrusive pop-ups aimed at influencing user actions. The Notice & Action system includes standard confirmations (e.g., acknowledgment emails, on-screen confirmations) that serve operational functions rather than behavioral manipulation.
5. Based on the Terms of Service, registration and account deletion processes are comparable in complexity. Account deletion is permitted at any time and, according to the documentation, is actioned through a standard account-management interface. There is no evidence that cancelation is subject to additional, unnecessary barriers or extended workflows relative to account registration.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 26.1.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ All advertisements presented on the provider's interface were clearly marked as such at the moment of display (real time); ▪ Each advertisement disclosed: <ul style="list-style-type: none"> – the natural or legal person on whose behalf the ad is presented; – the natural or legal person who paid for the ad (if different from point a); – meaningful, directly and easily accessible from the ad information on the main parameters used for targeting and, where applicable, how these parameters can be changed by the recipient; ▪ The information was clearly, concisely, and unambiguously presented and directly accessible from the advertisement itself. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. A walkthrough of the provider's web and mobile interfaces was performed to evaluate ad labelling, display, and access to transparency information.
2. All advertisements on the platform were identified as such through an interactive "i" icon, which appears directly on the ad at the moment of display. This form of labelling is consistently applied across formats and ensures that ads are clearly distinguishable from regular content.
3. Selecting the icon opens an About This Ad window containing information on (i) the advertiser's name and (ii) the reason why the user is seeing the advertisement. However:
 - No explicit distinction was made for the entity of beneficiary and payer,
 - No information was provided on how users may modify or control the parameters used for ad personalization.
4. It was further observed that partner links displayed through icons in the upper section of the platform interface are not labelled. These links redirect users to external platforms, but their unlabelled presentation may make it unclear whether they constitute advertisements or internal navigation elements. As a result, users may not immediately recognize that they are leaving the provider's platform environment.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Advertisements were identifiable through the "i" icon and offered real-time access to relevant transparency information. However, the absence of information on modifying targeting parameters, the lack of distinction between payer and beneficiary entities, and the unlabelled presentation of partner links reduce the overall clarity and transparency of advertising and promotional elements on the platform.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Extend the About This Ad interface to include clear guidance on how users can adjust parameters influencing ad targeting. ▪ Specify and disclose both payer and beneficiary entities where they differ. ▪ Introduce clear labelling for externally linked promotional icons. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>
--	---

<p>Obligation:</p> <p>Article 26.3.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider had a documented operational process to prevent the use of profiling for advertising purposes based on special categories of personal data as defined in Article 9(1) GDPR. 	<p>Materiality threshold:</p> <p>N/A</p>
--	--	---

<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. The provider's Cookie Policy and Privacy Policy were reviewed to assess whether profiling for advertising purposes involves the processing of special categories of personal data. 2. The Cookie Policy specifies that data collected through cookies are shared only with advertising partners assisting in ad delivery and campaign management. These partners process the data exclusively for technical and operational purposes such as displaying relevant ads, measuring performance, preventing fraud, and avoiding ad repetition. <ul style="list-style-type: none"> • Retargeting activities by partners are carried out only with the user's prior consent, and the data are explicitly stated to be non-identifying and not intended to personally identify users. • The policy also confirms that data are not transferred outside the European Economic Area unless adequate safeguards are in place. 3. The Privacy Policy defines the scope of personal data collected and processed by the provider, limited to identity, contact, and technical data voluntarily submitted by users through forms or direct interaction. There is no indication that sensitive data are collected, stored, or used for advertising or profiling purposes. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
--	--	--

<p>Recommendations on specific measures:</p> <p>N/A</p>	<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>
--	--

<p>Obligation:</p> <p>Article 27.1., 27.2.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider set out in its TOS, in plain and intelligible language, the main parameters used in its recommender systems; 	<p>Materiality threshold:</p> <p>N/A</p>
---	---	---

	<ul style="list-style-type: none"> ▪ The provider explained why certain information is suggested to recipients of the service, including: <ul style="list-style-type: none"> – the criteria most significant in determining the information suggested; – the reasons for the relative importance of the identified parameters; ▪ The TOS described the options available for recipients to modify or influence those parameters. 	
--	---	--

Audit procedures, results and information relied upon:

1. Inspected the provider's TOS and underlying documentation related to recommender systems.
2. Verified that *Article 9. Recommender System Transparency* of the TOS describes the recommender system logic applied. Specifically:
 - On the main page, recommendations are based on (i) the user's chosen location (country) and (ii) the video's popularity, determined by the total number of clicks from recipients (within selected location). The option for the recipients to change the location is stated.
 - Beyond the main page: suggestions are influenced by the chosen "category" (sub-genre)) or a particular content creator, keyword searches (the decisive criterion is the match between the entered keyword(s) and the video's title or 'tags' and within such searched videos, their popularity). The option for selecting different criteria is stated.
 - A feature of suggesting "related" videos is based on viewing history of all users. View history enables suggesting relevant videos based on the context of the respective video, considering criteria such as "popularity", "categories" or "tags".
3. Assessed whether the TOS clearly outlined the parameters used in recommending content and the option for the recipients to modify these parameters and provided explanations in plain and intelligible language. This criterion was confirmed.
4. While the TOS listed the key parameters and allowed user control over some inputs, it did not explicitly explain the relative importance of each parameter.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider has disclosed the main parameters of its recommender systems and the option for the recipients to modify these parameters in a structured and user-accessible format. However, the rationale behind the weighting of different parameters was not sufficiently detailed to satisfy the full audit requirements.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Expand the TOS to explicitly include a description of the relative importance of each parameter influencing recommendations. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>
--	---

<p>Obligation:</p> <p>Article 27.3.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ A functionality was made available to the users of the service allowing them to select and modify their preferred option within the recommender system; 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

	<ul style="list-style-type: none"> ▪ The functionality was directly and easily accessible from the section of the online interface where the recommender system applied. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted a walkthrough of the provider’s website including the main page, category (subgenre) pages, video display pages, and search bar, to verify the existence and accessibility of selection options. 2. Confirmed that users can influence the order of presented content by selecting categories, creators, or changing country settings, and that the system responds in real time to these changes. 3. Verified that these options are accessible directly from within the prioritised content sections, such as setting menu (country, category, history) and left-side submenu (categories, channels, porn-stars). <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>		<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 28.1.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider has implemented appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on its platform; ▪ Such measures are reflected in access controls, interface design, and risk mitigation processes. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed the platform’s TOS (<i>Article 2. Access</i>), which clearly state that the platform is intended solely for adults aged 18 or over. The TOS explicitly prohibits use of the platform by minors and informs users that by accessing the service, they confirm they are of legal age. This condition is reinforced via an age confirmation gate that requires users to affirm they are 18+ prior to entering the platform. This mechanism is standard for adult-content services. 2. Assessed the platform’s interface and access flow. The provider does not allow access to its main content pages without passing the age confirmation prompt. While no technical age verification is enforced, the voluntary self-declaration model is consistent with industry norms for non-registration-based access. Users may optionally enter a birth date in account settings, which aligns with practice where full verification is not legally mandated. 3. Reviewed the “Age Verification Tools Analysis and Reference Review”. The document outlines the provider’s evaluation of current age assurance technologies and recognizes that some emerging tools (e.g., AI estimation, ID-based verification) may offer stronger 		

protections, but also the analysis indicates that implementing biometric or ID-based systems on a platform like XNXX raises significant privacy, consent, and data storage risks, particularly in light of the sensitive nature of the service and the risk of chilling lawful adult use. It also highlights the absence of EU-wide standards for age verification in adult services, which complicates implementation. The provider reports ongoing internal discussions and consultations with stakeholders on implementing age assurance to balance safety with privacy and legal limits. This reflects intent and preparation.

4. In the uploaded authority-response document, the provider confirms, the following:
 - The platform is restricted to adults only and contains explicit warnings at entry,
 - It implements RTA labeling, enabling browser- and ISP-level parental filtering,
 - It provides detailed parental-control instructions, including device-level restrictions, DNS filters, safe-browsing tools, and network-level blockers,
 - The choice of measures is guided by proportionality, privacy protection, and avoidance of intrusive age-verification processes that would create new risks to minors' data.
5. Both risk-assessment documents provide evidence that protection of minors is treated as a core systemic-risk domain, with detailed identification, assessment, and mitigation. The updated 2025 methodology integrates A strengthened child-safety assessment lens, using the EC's Article 28 Minor Protection Guidelines² (5C framework). Protection of minors was prioritised as one of the highest inherent risk categories and one of the main areas targeted for mitigation improvements. Access-control measures were reviewed across documentation and user-facing interfaces. The platform applies:
 - Mandatory age-affirmation gates for all visitors,
 - Prominent warnings at entry and throughout legal pages that the site is intended strictly for adults 18+,
 - RTA tagging, enabling automatic blocking by parental-control tools,
 - Device-level safeguards supported by the platform's parental-control guide, which includes detailed instructions on enabling safe-search and content filter.

These measures are described extensively in the authority-response document (as mentioned above) as a core strategy to ensure that age assurance remains effective while privacy-preserving.

6. The platform articulates its intention to balance safety obligations with data minimization principles. The reports explicitly recognize the tension between effective age assurance and GDPR constraints, reflecting a nuanced understanding of dual regulatory compliance.

The platform's risk documentation supports a positive audit conclusion under Article 28.1 due to the documented governance, strategic prioritization, and commitment to iterative compliance improvements. The provider clearly understands its risk landscape and has embedded minor protection into its compliance roadmap, which reflects a good-faith effort and maturing governance in this critical area.

7. Conducted interviews with the Legal Team and Regulatory Director, who confirmed that while the provider does not currently perform ID checks or biometric analysis, it has initiated technical scoping into possible privacy-preserving assurance models suitable for a high-risk

² European Commission. (2025, October 10). *Communication — Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (C / 2025 / 5519)*. *Official Journal of the European Union*, C/2025/5519. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505519.

adult platform operating in the EU. The team emphasized the importance of avoiding overprocessing personal data.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider has implemented appropriate and proportionate measures to comply with the requirements of Article 28.1 during the audit period in all material respects. The platform enforces an adult-only access policy through visible disclaimers, mandatory self-declaration, and age restriction clauses in the TOS. These mechanisms are consistent with established norms for adult content platforms and reflect a baseline level of compliance.

However, the current measures rely primarily on user self-declaration and voluntary parental controls. They do not incorporate technical or identity-based age verification systems. While this approach may appear ineffective, the provider has demonstrated clear recognition of the risk and a documented, proactive commitment to evolving its safeguards. Risk assessments conducted in 2024–2025 explicitly highlight minor protection as a strategic and regulatory risk and outline pathways for integrating age assurance in future development cycles.

