

WebGroup Czech Republic a.s.

Independent Audit Report on XVideos.com

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

Report date: 21 April 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	5
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	83
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 XVideos.com - WebGroup Czech Republic a.s.

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 WebGroup Czech Republic a.s.

1. Introduction

We have been engaged by WebGroup Czech Republic a.s. (“WGCZ”, 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 XVideos.com (“platform”), operated by WGCZ. On 23 December 2023, the European Commission designated XVideos.com as a VLOP under Article 33 of the DSA. This designation triggered enhanced compliance obligations, effective from 23 April 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 23 April 2024 to 23 April 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 WGCZ as the provider of XVideos.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

XVideos.com is an adult content platform operated by WGCZ, 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 Member States of the European Union, 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 23 April 2024 to 23 April 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 XVideos.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 November 2024 and March 2025 and included the following procedures:

- structured interviews with senior management, content moderation team, compliance personnel, notice and complaint 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 WebGroup Czech Republic a.s., provider of XVideos.com, a very large online platform (VLOP) designated by the European Commission on 23 December 2023. The audit covers the period from 23 April 2024 to 23 April 2025, corresponding to the first year of enhanced obligations under the DSA.

XVideos.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, XVideos.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** - 32 obligations (50%) were assessed as fully compliant (“Positive”). These obligations are supported by mature and consistently implemented processes. Noteworthy examples include the notice-and-action mechanism (Art. 16), which met 100% of response-time requirements across all sampled cases; the internal complaints handling system (Art. 20(1)), which demonstrated timely, transparent redress procedures; the transparency of recommender systems (Art. 27(1)), which is integrated into user interfaces with appropriate parameter disclosures; and the biannual transparency reporting (Art. 42), which was found to be complete, accessible, and aligned with regulatory expectations. The provider also satisfied core disclosure duties (Arts. 11–12), implemented appropriate ad-labeling practices (Art. 26), and demonstrated working governance structures (Art. 41).
- **POSITIVE WITH COMMENTS** - 24 obligations (38%) were rated “Positive with comments”, reflecting that while the essential compliance threshold has been met, there remain procedural or operational opportunities for enhancement. These include, for instance, the systemic risk mitigation obligations (Arts. 34(1), 34(2)), where risk assessments were performed and mitigation was underway, but internal documentation and process standardisation lagged in approximately 39% of reviewed cases. Similarly, recommender system explainability (Art.

27(2)), while functional, could benefit from improved interface visibility and clearer default setting disclosures. In some cases, automated content moderation systems were in place but lacked comprehensive documentation or explicit user-facing transparency. These findings indicate maturity gaps, not failures, and none rise to the level of material non-compliance.

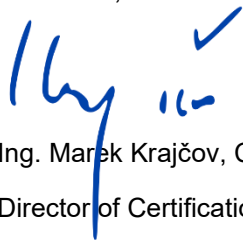
- **NEGATIVE** - 8 obligations (12%) were assessed as “Negative”, meaning the provider did not yet meet the minimum legal or functional adequacy standards set out by the DSA. These cases primarily concern obligations with technical or structural dependencies that have not yet been fully operationalised. Specifically, Article 34(3), which requires regular testing and auditing of algorithmic systems, was not implemented at the time of audit; evidence of testing regimes, version tracking, or audit trails for the recommender system was either incomplete or absent. Other negative findings included the lack of a trusted-flagger escalation channel (Art. 22(1)), no established process for identifying and suspending users for frequent misuse (Art. 23), and incomplete suspension data in transparency reporting (Art. 24(1)). Importantly, these gaps were not systemic in nature, did not result in immediate user harm or regulatory risk, and have been acknowledged by the provider with remediation measures underway. Implementation roadmaps for these items were provided and are scheduled for delivery within the next audit cycle. These issues are not considered systemic and are subject to roadmap-based implementation in Q3 2025.

The audit concludes that **WGCZ 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 21 April 2025



Ing. Marek Krajčovič, Company manager

Director of Certification body CERTICOM

Appendix 1 – Conclusions and Test Procedures per Obligation

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 Member States' authorities, the Commission 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: <ol style="list-style-type: none"> 1. Conducted a walkthrough of the provider's website and confirmed that a single point of contact for competent authorities accessible online through the dedicated form located at: https://info.xvideos.net/authority-contact 2. Navigated the website interface and confirmed that the contact point is accessible via the "More..." link in the footer of each page, followed by navigation through the "Support" section and selecting "Contact Us." Authorities are then instructed to choose the option "Contact Point for Authorities," which opens the relevant form. 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), 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. Conducted a walkthrough of the provider's website and confirmed that a single point of contact for competent authorities accessible online through the dedicated form located at: <https://info.xvideos.net/authority-contact>
2. Navigated the website interface and confirmed that the contact point is accessible via the "More..." link in the footer of each page, followed by navigation through the "Support" section and selecting "Contact Us." Authorities are then instructed to choose the option "Contact Point for Authorities," which opens the relevant form. Confirmed that the form is clearly titled to ensure continued visibility and usability for external stakeholders.
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), 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:	Audit criteria:	Materiality threshold:
Article 11.3	<p>Throughout the period, in all material respects:</p> <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.	N/A

Audit procedures, results and information relied upon:

1. Conducted a walkthrough of the provider's website and confirmed that a single point of contact for competent authorities accessible online through the dedicated form located at: <https://info.xvideos.net/authority-contact>
2. Navigated the website interface and confirmed that the contact point is accessible via the "More..." link in the footer of each page, followed by navigation through the "Support" section and selecting "Contact Us." Authorities are then instructed to choose the option "Contact Point for Authorities," which opens the relevant form. Confirmed that the form is clearly titled to ensure continued visibility and usability for external stakeholders.
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), 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.
6. Verified that both the form and the TOS provide information about specified languages that can be used to communicate with the designated point of contact. Confirmed that communication in English and Czech is accepted.
7. Verified that Czech is one of the official languages of the Member State where the provider has its main establishment (Czech Republic), and that English is broadly understood by Union citizens.

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	<p>Throughout the period, in all material respects:</p> <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 designated point of contact for service recipients, available at: <https://info.xvideos.net/contact>.
2. Examined the publicly available TOS (ToS), specifically Article 12, which states that “the requests are handled in a timely manner, not solely on the basis of automated means”.
3. Examined Article 12 of the publicly available TOS (ToS), which describes communication channels for general inquiries and specific categories of user requests. Confirmed that the provider distinguishes between different types of communication and provides specialized contact forms: A contact point for user available at <https://info.xvideos.net/contact>; a takedown form for copyright infringement reports available at <https://info.xvideos.com/takedown>; a form for reporting inappropriate content at <https://info.xvideos.com/takedown-amateur>.
4. Review of the ToS confirmed that the links provided correspond to the publicly available form on the website.
5. Navigated the website interface and confirmed that the contact point is accessible via the “More...” link in the footer of each page, followed by navigation through the “Support” section and selecting “Contact Us.” Authorities are then instructed to choose the option “Contact Point for Users,” which opens the relevant form.
6. Confirmed that the form is clearly titled to ensure continued visibility and usability. Verified that the contact form includes clear guidance for users on how to fill in the form.
7. Observed that the provider does not publicly specify how incoming messages are processed (e.g. expected response time, responsible unit), which may reduce user clarity regarding follow-up. Additionally, while English and Czech appear to be accepted, this is not explicitly stated for user-facing communication channels.

Conclusion:

Positive with comment – In our opinion, the audited provider complied with this Specified Requirement during the audit 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 (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.

Obligation:	Audit criteria:	Materiality threshold:
Article 12.2	Throughout the period, in all material respects: <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.	N/A

Audit procedures, results and information relied upon:

1. Conducted a walkthrough of the provider's website and confirmed that a public contact form for authorities is available at: <https://info.xvideos.net/contact>.
2. Navigated the website interface and confirmed that the contact point is accessible via the "More..." link in the footer of each page, followed by navigation through the "Support" section and selecting "Contact Us." Authorities are then instructed to choose the option "Contact Point for Users," which opens the relevant form. The form is clearly titled to ensure continued visibility and usability.
3. Examined Article 12 of the publicly available TOS (ToS), which describes communication channels for general inquiries and specific categories of user requests. Confirmed that the provider distinguishes between different types of communication and provides specialized contact forms: A contact point for user available at <https://info.xvideos.net/contact>; a takedown form for copyright infringement reports available at <https://info.xvideos.com/takedown>; a form for reporting inappropriate content at <https://info.xvideos.com/takedown-amateur>.
4. Review of the ToS confirmed that the links provided correspond to the publicly available form on the website.
5. Confirmed that the form is clearly titled to ensure continued visibility and usability. Verified that the contact form includes clear guidance for users on how to fill in the form.

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 14.1	<p>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 EEA;▪ The TOS must be drafted in language that is clear, intelligible, user-friendly, and unambiguous, ensuring that an average user can comprehend the key provisions;▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Auditors accessed the publicly available TOS on the provider via the "Legal Stuff" section, available at: <https://info.xvideos.net/legal/tos/>. The TOS were reviewed in both the complete and summary versions.
2. Chapter 8 of the TOS outlines content-related policies and restrictions. It clearly prohibits illegal content and sets out the basis for the removal of such content. Additionally, it describes grounds for suspending or terminating user access (e.g. repeated violations, serious breaches of legal provisions). The policy is articulated using specific, legally grounded terminology.
3. Within the same section (Chapter 8), the TOS indicate that the moderation process involves a combination of automated detection tools and human moderation. Importantly, the final decision to remove or restrict content is made by a human reviewer. The process is described as a layered approach, which aligns with DSA transparency standards.
4. Chapter 13.1 describes the availability of an internal complaint mechanism for users within the European Economic Area (EEA). The TOS state that users can challenge content removals, account suspensions, and other moderation decisions. Details are provided regarding how users may submit a complaint and expected response timeframes.
5. The audit team assessed the linguistic quality of the English version of the TOS. While the document follows a legalistic structure typical for platforms handling sensitive or regulated content, the wording is logically organized into titled sections with accessible headers. While some phrasing could be more simplified, the document overall satisfies the standard of intelligibility for a reasonably informed user.
6. Verified that both the full and summary versions of the TOS are published in all 24 official EU languages. Formats reviewed included HTML (on the website) and PDF downloads, which are structured and readable by machine tools. This complies with the DSA requirement for machine-readable access.
7. Additional verification activities:
 - Reviewed update history of the TOS to confirm regular maintenance and alignment with legal frameworks;
 - Confirmed that the ToS are linked from the footer on every page of the provider, ensuring consistent accessibility;
 - No indications were found of conflicting or ambiguous information between the summary and full version regarding moderation policies

Conclusion:

Positive – In our opinion, the Specified Requirements were met during the Evaluation 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);	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

	<ul style="list-style-type: none"> ▪ 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. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Interviewed responsible personnel and confirmed the existence of an established internal process to review and update the TOS when relevant changes occur. 2. Verified that significant changes are defined in internal documentation and that the Legal and Compliance teams are responsible for identifying, reviewing, and publishing update. 3. Inspected the public webpage [https://info.xvideos.net/legal/tos/] and verified that the updated TOS, including effective dates, is published in 24 official EU languages and is accessible via the provider's footer across all pages. 4. Confirmed that, given the absence of user registration for the majority of recipients of the service, individual notifications (e.g. email, pop-ups) are not technically feasible. 5. Found that the provider reasonably compensates for this by ensuring permanent, transparent, and machine-readable access to the latest TOS. 6. Inspected the Chapter 16, section "Summary of Recent Changes" within the TOS, which outlines latest updates made to the TOS. Verified that this section includes both the "effective date" and the "last amended" date, thereby ensuring transparency of modifications in accordance with the requirement. <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 14.4</p>	<p>Audit criteria: Throughout the period, in all material respects:</p> <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. 	<p>Materiality threshold: N/A</p>
--	---	--

Audit procedures, results and information relied upon:

1. Performed interviews with content moderation and compliance personnel to understand the measures implemented by the provider to ensure that restrictions under Article 14(1) were applied diligently, objectively, and proportionately.
2. Identified that the provider currently does not have any active policy, tooling, or procedure to detect or suspend users who submit manifestly unfounded notices.
3. Reviewed the moderation tooling and ticketing systems and confirmed the presence of structured moderation workflows combining human oversight with supporting automation. Verified that final enforcement decisions were human-led and linked to traceable logs.
4. Reviewed platform transparency reports (February–May and June–December 2024), which detailed content moderation actions, allocation of moderators by language, and escalation procedures.
5. Noted that although standard operating procedures exist, no formal internal document describes the complete lifecycle of a notice, moderation roles and responsibilities, escalation pathways, or automation triggers. The absence of a unified guidance document limits audit readiness and process consistency.
6. Reviewed the complaint-handling system and verified that while the system processes inbound complaints, it lacks mechanisms for identifying recurrent misuse. There is no evaluation of submission frequency or accuracy per user.
7. Confirmed availability of appeal options from both platform interface and email notifications.
8. While the platform removes accounts for severe violations, it does not perform the structured, multi-factor analysis required before suspending users based on repeated or abusive behaviour under Articles 23.1 and 23.2.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The content moderation workflow is human-led, enforcement decisions are documented diligently, and escalation procedures for complex or sensitive cases are followed. However, the absence of a formal internal guidance document describing the full moderation lifecycle and the lack of controls to detect misuse of the notice or complaint-handling systems represent material documentation and governance deficiencies.

