CERTICOM
CERTIFIKÁCIA SYSTÉMOV MANAŽÉRSTVA

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: 23 April 2026

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 64

Appendix 3 – Template for the Audit Report Referred to in Article 6 of Delegated Act 66

Appendix 4 – Audit Risk Analysis 69

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 (“EC”) 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 2025 to 23 April 2026. The audit was conducted independently by CERTICOM in accordance with ISAE 3000 (Revised).

This report is intended for submission to the EC 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 2025 to 23 April 2026. 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 non-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 EC 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 in April 2026 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.

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 DSA and Commission Delegated Regulation (EU) 2023/6807. The audit covers the period from 23 April 2025 to 23 April 2026.

XVideos.com is an adult-content video-sharing platform offering access to audiovisual content uploaded by users and content creators. The platform is accessible across EU Member States, supports multilingual Terms of Service (“TOS”), and operates with optional user registration. Given the nature of the service, the audit placed particular emphasis on illegal-content moderation, protection of minors, NCII, CSAM, recommender-system transparency, advertising transparency, systemic-risk assessment and mitigation, data-access readiness, and compliance governance.

The audit assessed the provider's compliance with obligations arising under Chapter III of the DSA, with particular focus on:

- contact points for authorities and users;
- TOS transparency and content moderation rules;
- notice-and-action and internal complaint-handling mechanisms;
- trusted flagger handling;
- misuse-management obligations under Article 23;
- advertising transparency and the advertising repository;
- recommender systems and non-profiling options;
- protection of minors;
- systemic risk assessments and mitigation measures;
- data access and regulatory cooperation;
- compliance function and management-body oversight;
- transparency reporting.

The audit methodology followed ISAE 3000 (Revised) and included structured interviews with senior management, the Compliance Function, Legal Team, Regulatory Director, Content Moderation Team, Notice and Complaint Team, IT Team and other relevant personnel. The procedures also included review of internal policies, process guidelines, transparency reports, risk assessment documentation, mitigation registers, system walkthroughs, interface checks, and selected evidence of regulatory cooperation and operational controls.

The provider cooperated with the audit team and provided access to relevant personnel, documentation and explanations necessary for the audit procedures. Where confidential regulatory correspondence or commercially sensitive technical information was reviewed, the audit considered procedural handling, governance and evidence of submission without reproducing confidential content in this report.

Key Findings:

- **POSITIVE - 55 obligations (approximately 81%)** were assessed as compliant in all material respects. These obligations were supported by operationally implemented controls, documented processes, or sufficient evidence of effective practice. Positive findings included, among others, the authority and user contact points under Articles 11 and 12; multilingual and accessible TOS under Article 14; the transparency reporting framework under Articles 15 and 42; notice-and-action mechanisms under Article 16; the internal complaint-handling system under Article 20; trusted flagger prioritisation under Article 22; publication and substantiation of average monthly active recipient figures under Articles 24(2) and 24(3); anonymised submission of Statements of Reasons to the DSA Transparency Database under Article 24(5); interface design under Article 25; advertising transparency under Article 26(1); the prohibition of special-category advertising profiling under Article 26(3); the non-profiled recommender option under Article 38; the advertisement repository obligations under Articles 39(1), 39(2) and 39(3); data-access and regulatory cooperation obligations under Article 40; compliance governance under Article 41; and systemic-risk documentation retention under Article 34(3).
- **POSITIVE WITH COMMENTS** - 12 obligations (approximately 18%) were assessed as compliant in all material respects, with areas for further formalisation, traceability or enhancement. These findings related to Articles 17(1)–(4), where statement-of-reasons communications are operational but should be further standardised; Article 18(2), where law-enforcement escalation exists but the fallback procedure for unidentified Member States should be more expressly documented; Articles 23(1), 23(2) and 23(3), where misuse and repeat-violation controls exist but require further formalisation, especially for manifestly unfounded

notices and complaints; Article 24(1), where transparency reporting is operational but Article 23 suspension categories and zero-case disclosures should be improved; Articles 27(1) and 27(2), where recommender parameters are disclosed but the relative importance of parameters should be clearer in the TOS; Article 28(1), where a layered minor-protection framework exists but stronger age-assurance measures remain under assessment; Articles 34(1) and 34(2), where systemic risk and risk-driver assessments were materially strengthened but should continue to develop quantitative evidence and supervisory feedback integration; and Article 35(1), where mitigation measures are broad and documented but protection of minors remains a high-priority residual risk.

- **NEGATIVE** - 1 obligation (approximately 1%) was assessed as not fully compliant in all material respects. This finding relates to Article 23(4). The provider's TOS included general prohibitions on illegal content and account-enforcement rights but did not yet describe in sufficient detail the specific misuse policy required under Articles 23(1) and 23(2), including clear examples of misuse, assessment factors, warning logic, suspension nature and duration, and related user-facing consequences. The deficiency is therefore primarily one of user-facing policy transparency and formalisation, rather than evidence of absence of all enforcement activity.

The audit concludes that WGCZ broadly complied with its DSA obligations during the examination period. The provider significantly strengthened its compliance framework compared to the previous review cycle. Key improvements include formalised content moderation guidelines, enhanced complaint-handling documentation, operational trusted flagger workflows, improved transparency reporting, anonymised submission of Statements of Reasons to the DSA Transparency Database, updated advertising transparency, a structured Mitigation Measures Register and Dashboard, a Recommender System Guideline, data-access readiness materials, and formalised compliance governance.

The provider also actively engaged with regulatory developments. The Compliance Officer, Legal Team, and Regulatory Director confirmed that the provider is considering its response to the EC's preliminary findings, remains in dialogue with the EC, and intends to comply with DSA requirements. These factors were considered as context in assessing Articles 28, 34, and 35, particularly regarding the protection of minors and age-assurance measures.

The audit used a contextual and risk-based approach consistent with the DSA, Delegated Regulation, and the proportionality principle. Ongoing improvements were not classified as non-compliance if the provider met the essential compliance threshold in all material respects. The only negative finding relates to Article 23(4) and does not indicate systemic non-compliance within the broader DSA control environment.

Overall, the provider's compliance posture is assessed as substantially mature and improving. Continued focus is recommended on finalizing the Article 23 misuse-policy framework in the TOS, further standardizing statements of reasons, strengthening quantitative risk-assessment evidence, documenting responses to EC supervisory feedback, and advancing effective, privacy-preserving age-assurance measures.

Bratislava, Slovakia 23 April 2026

Ing. Marek Krajčov, Company manager
Director of Certification body CERTICOM

Appendix 1 – Conclusions and Test Procedures per Obligation

List of Abbreviations

For ease of reference, the table below provides the abbreviations and acronyms used throughout this Independent Audit Report.

Abbreviation	Meaning
AD	Advertisement
ADR	Alternative Dispute Resolution
API	Application Programming Interface
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CERTICOM	CERTICOM s.r.o. / certification body performing the audit
CSAM	Child Sexual Abuse Material
CSV	Comma-Separated Values
ČTÚ	Czech Telecommunications Office / Český telekomunikační úřad
DMCA	Digital Millennium Copyright Act
DSA	Digital Services Act / Regulation (EU) 2022/2065
DSC	Digital Services Coordinator
EC	European Commission
EEA	European Economic Area
EU	European Union
FTE	Full-Time Equivalent
GDPR	General Data Protection Regulation / Regulation (EU) 2016/679
HTML	HyperText Markup Language
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
IESBA	International Ethics Standards Board for Accountants
IFAC	International Federation of Accountants
IP	Internet Protocol
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
LEA	Law Enforcement Authority
NCII	Non-Consensual Intimate Imagery
NGO	Non-Governmental Organization
PC	Personal Computer
QA	Quality Assurance
RFI	Request for Information
RTA	Restricted to Adults
SNAS	Slovak National Accreditation Service
SOP	Standard Operating Procedure
TOS	Terms of Service
UK	United Kingdom
URL	Uniform Resource Locator
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine
VPN	Virtual Private Network
WGCZ	WebGroup Czech Republic a.s.

Section 1 – Provisions Applicable to All Providers of Intermediary Services

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 11.1	Throughout the period, in all material respects: ▪ An intermediary service contact was designated; ▪ The Member States' authorities, the EC and the Board were able to communicate directly by electronic means with the intermediary service contact.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA contact point for authorities, and the position remains unchanged.

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: Contact us - Xvideos.com
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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 11.2	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA contact point for authorities, and its accessibility and presentation remain unchanged.

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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 11.3	Throughout the period, in all material respects: ▪ 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:

No changes were identified since the previous review of the DSA contact point for authorities, including its accessibility and the specified communication languages, which remain unchanged.

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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 12.1	Throughout the period, in all material respects: ▪ 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:

No changes were identified since the previous review of the DSA contact point for service recipients, including its accessibility, response handling transparency and language accessibility, which remain unchanged.

1. Conducted a walkthrough of the designated point of contact for service recipients on the provider's publicly accessible "Contact Us" page: https://info.xvideos.net/contact-us. Examined the publicly available contact point for users and confirmed that it is presented as the single point of contact for users pursuant to Article 12 of the DSA.
2. Observed that the contact page provides a communication channel by electronic means through a dedicated contact form for users, which is publicly accessible and user-friendly in design and structure.
3. Verified that the contact point remains publicly accessible via the provider's website interface and is clearly titled as a contact point for users.
4. Examined the instructions accompanying the contact form and confirmed that users are provided with clear guidance on how to use the form and when alternative forms should be used, depending on the nature of the request.
5. Examined Article 12 of the publicly available TOS (ToS), which describes communication channels for general inquiries and specific categories of user requests. Review of the ToS confirmed that the links provided correspond to the publicly available form on the website.
6. 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-us ; 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.
7. Observed that the provider now publicly discloses expected response handling information, including that an automated acknowledgement may be sent upon receipt and that responses are typically provided within 5 business days, subject to exceptions where additional verification, information, or higher request volume may apply.
8. Confirmed that the provider states that messages submitted through this form are not routed or assigned solely by automated tools and that each message is handled and reviewed by a human.
9. Examined the language accessibility information on the contact page and confirmed that users may contact the provider in English or Czech, while responses are generally provided in English
10. Based on the above procedures, we noted that the provider addressed the prior audit recommendation to improve transparency around response handling and language accessibility.

Conclusion:

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

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

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

	▪ 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.	

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA contact point for users, including its accessibility and presentation, which remain unchanged.

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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 14.1	Throughout the period, in all material respects: ▪ 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;	N/A

	▪ 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.	

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related TOS, including the transparency of moderation rules and complaint mechanisms, which remain unchanged.

1. Auditors accessed the publicly available TOS on the provider via the "Legal Stuff" section, available at:XVideos Terms of service - Xvideos.com. 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 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 use.
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 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 14.2	Throughout the period, in all material respects: ▪ The provider has established procedures to define and track what constitutes a "significant change" to the TOS (TOS); ▪ The provider publishes the updated TOS in a prominent, publicly accessible location, clearly stating the effective date. ▪ The provider uses available and reasonable mechanisms to inform recipients of the service, considering its technical and user model limitations; ▪ Any key changes are made transparent through summaries or changelogs, when feasible.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related process for updating and publishing the TOS, which remains unchanged.

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 Team and Compliance Team are responsible for identifying, reviewing, and publishing update.
3. Inspected the public webpage [XVideos Terms of service - Xvideos.com] 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.

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 14.4	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related measures under Article 14(4), which remain unchanged.

1. Performed interviews with Content Moderation team and Compliance Officer to understand the measures implemented by the provider to ensure that restrictions under Article 14(1) are applied diligently, objectively, and proportionately.
2. Examined the provider's formal internal document Content Moderation Process Guidelines, version MD-G-001, dated 1 March 2026, and confirmed that it establishes a unified moderation governance framework covering objectives, scope, roles and responsibilities, moderation workflow, notice-and-action, complaint handling, and enforcement measures.
3. Reviewed the guideline and confirmed that moderation personnel are required to act in accordance with proportionality, necessity, transparency, non-discrimination, and protection of fundamental rights, and that final enforcement decisions are not taken solely based on automated means.
4. Examined the moderation workflow and confirmed the existence of a structured process combining automated detection tools with human review, including escalation pathways for ambiguous or high-risk cases, documented decision categories, and traceable logging of enforcement actions.
5. Reviewed the notice-and-action and complaint-handling sections and confirmed that notices and complaints are processed through a documented ticket-based workflow, including evidence requests, reasoned final decisions, user notification, and internal review of appealed decisions.
6. Examined the sections on supervision, training, and misuse-related enforcement and confirmed that the provider has formalized responsibilities for moderator oversight, onboarding and training, and introduced a documented three-strike policy for repeated violations and abusive conduct.
7. Based on the above procedures, we noted that the provider has addressed the prior audit recommendation to formalize the moderation and notice lifecycle, define escalation logic, and implement a structured policy basis for repeated misuse cases.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 14.5	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related summary of the TOS, including its accessibility and content, which remain unchanged.