The provider has articulated the inherent tension between implementing adequate age verification and the risk of excessive personal data processing, particularly under the GDPR and Article 28.3 DSA. This shows a mature understanding of its dual obligations: protecting minors while minimizing data collection. While full technical enforcement is not yet in place, the governance structure, risk prioritization, and planning reflect a credible and responsible compliance posture.

Recommendations on specific measures:

- Continue exploring privacy-preserving age assurance technologies, such as AI-based age estimation, third-party verification tokens, or pseudonymized ID checks;
- Conduct technical feasibility testing and legal assessments for age-gating solutions that balance regulatory compliance with user privacy;
- Consider testing the effectiveness of existing age assurance.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 12 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 28.2.	Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Does not present advertisements based on profiling (as defined under GDPR Article 4(4)) using personal data when it is aware with reasonable certainty that the recipient of the service is a minor. 	N/A

Audit procedures, results and information relied upon:

1. Reviewed the provider’s advertising architecture and confirmed that the platform’s ad delivery system is non-personalized by design. The advertising logic operates on a contextual or placement-based basis, not on user behaviour, preferences, or identifiers.
2. Interviewed compliance team, who confirmed that no behavioural data or user profiles are used for ad targeting. Ads are delivered based on the type of content or category page being viewed, for example, a static ad served on a specific content category (e.g. “Amateur” or “VR”), rather than linked to a user’s browsing history, location, or declared preferences.

<p>The provider does not participate in programmatic ad networks that rely on cookies or personal identifiers for behavioural delivery.</p> <p>3. Confirmed that XNXX does not require account creation for content viewing. Since many users are anonymous (i.e., not logged in), and there is no collection of demographic or behavioural identifiers, the technical capacity for profiling is inherently absent.</p> <p>4. Reviewed the platform’s GDPR policy and data processing disclosures, which do not include profiling practices or automated decision-making related to users. Additionally, the platform’s TOS and Privacy Policy explicitly state that the service is for adults aged 18 and older and that users are not tracked for targeted advertising.</p> <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 28.3.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ Does not process additional personal data solely to determine whether a user is a minor; ▪ Maintains a privacy-conscious stance. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <p>1. Reviewed internal privacy policies and publicly available sources. The privacy policies and data processing disclosures confirm that no biometric, document-based, or behavioural profiling data is collected or inferred for age estimation purposes. The platform does not require or solicit date of birth (except optionally during account registration), nor does it utilize cookies or trackers to derive user age.</p> <p>2. Evaluated the “Age Verification Tools Analysis and Reference Review”, which presents a comprehensive examination of age assurance solutions and regulatory interpretations across jurisdictions. The analysis emphasizes that the provider treats technologies requiring additional personal data processing with caution, particularly document-based or biometric methods. This cautious approach is guided by concerns related to GDPR compliance, potential conflicts with the principle of data minimization, and limited user acceptance or feasibility for such methods within the adult content context.</p> <p>3. Reviewed the NKL risk management documentation, which confirm that while stronger minor protection is under consideration, any future solution must be “privacy-preserving by design”. The reports also emphasize that GDPR Article 5(1)(c) (data minimization) remains a guiding compliance standard alongside the DSA.</p> <p>Conclusion: Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>		<p>Recommended timeframe to implement specific measures: N/A</p>

Section 5 – Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks

<p>Obligation: Article 34.1.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider conducted a service-specific risk assessment by the DSA application date and at least annually thereafter; ▪ The provider assessed the dissemination of illegal content via its service; ▪ The provider assessed negative effects on fundamental rights under the Charter, including freedom of expression, privacy, child protection, and non-discrimination; ▪ The provider assessed effects on civic discourse, electoral processes, and public security; ▪ The provider assessed effects on gender-based violence, protection of minors and public health, and physical and mental well-being. 	<p>Materiality threshold: N/A</p>
---	--	--

Audit procedures, results and information relied upon:

1. Reviewed the 1st Risk Assessment (November 2024) and 2nd Risk Assessment (ongoing), as well as supporting documentation including the Risk Register, Risk Drivers Register, Mitigation Measures Register, and Action Plans 2024-25 and 2025-26.
2. The 2024 report sets out the service scope, categories and scoring for 83 scenarios across 12 risk categories and documents the inherent and residual risk assessment process and results; it shows predominantly medium inherent risks with strong risk reduction to low residual for the majority of scenarios.
3. The 2025 assessment refines the approach and updates the analysis. It introduces a quantified residual-risk model combining a Risk Reduction Factor (RRF) for control effectiveness and a Driver Impact Score (DIS) to reflect persistent influences from Article 34(2) drivers; the residual formula is explicitly documented and applied across scenarios. The report also formalises a Mitigation Measures Register with reasonableness, proportionality and effectiveness testing and records governance workshops and traceability. The 2025 analysis covers 81 systemic scenarios and 76 risk drivers, with 51 controls registered; it reports a reduction of the average risk from 14 (inherent) to 6 (residual) and no high residuals post-mitigation.
4. Both assessments explicitly identified and analysed all risk areas under Article 34(1).
 - Illegal content: Comprehensive coverage of CSAM, NCII, trafficking, deepfakes, revenge porn, and terrorist content; supported by incident data and automated-detection controls.
 - Fundamental rights: In-depth analysis of privacy, data protection, human dignity, freedom of expression, and non-discrimination risks; mitigations include improved appeal processes, bias testing, and privacy-by-design.
 - Civic and electoral risks: Both assessments found limited relevance for XNXX’s adult-content model but documented awareness of potential misuse (e.g. sexualised disinformation, deepfake harassment).
 - Gender-based violence: Detailed risk mapping to coercive content, deepfakes, and algorithmic amplification of misogyny,

<ul style="list-style-type: none"> • Protection of minors: Evaluated using EU 5C framework; with focus on age-assurance design and proportionality. • Public health and well-being: Considered exposure to harmful or addictive sexual content, unrealistic body norms, and misinformation about sexual health. <p>5. The 2024 report documents qualitative likelihood × impact scoring (1-25), control effectiveness analysis and residual prioritisation. The 2025 report moves to semi-quantitative reduction (RRF/DIS) and formalises control testing (reasonableness, proportionality, effectiveness), with visualised distributions for measures and residuals. It records cross-functional workshops (Content Moderation, Notice and Complaint, Tech, Support, Advertising) and recognises that best practice requires KPIs; at the time of assessment, broader KPI coverage is flagged as an action plan item. These points show that the latest assessment is ongoing, i.e., not only completed but feeding into a living risk-mitigation and measurement programme.</p> <p>6. A cross-functional governance structure was formalised in 2025. Workshops and validation sessions are documented.</p> <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, there is an opportunity for improvement. While the 2025 assessment introduces a numerical model and acknowledges the need for metrics, the current process remains primarily qualitative, relying on subjective scoring and narrative evaluation.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Define a structured set of key performance indicators (KPIs) for internally prioritized key areas of systemic risk. KPIs should include measurable indicators. These should be directly linked to the assessment of systemic risks and risk drivers. 	<p>Recommended timeframe to implement specific measures:</p> <p>Within 12 months from the audit conclusion.</p>

<p>Obligation:</p> <p>Article 34.2.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider assessed whether and how systemic risks were influenced by (a) recommender systems and other algorithmic systems; (b) content moderation systems; (c) TOS and their enforcement; d) advertisement selection and presentation systems; (e) data practices of the provider; ▪ The provider considered risks arising from manipulation of the service, inauthentic use, automated exploitation, and amplification effects; ▪ The provider considered relevant regional and linguistic aspects in the EU. 	<p>Materiality threshold:</p> <p>N/A</p>
--	--	---

Audit procedures, results and information relied upon:

1. Both the 1st Risk Assessment (November 2024) and the 2nd Risk Assessment (ongoing) contain explicit “driver” mappings linking systemic-risk categories (Article 34 (1)) to their potential influencing mechanisms (Article 34 (2)). The 2025 report expands this section into a Driver Impact Register, assigning each systemic-risk scenario one or more drivers with weighted impact scores. The methodology applies a Driver Impact Score (DIS) from 1 (low) to 5 (high), which feeds into the residual-risk formula and quantifies how much each operational domain contributes to overall risk exposure.
2. The audit relied on the Risk Driver Register (2025) containing 83 risk-driver entries extracted from the 2nd Risk Assessment (draft) supplemented by the Mitigation Measures Register. Each driver entry records driver type (RS - Recommender, CM - Content Moderation, TS - Terms of Service, AS - Advertising, DP - Data Practices, MA - Manipulation and Inauthentic Use, RL - Regional and Linguistic Risks, AV - Age Verification), residual likelihood and impact, existing controls and measures, the influence type, DIS. The 2025 cycle thus operationalises Article 34(2) through a quantitative linkage between system design factors and the residual systemic risks assessed under Article 34(1)
3. Art. 34.1.a: The audit confirms extensive evaluation of algorithmic drivers, such as amplification of exploitation or pirated material, echo chambers and sensationalism, user-choice transparency and non-profiling options.
4. Art. 34.2.b: The audit confirms extensive evaluation of moderation-related drivers, such as failure to timely remove high-severity illegal content, moderation-error drivers, procedural fairness drivers. Overall, moderation risks are well-identified, systematically rated, and supported by concrete mitigations (team training, ticketing system, appeal forms).
5. Art. 34.2.c: TOS-related drivers examine clarity, even-handed application, and the sufficiency of user-facing explanations about moderation, automation and appeals. The analysis demonstrates that TOS enforcement influences likelihood more than impact, e.g., uneven interpretation rather than intensified harm.
6. Art. 34.2.d: The audit confirms that risk assessment contains a set of advertising-system drivers, covering advertiser verification, ad-screening, biased engagement optimisation, covert political ads, and unsafe categories. The ad-repository and manual review mitigate systemic amplification; remaining weaknesses relate to manual-only screening and partial advertiser verification.
7. Art. 34.2.e.: The audit confirms extensive evaluation of data-privacy related drivers, such as breaches or insider leaks, persistent identifiers and insufficient consent controls, geolocation/IP/contact linkage to explicit content, indefinite holding of intimate content/metadata, advertisers/vendors receiving sensitive data without adequate safeguards.
8. Art. 34.2, para 2: The 2025 driver set captures bots/engagement farms, brigading/mobbing, malicious links/QRs and abusive notice “report-bombing”. These primarily increase likelihood that illegal or abusive material is amplified (or that lawful speech is over-removed), especially where engagement signals feed ranking.
9. Art. 34.2, para 3: The audit confirms that risk assessment contains a set of regional and linguistic drivers, such as detection coverage gaps in smaller EU languages (including slang or dialect blind spots), process alignment with stricter national rules, user-facing adaptation, and recommender parity across countries.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, there is an opportunity for improvement was noted. Current driver evaluation still relies mainly on qualitative or expert-weighted scoring, without embedded operational KPIs.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Define a structured set of key performance indicators (KPIs) for internally prioritized key areas of systemic risk. KPIs should include measurable indicators. These should be directly linked to the assessment of systemic risks and risk drivers. 	<p>Recommended timeframe to implement specific measures:</p> <p>Within 12 months from the audit conclusion.</p>
--	--