Recommendations on specific measures:

- Develop and formalize a Moderation and Notice Lifecycle Framework that clearly outlines roles, decision criteria, escalation logic, and automation thresholds.
- Implement mechanisms to log and evaluate notice originators and complaint sources over time to detect repeated misuse or manifestly unfounded submissions.
- Establish structured policies for user suspension in cases of abuse of the content reporting or complaint functions.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 14.5	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Accessed the publicly available summary of TOS through the "Legal Stuff" section of the provider's website: https://info.xvideos.net/legal/tos/. The TOS were reviewed in both their complete and summary versions. 2. Verified that the summary of TOS includes an overview of all full version TOS Chapters including summarizing text and useful links to contact forms and parental controls. 3. Verified that Chapter 13 includes a summary of the internal complaint-handling system and available dispute resolution mechanisms, including arbitration and out-of-court settlement options. 4. Assessed the linguistic clarity of the English version of the summary of TOS and determined that it was structured in plain, intelligible language appropriate for an average consumer. Section headers are clearly labeled, and legal concepts are explained in simplified terms. 5. Verified that the summary of TOS is made available both in HTML format on the website and as downloadable PDFs. Such formats are considered structured and readable by machine tools. <p>Conclusion: Positive – In our opinion, the Specified Requirements were met during the Evaluation Period, in all material respects.</p>		
Recommendations on specific measures: N/A		Recommended timeframe to implement specific measures: N/A

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:

1. Conducted a walkthrough of the provider's website at <https://info.xvideos.net/legal/tos/> and verified that the TOS are made available in all 24 official EU languages.
2. Verified that the language selection is enabled through a drop-down menu, displaying each option with the corresponding country flag and the language name written in its official form.

Conclusion:

Positive – In our opinion, the Specified Requirements were met during the Evaluation 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:
 - February–May 2024 (first reporting period); and
 - June–December 2024 (second reporting period).
2. Confirmed both reports are publicly available in PDF format, accessible via official channels. The June - December report demonstrated notable improvement in granularity, structure, and explanatory depth over the earlier version.
3. Confirmed publication frequency exceeds DSA requirements: The provider issues biannual reports, fulfilling and surpassing the Article 15(1) obligation of an annual report
4. 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.
5. The audit verified that no removal orders under Article 9 DSA were received during either reporting period. The provider disclosed eight information orders under Article 10 in the second report and reported an average response time of 15 days. However, the reports do not disaggregate these requests by Member State or content category, nor do they report median processing times, as explicitly required by the regulation. The first report did not include this category at all, as the second report does meet these criteria. The provider has made a material improvement in this area compared to the first reporting cycle.
6. 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 reports confirmed that no notices were submitted by trusted flaggers. However, the provider did not clearly differentiate whether actions taken were based on legal requirements or the provider's TOS, which is a material shortfall in relation to the DSA's requirements.
7. The second report notably improves 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.

The report categorizes these measures by content type and provides a basic matrix on content visibility impacts. This level of detail was absent from the first report, which only briefly mentioned moderation practices in general terms. However, even in the improved second report, there remains insufficient detail on moderator training, internal consistency checks, or oversight procedures.
8. Only the June – December 2024 report contains relevant data on internal complaint-handling systems. It outlines the number of complaints received, reasons for submission, decisions taken, reversal rates, and median resolution times. This inclusion represents a positive step toward alignment with Article 15 and Article 20. In contrast, the earlier report did not mention complaints, which indicates a failure to meet this requirement for that period.
9. Both reports describe the general use of automated tools in content moderation, particularly for triage and detection. The second report includes 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. However, neither report provides error rates, accuracy indicators, or 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 made visible progress in meeting the transparency requirements of Article 15 DSA, particularly with the release of the June – December 2024 report. The provider has established a biannual reporting cycle, which demonstrates proactive engagement with regulatory obligations. The second report addresses many of the gaps present in the first and provides significantly more detailed disclosures.

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.
- Although the reports describe the use of automated content moderation tools and the role of human review, they do not disclose accuracy metrics, error rates, or performance validation methods.
- The second report briefly refers to the existence of human moderators but does 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) 2024/2835 ¹, 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.
- Disclose accuracy metrics and error rates for automated moderation tools: The provider should publish (i) estimated accuracy indicators (e.g. precision, recall), (ii) false positive/negative rates, (iii) details of internal or third-party validation studies, and (iv) safeguards, such as mandatory human review for sensitive content.
- 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 9 (nine) 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

Obligation: Article 16.1	Audit criteria: Throughout the period, in all material respects: <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). 	Materiality threshold: N/A
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Reviewed the TOS, specifically the section "Notice and Action Procedure." The TOS include a structured notice and action process. This mechanism applies to both copyrighted and non-copyrighted content. Users can report content by: <ul style="list-style-type: none"> ▪ Using the "Report" Button available on each video page. ▪ Filing a dedicated abuse reporting form: https://info.xvideos.net/takedown-amateur <p>The copyright violations, a separate DMCA-based form is provided https://info.xvideos.com/takedown.</p> 2. Reviewed transparency reports published by WebGroup Czech Republic, a.s. for: <ul style="list-style-type: none"> ▪ February–May 2024 (first reporting period); and ▪ June–December 2024 (second reporting period). <p>These reports provided data on notice volumes, categories of content reported (e.g. CSAM, hate speech, copyright), and action outcomes. The second report offered more granular insight into the moderation process and the volume of notices received.</p> <p>Both reports confirm that the provider has implemented two distinct mechanisms enabling users and third parties to report suspected or alleged illegal content a "Report" button located directly below each video, and an "Abuse Reporting Form" accessible via the "Content Removal" section.</p> 3. Reviewed public-facing interfaces across multiple access points. Navigated the provider on desktop (Chrome, Firefox) and mobile browsers (iOS Safari, Android Chrome). On all tested versions, a "Report" button was visible underneath each individual video. This button is positioned adjacent to the title and engagement metrics and is clearly labelled. Confirmed that clicking the button leads to a streamlined submission interface, offering a dropdown menu of issue types, a free text field for contextual information, and fields for optional contact information (name and email). 4. Accessed and tested the "Abuse Reporting Form" via the "Content Removal" section. The form allows users to enter a reasoned explanation, specify the exact URL of the content in question, and provide contact details. Both reporting pathways are accessible without login. 5. Verified functionality across devices and interfaces. No issues encountered across standard desktop and mobile browsers. The "Report" button and form were accessible without errors and required no additional software, registration, or CAPTCHA verification. Confirmed that reports could be submitted exclusively via electronic means. 6. An organizational chart for the moderation function has been obtained, in which the roles associated with processing notifications are clearly distributed. All notices are processed 		

exclusively by human moderators, no automated or partially automated systems are used to decide or respond to reports.	
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 16.2	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Reviewed the TOS, specifically the section "Notice and Action Procedure." The TOS state that to be valid, a report must include: <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. <p>The TOSs explicitly warns that failure to include this information may result in the notice being delayed or invalidated.</p> 2. Accessed the platform interfaces as end users to evaluate the usability and data fields of both reporting mechanisms available on the platform: <ul style="list-style-type: none"> ▪ The contextual "Report" button beneath each video, and ▪ The dedicated "Abuse Reporting Form" found under the "Content Removal" section. <p>For both channels:</p> <ul style="list-style-type: none"> ▪ The forms present a dropdown of predefined violation categories: child sexual abuse material (CSAM), non-consensual content (NCII), hate speech, copyright, and others; ▪ Once a category is selected, a free-text field becomes available for the user to provide a reasoned explanation of why the content is suspected to be illegal (16.2(a)). Guiding text encourages specificity; ▪ When the user accesses the form via the Report button under a video, the system automatically captures and pre-fills the precise URL and video identifier (16.2(b)); ▪ The Abuse Reporting Form also contains a mandatory field for the user to manually paste the URL when reporting outside the content view; 		

<ul style="list-style-type: none"> ▪ Optional fields are provided for entering name and email address, with guidance about the consequences of leaving this blank (e.g., no confirmation or decision follow-up) (16.2(c)); ▪ Before submission, users are required to check a confirmation box that explicitly states: <i>"I confirm that I submit this report in good faith and that the information I provide is accurate to the best of my knowledge."</i> ((16.2(d))). <p>3. The audit reviewed February – May 2024 transparency report, which described general functionality of reporting tools, and June–December 2024 report, which provided more detailed breakdowns. The second report included illustrative summaries of how illegal content reports are classified, processed, and triaged, validating the system's capacity to gather all elements defined under Article 16.2.</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>	
Recommendations on specific measures: N/A	Recommended timeframe to implement specific measures: N/A

Obligation: Article 16.4	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Reviewed the TOS, specifically the section "Notice and Action Procedure." The TOS state that notifiers who provide an email address will receive confirmation of receipt and notification about the outcome of their report. Affected uploaders located in the EEA receive a statement of reasons if their content is removed or restricted. Both parties have the right to appeal via the internal complaint-handling system described in Chapter 13.1. of TOS.
2. Conducted direct walkthroughs of the content reporting mechanism available on the provider during the examination period. Using test accounts, the team submitted multiple notices under varying content categories (e.g., copyright infringement, CSAM, hate speech). For each submission where an email address was entered, the team received a confirmation email within one minute, confirming that the provider had received the report. These emails contained basic metadata.
3. Verified that the provider uses an automated trigger to initiate confirmation emails upon successful submission. The system is fully automated, not reliant on manual moderation review, and operates independently from decision workflows.
4. No user complaints were recorded in the June–December 2024 transparency report regarding missed confirmations. The February–May 2024 report did not reference confirmation-of-receipt practices. The June–December 2024 transparency report confirmed that confirmation emails are issued automatically when a contact email is provided. However, during testing and interviews, it was observed that no mechanism exists to verify the accuracy of email input at the time of submission (e.g., typo detection or domain validation). As a result, confirmation emails may silently fail if the user mistypes their email address, without any alert or fallback.

Conclusion:

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

Recommendations on specific measures:

While no material deficiencies were identified, the following opportunity for improvement is suggested:

- Implement real-time validation or verification of email input in the reporting interface (e.g., format check, typo detection, or optional email confirmation field) to reduce the risk of silent delivery failures.

Recommended timeframe to implement specific measures:

It is recommended to address the improvement opportunity within the next 12 months

Obligation:	Audit criteria:	Materiality threshold:
Article 16.5	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.	A performance materiality threshold of 5 % was applied for this obligation.

Audit procedures, results and information relied upon:

1. Inspected transparency reports published for February–May 2024 and June–December 2024. The second report disclosed that no enforcement actions are taken solely on the basis of automated tools. Instead, automation is used for initial filtering and prioritization (e.g. keyword matching, similarity detection), while human moderators remain the final decision-makers. Sensitive content types such as CSAM, hate speech, or non-consensual content are escalated to trained reviewers and/or legal counsel.
2. In sampled individual reporting cases, we as the notifier received a message from content@xvideos.com outlining (i) the reason for rejection (non-compliance with DSA formal requirements or insufficient identification of the content), (ii) a direct link to the internal complaint-handling system for appeal, (iii) a fallback contact channel (content@xvideos.com) for queries.
3. Interviewed platform personnel responsible for processing notices. It was confirmed that notifications are typically sent within 24 hours following a moderator's decision. It was also confirmed that human moderators are the final arbiters in all takedown decisions, in accordance with the TOS clause stating that no algorithmic decision-making is used.
4. Evaluated documentation practices, which demonstrates that decisions were consistently documented in ticketing systems.

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 16.6	Throughout the period, in all material respects: <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.	A performance materiality threshold of 5 % was applied for this obligation.

Audit procedures, results and information relied upon:

1. Reviewed the publicly available content reporting tool on the platform's website. It allows users to report content through a structured interface that collects the URL, content type, reason for reporting, and optional contact detail.
2. Reviewed the transparency reports covering February – May and June – December 2024. The second report includes greater detail on the content moderation system, including (i) involvement of human moderators in all final decisions, and (iii) routing of high-risk reports (e.g., CSAM, hate speech) to a senior moderation team for review.
3. Examined moderation logs stored in the platform's ticketing system and verified that decisions are traceable. These logs include metadata, action history, and linkage to user and content identifiers. There is currently no evidence of inconsistent or arbitrary handling. Escalation procedures for complex cases were observed in logs and confirmed during interviews.
4. Noted that there is currently no formal internal document describing the full lifecycle of a notice, decision-making roles, or automation disclosure triggers. While standard operating procedures exist in fragmented forms across teams, there is no unified guidance document that ensures consistency and audit readiness.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The content moderation workflow is human-led, decisions are documented diligently, and notices are processed within a reasonable timeframe. However, the lack of automation disclosure in individual user notifications constitutes a minor compliance 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) moderation workflows, (ii) use and limits of automation; (iii) internal escalation paths; (iv) required disclosures to notifiers

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 17.1, 17.2	<p>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;▪ The statement is issued no later than the moment the restriction is imposed;▪ Excludes deceptive high-volume commercial content.	<p>A performance materiality threshold of 5 % was applied for this obligation.</p>

Audit procedures, results and information relied upon:

1. Reviewed the TOS, specifically Chapter 8 and 13, which outline moderation measures and user rights. The TOSs 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 personnel 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 in the user's account dashboard;
 - use of predefined content classification tags linked to violation categories;
 - escalation procedures for sensitive cases (e.g., CSAM, non-consensual content).