1. Accessed the publicly available summary of TOS through the "Legal Stuff" section of the provider's website: XVideos Terms of service - Xvideos.com. 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 labelled, 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.

Conclusion:

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

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

Obligation: Article 14.6	**Audit criteria:** Throughout the period, in all material respects: ▪ 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:

No changes were identified since the previous review of the DSA-related publication of the TOS in the official EU languages, which remains unchanged.

1. Conducted a walkthrough of the provider's website at XVideos Terms of service - Xvideos.com 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: ▪ 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 the provider's public mandatory information page and confirmed that transparency reports for January-June 2025 and July-December 2025 are publicly accessible via the provider's official website: https://info.xvideos.net/legal/mandatory-information.
2. Reviewed the July-December 2025 transparency report published in a structured machine-readable CSV format and confirmed that the report package contains separate data tables covering report identification, average monthly active recipients, government orders, notices, own-initiative moderation, complaints, automated means, human resources, and qualitative disclosures.
3. Confirmed continued semi-annual publication of transparency reports. The reviewed package identifies a publication date of 28 February 2026 and references the previous report published on 29 August 2025, thereby exceeding the minimum annual frequency required by Article 15 DSA.
4. Examined the section on government orders and confirmed that the report now includes data on orders received under Articles 9 and 10 DSA, including content categories, scope by issuing Member State(s), and median response times.
5. Examined the section on notices under Article 16 and confirmed that the report includes the number of notices received, the number of specific items reported, median time to action, whether notices were submitted by trusted flaggers, and a distinction between actions taken based on law and actions taken based on the provider's ToS.
6. Reviewed the sections on own-initiative moderation and confirmed that the report provides both quantitative and qualitative information on proactive moderation, including content categories, types of restrictions applied, exposure indicators, and descriptions of human and automated moderation measures.
7. Examined the section on the internal complaint-handling system and confirmed that the report includes the number of complaints submitted, relevant complaint categories, outcomes (including upheld and reversed decisions), and median handling times.
8. Reviewed the disclosures on automated means and confirmed that the report now provides tool-specific information on purpose and performance, including reported accuracy, precision, and recall metrics for selected tools, together with data on measures taken solely by automated means and measures involving human review.
9. Based on the above procedures, we noted that the provider has addressed the prior audit recommendations to publish transparency reports in a machine-readable format, distinguish between law-based and TOS-based enforcement, and expand disclosures relating to automated moderation tools and moderation resources.

Conclusion:

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

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 16.1	Throughout the period, in all material respects: ▪ 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).	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's notice and action mechanism, including the accessibility, visibility and functionality of the electronic reporting channels, as well as the allocation of responsibilities for handling notices.

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:
    - Using the "Report" Button available on each video page.
    - Filing a dedicated abuse reporting form: https://info.xvideos.net/takedown-amateur

    The copyright violations, a separate DMCA-based form is provided https://info.xvideos.net/takedown.
2. 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 menu of issue types, a free text field for contextual information, and fields for optional contact information (name and email).
3. 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.
4. 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.
5. 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.
6. The audit team was provided with the "*Notice and Action – XVideos – process description*" workpaper, which describes the provider's notice and action mechanism and confirms the existence of three electronic notice submission channels: the abuse reporting form, the copyright infringement reporting form, and the in-content reporting button. The workpaper indicates that these mechanisms are easy to access, user-friendly, and enable notices to be submitted exclusively by electronic means. It also illustrates the visibility of the reporting

button underneath individual content and documents the notice-handling workflow, including automatic ticket creation, moderator review, category-based filtering, chronological handling of reports, and escalation or communication steps where additional evidence is required. This supports the assessment that the provider has an accessible and functional reporting mechanism across user interfaces and a clearly defined process for assigning responsibility for handling submitted notices.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 16.2	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's reporting form, including the availability of fields for a reasoned explanation, exact content location, reporter identification details, and a good faith declaration.

1. Reviewed the TOS, specifically the section "Notice and Action Procedure." The TOS state that to be valid, a report must include:
    - 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.

    The TOSs explicitly warns that failure to include this information may result in the notice being delayed or invalidated.
2. Accessed the platform interfaces as end users to evaluate the usability and data fields of both reporting mechanisms available on the platform:
    - The contextual "Report" button beneath each video, and
    - The dedicated "Abuse Reporting Form" found under the "Content Removal" section.

    For both channels:
    - The forms present a predefined violation categories: CSAM, 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;
- 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 have a good faith belief that the information and allegations contained therein are accurate and complete."* ((16.2(d))).

3. The Compliance Officer provided the "Notice and Action – XVideos – process description" workpaper, which describes the provider's notice submission mechanisms and confirms that the available reporting forms include fields enabling the submission of all elements required under Article 16.2, including a substantiated explanation, exact electronic location of the content, notifier identification details, and a good faith declaration. The workpaper also outlines the subsequent notice handling workflow, including ticket creation, moderator review, classification, communication with users where additional evidence is required, and decision outcomes.

Conclusion:

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

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

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

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's process for confirming receipt of submitted notices, including the automatic and timely issuance of confirmation emails where electronic contact details are provided.

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.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 16.5	Throughout the period, in all material respects: ▪ 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:

No changes were identified since the previous review of the provider's decision notification process, including the timely communication of outcomes to notifiers, information on redress options, and traceable documentation of any implemented restrictions.

1. 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.
2. 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.
3. 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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 16.6	Throughout the period, in all material respects: ▪ 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.	N/A

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, collecting the URL, content type, reporting reason, and optional contact details.
2. Reviewed the *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026. The guideline establishes a formal framework for the provider's content moderation and notice-and-action processes, including roles and responsibilities, moderation workflows, use and limits of automated tools, human review requirements, escalation paths, notice handling, and complaint handling. It also aims to provide operational clarity and ensure consistent implementation of moderation decisions across the platform.
3. The guideline confirms that the Notice and Complaint Team is responsible for receiving and evaluating notices submitted through the notice-and-action mechanism, assessing their legal qualification, coordinating interim actions when needed, and working with the Legal Team and Compliance Office in complex or borderline cases. It also specifies that content moderators maintain audit trails and ensure that decisions are based on evidence.
4. Reviewed the notice handling workflow described in the guideline. Each notice submitted through official reporting channels automatically creates a ticket in the internal notice-and-action tool. The ticket serves as the formal case file and records the notice text, reported content identifier, timestamps, moderator actions, communications, evidence requests, and outcome. The guideline requires that actions taken during review are reflected in the ticket record.
5. The guideline states that notices must be handled in a timely, diligent, non-arbitrary, and objective manner. Moderators must make a genuine effort to understand the notice, assess the reported content, request clarification when necessary, and apply the platform's rules and legal obligations consistently based on verifiable facts and legal criteria.
6. Reviewed the provider's documented use of automated tools. The guideline confirms automated systems support human moderation by applying checks and flagging potentially problematic content for review. However, automated systems do not make final enforcement decisions. Content flagged by automated tools must be reviewed by human moderators, and enforcement actions like takedown, ghosting, or account sanctions are reserved for trained moderators after confirming a violation.
7. Reviewed the final decision process described in the guideline. Content Moderators must issue a final decision after completing the review and considering relevant evidence. The decision must classify the notice as legitimate or illegitimate, select the relevant violation category if applicable, and determine whether interim measures are lifted or converted into enforcement action. When the ticket closes, the system sends a reasoned decision email to the reporting user, including the outcome, concise reasons, reference to the reported content, and information on the internal complaint-handling system.
8. 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.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 17.1, 17.2	Throughout the period, in all material respects: ▪ 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.	A performance materiality threshold of 5 % was applied for this obligation.

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. After the examination period, the provider also mapped the statement of reasons process in greater detail and commenced work on further formalising notification workflows across restriction types and user categories.
3. 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. We further note that the provider has subsequently mapped the statement of reasons process and commenced work on strengthening the relevant internal framework so that the process operates more consistently and transparently across enforcement scenarios.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Consolidate the existing notification practices into a more structured internal framework covering the main enforcement scenarios, including content removal, account-related restrictions, and other relevant limitation measures. ▪ Implement a traceability mechanism (e.g. dashboard view or email log) that records when and how each statement of reason was issued. ▪ Continue the ongoing work on mapping and formalising the statement of reasons process across different user account types and restriction categories, so that notification workflows are applied more consistently and can be more easily evidenced.	Within 9 months, to align with the upcoming annual compliance review cycle.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 17.3, 17.4	Throughout the period, in all material respects: ▪ Each statement of reason contains: – 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.	A performance materiality threshold of 5 % was applied for this obligation.

Audit procedures, results and information relied upon:

1. Reviewed a sample of notification emails and internal moderation logs. Each notice includes:
    - 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. At the same time, the provider has already identified the need to further standardise statements of reasons and has commenced work on templates and a more structured internal framework for these communications.

3. Notifications are easy to understand and include a link to the internal complaint form. However, statements do not always specify in sufficient detail whether the content was considered illegal or whether it was restricted solely for non-compliance with the platform's terms. Legal citations, jurisdictional references, and automation-related disclosures are not consistently included, even where such information would be relevant. The provider has acknowledged these shortcomings and is working on improvements intended to make statements of reasons completer and more consistent, although these measures were not yet fully implemented at the time of review.

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:

Positive with comment – Positive with comment – 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 the underlying reasons, the level of specificity and completeness required by the DSA is not always fully met in practice. In particular, legal basis references, differentiation between legal and TOS grounds, and certain additional disclosure elements are not yet communicated consistently in all cases. We further note that the provider has already commenced work on templates and related internal measures intended to improve the consistency, completeness and overall quality of statements of reasons, although these measures were not yet fully implemented at the time of review.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Continue the ongoing work on standardising statements of reasons through structured templates that incorporate, where relevant, (i) whether automation was involved; (ii) whether the restriction stems from legal or TOS grounds, with appropriate references; and (iii) the geographic scope and expected duration of the restriction, where applicable. ▪ Establish and maintain a centralized template library with version control in order to improve consistency, traceability and auditability across moderator teams and enforcement types. ▪ Implement a cross-checking process to ensure that all required Article 17(3) elements are present in each communication; ▪ Further enhance redress information so that statements of reasons more clearly reflect the available channels, including the internal complaint-handling system, out-of-court dispute settlement where applicable, and other legal remedies.	Within 9 months, to align with the upcoming annual compliance review cycle.

Obligation:	Audit criteria:	Materiality threshold:
Article 18.1	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the TOS, particularly Chapter 4 “Terrorism and Physical Harm Violence”, which prohibits content promoting terrorism or physical harm and affirms such content is removed and reported to law enforcement according to applicable laws.
2. Interviewed Head of Content Moderation Team and confirmed an established internal content moderation process including the obligation to report illegal content to authorities.
3. Reviewed the *Content Moderation Process Guidelines*, document version MD-G-001, dated 1 March 2026. The guideline establishes formal procedures for content moderation, escalation, enforcement, data preservation, and cooperation with law enforcement. It confirms the guideline applies to moderation workflows and is binding for personnel involved in moderation or related decision-making.
4. Verified the guideline defines categories of content subject to moderation, including illegal content such as CSAM, NCII, real sexual violence, terrorism-related content, extortion, blackmail, harassment, human trafficking indicators, and other content indicating threats to life or safety. It also defines the internal “Bad” classification for content that is undoubtedly illegal and triggers immediate escalation.
5. Reviewed the documented human moderation and advanced review process. The guideline confirms that when content is classified as “Bad” and requires cooperation with law enforcement, advanced reviewers must follow mandatory escalation and reporting. The process includes human review and confirmation before final enforcement and escalation.
6. Reviewed the documented cooperation with law enforcement procedure. The guideline specifies that when content is undoubtedly illegal and raises suspicion of serious criminal offences, especially those threatening life or safety, an enhanced enforcement pathway applies. This includes immediate content deletion, termination of the uploader’s account, preservation of relevant data in a restricted environment, and cooperation with law enforcement.
7. Verified the guideline describes the information and reporting process for law enforcement. Preserved data includes uploader data and other relevant information available to the provider. This data is stored in a restricted database for cooperation with verified law enforcement authorities. Verified police with access to the internal LEA tool are notified when new content relevant to their jurisdiction is preserved and can access the reported content, uploader information, and related metadata through the tool.
8. Verified the guideline documents system-managed preservation and submission controls. Content Moderators are instructed not to export or store preserved evidence locally. When content raises suspicion of a serious criminal offense, the case is submitted through the established LEA channel. After submission, the content is hidden from moderators, and the system displays a confirmation that it has been sent to law enforcement.