<p>Obligation:</p> <p>Article 34.3.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider preserved supporting documentation for each risk assessment conducted; ▪ Documentation was retained for at least three years from the date of assessment; ▪ The provider was prepared to share this documentation with the EC or DSC upon request. 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted interviews with the Compliance Officer function to confirm document retention practices relating to systemic risk assessments conducted under Articles 34 and 35 DSA. The team confirmed that all underlying materials, working files, and final reports from the 2024 and 2025 Risk Assessments were retained, including: <ul style="list-style-type: none"> • the Systemic Risk Register, Risk Driver Register, Mitigation Measures Register, and Action Plan, • associated workshop records and evidence logs created during cross-functional sessions, and • copies of the 2024 and 2025 final assessment reports approved by management. 2. Inspected the internal documentation structure described in the 2025 Risk Assessment Report, which specifies that all assessment deliverables are maintained in a centralised internal repository accessible to authorised functions only. Documentation is version-controlled, tagged by assessment year, and linked across the Risk Register and Mitigation Register for traceability. The process follows ISO 31000 principles integrated into NKL's DSA compliance framework. 3. Reviewed internal compliance policy contains section, which assign retention responsibilities to the Compliance Function acting as second-line assurance. Supporting materials, data logs, and registers are preserved for at least three years from the completion date of each annual assessment, in line with DSA Article 34(3). 4. No regulatory request for sharing risk documentation had been received at the time of the audit. However, the compliance team confirmed that a procedure exists for prompt response to EC or DSC requests. The procedure includes document retrieval procedures and designated points of contact for secure data transfer. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
--	--	--

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 35.1	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Reasonable, proportionate and effective mitigation measures, including (as applicable) those included in Article 35(1), points (a) to (k), were put in place tailored to the specific systemic risks identified pursuant to Article 34; ▪ The provider considered the impact of the mitigation measures on the fundamental rights of users. 	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed the 1st Risk Assessment (November 2024) and 2nd Risk Assessment (ongoing), as well as supporting documentation including the Risk Register, Risk Drivers Register, Mitigation Measures Register, and Action Plans 2024-25 and 2025-26. 2. The 2024 assessment did not rely on measure-based register. Instead, controls were captured only through Risk Register and mapped to respective identified risk scenarios. The effectiveness was assessed internally based on predefined effectiveness ratings; however, no formal documentation has been recorded. Such rationale informed residual risk assessment recorded in the Risk Register. 3. The 2025 assessment introduced the Mitigation Measures Register, which consolidates all existing controls into a measure-based register and allows evaluation of each measure’s reasonableness, proportionality, and effectiveness as standalone criteria. <p>The methodology applies a structured, qualitative scoring system:</p> <ul style="list-style-type: none"> • Reasonableness and proportionality are assessed through four targeted questions (two per criterion) rated on a three-point scale (Yes, Partly, No), converted into high, moderate, or low levels. The questions drew upon predefined topics such as timeliness, existing knowledge, user and platform integrity protection, and fundamental rights respecting. This ensures a transparent and consistent evaluation. • Effectiveness is assessed qualitatively based on expert judgment from measure owners and operational teams. Quantitative performance data (KPIs) were used for selected measures, where established indicators exist. <p>The evaluation combined desk research and cross-functional workshops involving key operational teams. These workshops were used to validate the relevance and adequacy of measures, evaluate their effectiveness, and discuss future KPI options.</p> <p>The 2025 methodology demonstrates improvement, is robust in structure and aligns with the audit criteria. The 2025 report recognises that best practice requires KPIs; at the time of assessment, broader KPI coverage is flagged as an action plan item. These points show that the latest assessment is ongoing, i.e., not only completed but feeding into a living risk-mitigation and measurement programme.</p> <ol style="list-style-type: none"> 4. Reviewed mitigation measures assessed in 2024 and 2025 risk assessment and their alignment with those suggested in Article 35(1) as follows: 		
--	--	--

- Point (a) – The platform implemented several design and functionality adjustments aimed at enhancing user awareness, safeguarding against unintended exposure to adult content, and strengthening advertising transparency:

User control and consent: Users are required to confirm age and acceptance of the Terms of Service before accessing the site. A cookie banner provides options to accept, reject, or manage cookies, while users may disable viewing history to prevent personalization.

Protection against unintended exposure: The homepage is blurred by default and displays a clear adult-content warning. Access is granted only after explicit confirmation, ensuring that users are aware of the nature of the content before entry.

Transparency and accountability: Advertisements are clearly marked with an “i” icon linking to an About This Ad window containing details on the advertiser and targeting parameters.

- Point (b) – The platform maintains comprehensive TOS and related policies that define user obligations, platform rules, and enforcement mechanisms:

Clarity and accessibility of the Terms of Service: The TOS establish a clear legal framework for all users, outlining age restrictions, prohibited content categories, and intellectual property rules. They explicitly forbid the upload of illegal, harmful, or non-consensual material and include references to parental control tools. The full text is accessible via a dedicated link on the platform, translated into all EU languages, and preceded by a user-friendly summary to support understanding.

User acknowledgement and enforcement: Upon first visit, users must explicitly confirm acceptance of the TOS before accessing any content. The page remains blurred until confirmation is given, reinforcing user awareness. Enforcement mechanisms include moderation practices including a three-strike policy for repeated copyright violations, leading to content and account disabling, termination.

Data protection and legal compliance: The accompanying Privacy Policy applies to registered users and specifies how personal data are collected and processed under the GDPR. It limits processing to legitimate purposes and ensures compliance with EU data protection standards.

- Point (c) – The platform operates a multi-layered moderation system combining automated detection, manual review, and structured notice-and-action procedures to ensure timely and accurate handling of illegal or harmful content:

Automated detection and pre-moderation controls: Automated tools identify known or suspected illegal material through fingerprinting, AI-based analysis, and risk scoring. Keyword filters supplement these tools by flagging prohibited terms.

Human moderation and notice processing: Dedicated moderation teams conduct manual review of uploads and reported content. Multiple reporting channels exist, each providing confirmation and some reasoned outcomes. Trusted flagger reports are prioritised, and a complaint-handling system enables users to appeal moderation decisions. All advertisements undergo manual review before and after publication, supported by the Advertiser Certification Program to ensure compliance.

Governance, training, and cooperation: Moderators receive structured onboarding and continuous training focused on the handling of sensitive material and illegal content categories. The multilingual team uses translator tools to cover diverse user

languages. Cooperation with law enforcement authorities and the Czech reporting portal stoponline.cz supports external escalation of criminal content.

- Point (d) – The platform’s algorithmic environment is designed to operate transparently and allow users to retain control over data influencing personalized recommendations. However, no structured testing or adaptation of the recommender system itself is currently in place.

User control and transparency: Users can manage cookie preferences before accessing the site and modify them at any time through a dedicated section. They may also deactivate viewing history, thereby preventing past interactions from influencing displayed recommendations.

Data governance framework: The Cookie Policy and Privacy Policy together ensure transparency in data collection and processing. Non-essential cookies require explicit consent and are used for personalization and advertising. Data are processed only within the EEA or under adequate safeguards and are not shared with unrelated third parties.

- Point (e) – The platform has established a comprehensive advertising control framework combining pre- and post-publication review, advertiser vetting, and transparency tools to ensure that advertising practices remain compliant and secure:

Transparency and user control: Most advertisements are visually marked with an information icon (“i”) that opens an About This Ad window containing the advertiser’s name and targeting parameters. However, partner links displayed through icons in the upper section of the platform interface are not labelled. This may make it unclear that a user is transitioning to external platforms. The Cookie Policy further ensures that advertising personalization operates only with user consent, distinguishing between essential and non-essential cookies and prohibiting data sharing with unrelated third parties.

Pre- and post-publication review: Each advertisement is manually reviewed before approval. Ads violating internal rules are rejected. Approved campaigns are continuously monitored after publication, with violations managed through a tiered process ranging from labeling to account termination.

Advertiser qualification and compliance: The Advertiser Certification Program restricts access to verified and compliant advertisers who meet predefined eligibility criteria. Certified advertisers undergo periodic re-evaluation, and violations can lead to suspension or permanent removal.

- Point (f) – The platform maintains internal governance structures and control mechanisms designed to identify and mitigate systemic risks across its operations. Compliance team demonstrated clear allocation of responsibilities, ownership of controls, as well as defined timelines for action points implementation.

The Compliance Officer was observed to coordinate DSA compliance implementation, ensuring oversight and cross-departmental communication. Internal workflows were described and operational in practice.

- Point (g) – The platform has established operational mechanisms to cooperate with trusted flaggers in accordance with Article 22 and acknowledges its obligations under Article 21 concerning out-of-court dispute settlement:

Trusted flagger registration and prioritisation: A dedicated Trusted Flaggers Registration page allows officially designated organisations from the EU to apply for registration. The system verifies each applicant before granting access. Once

verified, applicants receive activation confirmation and account credentials. Notices submitted by trusted flaggers are automatically prioritised and placed at the top of the moderation queue for expedited handling.

Handling of out-of-court dispute settlement decisions: TOS includes a specific reference to users' and notice submitters' right to access a certified out-of-court dispute-settlement body.

- Point (h) – During the audit period, the provider was not a signatory to any code of conduct under Article 45 nor a participant in a crisis protocol under Article 48. Nonetheless, the Compliance Team demonstrated familiarity with these cooperative mechanisms and indicated an intention to join such initiatives once relevant to the platform's operational context.
- Point (i) – The platform has implemented several informational and interface-level features designed to promote user awareness, ensure informed consent, and guide guardians in protecting minors from exposure to adult content:

User information and consent: Upon first entry, users receive clear on-screen notices confirming the website's adult nature and the requirement to be of legal age. Access to content remains blocked until explicit confirmation is provided. Users must also accept the Terms of Service and manage cookie preferences through a banner that offers options to accept, reject, or customize tracking settings.