Interviewed platform personnel responsible for content moderation and compliance. They confirmed that human moderators execute final enforcement decisions, and that statements of reasons are typically dispatched within 12 to 48 hours of the action.

3. Reviewed the June – December 2024 transparency report, which includes aggregated data on content moderation actions. The report affirms the use of structured notifications but does not disaggregate by restriction type or systematically explain how the DSA criteria are implemented across enforcement actions.
4. Verified that the platform's systems collect and store email addresses from registered users. Statements of reasons are therefore issued where contact details exist, consistent with Article 17(2). In the case of guest users, notifications cannot be issued unless a contact method was voluntarily provided. Content uploaders are registered users, and thus email addresses are available for outbound communication.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The notification system is functional and used consistently across user types. Users receive a justification when enforcement actions are taken. However, process documentation could be improved by formalizing internal SOPs for different types of user accounts and restriction categories.

Recommendations on specific measures:

- Consolidate existing practices into a unified *Notification SOP* covering all user categories (regular, verified, and channel accounts), and all types of enforcement measures.
- Implement a traceability mechanism (e.g. dashboard view or email log) that records when and how each statement of reason was issued.

Recommended timeframe to implement specific measures:

Within 9 months, to align with the upcoming annual compliance review cycle.

Obligation: Article 17.3, 17.4	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: A performance materiality threshold of 5 % was applied for this obligation.
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Reviewed a sample of notification emails and internal moderation logs. Each notice includes: <ul style="list-style-type: none"> ▪ the URL or title of the removed content; ▪ a description of the action taken (e.g. removal, account lockout); ▪ a general reason referencing either legal or TOS grounds (e.g., “non-consensual content”); ▪ a link to appeal via the internal complaint-handling form ▪ fallback contact through content@xvideos.com. 2. Decision templates exist but vary by moderator team and enforcement type. There is no centrally maintained repository of standardized templates, which limits consistency and auditability across the platform. Moderation personnel confirmed that decisions are made by humans. 3. Notifications are easy to understand and include a link to the internal complaint form. However, statements rarely specify whether content was illegal or simply violated the platform’s terms. Legal citations or jurisdictional references are not included, even when takedown decisions are legally grounded. 4. For all uploader types (regular, verified, channel), the user account settings provide access to current enforcement status, but not always the full statement of reason unless the email is checked. Conclusion: <u>Positive with comment</u> – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects, but with identified areas for enhancement. While content creators are consistently informed of moderation actions and reasons, the specificity, legal reference, and automation disclosures required by the DSA are not always met.		

Recommendations on specific measures: <ul style="list-style-type: none"> Standardize all statement of reasons into structured templates incorporating (i) whether automation was involved; (ii) whether the restriction stems from legal or TOS grounds, with citations; (iii) the geographic scope and expected duration of the restriction (where applicable); Maintain a centralized template library with version control; Implement a cross-checking process to ensure that all required Article 17(3) elements are present in each communication; Update redress information to reflect multiple channels (internal complaint, ADR, court). 	Recommended timeframe to implement specific measures: Within 9 months, to align with the upcoming annual compliance review cycle.
--	---

Obligation: Article 18.1	Audit criteria: Throughout the period, in all material respects: <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 Member States; The reporting process included transmission of all relevant and available information necessary to support investigation or intervention. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 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. Interviewed responsible personnel and confirmed the existence of an established internal content moderation process including the obligation of reporting illegal content to authorities. Assessed the design of relevant processes to determine whether they align with the requirements of Article 18(1). Examined documentation of the content moderation process and verified that the provider uses a designated internal classification to flag content that is undoubtedly illegal. Verified that flagged content in this category is manually uploaded to a shared law enforcement server (LEA) accessible to Interpol and relevant national police authorities. Verified that 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. Inspected that the following data is provided to law enforcement: the illegal content file, IP address of the uploader, and all related metadata. While the reporting process exists, we did not identify a formalized internal policy or framework explicitly detailing the procedure for informing the <i>Member States concerned of its suspicion</i>. 		

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 accessible by Interpol and national authorities. However, the absence of a formalized internal document clearly describing the process of informing the <i>Member States concerned of its suspicion</i> 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 <i>Member States concerned</i> when identifiable.	Recommended timeframe to implement specific measures: The identified measures should be implemented within 6 months.

Obligation: Article 18.2	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: 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) accessible to Interpol and relevant national police authorities.
5. Verified that 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.
6. Inspected that the following data is provided to law enforcement: the illegal content file, IP address of the uploader, and all related metadata.
7. 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

Obligation: Article 20.1.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Reviewed Chapter 13 of the TOS, which outlines the internal complaint-handling mechanism. The TOSs explicitly confirms the availability of a formal process for lodging complaints against decisions related to content moderation, service restrictions, and account or monetisation actions. The TOS states that both users and individuals who submit notices (including those unaffiliated with an account) are eligible to appeal decisions through this system. 2. Assessed access points for the internal complaint mechanism through two principal user flows: <ul style="list-style-type: none"> ▪ Platform interface access: Logged-in users are presented with an "Appeal this decision" button embedded directly in their notification centre or profile interface. This button initiates the complaint submission process and is pre-linked to the relevant case or decision; ▪ Email notification access: When a content or account-related decision is communicated via email, the message includes a direct hyperlink to initiate a complaint. These links are unique to the case in question and redirect the recipient to the same complaint form used within the logged-in interface. <p>In both cases, users are not required to provide additional login credentials beyond those used to access their accounts, ensuring a seamless experience.</p> 3. Conducted walkthroughs of both complaint submission channels. Each method leads to a standardised, web-based form that captures the decision identifier, the category of appeal, and provides a free-text field for the complainant to explain their rationale. There is no financial charge, registration barrier, or CAPTCHA blocking access, confirming that the system is entirely electronic and free of charge. 4. Interviewed key personnel from the platform's notice and complaint team. They affirmed that the internal complaint-handling system is integrated into both the enforcement and customer support workflows and that it is actively monitored. Staff explained that users without accounts may also file appeals via email if contact details were provided in the original notice, fulfilling the obligation to serve both account holders and notifiers more broadly. 5. Evaluated transparency reports for the periods February – May 2024 and June – December 2024 and verified that the complaint system was consistently operational. The June–December report includes references to the number of complaints submitted, categories of 		

<p>decisions challenged, and action outcomes (e.g., reversals, upheld decisions), demonstrating continuous use and accessibility of the system throughout the review period.</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 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"> 1. Reviewed the TOS (Section 13) outlining user rights post-decision. The public-facing terms correctly reference the user's right to lodge a complaint for a period of at least six months following content or account decisions. However, the platform's internal process description defines this pending status to last only 30 days, after which the content is permanently deleted unless a complaint is received. 2. Identified a material deficiency that the provider currently deletes the content prior to the end of the mandatory six-month complaint period if no complaint is lodged during the 30-day pending window. This poses a compliance risk, as content that has been removed cannot be reinstated or properly evaluated after deletion, thereby rendering the complaint-handling mechanism ineffective beyond the retention period. 3. Account termination follows a similar pattern: accounts flagged for TOS violations are deactivated and placed in a "pending deletion" state. Moderation teams retain internal access to account information for 7 to 30 days, depending on whether the account had uploaded content. If a complaint is not received within this window, account data and associated content are permanently deleted. 4. Interviewed personnel was confirmed that the retention durations (30 days for content; 7–30 days for accounts) were based on legacy data privacy practices and storage optimization protocols, not on DSA requirements. 5. While the complaint forms and access mechanisms themselves remain technically available for six months, the underlying data (content or account) may be deleted prematurely, meaning that complaints submitted after the retention window cannot be acted upon, defeating the purpose of the internal complaint-handling system for those decisions. <p>Conclusion:</p>		

Negative – In our opinion, the provider partially complied with the specified requirements during the examination period, in all material respects. While access to the complaint-handling interface is maintained for six months following a decision, the premature deletion of underlying content or account data (after 30 or fewer days) undermines the effectiveness of the complaint mechanism and prevents full compliance with the DSA.

Recommendations on specific measures:

- Extend the retention period for removed content and terminated accounts to match the six-month complaint window. This should apply to (i) content labelled as “pending deletion”, user accounts subject to suspension or termination;
- Amend platform data lifecycle policies to ensure that enforcement decisions (including metadata, moderation logs, and user communications) are retained and retrievable for at least 6 months from the date of user notification;
- Create internal documentation that aligns complaint eligibility windows with retention schedules. This should include a DSA-aligned data preservation policy for complaint-eligible decisions, and/or cross-team escalation guidance for complaints received during months 2–6, and integration of this policy into the complaint-handling SOPs and moderator training.

Recommended timeframe to implement specific measures:

The above changes should be implemented within 3 months, ensuring that all takedown and account-related decisions made after that point remain appealable and fully actionable for the full six-month window.

<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>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted walkthroughs of the complaint-submission interfaces on both mobile and desktop versions of the XVideos platform. The entry points for appeals were identified in two consistent locations: (i) within the user interface (UI) via the "Appeal" button attached to flagged content or account action, and (ii) via a hyperlink embedded in the user notification email informing the recipient of a moderation decision. Confirmed that the complaint form is accessible without login in cases where a user has been suspended or terminated, provided they retain access to the decision email. 2. Reviewed the design of the complaint form, which included: <ul style="list-style-type: none"> ▪ Dropdown fields for categorizing the reason for appeal; ▪ A mandatory free-text input field for users to describe their objections and provide context or evidence; ▪ Pre-filled metadata from the original notice, where applicable (such as content ID or decision reference), improving traceability and reducing user burden. 		

<p>3. Evaluated linguistic clarity and usability, drawing from the June–December 2024 transparency report and test sessions. The form uses concise labels, logical flow, and avoids complex legal language.</p> <p>4. Inspected the TOS (Chapter 13.1), which outlines the availability of the internal complaint-handling system and its applicability to decisions related to content, accounts, monetization, and service restrictions. This public documentation ensures users are aware of their rights and appeal mechanisms.</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 20.4.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <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. 	<p>Materiality threshold:</p> <p>A performance materiality threshold of 12.5% was applied.</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> The moderator 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). The moderator demonstrated how complaint tickets include: <ul style="list-style-type: none"> 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. <p>Reviewers must enter a justification and select a resolution outcome (e.g. content reinstated, account restored, complaint rejected) before closing the case</p> 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: <ul style="list-style-type: none"> Timeliness of resolution ranged from under 1 day to approximately 5 days; Decision rationales were clearly documented; 		

<ul style="list-style-type: none"> ▪ Notifications sent to users were shown, confirming reasoned communication and redress options. <p>4. 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:</p> <ul style="list-style-type: none"> ▪ A piece of content initially removed for nudity was reinstated after the user submitted contextual justification; ▪ An account whose monetization had been disabled was reactivated following a substantiated complaint regarding misclassification of a video. <p>In both cases, the reversals were implemented within 24 to 36 hours following the decision.</p> <p>5. 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.</p> <p>6. Although the procedures appear consistently applied in practice, the audit noted the absence of a formal internal document or playbook that defines key Article 20.4 concepts, such as “timely”, “diligent”, or “non-arbitrary”. Decision standards, escalation thresholds, and expected turnaround times are known to staff but remain informal.</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. Complaints are processed manually by trained staff, resolved within appropriate timeframes, and reversals are executed promptly when complaints are valid. 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>	
<p>Recommendations on specific measures:</p> <p>Develop and adopt a written Complaint Handling Policy, which should:</p> <ul style="list-style-type: none"> ▪ Define “timely”, “diligent”, and “non-arbitrary” in operational terms; ▪ 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:</p> <p>The above changes should be implemented within 6 months.</p>

<p>Obligation:</p> <p>Article 20.5.</p>	<p>Audit criteria:</p> <p>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); 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

	– other available redress options or escalation channels.	
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ▪ 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@xvideos.com) for further inquiry. 4. Assessed timeliness of notifications by comparing internal timestamps for complaint closure and user notification dispatch. In 14 out of 15 sampled cases, the notification was sent within 48 hours of the complaint decision. In one instance, the delay was approximately 72 hours, due to a weekend processing queue. <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 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: <ol style="list-style-type: none"> 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. 		