9. Verified the guideline also documents supplementary cooperation with the Czech reporting portal stoponline.cz, operated by CZ.NIC, for illegal content identified outside the provider's services where moderators have no authority or means to remove it. The guideline states that LEA escalations and external reporting actions are confidential and recorded in the internal audit trail.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 18.2	Throughout the period, in all material respects: ▪ The provider had a procedure in place for notifying the authorities of the Member State of its establishment or informing Europol or both, if the relevant Member State could not be identified with reasonable certainty.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the TOS, particularly Chapter 4 "Terrorism and Physical Harm Violence", which explicitly prohibits any content promoting terrorism or physical harm and affirms that such content is removed and reported to law enforcement in accordance with applicable laws.
2. Reviewed the *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026. The guideline formalizes the provider's moderation framework, including escalation procedures, enforcement measures, data preservation, and cooperation with law enforcement authorities. The guideline states that one of its objectives is to establish clear protocols for human moderator actions and cooperation with public authorities.
3. Verified that the guideline defines categories of content subject to moderation and identifies content classified as "Bad" as undoubtedly illegal content that triggers immediate escalation procedures. The relevant categories include CSAM, NCII, serious sexual violence, terrorist content involving imminent threats to life, extortion or blackmail involving threats to life or safety, human trafficking, and other content indicating an ongoing or completed criminal offence where there is a threat to the life or safety of a person or persons.
4. Reviewed the documented cooperation with law enforcement procedure. The guideline provides that, where content is classified as undoubtedly illegal and gives rise to suspicion of serious criminal offences threatening life or safety, the provider applies an enhanced enforcement pathway. This includes immediate content deletion, uploader account termination, preservation of relevant data in a restricted access-controlled environment, and cooperation with law enforcement authorities through the established LEA process.
5. Verified that preserved data is stored in a restricted database designed for cooperation with verified law enforcement authorities. The guideline states that verified police authorities with access to the internal LEA tool are automatically notified when new content relevant to their jurisdiction is preserved and may access the reported content, uploader information and related metadata through the tool.
6. Verified that the guideline also describes supplementary cooperation with the Czech reporting portal **stoponline.cz**, operated by CZ.NIC, for illegal content identified outside the provider's own services where the provider has no authority or technical means to remove

it. The guideline further states that all LEA escalations and external reporting actions are treated as confidential and recorded as part of the internal audit trail.

7. While the reporting process exists and responsible personnel confirmed that the fallback procedure is known in practice, we did not identify a formalized internal policy or framework explicitly documenting the procedure for informing the Member State of establishment or Europol when the relevant Member State cannot be determined with reasonable certainty. The *Content Moderation Process Guidelines* document the LEA cooperation process generally, including escalation, data preservation and law enforcement access; however, the specific Article 18(2) fallback procedure is not expressly documented.

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:	**Recommended timeframe to implement specific measures:**
Update the *Content Moderation Process Guidelines* to explicitly describe the fallback procedure under Article 18(2), including the requirement to notify the authorities of the Member State of establishment and/or Europol where the relevant Member State concerned cannot be identified with reasonable certainty.	The identified measures should be implemented within 6 months.

Section 3 – Additional provisions applicable to providers of online platforms

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's internal complaint-handling system, including its accessibility to users and notifiers, the scope of appealable moderation and account-related decisions, and its electronic and free-of-charge operation.

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:
    - 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.

    In both cases, users are not required to provide additional login credentials beyond those used to access their accounts, ensuring a seamless experience.
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. The guideline further describes the complaint submission and review process. Following a moderation decision, users are provided with an "Appeal this decision" option within the status interface, enabling them to submit a written explanation and supporting evidence. Once an appeal is submitted, the corresponding ticket is reopened and reviewed against the original decision record, including the violation category, enforcement measure applied, documented reasoning and any new evidence submitted by the complainant. This supports the assessment that the system enables complaints against moderation decisions and operates as an integrated electronic complaint-handling mechanism.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.2.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the TOS, Section 13, outlining user rights following moderation decisions. The public-facing terms refer to the right to lodge a complaint for at least six months following decisions concerning content or account-related restrictions.
2. Reviewed the *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026. The guideline formalizes the provider's moderation and complaint-handling framework, including enforcement measures, pending deletion status, complaint handling, appeal review, and retention of content or account data during the complaint-relevant period.
3. Verified that the guideline distinguishes between content taken down, content deleted, account termination, and account deletion. For content taken down, the guideline states that content remains accessible to the Content Moderation Team and Notice and Complaint Team for processing potential user complaints and remains in pending deletion status for a platform-defined period of at least six months. If no complaint is received within this period, or if a complaint is submitted and rejected, the content transitions to final deletion.
4. The interviewed IT team confirmed that the retention period was extended and that users can file a complaint within six months after the notice is reviewed (at which point the uploader is also informed about the ticket). The reviewed source code supports that

uploader and reporter access to appeal or complaint-related functionality is controlled by a six-month system logic.

5. Reviewed the *Notice and Action – XVideos – process description* workpaper. The workpaper confirms that, after a decision is made, the reporting user may file an appeal and that the system distinguishes between moderator-initiated discussions and user-initiated appeals. It also shows that appeal or discussion status is visible in the moderator interface and that moderators may accept, reject, or escalate/report the case, with manual justification required for escalation.
6. Based on the updated guideline, the previously identified deficiency concerning premature deletion of content after 30 days has been addressed for content moderation decisions, as the guideline now requires content in pending deletion status to be retained for at least six months and to remain accessible to the relevant moderation and complaint teams during that period. For account-related enforcement, the guideline also confirms that account termination remains subject to complaint and that account data is retained for complaint review until the pending deletion period and complaint process are completed.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.3.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's internal complaint-handling system, including its accessibility, user-friendly design, and ability to support the submission of sufficiently precise and adequately substantiated complaints.

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:
    - 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.

3. 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.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.4.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. In the previous audit, the complaint-handling process was demonstrated through a real-time walkthrough of the internal ticketing interface, including how complaints are received, assessed, resolved, and documented. During the current audit, a repeated walkthrough was not performed, as the Content Moderation Team and Notice and Complaint Team confirmed through inquiry that the complaint-handling process has not changed since the previous audit.
2. For the current audit period, conclusions were therefore based on the previously observed process, the updated *Content Moderation Process Guidelines*, the *Notice and Action – XVideos – process description workpaper*, and interviews with representatives of the Content Moderation Team and Notice and Complaint Team.
3. Reviewed the *Notice and Action – XVideos – process description workpaper*. The workpaper documents that, after a decision is made, the reporting user can file an appeal and that the system distinguishes between moderator-initiated discussions and user-initiated appeals. It further shows that the moderator interface identifies whether a case is under appeal or discussion, and that the moderator may accept, reject, or escalate/report the case, with manual justification required for escalation.
4. Reviewed the *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026. The guideline formalizes the internal complaint-handling process and states that the provider maintains a free-of-charge and electronic internal complaint-handling system for discussions and appeals/complaints, implemented directly in the notice-and-action tool and connected moderation interface. The guideline also requires complaints to be handled in a timely, non-discriminatory, diligent and objective manner.
5. Verified that the guideline describes the complaint review workflow. When an appeal is submitted, the corresponding ticket is reopened and the Content Moderator reviews the full original decision record, including the violation category, enforcement measure applied, documented reasoning, the user's appeal explanation, and any supporting evidence

provided. Where new facts or evidence are submitted, the moderator must reassess the content to determine whether those elements affect the original conclusion.

6. Verified that the guideline provides escalation rules for cases where the appeal raises doubts exceeding the moderator's confidence level, such as cases involving age uncertainty, consent, or other complex factual assessments. Such cases must be escalated to the Head of the Notice and Complaint Team for further review.
7. Verified that the guideline requires the moderator to select one of the available complaint outcomes (accept, reject, or escalate) and to support the selected outcome with a concise factual explanation in the ticket fields, ensuring traceability and consistency. The guideline further states that where the appeal provides sufficient grounds to conclude that the original decision was incorrect, the Content Moderator reverses the decision without undue delay.
8. Interviewed members of the Content Moderation Team and Notice and Complaint Team. They confirmed that the complaint-handling process continues to operate as previously demonstrated, that complaints are reviewed manually by trained personnel, that no automated decisions are made at the complaint stage, and that valid complaints resulting in reversal are actioned without undue delay. They further confirmed that the process described in the workpaper and the Content Moderation Process Guidelines reflects the process currently applied in practice.

Conclusion:

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.5.	Throughout the period, in all material respects: ▪ Complainants are informed of the provider's reasoned decision without undue delay; ▪ The decision notification includes – a clear explanation of the outcome, – reference to the out-of-court dispute settlement mechanism (Article 21 DSA); – other available redress options or escalation channels.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's complaint decision notification process, including the timely provision of reasoned outcomes, references to out-of-court dispute settlement, and other available redress or escalation channels.

1. Reviewed communication templates used by provider for notifying users of the outcome of internal complaints. These templates are filled in from the internal ticketing system and include placeholders for (i) moderator rationale for decision, (ii) complaint reference, (iii) a hyperlink to further redress information and out-of-court dispute settlement, (iv) contact email for follow-up queries.
2. Sampled complaint resolution emails sent to users during the audit period. The samples included both accepted and rejected complaints across various violation types (e.g., content takedowns, account restrictions, monetization issues). In each sampled case, the notification included a reasoned explanation, written in accessible language. The explanation typically addressed:
    - The substance of the complaint;
    - The basis for the provider's final decision;
    - Whether the original decision was upheld or reversed.
3. Verified inclusion of redress information in 100% of the sampled communications. The notifications consistently included a brief statement explaining the user's right to challenge the decision externally and a fallback contact (e.g., content@xvideos.com) for further inquiry.
4. Assessed timeliness of notifications by comparing internal timestamps for complaint closure and user notification dispatch. In 10 out of 10 sampled cases, the notification was sent within 48 hours of the complaint decision.

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 20.6.	Throughout the period, in all material respects: ▪ 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;	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's complaint decision-making process, including human supervision by appropriately qualified personnel and the absence of solely automated complaint decisions.

1. Performed interviews with members of the notice and complaint team, who are responsible for receiving and responding to user reports and notices. It was confirmed that no reports were received from trusted flaggers during the examination period, and that no dedicated process exists to flag or prioritise such notices. The team acknowledged that, while general

notices are resolved within 24 hours, no dedicated input channel or technical label exists to distinguish trusted flagger reports from general user notices.

2. Shadowed the complaint-handling and moderation process by observing live sessions with moderators. This included

   It was observed that moderators consistently followed internal procedures, exercised individual judgment, and in complex cases, engaged in peer consultation or escalation to senior personnel.

3. Inspected that all designated personnel had completed onboarding modules, including general moderation principles, platform-specific policy guidance, redress and reversal decision-making criteria.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 21.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's DSA-related arrangements for access to out-of-court dispute settlement, and the position remains unchanged.

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 January-June 2025 and July-December 2025 Transparency Reports 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.
3. 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 Officer 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.

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 22.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA trusted flagger process, including prioritisation, tracking and handling of trusted flagger notices, which remain unchanged.

1. Performed interviews with members of the Notice and Complaint Team and IT Team, who are responsible for reviewing user-submitted notices, including notices submitted by trusted flaggers. The team confirmed that the trusted flagger process has been implemented through a dedicated registration and dashboard workflow, and that trusted flagger notices are distinguished from general user notices within the moderation process.
2. Reviewed the *XVideos Implementation Overview Art. 22 DSA – Trusted Flaggers*. The document confirms that a dedicated trusted flagger section is available on the XVideos information page. This section describes the platform's commitment to cooperate with trusted flaggers and provides onboarding information for organisations seeking to register as trusted flaggers.
3. Reviewed the trusted flagger onboarding process. The implementation overview confirms that trusted flaggers must complete a dedicated registration form, after which the submitted application is manually reviewed by trained personnel. The applicant's trusted flagger status is verified against the official list of trusted flaggers maintained by the EC. Once verified, a dedicated account secured by login and password is created for the trusted flagger.
4. Reviewed the dedicated Trusted Flagger Dashboard. The implementation overview confirms that trusted flaggers have access to a dedicated dashboard enabling them to submit notices of potentially illegal content and track the handling of those notices. The dashboard includes a dedicated "Content removal" submission form and displays processing information such as reported date, last update, review date, status, video reference, and available actions. The implementation overview states that these notices are given priority in processing by the content moderation team.
5. Reviewed the Content Moderation Process Guidelines, document version MD-G-001, dated 1 March 2026. The guideline formally documents the trusted flagger process under Section 6.4 and confirms that the provider maintains a dedicated reporting mechanism for trusted flaggers through a separate section of the platform. It further confirms that only

organisations established in the EU, officially designated by a DSC and listed in the EC's trusted flagger database may be registered.