Guidance for parental control and safety: A dedicated Parental Controls page provides practical instructions and links to filtering tools on browsers, devices, and networks. The page also refers to a safe visual search engine for kids. This information is accessible before any explicit content is displayed.

Transparency and accessibility of information: The Terms of Service are written in all EU official languages and supported by explanatory summary. Accompanied by Cookie Policy and Privacy Policy, these documents are permanently accessible through the interface footer. Contact points for user support are provided through an online form and dashboard links.

- Point (j) – The platform has implemented a series of preventive and informational measures aimed at restricting minors' access to adult content and promoting user awareness of available parental controls:

Age warning and self-declaration: Upon first access, users encounter a clear age-warning message informing them that the website is intended exclusively for adults. Access to content remains blocked and blurred until the user confirms being of legal age and agrees to the Terms of Service.

Parental control and content-labelling tools: A dedicated Parental Controls page provides detailed guidance on enabling filtering functions across devices, browsers, and networks. The platform also applies an RTA (Restricted to Adults) label embedded in metadata across all pages and domains, facilitating external filtering and parental-control systems.

Reporting and support mechanisms: Multiple reporting tools allow users and third parties to signal illegal or harmful material, including abuse-reporting and copyright-infringement forms.

Concluded that the current self-validation mechanism, which relies solely on user confirmation of age, does not incorporate technical or identity-based age verification. Nonetheless, the provider demonstrates awareness of this field, as reflected in its risk assessment materials and corresponding Action Plan, which

commits to monitoring market developments in age-assurance technologies and to engaging in cooperation initiatives with NGOs in this field.

- Point (k) – It was confirmed that the provider requires uploaders to declare whether a video contains real or synthetic characters by selecting a dedicated field during the upload process. Users can also report suspected manipulated or misleading content through a dedicated function accessible directly from the video interface.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period. However, certain opportunities for improvement have been identified. While the 2025 assessment introduces a numerical model and acknowledges the need for metrics, the current process remains primarily qualitative, relying on subjective scoring and narrative evaluation. Some measures can be further enhanced through recommended safeguards in accordance with Article 35, specifically reasoned outcomes should be provided when using all reporting pathways. Structured testing mechanism for recommender system may help limit potential biases. Lastly, the self-declaration safeguard does not incorporate technical or identity-based age verification systems. However, the provider has demonstrated proactive commitment to evolving its safeguards. Minor protection remains as a strategic and regulatory risk and pathways for integrating age assurance in future development cycles are outlined.

Recommendations on specific measures:

- Develop and implement quantitative KPIs to measure the effectiveness of mitigation measures
- Consider establishing a structured testing of recommender systems
- Continue exploring privacy-preserving age assurance technologies, such as AI-based age estimation, third-party verification tokens, or pseudonymized ID checks

Recommended timeframe to implement specific measures:

The above measures should be implemented within 12 months.

<p>Obligation: Article 36.1.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider had defined internal protocols to respond to a crisis declared by the EC; ▪ If a crisis had been declared, the provider would have taken one or more of the following actions: <ul style="list-style-type: none"> – Assessed the extent to which their services contribute to the threat; – Identified the systems and processes significantly involved; – Monitored the contribution to the threat; – Implemented specific and proportionate mitigation measures; – Assessed the impact of such measures on fundamental rights; – Reported to the EC according to the specified schedule. 	<p>Materiality threshold: N/A – Not applicable. No crisis declared during the examination period.</p>
---	--	--

<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted interviews with the Compliance Officer to confirm whether formal internal procedures exist to address a crisis declared by the EC under Article 36 DSA. It was confirmed that the senior management acts as the designated crisis management contact point. The Compliance Office monitors EU-level developments, including guidance and templates published by the EC and the Board, ensuring that any activation of Article 36 measures can be implemented without delay. 2. Confirmed that, during the audit period, no crisis had been declared by the EC under Article 36 DSA. However, the provider demonstrated preparedness by maintaining a continuous monitoring system within its Compliance Office for EU-level crisis announcements or obligations. The contact point designated under Article 11 DSA is operational and capable of serving as the primary communication channel in crisis situations. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 38</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider offered at least one version of each recommender system that did not rely on profiling, as defined in Article 4(4) of Regulation (EU) 2016/679; ▪ The non-profiled option was clearly distinguishable and understandable for the recipients. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. A walkthrough of the provider’s web interface confirmed that the platform offers a recommender system option that does not rely on profiling. 2. Such option is easily clearly described and accessible to users through https://xnxx.com/history. 3. The platform provides a feature Enable/Disable History. When a user clicks on “Enable history” button, an informational pup-up window displays that a user needs to accept cookies storing the pages viewed for navigation purposes. Moreover, an “i” icon provides additional explanations stating that <i>“keeping this feature disabled prevents the recommendation system from providing you [a user] a personalized experience based on your [user’s] navigation history.”</i> Confirmed that such option is clearly distinguishable and understandable. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures: N/A</p>		<p>Recommended timeframe to implement specific measures: N/A</p>

Obligation: Article 39.1	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider made publicly available a repository of advertisements presented on their interface and accessible via a specific section of the interface; ▪ The repository provided a search and filter functionality supporting multicriteria queries; ▪ The repository was also accessible via API; ▪ The information remained available for the entire display duration of the ad and for at least one year after its last presentation; ▪ No personal data of the recipients to whom the ad was or could have been presented was included in the repository; ▪ Reasonable efforts were made to ensure the accuracy and completeness of the published information. 	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. A walkthrough of the provider’s web interface confirmed that the advertisement repository is publicly accessible through the platform’s subdomain (<https://info.xnxx.com/ad-repository>).
2. The section provides a searchable interface allowing multicriteria queries, including Date range, Country, and Advertiser name.
3. Links to an API search endpoint and API documentation are also provided, confirming that repository data are accessible via an application programming interface.
4. Confirmed that advertisements remain visible in the repository for the full duration of their display and for one year after their last presentation. The earliest selectable date within the search filter corresponds to exactly one year prior to the current date, confirming compliance with retention requirements.
5. Review of repository entries confirmed that no personal data of service recipients is displayed.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 39.2	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider included in the advertisement repository all information required: 	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

	<ul style="list-style-type: none"> - the content and subject of the advertisement, including product, service, or brand names and the subject of the advertisement; - the natural or legal person on whose behalf the advertisement is presented; - the natural or legal person who paid for the advertisement (if different from point ii); - the period during which the advertisement was presented; - whether the advertisement was intended to be presented to one or more groups of recipients, main targeting and excluding parameters used; - the commercial communications published pursuant to Article 26(2); - the total number of recipients reached, with aggregate breakdowns by Member State for the group(s) of recipients that the advertisement targeted. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Examined the advertisement repository’s structure and data content. The following information was confirmed to be available through the repository interface: 2. In section “Ad Details” each advertisement includes: <ul style="list-style-type: none"> • The visual or textual preview and is assigned a “Topic” category. • The Advertiser entity. • The First seen” and “Last seen” dates showing when each advertisement started and ended its visibility (or remains active). • The Country of appearance. • Impression data for the country of appearance (both numerical and percentage data). 3. Identified, the repository does not differentiate between the payer and the beneficiary when disclosing the advertiser’s entity. 4. The section “Audience Selection” each advertisement includes outlines targeting logic through defined parameters grouped as (i) Geographical locations and (ii) Contextual signals. Indicators “+”, “-”, and “±” denote inclusion, exclusion, or partial inclusion of the criteria. 5. Review of the provider’s Terms of Service (Article 7) confirmed that users are not permitted to upload or publish commercial communications. Consequently, the obligation under to provide transparency for user-declared advertising is not applicable during the audit period. <p>Conclusion:</p> <p>Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. An information about “advertiser” is provided, however, it is not distinguished between the paying entity and the beneficiary of the advertisement.</p>		
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Amend the repository data structure to separately identify the payer and the beneficiary when these differ. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>	

Obligation: Article 39.3	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider excluded the content and information about the payer and beneficiary of the advertisement (points (a), (b), and (c) of Article 39(2)) for advertisements removed or disabled due to alleged illegality or breach of TOS; ▪ In such cases, the provider included alternative information in line with Article 17(3)(a)–(e) or Article 9(2)(a)(i). 	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. The advertisement repository was reviewed to verify the information retained for removed or disabled advertisements. The following observations were made:
2. Advertisements that were removed or restricted remain listed in the repository.
3. Upon selecting “Click here for details,” users can view limited metadata including Advertiser, Topic, First seen and Last seen data, Country and Impressions data.
4. The visual content is not displayed and is replaced by a placeholder stating: “This content was removed because it didn’t follow our advertising standards.”
5. The Advertiser’s name continues to be shown in the repository for removed or disabled ads.
6. Apart from the placeholder message, no additional information is provided. Specifically, the repository is missing the statement of reasons or reference to the legal basis under Union or national law applicable to orders to act against illegal content.

Conclusion:

Positive with comment – The advertisement repository maintains visibility of removed or disabled advertisements and continues displaying selected information. However, the advertiser entity remains visible and statement of reasons or reference to legal basis is not displayed.

Recommendations on specific measures: <ul style="list-style-type: none"> ▪ Remove the advertiser’s name (both payer and beneficiary) for all removed or disabled advertisements. ▪ Amend the repository data structure to include statement of reasons or legal basis information. 	Recommended timeframe to implement specific measures: The identified measures should be implemented within 6 months.
---	--

Obligation: Article 40.1	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Access to data necessary to monitor and assess compliance with Regulation (EU) 2022/2065 was provided, at the reasoned request of the DSC of establishment or the EC, within the period specified in the request. 	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Compliance officer and management were interviewed to assess awareness of obligations under Article 40 and the readiness to respond to competent authority requests.
2. Internal procedures for receiving, verifying, and processing regulatory data access requests were reviewed. These were found to be present and operating in practice, though formal written documentation could be strengthened.
3. Two Requests for Information (RFIs) submitted by a competent authority were identified during the examination period.
4. No evidence of delays, regulator dissatisfaction, or non-response was identified during the audit. However, the absence of a codified response protocol may impact traceability in future.

Conclusion:

Positive with comments – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Two RFIs were handled cooperatively and within the required deadlines. However, internal handling procedures should be formalised and documented to ensure future scalability and oversight.