<p>2. Shadowed the complaint-handling and moderation process by observing live sessions with moderators. This included</p> <p>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.</p> <p>3. Inspected that all designated personnel had completed onboarding modules, including general moderation principles, platform-specific policy guidance, redress and reversal decision-making criteria.</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 21.1.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <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. 	<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 TOS was reviewed and found to contain clear reference to the right of users and notice submitters to access out-of-court dispute settlement bodies, once certified under the DSA. The reference was written in a manner compliant with the clarity and intelligibility standards required. 2. The June–December 2024 Transparency Report and the WGCZ Yearly Transparency Report were reviewed. These reports confirmed that, during the examination period, no certified out-of-court dispute settlement bodies had yet been made available in the Union. However, a commitment to enabling access was documented. 3. The platform’s user interface design was reviewed based on documentation and supporting audit evidence. It was confirmed that preparatory pathways had been developed to accommodate future referrals to certified dispute bodies. However, direct technical testing was outside the audit scope. 4. Interviews with compliance team were conducted. It was confirmed that internal complaint-handling protocols had been designed to accommodate escalation to certified bodies. However, no cases were referred during the period due to the absence of operational dispute entities. <p>Conclusion:</p>		

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, defined as ≤ 48 hours.; ▪ 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: <ol style="list-style-type: none"> 5. Performed interviews with members of the notice and complaint team, who are responsible for reviewing user-submitted notices, including those potentially submitted by trusted flaggers. The team confirmed that, although a registration form is available for trusted flaggers, and internal personnel are aware of the identities of registered trusted flaggers, there is no system in place to identify or label incoming notices as originating from trusted flaggers. Additionally, no technical mechanisms (such as tagging, filtering, or dedicated workflows) exist to distinguish or prioritize such reports. 6. During interviews it was confirmed that there is an internal procedure to verify trusted flagger status, which includes reviewing the registration request and approving it based on internal criteria. However, this process is not formally documented. 7. Shadowed the moderation workflow by observing a sample of content moderators at work. Moderators consistently applied platform policy and exercised discretion in judgment. However, they were not able to determine whether any notices originated from trusted flaggers, and thus, could not treat such notices with procedural priority. 8. Reviewed the trusted flagger registration form publicly available on the platform. The form states that once a trusted flagger is verified and confirmed by the provider, their notices will be prioritised. However, there is no automated or systemic link between this status and the moderation pipeline, and no confirmation template or audit trail was available to confirm any trusted flagger approval occurred during the period. 		
Conclusion: Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While there is a public registration form for trusted flaggers and an internal understanding of their role, the lack of technical infrastructure, formal verification workflow, and tagging capabilities means the platform cannot currently identify or prioritize such notices.		

Recommendations on specific measures: <ul style="list-style-type: none"> ▪ Implement tagging capabilities within the report-processing interface to clearly label notices from verified trusted flaggers; ▪ Document the trusted flagger verification process and create a confirmation template to formally acknowledge their status; ▪ Train moderators on how to identify and prioritise trusted flagger notices; ▪ Introduce a dashboard or log to track the lifecycle and timing of trusted flagger submissions separately from general reports. 	Recommended timeframe to implement specific measures: The above changes should be implemented within 6 months.
--	--

Obligation: Article 23.1.	Audit criteria: Throughout the period, in all material respects: <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 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 of time. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Interviewed the content moderation teams responsible for policy enforcement. They confirmed that account suspensions were issued during the reporting period for severe illegal content (e.g. CSAM, rape, zoophilia), but not under a structured process for “frequent and manifest” violations. 2. Reviewed a breakdown of content categories that resulted in account terminations during the reporting period (August 2023 – April 2024). This includes 377 terminations for underage content, 4 for active zoophilia, 3 for real rape, 6 for scatophilia. These terminations show that enforcement against illegal content is active. However, there was no indication that prior warnings were issued, or that the users had engaged in a pattern of repeat violations. The enforcement approach appears to be binary and content-triggered, not frequency-based. 3. During the reporting period, provider’s databases and moderation tooling were not designed to log or tag the reason behind account terminations. Specifically, the system (i) does not track whether the same user has repeatedly posted illegal content, (ii) cannot differentiate first-time violations from repeat offenses, (iii) does not maintain structured logs of warning issuance or measure duration of suspension versus termination, (iv) lacks standardized notification templates for warnings related to content misuse. 4. The platform’s TOSs includes general language that prohibits the posting of illegal or harmful content and reserves the right to remove such content and terminate accounts. However: <ul style="list-style-type: none"> • There is no reference to a policy of suspending users for frequent violations; • The ToS does not define what constitutes “manifestly illegal” content in specific terms; 		

<ul style="list-style-type: none"> • There is no clause detailing a warning system, reasons for account actions, or expected suspension duration; • Users are not informed through the ToS of the factors that will be taken into account when assessing repeated violations. <p>5. The specific evidence of structured enforcement under Article 23.1 was not provided because the provider confirmed that no suspensions were documented as being linked explicitly to “frequent” or “manifest” content violations; account restrictions taken were final, especially for severe violations (e.g., child sexual abuse material, terrorist content). The absence of a suspension layer in the moderation pipeline meant that warning and temporary suspension workflows were not implemented during the audit period.</p> <p>Conclusion:</p> <p>Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. Although the provider has an active enforcement process for removing illegal content and terminating accounts, this process is not designed to identify or manage repeat offenders under a formal “frequent and manifestly illegal” behaviour policy. Moreover, there is no evidence of prior warnings, structured suspension durations, or user-facing policies communicating these practices. The platform’s current enforcement is reactive and severity-based, rather than frequency-based.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Implement a graduated enforcement protocol. Define clear thresholds (e.g. 3 violations in 30 days) for “frequent and manifest” misuse and introduce internal flags to track repeat offenders. ▪ Introduce a warning and escalation framework. Develop structured warning notices and standardized templates for notifying users and managing appeals. ▪ Update the TOS and clearly outline misuse definitions, example scenarios, enforcement steps, suspension durations, and user rights. ▪ Log all warnings and suspensions in a structured database and enable traceability of timing, reasons, and outcomes. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 6 months.</p>

<p>Obligation:</p> <p>Article 23.2.</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 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; ▪ A warning is issued before any suspension, including justification and possible consequences; ▪ The suspension is temporary and proportionate; ▪ The responsible individuals are informed and apply the policy consistently. 	<p>Materiality threshold:</p> <p>N/A</p>
--	---	---

Audit procedures, results and information relied upon:

1. Interviews with the notice and complaint team, and content moderation team revealed that the provider currently does not have any active policy, tooling, or procedure to detect or suspend users who submit manifestly unfounded notices or complaints under Articles 16 or 20. The team confirmed that no suspensions were issued on this basis during the audit period.
2. Reviewed documentation of the Article 20 complaint-handling system. The system is designed to process and respond to user complaints, but there is no mechanism to evaluate the validity of submissions over time or to identify users engaging in misuse.
3. Reviewed platform-wide content reporting flow. Although the provider allows users to report content for review, there is no tracking of report originators, no log of frequency per user, and no designation of whether reports are well-founded or not.
4. The provider confirmed system limitations. It stated explicitly that it does not track suspensions linked to misuse of reporting systems and that the database was not designed to categorize such events during the audit period.

Conclusion:

Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While notice and complaint mechanisms are in place, there is no policy, tracking infrastructure, or warning/suspension mechanism to address misuse of those systems.

Recommendations on specific measures:

- Develop misuse detection mechanisms for notice/complaint systems, which will track report/complaint submissions per user and flag accounts showing unfounded or abusive behaviour patterns.
- Specify thresholds (e.g. % of rejected complaints within a timeframe) that trigger a warning or suspension review.
- Establish a structured warning and suspension workflow. Notify offending users with standardized messages and apply time-limited suspensions in repeat cases.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 23.3.	<p>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.	N/A

Audit procedures, results and information relied upon:

1. Interviews with the notice and complaint team, and content moderation team revealed that the provider currently does not have any active policy, tooling, or procedure to detect or suspend users who submit manifestly unfounded notices or complaints under Articles 16 or 20. The team confirmed that no suspensions were issued on this basis during the audit period.
2. Reviewed documentation of the complaint-handling system. The system is designed to process and respond to user complaints, but there is no mechanism to evaluate the validity of submissions over time or to identify users engaging in misuse.
3. Reviewed platform-wide content reporting flow. Although the provider allows users to report content for review, there is no tracking of report originators, no log of frequency per user, and no designation of whether reports are well-founded or not.
4. The provider confirmed system limitations. It stated explicitly that it does not track suspensions linked to misuse of reporting systems and that the database was not designed to categorize such events during the audit period.

Conclusion:

Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While the platform removes accounts for severe violations, it does not perform the structured, multi-factor analysis required before suspending users based on repeated or abusive behaviour under Articles 23.1 and 23.2.

Recommendations on specific measures:

Create and apply a standardized case review template that guides moderators through the required criteria before any suspension, ensuring decisions are justified, proportionate, and logged for transparency and auditability.

Recommended timeframe to implement specific measures:

The above changes should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 23.4.	<p>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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the TOS (February 2024 version) as published on XVideos.com, including all sections relevant to account use, prohibited activities, enforcement actions, and user responsibilities. The TOS prohibit illegal content and allow the provider to remove content or terminate accounts at its discretion. Section 3 ("Use of XVideos"): Prohibits uploading or posting illegal content, including non-consensual imagery, underage material, and other explicitly banned content. Section 7 ("Account Suspension or Termination"): States that XVideos may suspend or terminate access "for any reason," including violations of the ToS or applicable law.
2. However, the document does not contain (i) any reference to "frequent" or "repeated" violations as criteria for enforcement, (ii) a policy on misuse of notice and complaint mechanisms (e.g., false reports), (iii) examples or definitions of what behaviour would trigger warnings or suspensions under a misuse framework, (iv) explanation of suspension durations, proportionality, or case-by-case review factors, and (v) a description of users' rights or remedies in case of enforcement.
3. No annex or policy supplement is linked from the ToS that would fulfil these requirements.

Conclusion:

Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While the platform has reserved enforcement rights, it does not transparently communicate its policy regarding platform misuse, suspension criteria, or user rights related to frequent or abusive behaviour.

Recommendations on specific measures:

Revise the TOS to define misuse under Article 23, include clear examples (e.g., repeat violations, false complaints), specify enforcement criteria and durations, and explain user rights and suspension procedures.

Recommended timeframe to implement specific measures:

The above changes should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 24.1.	<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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the February – May 2024 and June – December 2024 transparency reports published by XVideos. Both were published on time and follow a structure broadly aligned with DSA expectations.
2. Verified that no out-of-court disputes under Article 21 were reported for either period. The reports did not include median durations, outcomes, or implementation rates for such disputes, nor placeholders indicating that no cases occurred. Interviews with the legal team confirmed that no disputes were submitted, and this was the reason for omission.
3. Examined the sections on user suspensions under Article 23:
 - The reports disclosed aggregated account terminations for provision of manifestly illegal content (e.g. 377 cases of underage content in the February – May report);
 - However, there was no breakdown of suspensions by type, as required: i.e., no data distinguishing between suspensions for illegal content, manifestly unfounded notices, or manifestly unfounded complaints.
4. Interviewed provider content moderation and notice and complaint teams. They confirmed that the platform does not currently have system-level tagging or tracking in place to distinguish between the three suspension types under Article 23. Suspensions were manually handled and not categorized in a structured way.
5. 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 9 months.

Obligation: Article 24.2.	Audit criteria: Throughout the period, in all material respects: <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;▪ Makes this information publicly accessible via the online interface (available to anyone without prior clearance or qualification).	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

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: 150 million
- August 17, 2023: 150 million
- February 29, 2024: 85 million
- August 17, 2024: 84 million
- February 17, 2025: 31 million

All publications appeared on the “Legal Stuff” > “Mandatory information/reporting” section of the public interface. Confirmed that figures were posted at six-month intervals, as required, and were visible and accessible at the time of the audit.

2. Reviewed explanatory text published on the providers information page. It states that:

- Early numbers (150M) were overestimated, using maximum assumptions to avoid underreporting.
- Later figures (e.g. 31M in Feb 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”.

3. No formal documentation or transparent methodology was published alongside the figures.

4. 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 formal obligations by publishing user numbers biannually in a public location and describing their basis. However, the lack of verifiable methodology, reliance on estimation over calculation, and absence of documentation limit the transparency and auditability of the reported figures.

Recommendations on specific measures:

- Replace “estimated” figures with systematically calculated values based on verifiable internal data;
- Document and retain the methodology used, including treatment of private/incognito sessions.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 24.3.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none">▪ Is prepared to supply the Commission or the Digital Services Coordinator (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.	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

Audit procedures, results and information relied upon:

1. Performed interviews with the compliance team to assess preparedness to respond to regulatory requests for updated average recipient data. Confirmed that no formal requests were received from the European Commission or any Digital Services Coordinator 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.

Conclusion:

Positive with comment – In our opinion, the provider is procedurally prepared to respond to requests under Article 24.3 and meets the formal requirement of responsiveness. 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.

Recommendations on specific measures:

Develop and document a clear methodology for calculating average monthly active recipients, including treatment of incognito and non-logged-in traffic.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 24.5.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ Submits to the European Commission, 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 Commission; ▪ Confirms that such submissions do not contain personal data. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Identified that no information was disclosed in the transparency reports or elsewhere indicating that the provider had submitted removal or restriction decisions (and associated reasons) to the European Commission's machine-readable database during the examination period. 2. The provider confirmed that while Article 17 decisions are recorded internally, the provider has not yet implemented a system to submit them to the Commission's database. 3. The compliance team acknowledged this as a known compliance gap and stated that efforts are underway to create automated submission functionality. The team also confirmed that they are aware of the requirement to exclude personal data from these submissions but noted that no formal review or redaction protocol is yet in place. Conclusion: Negative – In our opinion, the provider did not fully comply with the specified requirements during the examination period. While internal Article 17 decisions are maintained, no transmission to the Commission's machine-readable database occurred, and the required data pipeline and safeguards (e.g. personal data filtering) are not yet operational.		