6. Verified that the guideline documents a dedicated technical and organizational process for trusted flagger notices. Upon validation, a dedicated account is created and activated, and the trusted flagger may submit notices exclusively through the dedicated Authorities and Trusted Flaggers Dashboard. The dashboard supports submission, status tracking, access to outcomes and reasoning, and complaint submission where the trusted flagger disagrees with the provider's decision.
7. Verified that the guideline requires trusted flagger notices to be automatically flagged in the moderation system and displayed at the top of the moderation queue. Content Moderators are required to treat such notices as priority cases. The guideline states that trusted flagger notices must be processed within a maximum of 48 business hours, excluding weekends and holidays, unless legally justified circumstances require immediate action.
8. Verified that the guideline clarifies that priority affects ordering only and does not remove the requirement for independent human review. Moderators must still independently verify the content and apply normal standards of proof and categorisation. Trusted flagger notices and complaints are subject to the same timely, diligent, non-arbitrary and objective standards as general notices and complaints.
9. Based on the updated implementation documentation and guideline, the previously identified deficiency regarding the absence of technical infrastructure, formal verification workflow and tagging capabilities has been addressed. The provider now documents a dedicated registration process, manual verification against the official trusted flagger list, creation of dedicated trusted flagger accounts, dashboard-based notice submission and tracking, system flagging, queue prioritisation and timing requirements.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 23.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Interviewed the content moderation teams responsible for policy enforcement. They confirmed that account suspensions and terminations were issued during the reporting period for severe illegal content (e.g. CSAM, rape, zoophilia). This indicates that the provider maintained an active enforcement process against illegal content, although such measures were not yet operated under a fully structured process specifically designed for "frequent and manifest" violations. January-June 2025 and July-December 2025 Transparency Reports
2. Reviewed a breakdown of content categories that resulted in account terminations during the reporting period January-June 2025. This includes 268 terminations for underage content, 2 for active zoophilia, 6 for real rape, and 2 for scatophilia. These terminations demonstrate that enforcement against manifestly illegal content was active and operational during the period. However, the available evidence did not show that prior warnings were systematically issued, or that affected users had been assessed through a structured repeat-violation framework. In addition, the platform reported that it could not differentiate account terminations resulting from manifestly unfounded notices or complaints, because its database was not designed to track those distinctions during the reporting period. The enforcement approach therefore appeared primarily content-triggered and severity-based, rather than expressly frequency-based.
3. Reviewed the provider's databases and moderation tooling in relation to account terminations and suspensions. During the reporting period, these systems were not yet fully designed to log or tag the reason behind account terminations in a manner specifically aligned with Article 23(1). In particular, the system did not yet comprehensively track whether the same user had repeatedly posted illegal content, differentiate first-time violations from repeat offences, maintain structured logs of warning issuance, or systematically record suspension duration as distinct from termination. Standardized notification templates for warnings related to content misuse were also not yet formalised.
4. Reviewed the platform's TOS, which include general language prohibiting the posting of illegal or harmful content and reserve the right to remove such content and terminate accounts. This provided a general policy basis for enforcement action. However, the TOS did not yet specifically describe a policy of suspending users for frequent violations, define "manifestly illegal" content in operational terms for the purposes of Article 23(1), or explain a warning system, suspension duration, or the factors taken into account when assessing repeated violations.
5. Assessed whether specific evidence of a fully structured enforcement layer under Article 23.1 was available. The provider confirmed that suspensions were not documented as being linked explicitly to "frequent" or "manifest" content violations and that account restrictions for severe cases were typically final. Nevertheless, the audit confirmed that the provider had an active enforcement framework for illegal content and that the remaining gaps related primarily to the formalisation of a graduated warning-and-suspension model, repeat-offender tracking, and clearer user-facing policy articulation.

Conclusion:

Positive with comment – In our opinion, the provider maintained an active enforcement framework for addressing illegal content during the examination period, including removal of content and termination of accounts in severe cases, supported by general prohibitions set out in the TOS. However, this framework was not yet fully formalised into a dedicated Article 23(1) process specifically designed to manage users who frequently and manifestly provide illegal content. In particular, the warning layer, structured suspension periods, repeat-offender tracking, and user-facing transparency around such measures were not yet sufficiently developed. Accordingly, while the provider demonstrated substantive enforcement activity in this area, further formalisation was still needed to fully align the process with the specific requirements of Article 23(1).

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Formalise the existing enforcement framework into a graduated Article 23(1) process by defining clear thresholds for frequent and manifest provision of illegal content and introducing internal indicators to identify repeat offenders. ▪ Develop and implement a warning and escalation layer within the existing moderation process, including standardized notices, appeal-related communication, and reasonable suspension periods where appropriate. ▪ Update the TOS to describe more clearly the provider's policy for repeated illegal conduct, including illustrative misuse scenarios, enforcement steps, suspension logic, and user rights.	The identified measures should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 23.2.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Interviews with the Notice and Complaint team and Content Moderation team indicated that the provider does not currently operate a dedicated Article 23(2) process to identify or suspend users who frequently submit manifestly unfounded notices or complaints under Articles 16 or 20.
2. Reviewed the platform-wide reporting flow. The provider allows users to report content, but the evidence did not show systematic tracking of report originators, frequency per reporter, or whether reports are well-founded, unfounded, or manifestly unfounded.
3. The IT team confirmed that it does not separately track suspensions linked to misuse of reporting or complaint mechanisms and that its database was not designed to categorise such events during the relevant period.
4. Reviewed the provider's three-strike mechanism. The available information shows that the platform operates a repeat-infringer / repeat-violation approach, under which a user may receive strikes, and, after three strikes, the account may be terminated. The reviewed material refers mainly to copyright infringements and repeated uploads, rather than misuse of notice or complaint mechanisms.
5. Reviewed the *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026, section 5.5.5 Three-Strike Policy. This guideline improves the assessment because it provides evidence of an internal escalation framework for repeat violators. It refers to prior warnings, documentation, case-by-case assessment, audit trails, and mentions "unfounded reporting". This suggests that misuse of reporting mechanisms is at least contemplated internally.

6. However, the guideline remains broader and primarily focused on repeat uploaders of incompatible or illegal content. It does not clearly establish a dedicated Article 23(2) workflow for suspending the processing of notices or complaints submitted through Articles 16 and 20. It also does not clearly define thresholds, suspension duration, or the technical/process steps for suspending notice or complaint processing.
7. Reviewed the Article 23 compliance status report. The report notes that the platform's ToS describe a strike policy for repeated violations, but do not clearly define how long strikes last, the period within which strikes are counted, or how the mechanism applies to misuse of reporting and complaint systems. It also states that the Article 23(2) mechanism is not transparently addressed in the ToS.
8. The provider further explained that its current approach is not to block users from submitting notices or complaints solely because they previously submitted unfounded notices. The rationale is that such users may still later submit a relevant and well-founded notice, and that unfounded notices have not materially affected the operational effectiveness of the Notice and Complaint team. This is a relevant proportionality factor, but it does not replace the need for a defined Article 23(2) framework.

Conclusion:

Positive with comment – In our opinion, the provider maintained certain controls relevant to broader Article 23 misuse, including a three-strike mechanism, moderator escalation, prior-warning principles, case-by-case assessment, documentation requirements, and audit trails. However, the available evidence does not demonstrate a fully defined and operational Article 23(2) process. In particular, the provider did not show that it systematically identifies users who frequently submit manifestly unfounded notices or complaints, issues prior warnings specifically for such misuse, or suspends the processing of notices and complaints under Articles 16 and 20 where the statutory threshold is met.

The provider's approach not to block users from submitting notices or complaints is a relevant mitigating factor, as users who previously submitted unfounded notices may later submit relevant notices, and unfounded notices reportedly do not materially affect the team's effectiveness. Nevertheless, Article 23(2) still requires a structured reserve mechanism for clear and repeated misuse. Accordingly, the provider should not be assessed as having no relevant controls at all, but further formalisation is needed to align the process with Article 23(2).

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Formalise a dedicated Article 23(2) policy for misuse of Article 16 notices and Article 20 complaints, separate from the existing content-upload strike policy. ▪ 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. ▪ Update the ToS to describe the Article 23(2) misuse policy clearly, including examples, possible consequences, and the duration of any suspension.	The identified measures should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 23.3.	Throughout the period, in all material respects:	N/A

	▪ 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.	

Audit procedures, results and information relied upon:

1. Interviewed the Notice and Complaint team and Content Moderation team responsible for enforcement and escalation. The teams confirmed that the provider maintains an active enforcement process for severe illegal content and repeat violations. For misuse of notices and complaints, the provider explained that its current approach is generally not to block users solely because they previously submitted unfounded notices, since such users may later submit relevant and well-founded notices. The provider also indicated that unfounded notices have not materially affected the team's operational effectiveness.
2. Reviewed the Content Moderation Guideline, including section 5.5.5 on the Three-Strike Policy. The guideline sets out a standardized escalation mechanism for repeat violators, particularly users who repeatedly upload incompatible or illegal content. Before applying enforcement, Content Moderators must verify that the conduct is genuinely repetitive, prior warnings were issued, and no earlier strike was reversed following a successful complaint. The guideline also requires assessment of frequency, pattern, intent or negligence, impact on users and platform processes, and corrective behaviour.
3. Reviewed the provider's three-strike mechanism and repeat infringer information. The available material indicates that strike notifications may be displayed in the user account and that, after three strikes, the user account may be terminated. The mechanism appears most developed in the context of copyright and repeated content-related infringements.
4. Reviewed the Article 23 compliance status materials. The materials indicate that the platform applies immediate account removal for severe violations, such as CSAM, NCII, or terrorism-related content, and applies a three-strike policy for less severe repeated violations. This supports the conclusion that severity and absolute number of violations are considered in practice. However, the materials also identify gaps, including lack of clear proportional assessment and insufficient transparency around strike duration and counting periods.
5. Reviewed the platform's approach to misuse of reporting and complaint mechanisms under Article 23(2). The available materials indicate that this mechanism is not clearly regulated in the ToS and that users are not clearly informed how misuse of notice or complaint mechanisms could lead to restrictions. The materials also recommend creating internal guidance to distinguish bad-faith misuse from genuine user error
6. Assessed whether the provider performs the multi-factor assessment required by Article 23(3). The *Content Moderation Process Guidelines*, document version *MD-G-001*, dated 1 March 2026, provides evidence of a case-by-case assessment framework, including frequency, pattern, intent or negligence, prior warnings, impact, corrective behaviour, documentation, and audit trails. However, the process is not yet fully formalised across both Article 23(1) and Article 23(2), particularly in relation to proportional metrics and notice/complaint misuse.

Conclusion:	
Positive with comment – In our opinion, the provider maintained a case-by-case assessment framework relevant to Article 23(3) during the examination period. The provider's internal guidance requires moderators to assess whether conduct is genuinely repetitive, whether prior warnings were issued, whether earlier strikes were reversed, the frequency and pattern of conduct, the user's apparent intent or negligence, the impact on users and platform processes, and whether corrective behaviour followed earlier enforcement. These factors are broadly aligned with the multi-factor assessment required by Article 23(3). However, the process was not yet fully formalised across all Article 23 scenarios. In particular, the provider did not demonstrate a complete proportional assessment based on the ratio of problematic activity to total user activity, and the Article 23(2) process for frequent manifestly unfounded notices or complaints was not supported by sufficiently structured tracking or user-facing policy.	
Recommendations on specific measures: ▪ Formalise the Article 23(3) assessment into a standard case-review template or checklist for all Article 23(1) and Article 23(2) decisions. ▪ Develop a dedicated Article 23(2) assessment workflow for misuse of notice and complaint mechanisms. ▪ Update the ToS or relevant policy materials to explain the factors considered when assessing repeated misuse under Article 23.	**Recommended timeframe to implement specific measures:** The above changes should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 23.4.	Throughout the period, in all material respects: ▪ 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 provide the provider with a general basis 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. Assessed whether the TOS contain a detailed misuse policy specifically aligned with Articles 23.1 and 23.2. While the TOS establish a general enforcement basis, they do 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 behaviour that would trigger warnings or suspensions under a misuse framework, (iv) an explanation of suspension durations, proportionality, or case-by-case review factors, or (v) a detailed description of users' rights or remedies in case of enforcement under such a framework.
3. Verified whether any annex, linked policy supplement, or other public document connected from the TOS addressed these elements in greater detail. No such supplement was identified that would fulfil the specific transparency requirements under Article 23.4.
4. Considered the provider's overall policy posture and subsequent remediation planning. The review confirmed that the provider had already established general contractual rules on illegal content and account-related enforcement, but the dedicated misuse-policy layer required by Article 23.4 had not yet been fully articulated in the TOS. We further note that the provider has acknowledged this gap and planned a revision of the TOS to reflect misuse definitions, enforcement logic, and related user-facing information more clearly.