Recommendations on specific measures:

- Draft and approve a formal internal policy on receiving, tracking, and responding to data access requests from regulators.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 40.3.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none">▪ The provider was able, upon request by the EC or the DSC, to explain the design, logic, functioning, and testing of its algorithmic systems, including recommender systems.	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Examined internal materials describing the architecture and functioning of the platform's recommender system and other algorithmic processes relevant to content ranking and personalization.
2. The audit confirmed the existence of a recommender system process mapping. However, the audit noted that the mapping remains primarily descriptive and operational and would benefit from being developed into a formal explanatory document.
3. The Compliance Officer confirmed that the provider maintains a standing internal protocol for cooperation with the EC and DSC of establishment, under which technical and compliance teams coordinate responses to regulatory information requests.
4. While no formal request under Article 40(3) had been received during the audit period, the provider demonstrated preparedness to supply algorithmic explanations within the scope of its mapping and internal validation materials.

Conclusion:

Positive with comments – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, to strengthen regulatory readiness, the provider should consider developing this mapping into a formal explanatory framework that explicitly aligns with Article 40(3) requirements and supports structured regulatory disclosure.

Recommendations on specific measures:

- Develop the existing recommender system process mapping into a formal algorithmic systems explanatory document.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 9 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 41.1.	Throughout the period, in all material respects: <ul style="list-style-type: none">▪ The provider established a compliance function that (i) was independent from operational functions, (ii) included one or more designated compliance officers, (iii) appointed a compliance officer, (iv) was granted sufficient authority, stature, and resources, (v) maintained access to the provider's management body.	N/A

Audit procedures, results and information relied upon:

1. The audit confirmed that Mr. David Hradecký was designated as Compliance Officer. The appointment was made by the senior management, and the role was defined to include oversight of legal compliance, policy implementation, and ethical conduct.
2. Inspected the provider's Compliance Policy and Compliance Statute. These documents set out the function's responsibilities, confirm the compliance officer's authority, and specify structural independence from operational units.
3. Confirmed independence from operational functions through organizational statements and role descriptions. The Compliance Officer is not part of product, engineering, or monetization operations and operates separately from commercial management lines.

<p>4. Inspected reporting lines defined in the appointment letter and governance documents, which confirm direct access to the senior management and the authority to escalate matters independently.</p> <p>5. Reviewed access and decision-making authority, including (i) unrestricted access to internal records, (ii) discretion in resource allocation, (iii) ability to develop and enforce policies independently.</p> <p>6. Confirmed through interview records and documentation that no changes to the compliance function's structure or mandate occurred during the examination period.</p> <p>Conclusion: <u>Positive</u> – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 41.2.</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The management body ensured that the appointed compliance officers had the professional qualifications, knowledge, experience, and ability to fulfil their compliance responsibilities under the DSA; ▪ The Head of the Compliance Function was an independent senior manager with a distinct responsibility for compliance; ▪ The Head of the Compliance Function had direct reporting lines to the management body and was empowered to raise concerns relating to Article 34 risks or DSA non-compliance without prejudice; ▪ The removal of the compliance officer was subject to prior approval by the management body. 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Inspected Mr. Hradecký's professional credentials disclosed in internal documentation and management submissions. It was confirmed that he possesses over 20 years of experience in governance, risk, and compliance; holds certifications in compliance implementation (ISO 37301), anti-bribery auditing (ISO 37001), internal auditing (ISO 19011), and business continuity management (ISO 22301). These qualifications support his technical and professional capacity to fulfil the DSA compliance role. 2. Reviewed the Compliance Statute and Policy documents which define the compliance function as independent, under the oversight of a senior officer who reports directly to the management body. Interview evidence further supported that the compliance officer has unmediated access to board-level discussions and escalates matters as needed. 		

<p>3. Verified the organisational structure, which indicated that the Compliance Officer is structurally segregated from operational departments (e.g. content, engineering, or commercial). The structure confirmed that no operational overlap existed.</p> <p>4. Confirmed during interviews that the Compliance Officer had not been removed or reassigned since appointment. Management confirmed that any removal would require formal board approval, as per internal policy.</p> <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures: N/A</p>	<p>Recommended timeframe to implement specific measures: N/A</p>

<p>Obligation: Article 41.3.</p>	<p>Audit criteria: Throughout the period, in all material respects, the designated compliance officer(s):</p> <ul style="list-style-type: none"> ▪ Cooperated with the DSC and the EC; ▪ Ensured systemic risks (Art. 34) were identified, reported, and mitigated through reasonable, proportionate, and effective measures (Art. 35); ▪ Organised and supervised activities related to the independent audit (Art. 37); ▪ Informed and advised management and staff about relevant DSA obligations; ▪ Monitored the provider’s compliance with DSA obligations; ▪ Where applicable, monitored compliance with commitments under codes of conduct (Art. 45–46) or crisis protocols (Art. 48). 	<p>Materiality threshold: N/A</p>
<p>Audit procedures, results and information relied upon:</p> <p>1. Inspected the governance section of the 2025 Risk Assessment Report confirming that the Compliance Officer (functioning as NKL’s second-line assurance unit) was responsible for ensuring the platform’s compliance with the DSA. The role combined the statutory Compliance Officer under Article 41 DSA and the internal Risk Assessor under the ISO 31000 framework, granting authority over all compliance assurance activities, including interaction with external regulators and auditors. The officer’s documented responsibilities included cooperation with competent authorities, identification and mitigation of systemic risks, supervision of audits, and internal training and advisory functions.</p> <p>2. Reviewed correspondence logs and interview notes confirming that the Compliance Officer and the Compliance Office monitored all requests for information from the EC following the platform’s designation. The interview with Compliance Officer confirms that the provider benefited from insights obtained through the requests of information sent by the EC” and integrated these into the 2025 assessment methodology. While no formal enforcement actions or crisis communications occurred, the Compliance Officer maintained readiness for regulatory engagement and served as the single point of contact for such cooperation.</p>		

3. Examined the 2024 and 2025 systemic risk assessments and supporting documentation, which demonstrate that the Compliance Officer ensured:
 - Systemic risks were identified and assessed through structured cross-functional workshops,
 - Mitigation measures were developed and documented in the Mitigation Measures Register, aligned with Article 35 DSA,
 - Annual updates and follow-up reviews were performed.
4. The audit confirmed that the Compliance Officer organised and supervised audit-related activities, including the external DSA compliance audit and internal readiness review. The Compliance Officer coordinated document provision and management responses to audit queries.
5. Verified that the Compliance Officer and compliance team-members regularly informed and advised senior management and operational teams on DSA obligations. Evidence from the governance section of the 2025 assessment shows that the compliance team chaired workshops and provided interpretive guidance to operational teams.
6. Confirmed that the Compliance Officer actively monitored providers ongoing compliance with DSA obligations through continuous oversight of systemic-risk management, moderation practices and reporting obligations. The Compliance Officer maintained ownership of the Risk Register, Mitigation Measures Register supervised annual reassessments and provided independent review of mitigation effectiveness. Monitoring was consistent with ISO 31000 principles of continuous improvement and proportional control.
7. Verified that, during the audit period, no binding or voluntary code of conduct (Articles 45-46) nor crisis protocol (Article 48) applied to the provider. Nonetheless, the Compliance Officer maintained a watching brief on EU-level developments. The Compliance Officer also established procedures to integrate such commitments into the compliance program if adopted in the future.
8. Through document review and interviews, confirmed that the same designated officer fulfilled all DSA compliance duties throughout the review period. No interruptions or delegations of the role were recorded.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. However, the formal documentation of DSA training initiatives could be strengthened.

<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Establish structured DSA training logs and maintain evidence of briefings across relevant teams. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>
--	---

<p>Obligation:</p> <p>Article 41.4.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The name and contact details of the head of compliance were formally communicated to the EC; 	<p>Materiality threshold:</p> <p>N/A</p>
--	--	---

	<ul style="list-style-type: none"> ▪ If applicable, the same communication was prepared for the DSC of the Member State of establishment. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Examined the provider's appointment records confirming the designation of Mr. David Hradecký as the head of compliance and statutory Compliance Officer under Article 41 DSA. Supporting documentation included internal governance approvals and the organizational chart. 2. Interviewed management, who confirmed that the contact information for the Compliance Officer was transmitted to the EC shortly after appointment. 3. Reviewed contextual documentation and legal analysis regarding the Czech Republic's national DSA implementation status. During the audit period, it was confirmed that: <ul style="list-style-type: none"> • The ČTÚ had been formally identified as the future DSC, but • The national implementing legislation was still pending enactment, and the DSC had not yet assumed operational supervisory powers or established an official intake mechanism for DSA communications. <p>Therefore, while the provider identified ČTÚ as the expected authority, no official communication channel existed through which contact details could be transmitted. Compliance Officer confirmed that the provider maintains readiness to provide the same information to the DSC immediately upon activation of its supervisory role.</p> 4. Reviewed provider's internal compliance procedures, which include a standing protocol for notification to competent authorities. The procedure ensures that any future updates to the Compliance Officer's designation or contact details will be communicated without delay to both the EC and the national DSC once operational. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>		
<p>Recommendations on specific measures:</p> <p>N/A</p>		<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>

Obligation: Article 41.5.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The management body defined and oversaw the governance arrangements ensuring independence of the compliance function; ▪ A clear division of responsibilities was maintained across functions; ▪ Safeguards to prevent conflicts of interest were established; ▪ The management body was accountable for the sound management of systemic risks under Article 34. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Examined the Compliance Policy and related Compliance Statute, which together define the governance structure for compliance under Article 41 DSA. 2. The documents confirm that the Compliance Function operates independently of operational and commercial departments and reports directly to Senior Management. The Compliance Officer's appointment and authority are explicitly recognized by the Senior Management, demonstrating that the governance arrangements were defined and overseen at board level. 3. The Compliance Policy establishes that the provider's Senior Management holds overall responsibility for DSA compliance and ensures that integrity, accountability, and transparency principles are upheld. This framework assigns the Senior Management explicit responsibility for ensuring the Compliance Function's independence, approving systemic risk assessments, and reviewing audit outcomes. 4. Reviewed internal role definitions and organizational structures described in the Compliance Policy: <ul style="list-style-type: none"> • The Compliance Officer oversees DSA compliance, risk management, and training. • Operational units (moderation, advertising, IT, product) implement measures within their domains but do not influence the Compliance Officer's oversight decisions. • Senior Management supervises compliance outcomes. This separation ensures a clear division of responsibilities, avoiding overlap between assurance and execution functions and maintaining objective internal control. 5. The Compliance Policy and Leadership Declaration both affirm that conflict-of-interest prevention is a core element of compliance governance. The Compliance Function has independent decision-making authority, unrestricted access to records, and cannot be overruled by operational teams. Interviews confirmed that no active or potential conflicts of interest were identified during the audit period. 6. Conducted interviews and reviewed governance records, which confirmed that during the assessment period: <ul style="list-style-type: none"> • The Compliance Officer has unmediated access to the Senior Management; • Risk assessment and audit results are discussed in structured management meetings; • The Compliance Function remained stable throughout the period (no reassignment or change in mandate); Conclusion:		

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation:

Article 41.6.