Recommendations on specific measures: <ul style="list-style-type: none"> Establish a process and system for submitting Article 17(1) decisions and reasons to the Commission's machine-readable database; Implement a data sanitation protocol to ensure no personal data is included. 	Recommended timeframe to implement specific measures: The identified measures should be implemented within 6 months.
---	--

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. Inspected selected features of the provider's interface, including registration, login, and account termination.
2. Verified that the steps for account termination were no more complex than for registration.
3. Tested the logout function on both desktop and mobile versions of the platform. Verified that logout could be completed easily via the account section menu and was not hidden.
4. 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.
5. Verified through walkthroughs of selected interface elements that no misleading default settings or other forms of nudge techniques were generally present. Confirmed that user choices were in most cases presented in a visually neutral manner without disproportionate emphasis on any particular option. However, identified two isolated interface practices that may risk impairing user autonomy:
 - During the age and orientation confirmation process upon first access to the platform, one category appeared pre-highlighted with a distinct colour treatment, which could suggest a default or recommended choice to the user.
 - Upon account creation, the gender setting was pre-filled as "male" without requiring user input, representing a default setting not explicitly confirmed by the recipient of the service.
6. Identified that internal documentation addressing interface review against dark pattern has not been formalized.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The interface is generally structured in a way that enables users to make free and informed decisions, without the use of deceptive design patterns. However, two interface elements were identified that may risk unduly influencing user choice: (i) a pre-highlighted category during age confirmation at initial access, and (ii) a pre-set gender default upon account creation. Furthermore, we identified that internal documentation addressing interface review against dark patterns has not been formalized, which may limit consistency and auditability of future interface changes.

Recommendations on specific measures:

- Develop and formalize internal documentation (e.g. dark pattern review checklist or UI ethics framework) that outlines principles, risk indicators, and review procedures for interface design aligned with Article 25.
- Review and adjust the current default settings (remove pre-selection of gender and ensure equal visual weight in categories).

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 4 months.

Obligation:

Article 26.1.

Audit criteria:

Throughout the period, in all material respects:

- All advertisements presented on the provider's interface were clearly marked as such at the moment of display (real time);
- Each advertisement disclosed:
 - 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. Conducted a walkthrough of the provider's website and assessed advertising presentation, labelling, and ad information access across web and mobile platforms.
2. Identified two categories of advertisements on the platform:
 - Type A ads: Clearly marked with a red rectangular "AD" label and an "i" button. Upon interaction with the "i" label, users are redirected to an "About This Ad" page containing (i) reasons for seeing the ad and (ii) name of the advertiser.
 - Type B ads: Not marked with "AD", only feature an "i" label linking to similar "About This Ad" content. These ads are visually distinguished by layout (e.g. wider thumbnails, additional text elements, or distinct framing), making them less easily confusable with organic content.

3. Verified that for both ad types, the user can access meaningful targeting parameters and advertiser identification in real time via the “i” icon. However, we did not identify any information provided to users about how to change the targeting parameters used for advertisement personalization.
4. Inquired with respective personnel to understand the scope and structure of information provided about displayed advertisements. In correspondence with information provided in the advertisement repository, the disclosed name of the entity is labelled as “Advertiser,” which corresponds to the party that engages directly with the provider and financially sponsors the advertisement. While this typically reflects agencies or affiliates acting on behalf of product owners, the provider does not explicitly distinguish between the advertiser (payer) and the product owner (beneficiary), as required when these entities differ.
5. Inspected the provider’s risk assessment and confirmed that risks related to advertising transparency were identified, including Misleading advertisements not clearly distinguished from regular content, Breach of user trust through undisclosed sponsorships, and Failure to disclose information about advertisements required by applicable laws. Mitigation measures were described at a general level not distinguishing the above identified ad types.
6. Identified that internal documentation outlining procedures and/or requirements applicable to advertising transparency has not been formalized, particularly with regard to specifying how to handle situations where the natural or legal person who paid for the advertisement differs from the person on whose behalf the advertisement is presented.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Advertisements were clearly distinguishable, provided real-time access to advertiser and targeting parameter information. Nonetheless, inconsistencies in ad labelling between formats and the absence of internal documentation limit the auditability and procedural clarity of these compliance elements. Moreover, information about both payer and beneficiary and information how to change the parameters used for targeting advertisements was not presented to users, limiting the transparency of control over ad personalization settings.

Recommendations on specific measures:

- Standardize ad labelling across all ad types by adding a consistent “AD” or equivalent label, in addition to the “i” button, regardless of ad layout.
- Enhance the “About This Ad” section to include clear guidance for users on how to change the parameters that influence ad targeting.
- Develop internal documentation clarifying responsibilities and interface requirements related to elements of Article 26(1).
- Ensure that identified risks are consistently mitigated by enforceable internal controls.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 26.3.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Inspected the Privacy Policy, which states that processing of personal data is conducted in accordance with GDPR and identifies certain sensitive personal data categories (e.g. race, religion, sex preferences, dominant/submissive roles, sexual orientation) that may be collected.
2. Verified that while sensitive personal data are listed in the Privacy Policy, purposes of processing are only declared for selected categories (race and sexual orientation).
3. Verified that the purpose "advertisement" is only assigned to the cookie category "wpn_ad_cookie".
4. Observed that the Privacy Policy does not include a clearly documented prohibition or explicit restriction on the use of sensitive personal data for profiling in advertising contexts.
5. Identified that internal documentation outlining strict prohibitions or filtering of advertising based on Article 9(1) GDPR profiling was not available.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The privacy documentation indicates alignment with GDPR principles, providing selective information on sensitive personal data categories as well as the purpose of processing. However, the absence of a clearly documented prohibition on profiling-based advertisement using special categories of personal data introduces ambiguity regarding full compliance with Article 26(3) of the DSA.

Recommendations on specific measures:

- Formally document and adopt a policy that explicitly prohibits profiling-based advertisement using special categories of personal data as defined in Article 9(1) GDPR.
- Extend the Privacy Policy to clearly associate each sensitive data category with a declared processing purpose, explicitly excluding advertisement use where applicable.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation:

Article 27.1.,
27.2.

Audit criteria:

Throughout the period, in all material respects:

- The provider set out in its TOS, in plain and intelligible language, the main parameters used in its recommender systems;
- The provider explained why certain information is suggested to recipients of the service, including:
 - 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.

Materiality threshold:

N/A

Audit procedures, results and information relied upon:

1. Inspected the provider's TOS and underlying documentation related to recommender systems.

2. 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 criteria was confirmed.
3. Verified that Article 9 of the TOS describes the recommender system logic applied to different sections of the Website. Specifically:
 - On the main page: recommendations are based on (i) user-selected location (country) and (ii) popularity of videos (number of clicks). The option for the recipients to change the location is described.
 - In other sections: suggestions are influenced by the recipient's selection of categories (subgenres), specific content creators, keyword searches (matching tags and titles, popularity relevance), recipient's view history option, and collective viewing history.
4. Interview relevant personnel and verified relevance of the declared parameters. However, no internal documentation governing recommender transparency was identified.
5. Identified that, in addition to the main declared parameter "category" (straight/gay/trans), the system also uses "categories" (subgenre classification Amateur, Anal etc.) as a decisive ranking factor for suggested content. In our view, this constitutes a significant parameter influencing recommendation outputs, and its inclusion in the TOS should be considered by the provider.
6. Verified that Article 9 of the TOS clearly outlined the option for the recipients to modify these parameters in plain and intelligible language (as described above).
7. 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 transparency requirement. The platform also uses additional content classification parameters ("categories") which are not explicitly disclosed as part of the recommender system explanation. Further, internal documentation addressing recommender system transparency was not identified, which may hinder consistent implementation of obligations.

Recommendations on specific measures:

- Expand the TOS to explicitly include a description of the relative importance of each parameter influencing recommendations.
- Assess whether the use of subgenre-level "categories" materially influences content ordering and recommendations; if confirmed, expand the TOS.
- Develop internal documentation that clearly outlines policies and processes for ensuring transparency in recommender systems.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

Obligation: Article 27.3.	Audit criteria: Throughout the period, in all material respects:	Materiality threshold: N/A
-------------------------------------	--	--------------------------------------

	<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; ▪ The functionality was directly and easily accessible from the section of the online interface where the recommender system applied. 	
Audit procedures, results and information relied upon: <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, pornstars). 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 28.1.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Reviewed the platform's TOS, 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 XVideos 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. Reviewed risk-related documentation, including the accompanying Risk Management Framework, both of which underscore minor protection as a strategic, regulatory, and reputational risk. These documents explicitly identify the exposure of minors to adult content as a scenario with potentially major consequences. Minor protection is categorized under the “Protection of Minors” risk cluster and was assigned a high inherent risk level in the initial risk assessment phase. The residual risk, after current controls are factored in, remains medium, which triggers enhanced monitoring and targeted mitigation planning.

The risk of minor exposure is integrated into the broader ISO 31000-aligned risk management system. An Action Plan for medium-to-high risks includes periodic reassessment of age controls, resource allocation for solution research, and internal reviews.

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.
5. Conducted interviews with the compliance team, who confirmed that while XVideos 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 adult platform operating in the EU. The team emphasized the importance of avoiding overprocessing personal data.

Conclusion:

Positive with comment – 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: <ul style="list-style-type: none"> 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; Periodically test the effectiveness of existing age gates (e.g. A/B testing, audit logs) and report findings in the platform's risk assessment report. Establish a compliance working group responsible for implementing future Article 28.4 guidelines, including legal experts. 	Recommended timeframe to implement specific measures: The identified measures should be implemented within 9 months.
--	--

Obligation: Article 28.2.	Audit criteria: 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. 	Materiality threshold: 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. The provider does not participate in programmatic ad networks that rely on cookies or personal identifiers for behavioural delivery.
3. Confirmed that XVideos does not require account creation for content viewing. Since the majority of 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.
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.

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 28.3.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 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. 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. 3. Reviewed the WGCZ 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>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	

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:</p> <p>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>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Conducted inquiries with compliance team. Confirmed the provider performed two detailed, platform-specific risk assessments. 2. Reviewed both risk assessment alongside supporting documents: "RSK sources_impact on the assessment_complete.docx" and "OE expectation Argumentation - DRAFT.docx." The methodology is robust, involving a detailed risk matrix categorizing risks by likelihood and severity. Assessment processes involved: <ul style="list-style-type: none"> • External references and benchmarks from reputable organizations (e.g., WeProtect Global Alliance, Internet Watch Foundation). • Internal moderation data, logs of removals, user reports, and appeals analyses. • Expert consultations and workshop outputs documented within provided supporting materials. 3. Reviewed both risk assessments, confirming explicit identification and analysis of illegal content risks (Art. 34.1.a), including: <ul style="list-style-type: none"> • Child Sexual Abuse Material (CSAM), systematically tracked and managed through advanced hash-matching tools; • Non-Consensual Intimate Imagery (NCII), terrorist content, real rape footage, and violent material clearly documented and risk-rated; • Volume, frequency, and types of illegal content were supported by internal enforcement statistics and moderation team inputs; <p>The risk assessment links risks to explicit mitigations such as rapid content removal targets, manual moderation tiers, automated detection enhancements, and internal co.</p> 4. Thoroughly analysed in both assessments, with documented risks and controls for fundamental rights (Art. 34.1.b) including: <ul style="list-style-type: none"> • Detailed identification of risks related to wrongful removal or moderation errors, with mitigation through appeal processes, retraining of moderators, and improved moderation guidelines; 		

<ul style="list-style-type: none"> • Risks related to age verification systems and data retention practices; mitigation documented as implementation of data minimization practices, privacy-by-design principles, and enhanced encryption of sensitive data; • Explicit examination of biases in moderation tagging and categorization processes, with mitigations involving retraining moderators and revising automated moderation algorithms; • Detailed assessment of gaps in age verification methods, mitigated through strengthened identity verification solutions, geo-blocking tools, and age-gating methods. <p>5. The risk assessments included a qualitative evaluation indicating limited relevance of civic discourse, electoral processes, and public security risks (Art. 34.1.c), primarily due to the platform's specialized focus on adult content and lack of direct engagement with political or electoral discourse. The provider's risk assessments acknowledged these risk areas and offered a qualitative rationale for their limited applicability, referencing the platform's primary function as an adult content service with minimal overlap with political or civic discourse. This rationale is supported by usage data and platform design characteristics that inherently limit engagement in public debate or electoral activity.</p> <p>While the assessment did not include in-depth quantitative analysis for abuse in this area, the documentation shows an awareness of potential future relevance. The provider has noted that these topics will remain under observation and has expressed willingness to revisit them should any usage trends or third-party reports indicate emerging risks.</p> <p>6. Both assessments thoroughly analyse, with documentary evidence, the risks and control measures relating to gender-based violence, minors, and well-being (Art. 34.1.d):</p> <ul style="list-style-type: none"> • Risks related to exposure to violent or degrading content and harmful categories were extensively documented. • Mitigations explicitly documented include content categorization restrictions, enhanced reporting functionalities, and implementation of user-facing educational resources about consent and appropriate behavior. • Risks related to minors extensively mapped, with detailed implementation plans including robust age verification mechanisms, enhanced moderation workflows, and partnerships with external experts in child protection. <p>7. The platform's risk management approach clearly identifies risk severity and likelihood, contextualizing these within documented moderation logs and expert benchmarks. Specific control measures were identified, assigned, and documented clearly within the provided documentation.</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. The provider conducted two service-specific and methodologically sound risk assessments, supported by risk registers, external benchmarks, and mitigation dashboards. Each systemic risk category defined under Article 34.1 was addressed, with detailed analyses for illegal content, fundamental rights, gender-based violence, and protection of minors. The platform's justification for limited relevance of civic and electoral risks was consistent with its service type, though not supported by quantitative analysis. While risk assessments were timely and comprehensive, the process for pre-launch risk re-evaluation remains informal and could benefit from more structured integration into the product development cycle.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> ▪ Develop a formal update protocol that requires documented re-assessment of systemic risks prior to any significant feature rollouts, algorithmic changes, or business model updates; 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 10 months.</p>