Conclusion:

Negative – In our opinion, the provider partially complied with the specified requirements during the examination period, in all material respects. The TOS did not yet describe in a sufficiently clear and detailed manner the specific policy regarding misuse under Articles 23.1 and 23.2, including examples of misuse, the factors relevant for assessing such misuse, the nature and duration of suspensions, and the related user-facing consequences. Accordingly, while the platform had reserved enforcement rights and a general prohibition framework in place, further clarification and formalisation in the TOS was still needed to fully align with the requirements of Article 23.4.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Finalise the planned revision of the TOS so that they explicitly describe the provider's misuse policy under Articles 23.1 and 23.2. ▪ Include clear examples of relevant misuse, such as repeated provision of illegal content and repeated submission of manifestly unfounded notices or complaints. ▪ Describe more clearly the factors taken into account when assessing misuse, including frequency, severity, proportionality, and user intent where relevant. ▪ Specify in the TOS the nature and duration of suspensions that may be imposed, together with the related warning logic and user rights.	The above changes should be implemented within 6 months.

Obligation:	Audit criteria:	Materiality threshold:
Article 24.1.	Throughout the period, in all material respects, the provider includes in its biannual transparency reports: ▪ 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 January-June 2025 and July-December 2025 Transparency Reports published by XVideos. Both reports were published on time and followed a structure broadly aligned with DSA transparency reporting expectations. This confirms that the provider had an operational transparency reporting process in place during the relevant reporting periods.
2. Verified that no out-of-court disputes under Article 21 were reported for either period. The reports did not include median durations, outcomes, implementation rates, or explicit placeholders indicating that no cases occurred. Interviews with the legal team confirmed that no such disputes were submitted during the relevant periods, which explains the omission. The identified issue therefore relates primarily to the completeness and presentation of zero-case disclosures rather than to the omission of known dispute cases.
3. Examined the sections on user suspensions and enforcement actions under Article 23. The reports disclosed aggregated account terminations or enforcement outcomes related to manifestly illegal content, including categories such as underage content and other severe illegal content types. This demonstrates that the provider reported relevant enforcement activity and maintained data on serious content-related account actions.
4. However, the reports did not yet provide the full suspension breakdown required under Article 24(1), namely a distinction between suspensions imposed for the provision of manifestly illegal content, the submission of manifestly unfounded notices, and the submission of manifestly unfounded complaints.
5. Interviewed the provider's Content Moderation Team, Notice and Complaint Team, and Compliance Officer. They confirmed that the platform's enforcement processes were operational, but that system-level tagging and reporting fields were not yet fully implemented to distinguish between the three Article 23 suspension categories in a structured way. Suspensions and account-related enforcement actions were handled through existing moderation processes but were not categorized in the reporting database with the granularity required for Article 24(1).
6. The Compliance Officer attributed the missing breakdown to technical limitations in the enforcement database and data retrieval infrastructure. The provider further indicated that work is underway to implement structured reporting fields, categorisation of suspension types, and improved tracking functionality for future reporting cycles.

Conclusion:

Positive with comment – In our opinion, the provider maintained an operational transparency reporting process during the examination period and published the relevant biannual transparency reports. The reports included information on moderation and enforcement activity, and no evidence was identified that out-of-court dispute settlement cases under Article 21 had occurred but were omitted. However, the reports did not yet provide the full level of granularity required under Article 24(1), in particular the breakdown of Article 23 suspensions by category and clearer zero-case

disclosures for out-of-court dispute settlement information. The provider has acknowledged these limitations and indicated that improvements to reporting fields, tagging, and tracking functionality are underway. Accordingly, the provider demonstrated substantive progress in transparency reporting, while further technical and reporting enhancements remain necessary to fully align with the specific Article 24(1) disclosure requirements.	
Recommendations on specific measures: ▪ Continue the ongoing work to implement structured reporting fields for suspensions under Article 23, distinguishing between manifestly illegal content, manifestly unfounded notices, and manifestly unfounded complaints. ▪ Enhance moderation and enforcement systems to support consistent tagging and categorisation of enforcement actions for transparency reporting purposes. ▪ Integrate suspension logging and reporting dashboards into the provider's reporting workflow to improve traceability, auditability, and consistency across future reporting cycles.	**Recommended timeframe to implement specific measures:** The above changes should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 24.2.	Throughout the period, in all material respects: ▪ 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).	N/A

Audit procedures, results and information relied upon:

1. Reviewed the publicly accessible Mandatory Information / Reports section available through the provider's online interface. The page includes a dedicated section for average monthly XVideos recipients of the service in the EU and is accessible without login, registration, or prior clearance.
2. Verified that the provider published the number of average monthly active recipients of the service in 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
    - August 9, 2025: 33 million
    - February 17, 2026: 33 million
3. Verified that the information remains publicly available in the provider's Mandatory Information / Reports section and that the page also contains links to transparency reports, risk assessment reports, independent audit reports, and audit implementation reports.

4. Reviewed the explanatory text published on the page. The provider states that earlier numbers were significantly higher because it was previously difficult to calculate an accurate number due to the large proportion of users visiting through incognito browsers. The provider further explains that it later found a way to account for such traffic and therefore published revised, more realistic figures.
5. The audit team was not granted access to internal datasets, logs, or the algorithm used to calculate or estimate the six-month averages. Accordingly, audit procedures were limited to inspection of the publicly available information and management explanations regarding the basis for the reported figures.¨
6. Based on the published dates, the provider has continued to disclose average monthly recipient figures on an approximately semi-annual basis.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 24.3.	Throughout the period, in all material respects: ▪ Is prepared to supply the EC or the DSC with updated information on average monthly active recipients, upon request and without undue delay; ▪ Is able to substantiate the figure and explain the methodology used for its calculation; ▪ Does not transmit any personal data when fulfilling these obligations.	N/A

Audit procedures, results and information relied upon:

1. Performed interviews with the Compliance Officer and IT Team to assess preparedness to respond to regulatory requests for updated average recipient data. The teams confirmed that no formal requests were received from the EC or any DSC during the examination period. The teams further confirmed that, if such a request were received, the provider would be able to retrieve and provide updated average monthly active recipient information without undue delay.
2. Reviewed the Methodology for the calculation of monthly unique recipients, document version 1.0, dated 27 February 2026. The methodology documents the provider's approach for deriving average monthly recipient figures using internal first-party data and defined estimation and deduplication principles. The document also provides a structured basis for explaining how the reported figures are prepared, while taking into account technical limitations related to different types of user access.
3. Verified that the methodology addresses key aspects relevant to substantiating the reported figures, including the use of internal traffic data, treatment of repeat access, consideration of privacy-preserving browsing modes, and adjustment for potential duplicate counting. The detailed calculation logic was reviewed for audit purposes but is not reproduced here due to its confidential and commercially sensitive nature.
4. Assessed whether the documented methodology would enable the provider to substantiate and explain the reported figures if requested by the EC or a DSC. Based on the

documentation reviewed and inquiry with the Compliance Officer, the provider has a documented framework to support the preparation and explanation of updated recipient figures.

5. Assessed whether personal data would be transmitted in fulfilling the obligation. The methodology and related reporting approach are based on aggregated recipient figures. No evidence was identified that personal data would be required to be transmitted when providing updated average monthly active recipient information. However, as no formal regulatory request was received during the examination period, the actual response package was not tested.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 24.5.	Throughout the period, in all material respects: ▪ Submits to the EC, without undue delay, all decisions and statements of reasons referred to in Article 17.1. DSA; ▪ Ensures these decisions are transmitted to a publicly accessible machine-readable database managed by the EC; ▪ Confirms that such submissions do not contain personal data.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the provider's transparency-related documentation and follow-up information and confirmed that the provider has implemented the obligation under Article 24(5) DSA with respect to XVideos. Since July 2025, anonymized Statements of Reasons pursuant to Article 17 DSA have been published in the DSA Transparency Database.
2. The provider confirmed that Article 17 decisions are recorded internally and are transmitted to the EC's publicly accessible machine-readable database through an operational submission workflow. This process has been functioning since July 2025 and covers the relevant removal and restriction decisions falling within the scope of Article 24(5) DSA.
3. The Compliance Officer confirmed that the provider has implemented safeguards to ensure that submissions to the EC's database do not contain personal data. The submission process is automated and includes the necessary filtering measures to prevent the transmission of personal data.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. Article 17 decisions and associated Statements of Reasons are maintained internally and, since July 2025, anonymized Statements of Reasons have been submitted to and published in the DSA Transparency Database. The provider also confirmed

that appropriate safeguards are in place to prevent the inclusion of personal data in such submissions.	
Recommendations on specific measures: N/A	**Recommended timeframe to implement specific measures:** N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 25.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Inspected selected features of the provider's interface, including registration, login, and account termination. The reviewed user journeys did not indicate that users were deceived, manipulated, or materially impaired in their ability to make free and informed decisions.
2. Verified that the steps for account termination were no more complex than for registration. The account termination process was accessible through the user account interface and did not appear to impose unnecessary friction or disproportionate steps compared to account creation.
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 or made unnecessarily difficult.
4. Reviewed the presence and frequency of pop-up windows and system prompts. Verified that user choices, including age verification, category selection, and cookie preferences, were not repeatedly requested or imposed after a choice had already been made. No evidence was identified of repeated prompts or coercive interface patterns that would materially distort user decision-making.
5. Verified through walkthroughs of selected interface elements that no misleading default settings or other forms of nudge techniques were generally present. User choices were, in most cases, presented in a visually neutral manner without disproportionate emphasis on any option. Two isolated interface elements were noted during the previous review: (i) a pre-highlighted category during the age and orientation confirmation process upon first access to the platform, and (ii) a pre-filled gender setting upon account creation. Based on the updated assessment, these elements are considered isolated design features and, in the absence of further regulatory guidance, do not in themselves demonstrate material deception, manipulation, or impairment of users' ability to make free and informed decisions.

6. Reviewed whether internal documentation addressing interface review against dark patterns had been formalized. No dedicated dark pattern review checklist or UI ethics framework was identified. However, based on the nature of the observations and the overall interface walkthrough, this was assessed as an area for future documentation enhancement rather than a material compliance deficiency.
7. Reviewed the provider's position set out in the Audit Implementation Report. The provider stated that it does not consider immediate implementation of the previously recommended interface adjustments necessary in the absence of specific EC guidance under Article 25(3) DSA. The provider further stated that its interface design practices were implemented in good faith with the intention of enabling users to make free and informed decisions, and that it remains prepared to reassess and adjust relevant interface elements and documentation if future EC guidance indicates that such changes are required.

Conclusion:

Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The reviewed interface was generally structured in a way that enabled users to make free and informed decisions, without evidence of deceptive, manipulative, coercive, or materially distorting design patterns. Account termination and logout were accessible, user choices were not repeatedly imposed after selection, and the reviewed interface elements were generally presented in a neutral manner. The previously identified observations relating to a pre-highlighted category at initial access and a pre-filled gender field upon account creation are considered isolated design elements and, in light of the provider's position in the Audit Implementation Report and the absence of specific EC guidance under Article 25(3) DSA, do not amount to a material compliance deficiency. The previous assessment is therefore considered to have applied a conservative interpretation, and the provider's compliance status is assessed as positive.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Continue to monitor the development of EC guidance under Article 25(3) DSA concerning the design and organisation of online interfaces. ▪ Reassess the relevant interface elements when further EC guidance becomes available, in particular with respect to default selections, visual prominence, and neutral presentation of user choices.	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 26.1.	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;	N/A

	▪ The information was clearly, concisely, and unambiguously presented and directly accessible from the advertisement itself.	