Audit criteria:

Throughout the period, in all material respects:

- The management body approved and reviewed, at least annually, the strategies and policies for identifying, managing, monitoring, and mitigating systemic risks under Article 34 DSA.

Materiality threshold:

N/A

Audit procedures, results and information relied upon:

1. Reviewed the 2024 Systemic Risk Assessment, which includes an approval block showing that the risk assessment and associated risk-management framework were signed and approved by the statutory representative of NKL Associates s.r.o. on 13 November 2024.
2. Reviewed the 2025 2nd Systemic Risk Assessment, which states that the assessment is the annual update to the prior year's risk assessment, prepared under ISO-aligned risk-management processes. The document contains a dedicated section describing the role of senior management, confirming that they:
 - approve the risk-management documentation;
 - endorse the systemic-risk strategy;
 - review the risk assessment annually; and
 - ensure appropriate resource allocation for risk mitigation.
3. Reviewed statements in both risk assessments confirming periodicity, including explicit references to the systemic-risk assessment being conducted annually, and forming part of a broader risk-register and mitigation-process review cycle. Both documents describe annual updates to the risk categories, methodologies, and mitigation strategies, indicating a recurring top-level review.
4. Reviewed the risk-governance framework integrated into both documents, which sets out that the Compliance Function prepares the annual risk assessment and reports directly to senior management. Senior management is documented as responsible for approving the risk-management strategy and validating the risk appetite and mitigation priorities for the platform. This governance architecture demonstrates embedded annual oversight.
5. Noted that dedicated board-meeting minutes or standalone approval resolutions were not included in the audit file. However, approval signatures in the 2024 risk assessment, together with the governance statements and annual-review structure described in the 2025 assessment, provide sufficient evidence that senior management reviewed and approved the systemic-risk strategies and policies during the examination period.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 41.7.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The management body devoted sufficient time to risk-related matters; ▪ It was actively involved in decisions related to risk management; ▪ Adequate resources were allocated for managing systemic risks identified in accordance with Article 34 DSA. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Reviewed the Risk Management Guideline. The document establishes the governance structure for systemic-risk management, designating Senior Management as the accountable body for approving systemic-risk assessments, mitigation priorities, and resource allocation.
2. The guideline explicitly confirms that Senior Management:
 - Sets risk appetite and validates all risk-management documentation,
 - Reviews and endorses the annual Systemic Risk Assessment and relevant registers,
 - Allocates necessary resources (staffing, tooling, and budget) to sustain risk-mitigation activities. These provisions evidence that the management body devoted structured time to risk oversight and decision-making during the audit period.
3. The Compliance policy links DSA risk governance directly to resource planning, requiring that staffing, technology tools, and advisory support correspond to the scale of systemic-risk exposure identified under Article 34 DSA. It also requires regular reporting from the Compliance Officer to Senior Management, ensuring informed resource allocation and board-level monitoring of risk trends. This confirms formal oversight mechanisms and active involvement of the Senior Management in risk-related decisions.
4. The framework defines the interrelation between the Compliance Function / Risk Assessor and Senior Management, establishing a two-line assurance model. The Compliance Function designs and executes the ISO 31000-based methodology, conducts risk workshops, updates the risk assessment relevant documentation, and reports directly to Senior Management. Senior Management reviews systemic-risk outputs, sets strategic priorities, and validates resource allocation.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 42.1.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider must demonstrate that it publishes transparency reports on a biannual basis, and within regulatory timelines; ▪ Reports must include all disclosures required under Article 15 and be publicly accessible. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Audit inspection of the XNXX Information Portal (<https://info.xnxx.com>) confirmed the existence of a dedicated “Mandatory Information / Reports” section. The webpage lists and hyperlinks the following reports:
 - June–December 2024 (first reporting period); and
 - January–June 2025 (second reporting period).

Version control dates confirmed that these documents were finalized within the regulatory timeframes required under Article 42(1). These reports demonstrate a biannual publication cycle. The level of detail and structure were consistent with the Article 15 and Article 42(1) standards.

2. Version-control and internal compliance logs demonstrated that each report was finalized and posted within two months of the close of its respective reporting period. The Compliance Office maintains a DSA deliverables calendar that schedules drafting, legal review, and management approval to ensure adherence to regulatory deadlines.
3. Direct access tests validated that transparency reports and user-metric disclosures are publicly viewable without authentication or geographic restriction. The accessibility path and consistent formatting demonstrate an institutionalized publication process rather than ad hoc reporting.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A
---	---

Obligation: Article 42.2.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Reports contained disaggregated information on moderation staffing by EU language; ▪ Qualifications, linguistic capacity, and training of staff were disclosed; ▪ Moderation accuracy metrics were presented by language group; ▪ The report was published in at least one official EU language. 	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. The following transparency reports were reviewed:
 - July – December 202 (first reporting period); and
 - January - June 2025 (second reporting period).
2. Each report included a section titled “Moderation Workforce and Linguistic Distribution”, which detailed the number of human moderators allocated per EU language. Data were presented as full-time equivalents (FTEs) and total staff counts across major EU linguistic groups (including English, French, German, Spanish, Polish, Czech, and Italian). The information demonstrated active coverage of multiple EU languages and confirmed that disaggregated workforce statistics were provided for the relevant period.
3. The reports included moderation performance metrics, including accuracy levels based on sample reviews, escalation statistics, and correction rates following user complaints. Where available, these metrics were disaggregated by language, particularly for high-traffic jurisdictions. However, in some instances, smaller language groups were aggregated due to insufficient volume. The methodology for calculating accuracy was explained, referencing internal audit procedures and human QA reviews.
4. Both transparency reports were published in English, which is an official language of the EU, satisfying the minimum publication requirement under Article 42(2). No evidence was found of supplementary translations for other EU audiences; however, accessibility through the XNXX information portal was verified, confirming compliance with publication standards.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Obligation:	Audit criteria:	Materiality threshold:
Article 42.3.	Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider included in its biannual transparency reports the average number of monthly recipients of the service; ▪ This data was broken down by each EU Member State, as required under Article 42(3) and in alignment with Article 24(2) DSA. 	N/A

Audit procedures, results and information relied upon:

1. The following transparency reports were reviewed:
 - July – December 202 (first reporting period); and
 - January - June 2025 (second reporting period).
2. Both transparency reports were reviewed for inclusion of user-metric disclosures. Each report contained a dedicated section presenting the average monthly recipients of the service. The data were presented in tabular form, showing the average number of monthly active users for each of the 27 EU Member States. Supporting notes included in the transparency reports explained how user metrics were determined. The calculation

<p>accounted for privacy-related limitations and adjustments for anonymous browsing sessions (as shown on the XNXX Information Portal).</p> <p>3. Both transparency reports were published in English, which is one of the official languages of the EU, meeting the publication-language requirement. The reports and user metrics were directly linked within the same section of the XNXX Information Portal, ensuring that both narrative transparency and quantitative user data were available to the public and regulators.</p> <p>4. The Compliance Officer confirmed that the average monthly recipient calculations are coordinated by the IT team.</p> <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.</p>	
<p>Recommendations on specific measures:</p> <p>N/A</p>	<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>

<p>Obligation:</p> <p>Article 42.4</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> ▪ The provider transmitted to the DSC of establishment and the EC, without undue delay: <ul style="list-style-type: none"> – a report setting out the results of the risk assessment; – the specific mitigation measures put in place; – the audit report; – the audit implementation report; – information about the consultations conducted in support of the risk assessments and design of the risk mitigation measures (if applicable); ▪ The provider made these information publicly available within three months of receiving the audit report. 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. The Compliance Officer confirmed the existence of a formal regulatory submission workflow, which governs document preparation, internal approval, and communication with the EC and the future Czech DSC (ČTU). The workflow specifies that all statutory submissions are to be made “without undue delay” once finalized and approved by Senior Management. 2. The compliance team confirmed that, as of the audit date, the initial audit under Article 37 DSA was ongoing and that no audit report or audit implementation report had yet been issued or received. As a result, the formal transmission of the full audit deliverables had not yet occurred, though preparatory documentation (risk assessment and mitigation summary) was made available internally in anticipation of submission. 3. In line with Article 42(4), the obligation to publish risk- and audit-related information only arises after receipt of the final audit report. Given that this was the provider’s first Article 37 audit, no such report had been received during the audit period. Accordingly, no statutory deadline for publication had yet commenced, and no publication obligation was active at the 		

time of review. The Compliance Officer confirmed readiness to make the required materials publicly accessible through the XNXX information portal (info.xnxx.com) within three months of audit completion.

4. Verified that the Compliance Function maintains a centralized repository for all Article 34-42 documentation and correspondence logs.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.

Recommendations on specific measures:

N/A

Recommended timeframe to implement specific measures:

N/A

Appendix 2 – Details on Obligations Outside the Scope of the Audit Assessment

Article	Rationale
13	The provider is established in the Czech Republic, with a registered office located at Krakovská 1366/25, Nové Město, 110 00 Praha 1. Therefore, the obligations under Article 13 do not apply to the provider during the examination period.
14.3	Based on the review of the provider's TOS (Article 2), the website prohibits the enter and use of the website for persons under the age of 18 and/or under the age of majority in the jurisdiction in which the person resides or from which is accessing the website. Given this restriction, the service is neither primarily directed at minors nor predominantly used by them, and therefore the obligation under Article 14(3) does not apply to the provider during the examination period.
16.3	Article 16(3) has solely a declaratory character and does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
17.5	Article 17(5) is solely descriptive in nature and does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
19	Article 19 is solely a conditional exclusion clause and does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
21.2-21.5	Articles 21(2), 21(3), 21(4), and 21(5) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
22.2-22.5	Articles 22(2), 22(3), 22(4), and 22(5) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
22.6	The provider does not have information including that a trusted flaggers has submitted a significant number of insufficiently precise, inaccurate or inadequately substantiated notices through the mechanisms referred to in Article 16.
22.7-22.8	Articles 22(7) and 22(8) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
24.4	Article 24(4) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
24.6	Article 24(6) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
25.3	Article 25(3) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
26.2	Based on the review of the provider's TOS (Article 7), users are explicitly prohibited from uploading or publishing content that constitutes commercial communications or advertisements. As a result, the obligation to provide functionality for user-declared commercial communications under Article 26(2) does not apply to the provider during the examination period.
28.4	Article 28(4) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.