<ul style="list-style-type: none"> Enhance procedural traceability by version-controlling the risk register and linking it to development milestones or mitigation effectiveness reviews. 	
--	--

Obligation: Article 34.2.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
-------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Reviewed both initial and second risk assessments, confirming explicit coverage of how systemic risks may be affected by platform-level design and policy.
2. Art. 34.2.a: Risk assessments describe the platform's limited use of personalized recommender systems due to its "history toggle" functionality. According to internal documentation and the April 2025 report, most recommendations rely on popularity, keyword relevance, and broad interest clusters. Identified risks such as over-exposure to harmful material or behavioural loops were rated as low due to the limited personalisation. Mitigation steps included moderator-curated homepage feeds, opt-out mechanisms, and scheduled review of trending content categories.
3. Art. 34.2.b: The platform relies on layered content moderation systems (automated + human). Risks related to systemic bias, over-removal, or under-removal were explicitly acknowledged. Supporting evidence from internal logs and moderation statistics was used. Mitigations included tiered moderation workflows, and appeal mechanisms with outcome tracking.
4. Art. 34.2.d: While the platform uses limited programmatic advertising, risks tied to ad targeting and impression manipulation were flagged. These were assessed as low severity but acknowledged, with measures like filtering of ad categories, no personalized behavioural tracking, and Internal audits of ad placements.
5. Art. 34.2.e: Evaluated in connection to privacy risks, with references to age verification technologies, cookie usage minimization, server-side access controls. Risks related to third-party data misuse were partially documented.
6. Art. 34.2, para 2: The 2025 report acknowledged manipulation vectors like bot accounts, re-uploading of flagged material, and circumvention of upload filters. Mitigations include fingerprinting/hash matching tools (e.g., PhotoDNA), CAPTCHA/barrier uploads for repeat offenders, enhanced abuse detection algorithms.
7. Art. 34.2, para 3: The platform considered linguistic risks via content category tagging and specific geo-restriction policies for sensitive topics. According to the risk documentation,

<p>more granular regional risk analysis is planned for future cycles, particularly for countries with higher user volume or differing legal thresholds.</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. The assessment addressed how the provider's systems influence systemic risks. All categories under Article 34.2 were included, with risks rated and linked to mitigation strategies. However, quantitative scenario analysis of manipulation effects and region-specific risks could be further strengthened in future assessments.</p>	
<p>Recommendations on specific measures:</p> <ul style="list-style-type: none"> Develop structured scenario analysis to simulate coordinated manipulation and automated exploitation on the platform; Enhance geographic segmentation of risk analysis, especially in high-volume EU jurisdictions, and link it to localized enforcement policies. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 10 months.</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 Commission or Digital Services Coordinator 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"> Conducted interviews with the compliance team to confirm document retention practices specific to risk assessments. The team confirmed the retention of all underlying materials, working files, and final reports for both the 2024 and 2025 risk assessments. Confirmed that both the risk assessments (including supporting evidence such as Risk Registers, Mitigation Dashboards, expert source listings, and moderation data logs) are securely stored and versioned, as documented in the platform's internal registry. Reviewed the "MD_G_01_Risk Management Guideline_v1", which outlines internal procedures for maintaining, version-controlling, and archiving key compliance documents, including risk assessments. This guideline specifies that all formal assessments and their supporting documentation must be retained in centralized, access-controlled internal repositories for at least three years. 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 Commission or Digital Services Coordinator 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. <i>Definition of reasonable: measures which are appropriate to the nature and magnitude of the systemic risk.</i>	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

- Art. 35.1.a.: Design adaptations were implemented to address risks of compulsive usage, exposure to harmful or non-consensual content, and user safety vulnerabilities. Measures were verified through inspection of internal risk assessment documentation, interview notes, and live product demonstrations.

It was confirmed that the provider implemented interface-level risk mitigation measures aimed at reducing systemic risks related to exposure to illegal and harmful content, advertising transparency, and profiling.

Evidence obtained during the audit indicated that the homepage recommender system is designed to prioritise content using location-based, category-based and popularity-based ranking, with users able to manually adjust location/category settings. It was further confirmed that a non-profiled recommendation mode is available through a disable “History” feature, which stops the platform from storing or using behavioural data to personalise results.

The advertisement interface employs consistent visual labels (either a red “AD” or an “i” icon) to distinguish ads from regular content. This mechanism supports users’ ability to identify sponsored content and mitigates deception through design. In addition, access to age-restricted content is gated by blurred thumbnails and confirmation prompts, representing content-specific interface barriers to protect minors.

Based on obtained evidence, it is concluded that reasonable and proportionate adaptation measures were implemented in line with Article 35(1)(a).
- Art. 35.1.b.: The most recent version of the TOS (February 2024) was reviewed. Interviews were conducted with personnel from the compliance team. Based on this review, it was established that updates to the platform’s TOS had been made in alignment with identified systemic risks.

The updated terms included explicit prohibitions on content categories such as non-consensual sexual content, sexual depictions of minors (real or simulated), hateful or discriminatory material, and content involving coercion or violence. References to regulatory obligations under the DSA were included in relevant sections, particularly Section 3.3. A mapping between content types identified in the systemic risk assessment and prohibited categories in the TOS was provided during the audit process and was verified.

Enforcement mechanisms were examined. Enforcement actions were found to be supported by a multi-tiered moderation protocol, with automatic filtering, human verification, and escalation logic embedded into the moderation workflow. Decision matrices and enforcement policy documentation were reviewed and confirmed to reflect risk sensitivity (e.g., immediate removal in cases of CSAM indicators, escalation for edge-case review in contextually complex scenarios).

Based on the available evidence and the procedures performed, it was concluded that the provider's TOS were adapted in a manner consistent with Article 35(1)(b). The enforcement framework was found to be appropriately designed and effectively implemented, with due consideration given to systemic risks and user rights, including rights to appeal and redress.

3. Art. 35.1.c.: Content moderation processes were adapted to address risks related to the dissemination of illegal and harmful content, including hate speech, non-consensual material, and cyber violence. Processes were reviewed, including moderation workflows, and the internal mitigation measures register. Interviews were conducted with content operations and compliance personnel.

A hybrid moderation system was employed, combining automated detection (AI classifiers) with human reviewers. Human moderators were allocated by language and content type, with escalation paths in place for sensitive categories.

SLAs for notice processing were defined and tracked. For example, content flagged as potentially illegal hate speech or involving minors was subject to a 24-hour response window. Performance reports showed compliance rates above 95% for high-priority queues.

The moderation system was assessed as appropriately designed, proportionate to identified risks, and operationally effective throughout the audit period.

4. Art. 35.1.d.: It was confirmed that the provider has implemented processes for the oversight, and adaptation of its algorithmic systems, including recommender systems. The assessment was limited to on-site controls and documentation reviews. No technical audit of algorithmic models, source code, or statistical accuracy was performed.

Evidence obtained through key personnel interviews indicated that the provider's recommender functionalities are governed by a defined compliance framework. This framework sets out ranking parameters (including content category, user region, tag matching, and engagement metrics), user transparency mechanisms, and non-profiling options in accordance with Article 38 DSA.

Processes for maintaining version-controlled documentation and providing transparency to users were in place. Ranking logic was based on user-selected categories, regional signals, tag relevance, and engagement data.

Based on the evidence reviewed, and within the scope of on-site controls, it is concluded that reasonable and proportionate measures were implemented.

5. Art. 35.1.f.: It was confirmed that the provider had implemented internal structures, controls, and governance practices designed to support the detection and mitigation of systemic risks. The audit covered onsite control assessments, review of internal materials (including the Mitigation Measures Register and Dashboard, and interviews with representatives from compliance team. The register demonstrated assignment of control owners, mitigation deadlines, and performance indicators across key risk areas such as content moderation, recommender systems, and advertising. Clear role definitions and oversight responsibilities were confirmed. The compliance officer was observed to be actively coordinating DSA compliance activities.

However, while the existence and operation of internal processes were clearly described and verified during interviews, some of the procedures, such as content moderation process, were not formally documented in a consolidated or standardised format. Key workflows were described in practice but lacked formal policy articulation or centralized procedural documentation.

As a result, it is concluded that reasonable and proportionate measures were implemented to reinforce internal processes and supervision. However, greater formalization and documentation of ongoing maintenance and escalation procedures is recommended to enhance operational clarity and auditability.

6. Art. 35.1.g.: It was found that general awareness of trusted flagger obligations existed, but technical and procedural mechanisms for prioritizing such notices had not been fully implemented during the audit period.

Through interviews with moderation and compliance staff, and by observing active workflows, it was confirmed that no tagging, filtering, or separate workflow currently exists to identify or prioritize notices submitted by trusted flaggers. Moderators are not able to distinguish these notices from general user reports, and no system logs or audit trails were available to verify whether any trusted flagger submissions had occurred or received preferential handling.

An internal process to review and approve trusted flagger applications was described but was not formally documented. The trusted flagger registration form publicly states that such notices will be prioritized once verified, but no technical link between verified status and moderation processes was established or operational.

At the time of audit, no out-of-court dispute settlement decisions had been received. A general understanding of obligations under Article 21 was confirmed through interviews, but fallback or implementation procedures were informal and not documented.

7. Art. 35.1.h.: It was confirmed that during audit period the provider had not formally participated in any recognised code of conduct under Article 45 or crisis protocol under Article 48. However, the compliance team demonstrated awareness of these instruments and expressed intent to engage with relevant frameworks as they become applicable.

According to the risk assessment the provider has been actively monitoring the development of industry-wide standards, particularly those related to the prevention of child sexual abuse material (CSAM), non-consensual content, and harmful algorithmic amplification. The provider acknowledged that no sector-specific code or crisis protocol currently exists for adult platforms under the DSA but stated that “accession to recognised codes of conduct or crisis mechanisms will be evaluated once established and relevant to the service type.”

No documentation was provided to evidence participation in, or alignment with, any formal multi-stakeholder initiative or emergency risk response protocol. Internal procedures relating to cross-platform cooperation were not defined beyond informal contact channels.

Based on the available evidence, it is concluded that the platform’s approach to Article 35(1)(h) was in a preparatory phase. While awareness and intention were demonstrated, formal cooperation mechanisms were not yet in place during the audit period. Further development and documentation of structured cooperation are recommended once recognised instruments under Articles 45 and 48 are accessible and applicable.

8. Art. 35.1.i.: It was confirmed that the provider had implemented a range of user-facing measures designed to improve awareness of platform functionality, risk mitigation tools, and content labelling practices.

The risk assessment describes these measures as part of a broader strategy to support informed user behaviour and reduce exposure to high-risk content categories. The report also highlights plans to expand visibility of safety information and reinforce user understanding of content reporting tools.

Additionally, interface adaptation included clear access to content preferences, language settings, and category selection filters. Help materials were accessible in multiple languages and covered platform rules, reporting pathways, and privacy options. Users were able to adjust personalisation and content exposure settings without requiring account registration.

9. Art. 35.1.j.: It was confirmed that WebGroup had implemented a set of measures aimed at limiting the exposure of minors to harmful content and protecting their rights on the platform.

The measures focused primarily on age-gating, interface warnings, and content restriction, in line with the nature of the service and its adult-only positioning.

Based on review of the risk assessment and interviews with compliance and platform operations personnel, the platform's current approach includes a strict 18+ access model, enforced through an initial age-declaration screen and reinforced with pre-play warnings on sensitive content. Certain tags (e.g. "teen," "rough," "abuse") trigger additional interface friction and flagging rules to avoid unintended exposure to age-sensitive material.

The platform also maintains a policy prohibiting content featuring real or simulated minors, and automated filters are applied to detect and flag such content during upload. These processes are combined with human moderation layers, as confirmed during audit shadowing of content review operations.

Parental controls are limited, as the platform is not designed for use by minors under any circumstances. Instead, emphasis is placed on preventing access altogether, supported by device-level restrictions and disclaimers encouraging the use of third-party parental control tools.

However, age verification is based solely on user self-declaration, without biometric, document-based, or third-party identity verification. While appropriate for the current adult-only service model, this approach may not fully mitigate the risk of minor access in practice.

It is concluded that reasonable and proportionate measures have been implemented to protect the rights of the child, with emphasis on exclusion-based controls and content gating. Further strengthening of age verification mechanisms—where technically and legally feasible—should be considered to improve assurance of access restriction effectiveness.

10. Art. 35.1.k.: It was confirmed that the provider had introduced basic mechanisms to identify and label content suspected to be artificially generated or manipulated, in order to support user awareness and reduce the risk of deception.

The risk assessment states that the platform has adopted an internal tagging process for media flagged as "synthetic," "AI-generated," or "visually manipulated." This applies primarily to content uploaded under categories or tags commonly associated with digitally altered imagery. In such cases, a visible badge or label is applied on the playback interface to alert viewers to the nature of the content.

Users are also provided with a dedicated reporting function allowing them to flag content they suspect to be falsely presented or misleading in nature. This reporting route was tested during the audit and found to be accessible from the video interface with appropriate categorisation options.