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 information about why the advertisement is shown and information about the relevant advertising entities.
    - 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, users can access meaningful advertising information in real time via the "i" icon. The updated "About This Ad" page displays both required entities separately, namely the payer shown as "Paid by …" and the beneficiary shown as "On behalf of …". In the reviewed example, the payer and beneficiary were the same entity; however, the interface correctly displayed both fields separately.
4. Verified that the updated "About This Ad" page provides clear and actionable information on how users can modify or influence the targeting parameters used for ad personalisation. The page includes a "Manage your ad preferences" section explaining the effect of disabling ad personalisation and provides a direct action through the "Manage personalized ads" button. Additional controls are available through the CMP / cookie preferences interface, where users can manage Advertising Cookies, which may affect ad personalisation.
5. Inquired with respective personnel to understand the scope and structure of information provided about displayed advertisements. Based on the updated implementation, the previous limitation relating to the distinction between the payer and the beneficiary of the advertisement has been addressed through separate "Paid by …" and "On behalf of …" fields in the "About This Ad" interface.
6. Reviewed the provider's follow-up materials and implementation status. The provider has completed the update of the "About This Ad" functionality to include information about both the payer and beneficiary of advertisements and to provide users with practical mechanisms to modify or influence ad personalisation settings. Internal documentation outlining advertising transparency procedures remains an area for continued formalisation and auditability improvement.

Conclusion:

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

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

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

Audit procedures, results and information relied upon:

1. The provider's Privacy Policy and advertising-related disclosures were reviewed to assess whether profiling for advertising purposes involves the processing of special categories of personal data as defined in Article 9(1) GDPR.
2. The Privacy Policy identifies certain special categories of personal data, including race, ethnicity, religion, sexual preference, dominant/submissive role, and sexual orientation. The purposes assigned to such data are service-related, including user profile customisation, interaction between users, search filtering, basic customer segmentation, and content personalisation. There is no indication that these special categories of personal data are used for advertising profiling or advertisement personalisation.
3. The advertising-related cookie identified as "wpn_ad_cookie" was reviewed. The Privacy Policy states that this cookie is used for the proper display of the Website, specifically to rotate advertising banners every 24 hours to avoid displaying the same advertisements to the user. The cookie is expressly described as not tracking browsing history. The cookie is also expressly described as not being used for user profiling or advertisement personalisation.
4. The provider's advertising transparency implementation was reviewed, including the updated "About This Ad" and ad preference controls. These controls provide users with advertising preference management options and direct users to cookie preference settings, including Advertising Cookies, which may affect ad personalisation settings.
5. Based on the documentation reviewed, no evidence was identified that special categories of personal data are used for profiling-based advertising. The reviewed materials support the conclusion that advertising-related processing is not based on Article 9(1) GDPR data and that the advertising cookie is used for operational ad display purposes rather than profiling or personalisation based on sensitive data.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 27.1., 27.2.	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:	N/A

	– the criteria most significant in determining the information suggested; – the reasons for the relative importance of the identified parameters; ▪ The TOS described the options available for recipients to modify or influence those parameters.	

Audit procedures, results and information relied upon:

1. Inspected the provider's TOS and underlying documentation related to recommender systems, including the Recommender System Guideline, version MD-G-001, dated 01.03.2026. The Recommender System Guideline sets out the governance framework, configuration standards, and transparency obligations related to recommender systems deployed on the platform. It expressly addresses Article 27 DSA and refers to Article 38 DSA in relation to the non-profiling recommender option
2. Assessed whether the TOS and supporting documentation clearly outlined the main parameters used in recommending content and the options available for recipients to modify or influence those parameters. The Recommender System Guideline supports this assessment by defining recommender system entry points, ranking parameters, user control options, and transparency obligations.
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. Reviewed the Recommender System Guideline's description of ranking logic and relative importance. It identifies the main parameters as primary category, country, and optional viewing history. It further explains that the system does not assign fixed numerical weights but uses multi-step logic and cached statistical associations derived from aggregated user behaviour.
5. Verified that users can modify or influence recommender parameters. The Recommender System Guideline states that users can change their primary category and country through account or navigation settings and can enable or disable viewing history through the user interface. When History is disabled, personalised recommendations based on viewing history are bypassed.
6. Reviewed the non-profiling recommender option. It states that the platform offers a configuration not based on profiling through the History feature. If History is disabled, recommendations are generated without using the user's viewing history. If the user enables History, a pop-up explains that a cookie storing viewed pages is required and provides Accept and Deny options.
7. While the TOS listed the key parameters and allowed user control over some inputs, they did not explicitly explain the relative importance of each parameter in sufficient detail. We further noted that the provider has planned formalisation measures in this area, including approval of the relevant internal SOP and a subsequent update of the TOS based on that framework.

Conclusion:

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

of its recommender systems and the options available for recipients to modify or influence them in a structured and user-accessible manner. The Recommender System Guideline further supports compliance by documenting recommender entry points, ranking logic, relative importance of parameters, user control options, governance responsibilities, and the non-profiling option linked to the History feature. However, the provider should continue ensuring that the public-facing TOS remain aligned with the more detailed Recommender System Guideline, particularly regarding the relative importance of parameters and the distinction between personalised and non-personalised recommendation modes.	
Recommendations on specific measures: ▪ Continue the ongoing work on updating the TOS so that they explicitly include a clearer description of the relative importance of the principal parameters influencing recommendations.	**Recommended timeframe to implement specific measures:** The identified measures should be implemented within 12 months.

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

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's recommender system controls, including the availability and accessibility of user options to select and modify their preferred content presentation settings.

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:	Audit criteria:	Materiality threshold:
Article 28.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the platform's TOS and access flow. The platform is intended exclusively for adults aged 18 or over and users are required to confirm that they meet the applicable age threshold before accessing the service. The access flow includes an adult-content warning, age self-confirmation, acceptance of the TOS, and default blurring of content before entry. These measures create entry friction and reduce accidental exposure, although they remain based primarily on self-declaration.
2. Reviewed the draft of the 2026 Risk Assessment Report and related risk documentation. The provider significantly enhanced its systemic risk assessment methodology compared to the previous cycle by introducing a two-layer model distinguishing systemic risks from risk drivers, strengthening cross-functional governance, and linking risks to mitigation measures and responsible functions. Protection of minors remains one of the most sensitive risk areas, with residual high-risk exposure concentrated in scenarios involving minors accessing or being exposed to pornographic content.
3. Reviewed the provider's mitigation measures for protection of minors. The measures include adult-content warnings, age self-confirmation, TOS acceptance before access, default content blurring, automated RTA metadata tagging, and guidance on parental controls and access restriction tools. The provider's own assessment recognises that these measures form a layered minor-protection architecture but are not individually equivalent to robust age-assurance mechanisms and cannot fully prevent determined circumvention.
4. Reviewed the draft of the Risk Register and Dashboard. The register identifies several protection-of-minors scenarios, including minors accessing pornographic content, systematic exposure through content-delivery systems, exposure through discovery features, sexually explicit advertising, and contact-related risks. For key scenarios, the response strategy is to reduce the risk, including through cooperation with the EC on identifying a sufficient age-assurance solution and defining KPIs for protection of minors.
5. Conducted interviews with the Compliance Function, Legal Team, and Regulatory Director. They confirmed that the provider is actively considering how to respond to the EC's preliminary findings, is engaged in dialogue with the EC, and intends to comply with applicable regulatory expectations. The interviewees also stated that the provider is participating in EC activities related to testing EU age-verification tools and is monitoring the development of privacy-preserving age-assurance solutions.
6. Based on interviews, the provider reported that age-assurance solutions have been deployed in certain jurisdictions, including France, the UK, and Australia. For France, the available information indicates that users may be required to verify age through age-assurance measures such as AgeGO. The provider also stated that, apart from jurisdiction-specific age-assurance implementation, there have not yet been significant global changes to the website access flow.
7. Based on interviews with the Compliance Officer, Legal Team, and Regulatory Director, the audit also considered the existence of EC preliminary findings concerning Article 28(1), Article 34, and Article 35. These findings were treated as contextual information provided

during interviews. The teams confirmed that the provider is assessing options for responding to the EC's concerns and continuing the regulatory dialogue.

8. Assessed the proportionality considerations raised by the provider. The provider has consistently highlighted the need to balance minor protection with privacy, data minimisation, avoidance of excessive identity-linked processing, and the protection of lawful adult access. At the same time, the provider's own risk documentation recognises that self-declaration, warnings, blurring, parental controls, and RTA tagging are supporting safeguards rather than robust standalone age-verification measures.

Conclusion:

Positive with comment – In our opinion, the provider maintained a structured and evolving framework for protecting minors during the examination period, including adult-only TOS clauses, age self-confirmation, access warnings, default content blurring, RTA metadata tagging, parental-control guidance, risk assessment, and documented mitigation planning. The provider has also enhanced its risk-management framework and has begun or reported jurisdiction-specific age-assurance deployments in certain countries, while engaging with the EC and considering further steps to respond to regulatory expectations.

However, the provider's general EU access model continues to rely primarily on self-declaration and supporting safeguards rather than robust age verification at the point of entry. The provider's own documentation recognises that these measures reduce accidental exposure but do not fully prevent determined minors from accessing adult content. Protection of minors therefore remains a high-priority residual risk requiring further mitigation. The EC's preliminary concerns, as relayed during interviews, further support the need for stronger and more consistent age-assurance measures.

Accordingly, while the provider has demonstrated a credible governance framework, active risk recognition, and ongoing compliance efforts, further formalisation and technical implementation are still needed to fully align the platform with the high level of privacy and security expected under Article 28(1).

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
• Continue engaging with the EC and relevant regulators, including participation in testing of EU age-verification tools; • Document the provider's response strategy to the EC's preliminary findings, including legal assessment, technical options, implementation timeline, and responsible owners. • Expand the protection-of-minors KPI framework to measure effectiveness of access controls, age-assurance measures, parental-control guidance, and content-blurring mechanisms. • Maintain jurisdiction-specific deployments, including France, the UK, and Australia, and assess whether lessons learned can be applied more broadly across the EU.	The identified measures should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 28.2.	Throughout the period, in all material respects: ▪ Does not present advertisements based on profiling (as defined under GDPR Article 4(4)) using personal data when it is aware	N/A

	with reasonable certainty that the recipient of the service is a minor.	

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's advertising practices, including the continued absence of profiling-based advertising using personal data and the use of non-personalized, contextual or placement-based ad delivery.

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 Officer, 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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 28.3.	Throughout the period, in all material respects: ▪ Does not process additional personal data solely to determine whether a user is a minor; ▪ Maintains a privacy-conscious stance.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's age-related data processing practices, including the continued absence of additional personal data processing solely to determine whether a user is a minor and the maintenance of a privacy-conscious, data-minimizing approach.

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.

Conclusion:

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

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 34.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Conducted inquiries with the Compliance Team, Legal Team and Regulatory Director. Confirmed that the provider conducted annual service-specific systemic risk assessments and subsequently enhanced the methodology for the 2026 assessment cycle. The Compliance Officer and Legal Team also informed us that the EC had extended proceedings and communicated preliminary findings concerning, among others, Articles 34(1) and 34(2), primarily focused on systemic risks relating to minors. The Legal Team and Regulatory Director further explained that the provider is considering how to respond to the EC's preliminary findings, remains in dialogue with the EC, and intends to comply with applicable DSA requirements.
2. Reviewed the drafts of the 2026 Systemic Risk Assessment Report, Risk Register and Dashboard, and Mitigation Measures Register. The 2026 assessment introduced a more advanced two-layer methodology, distinguishing between systemic risks under Article 34(1) and risk drivers under Article 34(2). It also formalised residual-risk scoring using mitigation effectiveness and driver impact assessment.
3. Verified that the assessment covered a broad and platform-specific risk universe. The 2026 risk assessment assessed 92 systemic-risk scenarios across 13 risk categories, including dissemination of illegal content, data privacy, privacy and family life, protection of minors, gender-based violence, physical and mental well-being, public health, public security, non-discrimination, freedom of expression, and civic and electoral impact.
4. Reviewed the assessment of illegal content risks under Article 34(1)(a). The Risk Register identifies dissemination of illegal content as the largest risk category, including scenarios relating to CSAM, NCII, grooming, CSAM links, malware or phishing links, coercive or abusive content, trafficking-related activity, terrorist content, hate speech, and other prohibited or harmful material.
5. Reviewed the assessment of fundamental-rights risks under Article 34(1)(b). The assessment covers risks relating to privacy and family life, data protection, human dignity, freedom of expression and information, non-discrimination, and the rights and protection of minors. The 2026 report also notes that the highest inherent-risk concentrations arise in sensitive areas such as privacy, protection of minors, gender-based violence, and dissemination of illegal content.