29-32	The provider does not enable recipients of the service to conclude distance contracts with traders. Consequently, the obligations under Articles 29 to 32 do not apply to the provider during the examination period.
33	Article 33 does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
35.2-35.3	Articles 35(2) and 35(3) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
36.2-36.11	Articles 36(2), 36(3), 36(4), 36(5), 36(6), 36(7), 36(8), 36(9), 36(10), and 36(11) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
37.1	The audit was conducted as the provider's first independent audit in accordance with the specified requirements under Article 37. Therefore, the obligations under Article 37(1) were not applicable during the examination period.
37.2	The access conditions, cooperation measures, and any limitations or constraints encountered during the audit were formally addressed in Sections 7 ("Access and Cooperation") and 8 ("Limitations and Disclaimers") of the audit report.
37.3-37.5	Articles 37(3), 37(4), and 37(5) set requirements for the independent auditing organization. Assessing compliance with these provisions would constitute a self-audit by the auditing organization itself. Therefore, they are applicable and considered within the scope of the audit.
37.6	The audit was conducted as the provider's first independent audit in accordance with the specified requirements under Article 37. No audit report or audit implementation report had yet been submitted to the Commission. Therefore, the obligations under Article 37(6) were not applicable during the examination period.
37.7	Article 37(7) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
40.2	Article 40(2) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
40.4-40.7	During the audit period, these provisions were in progress but not yet applicable. As the obligations only become effective on 29 October 2025, these requirements were considered transitional and excluded from audit scope.
40.8-40.11	Articles 40(8), 40(9), 40(10), and 40(11) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
40.12	Due to the absence of an operational vetting authority in the Czech Republic, lack of certified researchers, and the pending adoption of technical rules by the European Commission, the obligations under Article 40(12) DSA are currently non-operational and therefore out of audit scope.
40.13	Article 40(13) does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
42.5	As confirmed in the audit procedures for Article 42(4), the provider had not yet received the audit report pursuant to Article 37(4) and thus was not required to publish any of the documentation listed in Article 42(4). As no public disclosure had occurred, the conditional exception set out in Article 42(5) regarding redaction of confidential or security-sensitive information had not been triggered.

43.1-43.7	Articles 43(1), 43(2), 43(3), 43(4), 43(5), 43(6), and 43(7) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
------------------	---

Appendix 3 – Template for the Audit Report Referred to in Article 6 of Delegated Act

Section A: General Information

1. Audited service:	
XNXX.com (adult-content video-sharing platform)	
2. Audited provider:	
NKL Associates s.r.o. (NKL)	
3. Address to the audited provider:	
Krakovská 1366/25, Nové Město, 110 00 Praha 1, Czech Republic	
4. Point of contact of the audited provider:	
Single point of contact for authorities: https://info.xnxx.com/authority-contact (web form)	
5. Scope of the audit:	
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 – the report provides a reasonable-assurance assessment of compliance with all obligations and commitments referred to in Article 37(1) DSA that are applicable to NKL.
i. Compliance with Regulation (EU) 2022/2065	
Obligations set out in Chapter III of Regulation (EU) 2022/2065:	
Audited obligation	Period covered
Section 1 (Arts 11-15) – obligations for all intermediary services Section 2 (Arts 16-18) – additional duties for hosting services / online platforms Section 3 (Arts 19-28) – additional duties for online platforms Section 5 (Arts 34-42) – VLOP-specific duties (systemic-risk management, data access, audits, etc.)	13 November 2024 – 13 November 2025
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
N/A: During the period under review NKL had not acceded to any code of conduct under Arts 45-46 DSA nor to a crisis protocol under Art 48, so no such commitments were audited.	N/A
6. a. Audit start date:	b. Audit end date:
13 October 2025 (fieldwork commenced)	10 November 2025 (fieldwork completion / "as-of" date for findings)

Section B: Auditing organization

1. Name(s) of organization(s) constituting the auditing organization:
CERTICOM s.r.o. (Commercial Register no. 35 987 211) – accredited conformity-assessment and assurance provider according to standard ISO /IEC 17021-1:2015 – together with its accredited certification body CERTICOM, Pod Donátom 907/5, 965 01 Žiar nad Hronom, Slovak Republic.
2. Information about the auditing team of the auditing organization:
Ing. Marián Illovský (lead auditor)
3. Auditors' qualification:
a. Overview of the professional qualifications of the individuals who performed the audit, including domains of expertise, certifications, as applicable:
Marián Illovský , a lead auditor, graduated from the University of Economics in Bratislava's Faculty of Economic Informatics, Department of Operational Research and Econometrics. With over two decades of experience in auditing and information security management, Marián has held various roles. Between 2004 and 2019, he served as the head of the internal IT audit unit at POŠTOVÁ BANKA in Bratislava, Slovakia, where he was responsible for developing the bank's IT audit function. From 2008 to 2022, he worked for EUROGIRO in Copenhagen, Denmark, as a member of the Security group. His role involved auditing all members worldwide. Since 2014, Marián has been a freelancer specialising in auditing of IT, IS, OT and cybersecurity. Additionally, from 2011, he has been an external expert and assessor for ISO 27001 for the Slovak National Accreditation Service in Bratislava, Slovakia. He has continued his work with ISO 20000-1, ISO 22301 and eIDAS. Furthermore, since 2017, he has also been an external expert and assessor for eIDAS at the Public Institute Slovenian Accreditation in Ljubljana, Slovenia. Marián holds several certifications, including Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Data Privacy Solution Engineer (CDPSE), Certified Information Security Manager (CISM), Certified cybersecurity auditor (Slovak certification), Certified cybersecurity manager (Slovak certification) and Global Industrial Cyber Security Professional (GICSP).
b. Documents attesting that the auditing organisation fulfils the requirements laid down in Article 37(3), point (b) of Regulation (EU) 2022/2065 have been attached as an annex to this report:

<ul style="list-style-type: none"> - Certificate of accreditation to carry out certification of quality management systems according to the ISO 9001:2015 No. : Q-003 - Certificate of accreditation to carry out certification of environmental management systems according to the ISO 14001:2015 No. : R-005, - Certificate of accreditation to carry out certification of occupational health and safety management system in accordance with requirements of standard ISO 45001:2018, No.: R-015 - Certificate of accreditation to carry out certification of Information Security Management System according to the ISO/IEC 27001:2022 No.: R-153 - Certificate of accreditation to carry out certification of anti-bribery management system in accordance with requirements of standard ISO 37001:2016 No.: R-136 <p>Information about certification body CERTICOM you can check on IAF (International Accreditation Forum) website direct link https://www.iafcertsearch.org/certification-body/147c1769-3026-55c0-97d0-607ccbd65996</p>
4. Auditors' independence:
<i>a. Declaration of interests</i>
CERTICOM s.r.o., its certification body and every member of the audit team declare that they: 1) held no financial, ownership or governance interest in NKL Associates s.r.o.; 2) received no other services, fees or gifts from the provider beyond the fixed audit engagement fee; 3) are free of any personal, family or employment ties with the audited provider.
<i>b. References to any standards relevant for the auditing team's independence that the auditing organization(s) adheres to</i>
IFAC Code of Ethics for Professional Accountants (IESBA) – parts relating to assurance engagements ISO /IEC 17021-1:2015, cl. 5 (impartiality) – requirements for certification- and audit bodies ISAE 3000 (Revised) – independence provisions for non-financial assurance
<i>c. List of documents attesting that the auditing organization complies with the obligations laid down in Article 37(3), points (a) and (c) of Regulation (EU) 2022/2065 attached as annexes to this report. Attachment 3 and 5 to Annex 1</i>
referred to in paragraph b) above
5. References to any auditing standards applied in the audit, as applicable:
ISAE 3000 (Revised) – International Standard on Assurance Engagements Commission Delegated Regulation (EU) 2023/6807 – specific DSA audit methodology ISO 19011:2018 – Guidelines for auditing management systems (used for sampling and interview technique)
6. References to any quality management standards the auditing organization adheres to, as applicable:
ISO /IEC 17021-1:2015 – Conformity assessment – Requirements for bodies providing audit and certification of management systems (accredited by SNAS – Slovak National Accreditation Service) Internal quality management system aligned to ISO 9001:2015, monitored through annual management reviews and SNAS surveillance audits.

Section C: Summary of the main findings

1. Summary of the main findings drawn from the audit (pursuant to paragraph 37(4), point (e) of Regulation (EU) 2022/2065) :
A description of the main findings drawn from the audit can be found in Appendix 1 of the Independent Assurance Report.
SECTION C.1: Compliance with Regulation (EU) 2022/2065
<i>a. Audit opinion for compliance with the audited obligations referred to in Article 37(1), point (a) of Regulation (EU) 2022/2065:</i>
The audit opinion for compliance with the audited obligations set out in Chapter III of Regulation (EU) 2022/2065 can be found in the Section Executive Summary of the Independent Assurance Report.
<i>b. Audit conclusion for each audited obligation:</i>
The audit conclusion for each audited obligation can be found in Appendix 1 of the Independent Assurance Report.
SECTION C.2: Compliance with voluntary commitments in codes of conduct and crisis protocols
<i>a. Audit opinion for compliance with the commitments made under the Code of Conduct or crisis protocol covered by the audit:</i>
N/A: No Union codes of conduct under Articles 45 or 46 or crisis protocols under Article 48 had been adopted by the audited provider during the examination period.
<i>b. Audit conclusion for each audited commitment:</i>
N/A – there were no commitments in scope.
SECTION C.3: Where applicable, explanations of the circumstances and the reasons why an audit opinion could not be expressed
A full description of the impediments and our alternative procedures is provided in the Appendix 1 of the Independent Assurance Report under the respective obligation headers.