Interviews with content moderation team confirmed that flagged synthetic content is routed to specific queues for further review. Where manipulation is confirmed and poses a risk of harm (e.g. deepfakes presented as authentic recordings), content may be removed or further marked.

Based on the evidence reviewed, it is concluded that initial measures were implemented to address synthetic and manipulated media in accordance with Article 35(1)(k), primarily through user-facing labelling and manual review. To strengthen compliance, the platform is advised to formalise detection criteria and explore automated content identification tools.

Conclusion:

Positive with comments – The provider implemented reasonable, proportionate, and effective mitigation measures tailored to the systemic risks identified under Article 34. Controls were in place across all relevant subpoints (a–k), and internal teams demonstrated operational awareness of associated obligations.

The assessment confirmed the presence of adapted moderation workflows, recommender governance, age-restriction interfaces, transparency mechanisms, and governance-level documentation. However, limitations were noted in the formal documentation of certain processes (e.g. maintenance workflows, trusted flagger procedures), as well as the lack of structured

participation in cooperative protocols. Technical audit coverage was limited to process-level controls.	
Recommendations on specific measures: <ul style="list-style-type: none"> • Formalise and document procedures related to maintenance, escalation, and systemic risk tracking (Art. 35(1)(f)); • Implement technical tagging and routing for trusted flagger notices and create verifiable audit trails (Art. 35(1)(g)); • Join applicable codes of conduct and crisis protocols once available for the sector (Art. 35(1)(h)); • Strengthen age assurance measures, including exploration of privacy-preserving third-party verification tools (Art. 35(1)(j)); • Introduce automated or hybrid detection tools for synthetic and manipulated media (Art. 35(1)(k)). 	Recommended timeframe to implement specific measures: The above measures should be implemented within 12 months.

Obligation: Article 36.1.	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> ▪ The provider had defined internal protocols to respond to a crisis declared by the European Commission; ▪ 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 Commission according to the specified schedule. 	Materiality threshold: N/A – Not applicable. No crisis declared during the examination period.
-------------------------------------	---	--

Audit procedures, results and information relied upon:

1. Interviews were conducted with the compliance team to assess awareness and preparedness for Article 36 obligations. Compliance officer confirmed that no crisis was declared by the European Commission during the audit period. Internal escalation protocols were discussed; a basic contingency plan exists, but no formalised, documented “crisis protocol” tailored specifically to a DSA-declared crisis was provided.
2. The platform’s risk management documentation and governance materials include general references to emergency responses, but without detailed, DSA-aligned procedural steps. As per the assessment of Article 35(1)(h), it was further confirmed that the provider had not participated in any recognised crisis protocol (under Article 48) or signed a code of conduct (under Article 45) during the audit period.
3. Internal statements indicated that the provider is monitoring regulatory developments and intends to join relevant protocols once sector-specific frameworks are available, particularly in relation to CSAM and algorithmic harm. However, no structured mechanism for crisis response across platforms was in place.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. No crisis was declared during the period, and the provider demonstrated awareness of its Article 36 obligations. While internal procedures exist for handling urgent situations, they are not yet fully aligned with DSA crisis protocol standards. Cooperation under Article 35(1)(h) remained informal and preparatory.

Recommendations on specific measures:

- Formalise a DSA-specific crisis response protocol, including stakeholder roles, notification chains, and mitigation steps;
- Document internal crisis governance and escalation measures clearly, linking them with risk mitigation obligations under Articles 34–36;
- Define a roadmap for participation in crisis protocols under Article 48 once relevant for the provider’s sector;
- Initiate planning for cooperation structures with other platforms and regulators during crisis events.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 8-12 months.

Obligation: Article 38	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
----------------------------------	---	--------------------------------------

Audit procedures, results and information relied upon:

1. Inquired with respective personnel to understand the design and logic of recommender systems in both profiled and non-profiled modes.
2. Confirmed with the personnel that when the history is disabled, the recommender systems no longer use nor track recipients' behaviour. Instead, only popularity and keyword matching parameters are used. However, the provider does not explicitly state whether other identifiers (e.g. IP-based geolocation) are used to personalise content when history is disabled, leaving room for ambiguity.
3. Conducted a walkthrough of the provider's website and identified the disable "History" feature, accessible through the setting menu.
4. Identified that the platform does not provide a plain-language explanation for the recipients of what changes in recommendation logic when history is disabled.
5. Assessed, that the current feature terminology may not sufficiently communicate that this switch disables profiling.
6. No internal documentation governing recommender transparency, specifically non-profiling feature, was identified.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Within the user interface, there is a disable "History" feature enabling platform recommendation without user's behavioural data input. However, it is not clear whether other identifiers are used to personalise the content. The feature is also not clearly labelled as an opt-out from profiling, and the absence of an explanatory notice limits transparency for users making informed choices about personalisation.

Recommendations on specific measures:

- Develop internal documentation that clearly outlines policies and processes for ensuring transparency in recommender systems, including non-profiling feature.
- Rename or relabel the feature "Disable History" to more clearly reflect its function as a non-profiled recommendation mode.
- Clarify whether any form of user identifiers (e.g. IP geolocation) are used in non-profiled mode and confirm that this does not constitute profiling under Article 4(4) GDPR.

Recommended timeframe to implement specific measures:

The identified measures should be implemented within 6 months.

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;	Materiality threshold: N/A
------------------------------------	---	--------------------------------------

	<ul style="list-style-type: none"> ▪ 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. 	
--	---	--

Audit procedures, results and information relied upon:

1. Conducted a walkthrough of the provider's website and confirmed that an ad repository was made public within the interface, accessible via the provider's footer across all pages (through "More..." link leading to INFORMATION AND LINKS site containing also the "AD REPOSITORY" link).
2. Reviewed the ad repository section available at <https://info.xvideos.net/ad-repository>.
3. Confirmed that the ad repository section provides both interface with searchable tool that allows multicriteria queries (i.e., Date range, Country, Advertiser Name) and links to "API Search Endpoint" and corresponding "API Documentation Page". Validated that an API interface is available.
4. Inquired with respective personnel to understand the retention period and update frequency of advertisement information within the ad repository. Confirmed that the information is provided through the repository for the entire period during which the advertisement is displayed on the platform. Identified that there is an estimated time lag of up to one hour between the moment an advertisement is shown on the platform and the moment the impression appears in the repository. This delay is due to technical processing and storage requirements. Additionally, confirmed that information in the ad repository remains accessible for one year after the advertisement was last displayed, as evidenced by the available date selection feature, where the earliest selectable date is exactly one year prior to the current date.
5. Verified that no personal data concerning recipients of the service was visible in the repository entries.

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. 	
--	---	--

Audit procedures, results and information relied upon:

1. Inquired with respective personnel to understand the scope and structure of information included in the advertisement repository and confirmed the following information are provided within the ad repository interface:
 - The repository is structured to display visual or textual representations of each ad (image, video, or URL), supplemented by a categorisation feature that assigns a "Topic" reflecting the nature of the advertised product or service;
 - The repository discloses the name of the entity labelled as "Advertiser," which corresponds to the party that engages directly with the provider and financially sponsors the advertisement. While this typically reflects agencies or affiliates acting on behalf of product owners, the system does not explicitly distinguish between the advertiser (payer) and the product owner (beneficiary), as required when these entities differ.
 - The repository displays both the "First seen" and "Last seen" dates for each advertisement, clearly indicating when an ad began and ended its visibility on the platform (or that it is still active). Technical limitations restrict the "First seen" date to a maximum of 12 months prior to the search date. Entries older than 12 months are marked with a note ("or before"). Despite this restriction, in our opinion, the current setup meets the obligation in practice by ensuring visibility over the required 12-month post-display period.
 - The repository includes a dedicated section labelled "Audience Selection," which outlines the targeting logic through a set of structured parameters ("Criteria Applied"). Two overarching categories are used: (i) Geographical locations and (ii) Contextual signals, the latter encompassing sub-criteria including content categories, device type, operating system, browser type and language, time schedule, keyword-based page context and retargeting. The repository uses symbolic indicators ("+", "-", "+ -") to signal inclusion, exclusion, or partial targeting across these parameters. Particular groups of recipients might be targeted or excluded using these parameters.
 - The repository provides aggregated impression data per advertisement, including a breakdown by individual EU/EEA Member States and for the EU as a whole. This

<p>data is accessible within the Ad Detail screen under the “Impression for country” field, which presents both numerical ranges and percentage shares per location.</p> <p>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) (audit criteria number vi) does not apply to the provider during the examination period.</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> <ul style="list-style-type: none"> N/A 	<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>

<p>Obligation:</p> <p>Article 39.3</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <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). 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> Inquired with respective personnel to understand the scope and structure of information for removed or disabled advertisements included in the advertisement repository and confirmed the following information are provided within the ad repository interface: <ul style="list-style-type: none"> The removed or restricted advertisements are listed in the repository interface; Identified that when clicking the “Click here for details” link on removed ads, the following fields are displayed: Advertiser, Topic, First seen, Last seen, Impressions, and Country; Assessed that visual content is not displayed in the repository and is replaced with a placeholder reading: "This content was removed because it didn't follow our advertising standards." Assessed that contrary to the restriction, the name of the Advertiser (natural or legal person who paid for the advertisement/on whose behalf the advertisement is presented), continues to be displayed in the repository. Identified that, aside from the placeholder message stating that the content was removed for not complying with advertising standards, the repository does not include the additional information required under Article 39(3), specifically information required for the statement of reasons (Article 17(3)(a)–(e), nor a reference to the legal basis under Union or national law for the order to act against illegal content (Article 9(2)(a)(i)). <p>Conclusion:</p>		

Negative – In our opinion, the provider partially complied with the specified requirements during the examination period, in all material respects. While the repository includes a placeholder for removed or disabled advertisements and maintains selected metadata fields (e.g. impression data, topic), it fails to fully comply with Article 39(3) by continuing to display the advertiser's identity and omitting the required statement of reasons as per Article 17(3)(a)–(e) and the applicable legal basis under Union or national law.

Recommendations on specific measures:

- Remove or anonymize the advertiser name from repository entries related to removed or disabled advertisements.
- Implement a structured mechanism for including the statement of reasons required by Article 17(3)(a–e) and legal basis information pursuant to Article 9(2)(a)(i), for any advertisement removed due to alleged illegality or TOS incompatibility.

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 Digital Services Coordinator of establishment or the European Commission, within the period specified in the request. 	Materiality threshold: N/A
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 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 separate Reasoned Requests for Information (RFIs) submitted by a competent authority were identified during the examination period. Both were confirmed to have been responded to: <ul style="list-style-type: none"> • The first RFI (July 2024) involved systemic risk mitigation measures; • The second RFI (December 2024) related to algorithmic transparency and recommender system configuration. 4. Submission logs, internal correspondence, and delivery receipts were reviewed. In both cases (i) the provider requested deadline extensions, which were either granted or implicitly accepted, and responses were ultimately submitted within the adjusted timeframes, (ii) coordination across functions was visible, (iii) the content was tailored to the request, although due to confidentiality restrictions, the audit team did not assess the content quality in detail. 5. 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. <p>Conclusion:</p>		

Positive with comments – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Two reasoned requests 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 41.1.

Audit criteria:

Throughout the period, in all material respects:

- 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.

Materiality threshold:

N/A

Audit procedures, results and information relied upon:

1. Reviewed the "Compliance Officer Appointment" resolution dated 22 March 2024, confirming the designation of Mr. David Hradecký as compliance officer. The appointment was made by the Board of Directors, and the role was defined to include oversight of legal compliance, policy implementation, and ethical conduct.
2. Inspected the Compliance Policy (MD_S_3_Compliance Policy_V1_FINAL.docx) and Compliance Statute (MD_S_0_Compliance Statute_V1_DRAFT.docx). 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.
4. Inspected reporting lines defined in the appointment letter and governance documents, which confirm direct access to the Board of Directors and the authority to escalate matters independently.
5. Reviewed access and decision-making authority, including (i) unrestricted access to internal records (as stated in the Appointment Letter), (ii) discretion in resource allocation, (iii) ability to develop and enforce policies independently.
6. Assessed sufficiency of resources based on the mandate, role description, and compliance framework presented in the Response to RFI 1 (July 2024). The compliance office was reported to have adequate support to fulfil its statutory mandate under the DSA.
7. Reviewed the Compliance Declaration (MD_S_1_Compliance_Declaration_Leadership.docx) signed by the appointed officer, affirming functional independence, reporting obligations, and ethical standards.
8. Confirmed through interview records and documentation that no changes to the compliance function's structure or mandate occurred 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 41.2.	Audit criteria: Throughout the period, in all material respects: <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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> 1. Reviewed the official Board Appointment Letter (March 2024) which confirmed the designation of Mr. David Hradecký as Head of the Compliance Function. The letter established his seniority, independence from operational units, and direct line to the management body. 2. 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. 3. 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>4. 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>5. 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:</p> <p>N/A</p>	<p>Recommended timeframe to implement specific measures:</p> <p>N/A</p>