6. Reviewed the assessment of civic discourse, electoral processes and public security under Article 34(1)(c). The Risk Register includes dedicated scenarios for civic and electoral impact, including political disinformation, coordinated manipulation, political advertising misuse, and sexualised disinformation targeting public figures. These risks were assessed as less central to the platform's adult-content service model but were nevertheless identified and assessed.
7. Reviewed the assessment of gender-based violence, protection of minors, public health, and physical and mental well-being under Article 34(1)(d). The Risk Register includes dedicated scenarios for gender-based violence, protection of minors, public health, and well-being. The 2026 assessment identifies remaining high residual-risk exposure as concentrated mainly in protection of minors and certain illegal-content scenarios, including CSAM-link sharing and grooming or coercive contact involving minors.
8. Assessed whether the risk assessment process incorporated follow-up and continuous improvement. The 2026 report includes a residual-risk management roadmap, including monitoring of EU guidance, development of KPIs for mitigation effectiveness, a dedicated KPI framework for protection of minors, research monitoring, external audits, and cooperation with the EC on identifying a sufficient age-assurance solution.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider conducted service-specific systemic risk assessments and, in the 2026 cycle, materially strengthened the methodology, documentation, traceability and governance of the assessment. The updated framework distinguishes systemic risks from risk drivers, assesses a broad set of platform-specific risks, links risks to mitigation measures and responsible functions, and includes residual-risk scoring and follow-up actions. The assessment covers each Article 34(1) category, including illegal content, fundamental rights, civic and electoral risks, public security, gender-based violence, protection of minors, public health, and physical and mental well-being.

However, the provider should continue strengthening the evidential and quantitative basis of the assessment, particularly for protection of minors and other high residual-risk scenarios. In light of the interview information concerning the EC's preliminary findings, the provider should ensure that its response to the EC, ongoing supervisory dialogue, and intended compliance actions are clearly reflected in the risk-management roadmap and future assessment cycles.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Continue developing the dedicated KPI framework for protection of minors and other high residual-risk areas; ▪ Further strengthen quantitative evidence supporting likelihood, severity and residual-risk scoring; ▪ Document the provider's response strategy and follow-up actions in relation to the EC's preliminary findings and supervisory dialogue.	The identified measures should be implemented within 12 months.

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

	▪ 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.	

Audit procedures, results and information relied upon:

1. Reviewed the draft of the 2026 Systemic Risk Assessment Report and Risk Register. The updated methodology expressly distinguishes Article 34(1) systemic risks from Article 34(2) risk drivers, allowing the provider to assess not only what harms may arise, but also which service features, governance arrangements or operational factors may cause or intensify those harms.
2. Reviewed the draft of the Risk Driver Register and Dashboard. The provider assessed 95 risk drivers across relevant operational and governance domains. The driver categories include content moderation, age assurance and access controls, advertising systems, data-related practices, manipulation and inauthentic use, regional and linguistic disparities, recommender and algorithmic systems, ToS governance, and authority contact-point arrangements.
3. Assessed coverage of recommender systems and other algorithmic systems under Article 34(2)(a). The 2026 report recognises recommender and content-discovery systems as relevant to systemic-risk exposure because they influence which content is surfaced, prioritised and repeatedly shown. It also notes user-facing controls, including category, location and viewing-history settings, with viewing-history-based personalisation not enabled by default.
4. Assessed coverage of content moderation systems under Article 34(2)(b). The report describes a layered moderation framework combining automated tools, trained human review, reporting channels, escalation procedures, complaint-handling mechanisms and repeat-offender enforcement rules. These elements were assessed as key controls affecting illegal content, protection of minors, gender-based violence and freedom of expression risks.
5. Assessed coverage of TOS and enforcement under Article 34(2)(c). The Risk Driver Register includes ToS governance and enforcement as risk drivers, including risks that unclear or inconsistently enforced terms may affect user rights, reporting, moderation, access controls, and protection of minors.
6. Assessed coverage of advertisement selection and presentation under Article 34(2)(d). The 2026 report identifies advertising integrity as a specific risk area and records controls including pre-publication review, post-publication monitoring, advertiser certification, ad-transparency notices, advertising repository, and impression-related data.
7. Assessed coverage of data-related practices under Article 34(2)(e). The Risk Register includes data privacy and protection risks, including risks related to sensitive data, profiling, consent, secondary use, and links between intimate content and identifiable persons. These risks are assessed together with relevant drivers such as age assurance, data-related practices and recommender systems.
8. Reviewed the assessment of manipulation, inauthentic use, automated exploitation and amplification effects. The 2026 report identifies manipulation and inauthentic use as relevant drivers, including bots, fake accounts, engagement manipulation, coordinated harassment, abusive reporting, misuse of links, and exploitation of reporting or dispute mechanisms.
9. Reviewed the assessment of regional and linguistic factors in the EU. The 2026 report identifies regional and linguistic disparities as structural risk drivers affecting detection, moderation, reporting, redress and recommender settings across EU jurisdictions. It

recognises risks related to uneven language coverage, weaker protection in smaller language markets and inconsistent regional configurations.

10. Conducted inquiries with the Legal Team and Regulatory Director. They confirmed that the provider is considering how to respond to the EC's preliminary findings, remains engaged in dialogue with the EC, and intends to align its risk assessment and mitigation approach with regulatory expectations, particularly in relation to minors, age assurance and related systemic-risk drivers.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider assessed how systemic risks may be influenced by the main Article 34(2) factors, including recommender and algorithmic systems, content moderation, ToS enforcement, advertising systems, data-related practices, manipulation and inauthentic use, and regional and linguistic factors. The 2026 two-layer methodology materially improves the structure of this assessment by separating systemic harms from the operational drivers that may cause or intensify them.

However, further strengthening remains appropriate, particularly in relation to quantitative scenario analysis, manipulation and automated exploitation testing, regional segmentation, and the evidential basis for high-risk drivers such as age assurance and minors' access. The interview information concerning the EC's preliminary findings further supports the need to keep Article 34(2) risk-driver analysis under active review and to document how supervisory feedback is reflected in future assessment cycles.

Recommendations on specific measures:	**Recommended timeframe to implement specific measures:**
▪ Develop more structured scenario analysis for coordinated manipulation, automated exploitation, abusive reporting, and amplification effects; ▪ Strengthen quantitative indicators for recommender, moderation, advertising, data-practice and age-assurance drivers; ▪ Document how the provider's dialogue with the EC and response to preliminary findings are reflected in updated risk-driver analysis and mitigation planning.	The identified measures should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 34.3.	Throughout the period, in all material respects: ▪ The provider preserved supporting documentation for each risk assessment conducted; ▪ Documentation was retained for at least three years from the date of assessment; ▪ The provider was prepared to share this documentation with the EC or DSC upon request.	N/A

Audit procedures, results and information relied upon:

1. Conducted interviews with the Compliance Officer to confirm document retention practices specific to systemic risk assessments. The provider confirmed that final risk assessment reports and supporting materials for the 2024, 2025 and 2026 assessment cycles are retained, including working files, risk registers, mitigation registers, dashboards, supporting evidence and related governance materials.

2. Reviewed the draft of the 2026 Systemic Risk Assessment Report. The report states that it is intended to be read together with the Risk Register, the Mitigation Measures Register and the Action Plan, and that these documents are maintained for access by internal stakeholders, external auditors and regulators. It also confirms that the assessment is reviewed and updated annually to reflect new risks, revised controls, operational changes and regulatory developments.
3. Reviewed governance arrangements described in the 2026 Systemic Risk Assessment Report. The Compliance Function is responsible for designing and maintaining the ISO 31000-based methodology, chairing risk workshops, updating registers, preparing annual and ad hoc systemic-risk assessments, and assigning, monitoring and verifying mitigation measures. Senior Management is responsible for reviewing the annual systemic-risk assessment and supporting documentation.
4. The Compliance Officer and Legal Team further confirmed during interviews that the provider had received information requests from the EC in relation to DSA systemic-risk obligations and had responded through the designated internal process. They also confirmed that the provider remains able to retrieve and share relevant risk-assessment documentation with the EC or the DSC upon request.
5. Reviewed the provider's internal retention approach as described by the Compliance Officer. The provider confirmed that risk assessment documentation is stored in access-controlled internal repositories and retained for at least three years from the date of the relevant assessment. No exceptions to the retention period were identified during the review.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 35.1	Throughout the period, in all material respects: ▪ 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. *Definition of reasonable: measures which are appropriate to the nature and magnitude of the systemic risk.*	N/A

Audit procedures, results and information relied upon:

1. Reviewed the draft of the 2026 Systemic Risk Assessment Report, Risk Register and Dashboard, and Mitigation Measures Register. The 2026 assessment confirms that the provider maintains a broad and layered mitigation framework across automated tools, content moderation, TOS and policy controls, recommender systems, data protection, protection of

minors, advertising, user support and user verification. The framework is linked to systemic risks, risk drivers, control owners and residual-risk scoring.

2. Reviewed the draft of the Mitigation Measures Register and Dashboard. The register documents 56 mitigation measures, including control category, control type, owner, effectiveness, proportionality, reasonableness and risk reduction factor. The majority of measures were assessed as highly reasonable and highly proportionate, with no measures assessed as low proportionality.
3. Art. 35(1)(a): Reviewed design and interface adaptations. The provider implemented measures such as adult-content warnings, default content blurring on entry, age self-confirmation, cookie and tracking preference controls, user reporting routes, user-controlled recommendation settings, and ad transparency notices. These measures are relevant to risks concerning exposure to harmful content, user autonomy, advertising transparency and personalisation.
4. Art. 35.1.b.: The most recent version of the TOS was reviewed. Interviews were conducted with personnel from the Compliance Officer and Legal 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, hateful or discriminatory material, and content involving coercion or violence. The TOS also provide a general legal basis for content removal, account restrictions, complaint handling, and user redress. 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 framework, with automated detection, human verification, escalation logic, and differentiated treatment of severe violations. The updated Mitigation Measures Register further documents structured moderation procedures, escalation for repeat illegal content offenders, and internal classification of manifestly illegal content.

   Based on the available evidence and the procedures performed, it was concluded that the provider's TOS and related enforcement framework were adapted in a manner consistent with Article 35(1)(b), with due consideration given to systemic risks and user rights, including appeal and redress mechanisms.
5. Art. 35.1.c.: Content moderation processes were adapted to address risks related to the dissemination of illegal and harmful content, including CSAM, NCII, hate-related content, cyber violence, and other prohibited categories. Processes were reviewed, including moderation workflows, internal guidelines, the Mitigation Measures Register and Dashboard.

   A hybrid moderation system was employed, combining automated detection tools with human review. The register documents several automated and semi-automated tools, including fingerprint-based detection, AI-based analysis, SafetyNet-related checks, keyword filtering, and flagged-text review. These measures are supplemented by human moderator review and escalation pathways for sensitive or ambiguous cases.

   The Mitigation Measures Register further documents manual review of uploaded videos, moderation team training, multilingual moderation coverage, structured moderation procedures, abuse reporting forms, copyright reporting forms, in-product reporting tools, human review and decision-making for reported videos, and appeals and complaint-handling workflows. These measures are assessed in the register as generally highly reasonable and proportionate, with several content moderation controls assessed as highly effective.

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

6. 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 interviews and documentation review 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-related indicators, as well as user transparency mechanisms and non-profiling options.

   The Mitigation Measures Register documents recommender system criteria, periodic review of recommender system algorithms, user-controlled content preferences, and user-controlled content selection. Users can influence recommendations through selected preferences, categories, tags, performers, keywords, location and history-related settings.

   Based on the evidence reviewed, and within the scope of process-level controls, it is concluded that reasonable and proportionate measures were implemented in relation to recommender systems.

7. Art. 35.1.e.: Reviewed the provider's advertising-related mitigation measures. The Mitigation Measures Register documents several dedicated advertising controls, including ad transparency notices, pre-publication review, ongoing post-publication ad monitoring and enforcement, advertiser eligibility and certification controls, an advertising repository, and impression-related advertising data.

   Advertisements are subject to manual review before approval and publication. During this review, elements of the advertisement are checked against internal advertising rules, and non-compliant advertisements are rejected. The review process is supported by tools such as antivirus scanners, URL analysis, VPNs, and translation utilities. Additional checks are carried out for advertisements targeting users in the EU, UK, or California to verify compliance with applicable data protection requirements.