Section D: Description of the findings: compliance with Regulation (EU) 2022/2065

SECTION D.1: Audit conclusion for obligation
I. Audit conclusion:
The individual conclusion (Positive, Positive with comments, or Negative) for every obligation audited under Article 37(1)(a) DSA is set out in Appendix 1 of the Independent Assurance Report.
II. Audit procedures and their results:
1) Description of the audit criteria and benchmarks (together the 'Specified Requirements'), and materiality threshold used by the auditing organization pursuant to Article 10(2), point (a) of this Regulation:

The auditors applied the following criteria:	
<ul style="list-style-type: none"> a) Relevant DSA legal obligations (including Articles 11–27, 34–42), b) Interpretative guidance from the European Commission, c) ISAE 3000 (Revised) as the assurance standard, d) Principles of legality, transparency, accountability, and proportionality under Article 3(2)(b) of the Delegated Regulation. 	
2) Audit procedures, methodologies, and results:	
<p>a. <i>Description of the audit criteria and benchmarks (together the 'Specified Requirements') and materiality threshold used by the auditing organization pursuant to Article 10(2), point (a) of this Regulation:</i></p>	
Details outlining the audit procedures conducted, the methodologies applied to evaluate compliance, and the rationale for selecting those specific approaches, including, where applicable, sample sizes determined, and sampling techniques used are provided in Appendix 1 of the Independent Assurance Report.	
<p>b. <i>Description, explanation, and justification of any changes to the audit procedures during the audit:</i></p>	
No material changes to the planned audit procedures occurred during the engagement. Minor adaptations were made to accommodate interface limitations or clarification requests, without impacting audit independence or scope.	
<p>c. <i>Results of the audit procedures, including any test and substantive analytical procedures:</i></p>	
Results included (i) structured interviews with internal teams (moderation, compliance, legal), (ii) review of TOS, transparency reports, and complaint-handling records, (iii) walkthroughs and live testing of reporting and moderation tools, (iv) sampling of moderation records, (v) functional and accessibility checks of user interfaces. These procedures informed the audit conclusions detailed in Appendix 1.	
3) Overview and description of information relied upon as audit evidence, including, as applicable:	
Details regarding the audit evidence reviewed, such as documentation, system outputs, and interviews, are provided in Appendix 1 of the Independent Practitioner's Assurance Report	
4) Explanation of how the reasonable level of assurance was achieved:	
Details regarding the methodology and procedures used to obtain a reasonable level of assurance are provided in the Appendix 1 of the Independent Assurance Report.	
5) In cases when:	
<p>a. <i>a specific element could not be audited, as referred to in Article 37(5) of Regulation (EU) 2022/2065, or an audit conclusion could not be reached with a reasonable level of assurance, as referred to in Article 8(8) of this Regulation, provide an explanation of the circumstances and the reasons:</i></p>	
An account of any circumstances that limited auditability or prevented the issuance of a conclusion with reasonable assurance is set out in the Appendix 1 of the Independent Assurance Report.	
6) Notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit.	
All relevant system updates and feature modifications introduced during the audited period, along with an explanation of how they were considered in the audit approach, are described in the Appendix 1 of the Independent Assurance Report.	
7) Other relevant observations and findings:	
Supplementary findings and contextual observations made during the audit are summarised in the Appendix 1 of the Independent Assurance Report.	
SECTION D.2: Additional elements pursuant to Article 16 of this Regulation	
1) An analysis of the compliance of the audited provider with Article 37(2) of Regulation (EU) 2022/2065 with respect to the current audit:	
The access conditions, cooperation measures, and any limitations or constraints encountered during the audit were formally addressed in Sections 7 ("Access and Cooperation") and 8 ("Limitations and Disclaimers") of the audit report.	
2) Description of how the auditing organization ensured its objectivity in the situation described in Article 16(3) of the Delegated Regulation:	
N/A: The auditing organisation had not conducted any prior audits under Article 37(2) for this provider.	

Section E: Description of the findings concerning compliance with codes of conduct and crisis protocol

N/A, no codes of conduct and crisis protocols were adopted in the evaluation period.

Section F: Third parties consulted

N/A, no third parties were consulted.

Section G: Any other information the auditing body wishes to include in the audit report (such as a description of possible inherent limitations).

Please refer to the Independent Assurance Report.t for additional information.

Date:	13.11.2025	Signed by:	Ing. Marek Krajčov, company manager
Place:	Bratislava, Slovakia	In the name of:	CERTICOM s.r.o.
		Responsible for:	Entire engagement

Appendix 4 – Audit Risk Analysis

1. Introduction

This Annex presents the auditor’s assessment of risks that could affect the ability to provide a reasonable assurance conclusion on the compliance of NKL Associates s.r.o., provider of the platform XNXX.com, with its obligations under Regulation (EU) 2022/2065 (Digital Services Act, “DSA”). The purpose of this Annex is to identify and contextualize audit risks encountered during the engagement, assess their impact on the audit process and outcomes, and transparently communicate any limitations relevant to the assurance opinion.

The assessment is provided in accordance with Article 3(2)(a) of Commission Delegated Regulation (EU) 2023/6807, and follows the principles of professional skepticism, proportionality, and audit independence.

2. Scope and methodology

The audit covered the compliance period from 13 November 2024 to 13 November 2025, corresponding to the first full year of DSA compliance obligations following the platform’s designation as a Very Large Online Platform (VLOP) on 10 July 2024.

The risk analysis reflects:

- the nature of the platform, including its public accessibility, user-generated content, sensitive content classification, and user privacy emphasis,
- the size, complexity, and maturity of the platform’s compliance function,
- the degree of formalization of internal policies, procedures, controls, and data infrastructure supporting DSA compliance.

Audit procedures included:

- document review, structured interviews, and process walkthroughs with relevant personnel,
- live observation of content moderation and complaint-handling interfaces,
- sampling and inspection of backend processes and decision-tracking,
- guided access to platform functionalities and test accounts.

Each applicable DSA article was assessed using the following structure:

- a summary of the regulatory obligation,
- identified audit limitations encountered during the engagement,
- a conclusion on residual risk and its impact on the assurance conclusion.

3. Risk classification and interpretation

The assessment applies the following two-dimensional scale:

- **Residual risk:**
 - *Low* - minor procedural or documentation limitations that do not affect control operation or legal adequacy
 - *Medium* - gaps in documentation, systematization, or audit trail that may introduce variability in compliance effectiveness

- *High* - structural or systemic concerns with legal compliance or control implementation (not observed in this audit)
- **Impact on assurance:**
 - *Low* - no material effect on the auditor’s ability to issue a positive assurance conclusion
 - *Medium* - requires additional explanatory context; may affect the scope of the opinion in isolated areas
 - *High* - would preclude a positive conclusion; triggers a qualified or adverse opinion (not applicable here)

4. Audit limitations

The auditor did not have direct backend system access, nor were automated test logs or historical data queries available for all systems. However, these limitations were mitigated through:

- Supervised access to live system environments
- Interviews and demonstrations with relevant personnel
- Random sampling of frontend and backend outputs
- Contextual triangulation with policies and logs

In cases where compliance processes were manual, undocumented, or under development, the auditor evaluated both the operational reality and the platform’s demonstrated intent and progress toward maturity.

5. Interpretation of findings

Where evolving compliance was observed - such as in areas undergoing documentation standardization or system development - these were treated as *low or medium residual risk* based on evidence of implementation, intention, and control effectiveness.

No finding reached a level that would prevent a positive assurance conclusion.

6. Audit risk assessment

Overview

DSA article	Residual risk level	Impact on assurance
Article 16	Low	Low
Article 20	Low	Low
Article 27	Medium	Medium
Article 34(1)	Low	Low
Article 34(2)	Low	Low
Article 34(3)	Low	Low
Article 35	Low	Low
Article 36	Low	Low
Article 42	Medium	Medium

Article 16 – Notice and Action mechanism

Regulatory obligation summary

Platforms must implement easily accessible and user-friendly notice and action mechanisms that allow users or entities to notify the presence of allegedly illegal content. Notices must be processed diligently

Audit limitations

Auditors did not have direct access to backend logs but were allowed to observe live operations and sampling. All data access was guided.

Conclusion on risk level and assurance impact

Despite some procedural informality, the implementation is functional and adequate. No systemic gaps identified.

Residual risk: Low

Impact on assurance: Low

Article 20 – Internal complaint-handling system

Regulatory obligation summary

VLOPs must establish an internal complaint-handling system allowing users to contest moderation decisions and seek redress within clearly defined timelines.

Audit limitations

Back-office complaint logs are maintained semi-manually. Future systematization may enhance auditability.

Conclusion on risk level and assurance impact

Process meets the legal requirement. Documentation maturity is improving.

Residual risk: Low

Impact on assurance: Low

Article 27 – Recommender system transparency

Regulatory obligation summary

Platforms must explain how recommender systems operate and provide at least one option that does not rely on profiling.

Audit limitations

Lack of backend access or testing audit trail; reliance on staff demonstrations and frontend behavior.

Conclusion on risk level and assurance impact

Transparency achieved through interface; backend limitations reduce auditability.

Residual risk: Medium

Impact on assurance: Medium

Article 34(1) – Systemic risk assessment

Regulatory obligation summary

VLOPs must conduct systemic risk assessments, focusing on dissemination of illegal content, impact on minors, public discourse, and fundamental rights.

Audit limitations

None material; full documentation and walkthrough were provided.

Conclusion on risk level and assurance impact

Mature and well-aligned with regulatory requirements.

Residual risk: Low

Impact on assurance: Low

Article 34(2) – Mitigation of systemic risks

Regulatory obligation summary

Providers must identify and implement appropriate mitigation measures to address the systemic risks assessed.

Audit limitations

Observed documentation was sufficient but lacked automation or full traceability.

Conclusion on risk level and assurance impact

Mitigation practices are structured but can benefit from systematization.

Residual risk: Low

Impact on assurance: Low

Article 34(3) – Testing of systemic risk mitigations

Regulatory obligation summary

VLOPs must test the effectiveness of their systemic risk mitigations, including through simulations and case studies.

Audit limitations

Absence of documented test plans or results for specific mitigation strategies.

Conclusion on risk level and assurance impact

Structured testing of mitigation effectiveness is under development.

Residual risk: Low

Impact on assurance: Low

Article 35 – Crisis response mechanism

Regulatory obligation summary

Platforms must have protocols in place to act immediately upon identification of crisis situations impacting public security or health.

Audit limitations

No practical invocation of protocols observed (crisis-free audit period).

Conclusion on risk level and assurance impact

Policy is present and structured; readiness can be demonstrated.

Residual Risk: Low

Impact on Assurance: Low

Article 36 – Data access for supervisory authorities

Regulatory obligation summary

VLOPs must provide access to data and documentation to competent authorities upon request.

Audit limitations

None; documentation was available and aligned with requirements.

Conclusion on risk level and assurance impact

Compliant and procedurally mature.

Residual risk: Low

Impact on assurance: Low

Article 42 – Transparency reporting

Regulatory obligation summary

VLOPs must publish detailed transparency reports on content moderation, notices, and enforcement actions, including use of automated tools.

Audit limitations

Semi-manual data extraction and compilation methods.

Conclusion on risk level and assurance impact

Reports are complete and compliant, though backend automation can be improved.

Residual Risk: Medium

Impact on Assurance: Medium