<p>Obligation:</p> <p>Article 41.3.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects, the designated compliance officer(s):</p> <ul style="list-style-type: none"> ▪ Cooperated with the Digital Services Coordinator (DSC) and the European Commission; ▪ 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:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Inspected the Risk Management Guideline (MD_G_01_Risk Management Guideline) and associated Risk Register and Assessment Reports, confirming that risk mapping aligned with Article 34 categories and was directly overseen by the Compliance Officer. The compliance officer was documented as the process owner for coordinating identification, validation, and mitigation of systemic risks. 2. Reviewed mitigation tracking and implementation in the "Mitigation Measures Dashboard." Confirmed that the measures were tailored, tracked, and updated through internal governance structures monitored by the compliance function. Linkage to Article 35(1) elements was established. 3. It was confirmed that the compliance officer facilitated the collection of materials, participated in interviews, and provided oversight on risk mapping consistency with audit obligations under Article 37. 4. Interviewed and reviewed communication logs with internal leadership. Verified that DSA obligations were communicated through compliance briefings, policy summaries, and ad 		

<p>hoc advisory notes to product and legal departments. However, training logs and evidence of broader staff awareness campaigns were limited.</p> <ol style="list-style-type: none"> Confirmed through documentation (including governance reporting files) that the compliance officer has formal reporting rights to the management body and escalated systemic risks during the period. Escalation documentation and management-level reporting were available and confirmed. Found no indication that the platform had yet joined a sector-wide code of conduct or crisis protocol under Articles 45–48. Therefore, no compliance monitoring under those provisions was applicable. <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. The compliance officer demonstrably performed core responsibilities related to risk oversight, audit coordination, and internal advisory. The risk identification and mitigation process were operational and tracked, and compliance monitoring with DSA obligations was in place.</p> <p>However, broader staff engagement and the formal documentation of DSA training and communication initiatives could be strengthened.</p>	
<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; Develop a formal internal compliance reporting dashboard with traceable escalation actions; Reassess applicability of Articles 45–48 and document internal readiness to monitor those frameworks when adopted. 	<p>Recommended timeframe to implement specific measures:</p> <p>The identified measures should be implemented within 8-12 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 European Commission; If applicable, the same communication was prepared for the Digital Services Coordinator (DSC) of the Member State of establishment. 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> Reviewed internal appointment records for the compliance officer (Mr. David Hradecký), including internal decision logs and organizational chart references. Interviewed management, who confirmed that the contact information for the compliance officer was transmitted to the Commission shortly after appointment; Assessed contextual legal constraints in the Czech Republic: <ul style="list-style-type: none"> As of the audit period, the Czech Telecommunications Office (CTU) had been designated as the future Digital Services Coordinator (DSC), but did not yet exercise formal supervisory powers, as the national adaptation law had not been enacted; 		

<ul style="list-style-type: none"> Therefore, while the DSC of establishment was nominally identified, no official communication channel or operational intake procedure was available during the audit period. <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 41.5.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <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. 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> Reviewed the Compliance Statute (MD_S_0_Compliance Statute_V1_DRAFT), which outlines the formal role and reporting lines of the compliance function. It confirms that the compliance officer reports directly to the management body and is not part of operational or commercial departments, safeguarding functional independence. Inspected the Compliance Policy (MD_S_3_Compliance Policy_V1_FINAL), which sets out the division of responsibilities between operational teams and compliance officers. It specifies that compliance reviews and risk assessments are coordinated by the compliance function but require board oversight and endorsement, establishing dual accountability. Reviewed the Leadership Declaration (MD_S_1_Compliance_Declaration_Leadership), in which the management body acknowledges its responsibility for compliance oversight, conflict-of-interest prevention, and resource allocation to the compliance structure. The declaration confirms the board's commitment to integrity and independence. Inspected the Risk Management Guideline (MD_G_01_Risk Management Guideline_V1_FINAL). It designates the management body as the approver of systemic risk assessments and defines escalation paths. The document provides a structured framework for how systemic risk ownership is distributed and reviewed at the governance level. Conducted interviews and reviewed governance records, which confirmed that during the assessment period: <ul style="list-style-type: none"> The compliance function had unmediated access to the board; Risk reporting was integrated into periodic management reviews; The compliance officer had not been reassigned, indicating structural stability; 		

<ul style="list-style-type: none"> No active conflicts of interest were disclosed, and conflict-monitoring responsibilities were assigned to the compliance function. <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 41.6.</p>	<p>Audit criteria:</p> <p>Throughout the period, in all material respects:</p> <ul style="list-style-type: none"> 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. 	<p>Materiality threshold:</p> <p>N/A</p>
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> Reviewed the Risk Management Guideline (MD_G_01_Risk Management Guideline_V1_FINAL), which assigns the approval of the risk register and associated mitigation strategies to the management body. The guideline specifies that periodic reviews must occur at least annually or following significant risk events. Inspected the Compliance Policy (MD_S_3_Compliance Policy_V1_FINAL), which mandates that strategic risk responses, including mitigation pathways, be documented and approved at the board level. The policy outlines collaboration between the compliance function and the board in reviewing mitigation measures. Reviewed the Compliance Declaration (MD_S_1_Compliance_Declaration_Leadership) signed by management, affirming their oversight responsibility for systemic risk exposure and the design and review of risk-mitigation policies. Reviewed versioning and approval records embedded in the compliance documents and guidelines, which showed that several risk governance policies were established and signed off by senior leadership during the review period. However, no dedicated board-level minutes or annual strategic risk review records were included in the audit file. Conducted interviews with the compliance officer and senior managers, who confirmed that risk mitigation strategies, including those covering disinformation, content safety, and profiling, were brought before management during internal planning sessions and risk assessment briefings. Noted absence of a central board approval log specific to risk strategies but established that review and validation of risk frameworks were embedded into broader compliance oversight processes at the management level. <p>Conclusion:</p> <p>Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Risk mitigation policies were defined and reviewed</p>		

under the governance of the management body, and systemic risk categories under Article 34 were documented and linked to strategic response measures.

However, formal documentation of annual board-level review and sign-off of these strategies could be improved for traceability and audit readiness.

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:

- 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 (MD_G_01_Risk Management Guideline_V1_FINAL), which designates the management body as the responsible entity for validating systemic risks and approving mitigation resource allocation. It references periodic engagement of leadership on risk-related decisions.
2. Reviewed the Compliance Policy (MD_S_3_Compliance Policy_V1_FINAL), which states that resource planning — including staffing, tooling, and external advisory support — must be aligned with risk exposure as assessed under Article 34 and be overseen by senior management.
3. Reviewed the Compliance Declaration by Leadership, which affirms that management acknowledges its role in allocating sufficient personnel and infrastructure to ensure operational risk mitigation capacity.
4. Interviewed the compliance officer, who indicated that during the reporting period:
 - Dedicated staff were assigned to content moderation, data privacy, and technical platform integrity;
 - The management body was consulted during the development of the risk register and approved the prioritization of mitigation tracks;
 - Budgetary resources were approved for implementing friction-based design changes and compliance analytics tools.

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. Reviewed transparency reports published by the provider for:

- February–May 2024 (first reporting period); and
- June–December 2024 (second reporting period).

Version control dates confirmed that these documents were finalized within the regulatory timeframes required by Article 42(1). Together, they evidenced a semiannual reporting cadence, meeting the frequency requirement of at least once every six months.

2. The reports were reviewed to confirm that they were published within two months of the relevant reporting period. Internal documentation showed that the compliance team maintained a calendar of key DSA deliverables, including report deadlines, and that report drafting and approval workflows were initiated in advance to meet statutory deadlines.
3. Through interviews with the compliance officer, it was confirmed that transparency reporting is integrated into the provider's broader DSA governance framework. The compliance team was responsible for drafting and coordinating approval of the reports, with direct reporting lines to the senior management.
4. The audit independently verify that the reports were made publicly accessible on the XVideos.com: section "Information and Links" (on the website's footer) → "Legal stuff" → "Mandatory information / 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: <ol style="list-style-type: none"> 1. The XVideos “Transparency Report – June to December 2024” and the “WGCZ Yearly Transparency Report” were reviewed in detail. The reports contained dedicated sections presenting the number of human resources allocated to content moderation, disaggregated by each applicable official EU language. These included full-time equivalents (FTEs) and total moderator counts across multiple regional and linguistic segments. Staffing data were presented in tabular format and covered at least the major EU languages served by the platform. 2. The audit reviewed narrative sections of the reports that described the qualifications required for moderation staff. These included minimum experience requirements, demonstrated linguistic proficiency, and familiarity with relevant content safety frameworks. In addition, reference was made to onboarding procedures and ongoing training programs provided to moderators. The documentation noted that linguistic expertise was matched to language-specific moderation requirements, although varying levels of detail were provided across language categories. 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. The audit confirmed that the transparency reports were published in English, which is one of the official languages of the European Union. While English suffices for DSA compliance, the reports did not include additional translations for other EU audiences. Nonetheless, publication and accessibility requirements were deemed to be met. <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. Transparency reports contained relevant staffing, qualification, and accuracy information as required. However, the presentation of moderator qualifications and linguistic segmentation varied in structure across documents and would benefit from improved standardisation and expanded coverage for smaller language groups.</p>		
Recommendations on specific measures: <ul style="list-style-type: none"> • Develop and apply a consistent table structure for reporting human moderation resources and qualifications by language across all reporting periods; • Include a structured overview of moderator training content, frequency, and evaluation methods, with clarity on updates between cycles; 	Recommended timeframe to implement specific measures: The identified measures should be implemented within 9 months.	

<ul style="list-style-type: none"> Ensure that language-specific accuracy data are included for all major and medium-volume EU languages, and clarify methods used where aggregation is applied. 	
---	--

Obligation: Article 42.3.	Audit criteria: 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. 	Materiality threshold: N/A
Audit procedures, results and information relied upon: <ol style="list-style-type: none"> The “XVideos Transparency Report – June to December 2024” and the “WGCZ Yearly Transparency Report” were reviewed. Both reports included a dedicated section outlining user metrics, specifically the number of average monthly active recipients of the platform per Member State. The data was structured in tabular format and included figures for each of the 27 EU Member States. The reports were found to be published in English, fulfilling the requirement of being available in at least one official EU language. The relevant metrics were publicly accessible on the provider’s dedicated transparency landing page. <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 42.4	Audit criteria: Throughout the period, in all material respects: <ul style="list-style-type: none"> The provider transmitted to the Digital Services Coordinator of establishment and the Commission, 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); 	Materiality threshold: N/A
------------------------------------	--	--------------------------------------

	<ul style="list-style-type: none"> ▪ The provider made these information publicly available within three months of receiving the audit report. 	
<p>Audit procedures, results and information relied upon:</p> <ol style="list-style-type: none"> 1. Inquired compliance team to gain an understanding of the internal processes and timelines for transmitting risk-related documentation to the Commission and the Digital Services Coordinator. 2. Verified the existence and content of the transmitted documentation. 3. Confirmed with the compliance team that these documents were submitted to the competent authorities. 4. Acknowledged that this is the provider's first audit conducted pursuant to Article 37. Therefore, no audit report or audit implementation report had yet been issued, submitted, or published by the provider. 5. Identified that, accordingly, no publication obligation under Article 42(4) had yet arisen. The deadline to publish the documents listed under points (a) to (e) only begins once the audit report is received. As such, the provider was not yet required to make the reports publicly available and had not done so at the time of the audit. <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>

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.
40.8-40.11	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:	
XVideos.com (adult-content video-sharing platform)	
2. Audited provider:	
WebGroup Czech Republic a.s. (WGCZ)	
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.xvideos.net/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 WGCZ.
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.)	23 April 2024 – 23 April 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 WGCZ 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:
11 November 2024 (fieldwork commenced)	21 March 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 Kolembus (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:	
Lead auditor Marián Kolembus graduated from the Slovak University of Technology in Bratislava, Faculty of Chemical Technology. In the period 1997-2003 he worked at ISTROCHEM, as a quality specialist and subsequently as the head of the metrology department. Since 2003 he has been working at TEMPEST, as, where he is a senior consultant engaged in professional consultations in the areas of management systems, process improvement, business continuity management, risk analysis in the area of information security and security projects and development of security documentation, implementation and maintenance of information security management systems, ensuring personal data protection and project management. He began working as an external lead auditor of management systems in 2016, and is currently the lead auditor of eight management systems at the CERTICOM certification body - ISO 9001: Quality Management System, ISO 14001: Environmental Management System, ISO 45001: Occupational Health and Safety Management System, ISO/IEC 20000-1: IT Service Management System, ISO 22301: Business Continuity Management System, ISO/IEC 27001: Information Security Management System, ISO 37301: Compliance Management System and ISO 37001: Anti-Corruption Management System. (https://www.certicom.sk/nas-tim-certicom/)	
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 	

<p>- 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> <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:
a. Declaration of interests
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 WebGroup Czech Republic a.s.; 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.
b. References to any standards relevant for the auditing team's independence that the auditing organization(s) adheres to
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
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
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
a. Audit opinion for compliance with the audited obligations referred to in Article 37(1), point (a) of Regulation (EU) 2022/2065:
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.
b. Audit conclusion for each audited obligation:
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
a. Audit opinion for compliance with the commitments made under the Code of Conduct or crisis protocol covered by the audit:
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.
b. Audit conclusion for each audited commitment:
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: 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:

a. 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:	
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.	
b. Description, explanation, and justification of any changes to the audit procedures during the audit:	
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.	
c. Results of the audit procedures, including any test and substantive analytical procedures:	
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:	
a. 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:	
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:	21.04.2025	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 WebGroup Czech Republic a.s., provider of the platform XVideos.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 23 April 2024 to 23 April 2025, corresponding to the first full year of DSA compliance obligations following the platform's designation as a Very Large Online Platform (VLOP) on 23 December 2023.

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