   The provider also maintains post-publication monitoring and enforcement for advertisements. Potential violations are investigated and addressed through a tiered enforcement process, including labelling measures, campaign rejection, suspension of repeat violators, or immediate bans in severe cases.

   The updated advertising implementation further confirms that "About This Ad" now includes payer and beneficiary information, ad preference controls, and targeting-related information. The Ad Repository also supports removed-ad filtering, removal reasons, hidden advertiser identity for removed ads, and audience selection information.

   Based on the evidence reviewed, it is concluded that the provider implemented reasonable, proportionate and effective measures in relation to advertising systems and advertising transparency.

8. 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 on-site control assessments, review of internal materials, including the Mitigation Measures Register and Dashboard, and interviews with representatives from the Compliance Team.

   The updated Mitigation Measures Register demonstrates assignment of control owners, control categories, control types, effectiveness assessments, proportionality assessments, reasonableness assessments, and risk reduction factors across key risk areas such as content moderation, advertising, automated tools, data protection, protection of minors, recommender systems, TOS and policies, user support, and user verification.

Clear role definitions and oversight responsibilities were confirmed. The Compliance Officer was observed to be actively coordinating DSA compliance activities, and the register provides a consolidated framework for monitoring mitigation measures and their operation.

Based on the evidence reviewed, it is concluded that reasonable and proportionate measures were implemented to reinforce internal processes, supervision, and systemic-risk governance.

9. Art. 35.1.g.: Reviewed the provider's measures concerning cooperation with trusted flaggers and handling of notices. The updated Mitigation Measures Register documents priority treatment of trusted flagger notices and a dedicated registration process for trusted flaggers.

   Notices submitted by trusted flaggers are treated on a priority basis and are specifically flagged within the workflow. The register indicates that such notices are automatically moved to the top of the moderation queue for accelerated handling.

   The dedicated trusted flagger registration process limits access to organisations established in the EU, formally designated by the competent DSC, and listed in the public database maintained by the EC. Applications require official organisational information and are subject to verification before activation.

   Based on the updated evidence, the previously identified concerns relating to the absence of technical prioritisation and formal trusted flagger workflow have been addressed. It is concluded that reasonable and proportionate measures were implemented in relation to Article 35(1)(g).

10. Art. 35.1.h.: It was confirmed that during the 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 and interviews, the provider has been monitoring the development of industry-wide standards, particularly those related to the prevention of CSAM, NCII and harmful algorithmic amplification. The provider acknowledged that no sector-specific code or crisis protocol currently exists for adult platforms under the DSA and stated that accession to recognised codes of conduct or crisis mechanisms will be evaluated once established and relevant to the service type.

    Based on the available evidence, the provider's approach to Article 35(1)(h) was appropriate considering the current availability and applicability of such instruments. No material deficiency was identified, as no applicable sector-specific code or crisis protocol was available for the provider to join during the period under review.

11. 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, reporting options, content labelling practices, and user controls.

    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. Interface adaptations included access to content preferences, language settings, category selection filters, cookie preferences, tracking controls, reporting routes, and user support channels.

    The Mitigation Measures Register further documents contact channels for user support, cookie consent and preference controls, viewing-history controls, reporting tools, and user-facing transparency measures. These measures support user awareness and enable users to exercise a degree of control over content exposure, personalisation and reporting.

    Based on the evidence reviewed, it is concluded that reasonable and proportionate awareness and user-support measures were implemented.

12. Art. 35.1.j.: It was confirmed that the provider 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 an adult-only access model, age-gating, interface

warnings, content blurring, parental-control information, RTA metadata tagging, upload restrictions, and content moderation.

Based on review of the risk assessment, the Mitigation Measures Register, and interviews with compliance and platform operations personnel, the platform's current approach includes a strict 18+ access model, an age self-confirmation gate, adult-content warnings, TOS acceptance before access, default content blurring on entry, and automated RTA metadata tagging.

The platform also maintains policies 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 and uploader verification controls. The register documents channel verification and user account verification procedures intended to reduce the probability of illegal or non-consensual uploads by requiring identity or authorship checks before upload access is granted.

It is acknowledged that age self-declaration and parental-control tools are not standalone age-assurance mechanisms and their effectiveness is limited. However, taken together with content blurring, adult warnings, RTA tagging, upload verification, automated detection, and human moderation, the provider's layered approach is assessed as reasonable and proportionate to the nature of the service.

Based on the evidence reviewed, it is concluded that reasonable and proportionate measures have been implemented to protect minors and reduce the risk of exposure to harmful content.

13. Art. 35.1.k.: It was confirmed that the provider had introduced mechanisms to identify, review, and address content suspected to be artificially generated, visually manipulated, or otherwise misleading in nature.

    The risk assessment states that the platform has adopted an internal tagging process for media flagged as synthetic, AI-generated, or visually manipulated. Users are also provided with reporting mechanisms enabling them to flag content they consider falsely presented or misleading.

    The Mitigation Measures Register further documents automated tools and human review processes that support identification and escalation of potentially harmful or incompatible content. These include AI-based analysis, fingerprinting tools, keyword filtering, flagged-text review, manual review of uploaded videos, and structured moderation procedures. Where manipulation is confirmed and poses a risk of harm, content may be removed, further marked, or escalated for additional review.

    Based on the evidence reviewed, it is concluded that measures were implemented to address synthetic and manipulated media in accordance with Article 35(1)(k), primarily through user-facing reporting, labelling or tagging practices, automated detection support, and human review.

14. Conducted inquiries with the Compliance Officer, Legal Team and Regulatory Director. They informed us that the EC had communicated preliminary findings concerning Articles 34 and 35, with particular focus on minors-related risks and mitigation measures. The Legal Team and Regulatory Director stated that the provider is assessing how to respond to the EC's preliminary findings, remains in dialogue with the EC, and intends to comply with applicable DSA requirements.

15. Assessed the overall effectiveness of the mitigation framework. The 2026 assessment concludes that the provider's control environment materially reduces risk across most categories. Of 92 assessed scenarios, 52 were classified as low residual risk, 33 as medium residual risk and 7 as high residual risk. The remaining high residual risks are concentrated in protection of minors and a narrow subset of illegal-content risks, including CSAM-link sharing and grooming or coercive contact involving minors.

Conclusion:

Positive with comment – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects. The provider implemented a broad set of

reasonable, proportionate and documented mitigation measures tailored to the systemic risks identified under Article 34. The measures cover the main areas referred to in Article 35(1), including design adaptations, TOS and enforcement, content moderation, recommender systems, advertising systems, internal governance, trusted flagger handling, user awareness, protection of minors and synthetic or manipulated media. However, important limitations remain in relation to protection of minors. The current measures, including age self-confirmation, warnings, blurring and RTA tagging, are relevant and proportionate as part of a layered safeguard model, but they are not equivalent to robust age verification and cannot fully prevent circumvention. This is consistent with the provider's own residual-risk assessment, which continues to identify protection of minors as a priority high-risk area.	
Recommendations on specific measures: • Continue developing the KPI framework for mitigation effectiveness, prioritising protection of minors and other high residual-risk scenarios; • Document the provider's response strategy and follow-up actions in relation to the EC's preliminary findings and supervisory dialogue; • Continue assessing age-assurance options and document the reasoning for selected measures, including effectiveness, proportionality, privacy impact and technical feasibility.	**Recommended timeframe to implement specific measures:** The identified measures should be implemented within 12 months.

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 36.1.	Throughout the period, in all material respects: ▪ The provider had defined internal protocols to respond to a crisis declared by the EC; ▪ If a crisis had been declared, the provider would have taken one or more of the following actions: – Assessed the extent to which their services contribute to the threat; – Identified the systems and processes significantly involved; – Monitored the contribution to the threat; – Implemented specific and proportionate mitigation measures; – Assessed the impact of such measures on fundamental rights; – Reported to the EC according to the specified schedule.	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. The Compliance Officer confirmed that no crisis was declared by the EC during the audit period. The Compliance Team demonstrated awareness of the provider's obligations under Article 36 DSA and confirmed that crisis-related readiness is addressed through the provider's internal compliance governance framework.
2. Reviewed the Compliance Policy, including the section "Crisis Protocols and Crisis Response." The policy confirms that WGCZ does not currently participate in the drawing up, testing, or application of voluntary crisis protocols under Article 48 DSA, as no relevant crisis protocol has been initiated by the EC to which WGCZ has been invited or is required to adhere. The policy nevertheless recognises that crisis protocols may be established at EU level to address extraordinary circumstances limited to public security or public health, and that WGCZ may be required to adopt specific crisis response measures based on a EC decision under Article 36 DSA.
3. Verified that the Compliance Policy defines structured readiness measures for potential crisis situations. Senior Management is designated as the crisis management contact point and coordinates with the electronic contact point established under Article 11 DSA. The Compliance Office is responsible for monitoring EU-level developments concerning crisis protocols and Article 36 crisis response mechanisms, including guidance and reporting templates published by the EC or the European Board for Digital Services.
4. Verified that the Compliance Policy defines the internal response workflow to be triggered if a crisis protocol is initiated or if the EC adopts a decision under Article 36 requiring WGCZ to act. The policy states that Senior Management will trigger an internal crisis response workflow, including assessment of the platform's role in the crisis, identification and application of effective and proportionate measures, and documentation of all actions taken.
5. Verified that the Compliance Policy expressly requires fundamental rights considerations to be taken into account in any crisis response. In particular, the policy states that WGCZ will take due account of users' fundamental rights, including freedom of expression, freedom of information, and non-discrimination. It further states that all measures will remain proportionate and strictly time-bound, in line with the DSA.
6. Reviewed the provider's position regarding participation in codes of conduct and crisis protocols. The Compliance Policy confirms that WGCZ does not currently participate in EU-level voluntary codes of conduct or crisis protocols because no applicable framework is currently relevant to the nature of WGCZ's services or required in the present regulatory context. However, the policy establishes readiness measures, including monitoring of EU-level developments and initiation of an internal project led by the Compliance Office if participation becomes applicable.
7. Based on the above procedures, it was confirmed that the provider has formalised its crisis-readiness approach in the Compliance Policy. Although no crisis was declared during the examination period and no Article 48 crisis protocol was applicable, the provider has defined governance responsibilities, monitoring duties, escalation logic, response workflow, documentation expectations, proportionality requirements, and fundamental rights safeguards for potential future crisis situations under Article 36 DSA.

Conclusion:

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

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

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

Audit procedures, results and information relied upon:

1. Inquired with relevant personnel to understand the design and logic of recommender systems in profiled and non-profiled modes. The provider confirmed that personalised recommendations are linked to the optional History feature and that, when History is disabled, recommendations are generated without using the user's viewing history.
2. Reviewed the Recommender System Guideline, version MD-G-001, dated 01.03.2026. The Guideline expressly addresses Article 38 DSA and states that the platform provides users with at least one recommender system configuration that is not based on profiling. It further defines user profiling by reference to Article 4(4) GDPR.
3. Reviewed the Guideline's description of recommender system parameters. The main parameters identified are primary category, country, and optional viewing history. The Guideline explains that viewing history is used only if the user has enabled the History feature; if disabled, personalised logic is bypassed and recommendations are generated using aggregated behavioural patterns and keyword/tag relevance only.
4. Conducted a walkthrough of the user interface and verified the availability of the History control in the settings menu. The Guideline states that users can activate or disable this feature through the User Interface submenu, and the screenshots on pages 11-12 show the relevant History toggle and explanatory pop-up.
5. Reviewed the platform's explanation of the non-profiling option. The Guideline states that when History is disabled, recommendations are generated without using the user's viewing history. It also records that, where a user attempts to enable History, a pop-up informs them that this requires accepting a cookie storing pages viewed for navigation purposes, with immediate Deny and Accept options. The information icon further explains that keeping the feature disabled prevents the recommender system from providing a personalised experience based on navigation history.
6. Reviewed the Guideline's description of homepage, search, related-video and suggested-video recommendations. The documentation explains that non-history-based recommendations rely on contextual and aggregated signals, such as category, country, keyword/tag relevance, clicks, popularity, and aggregated navigation patterns, rather than an individual user's viewing history.
7. Assessed whether the non-profiled option is clearly distinguishable and understandable. The History toggle is accessible in the user interface, and the pop-up provides a plain-language explanation of the effect of enabling or disabling the feature. The current terminology does not use the legal term "non-profiling", but it explains the practical effect to users, namely that disabling History prevents personalised recommendations based on navigation history.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 39.1	Throughout the period, in all material respects: ▪ The provider made publicly available a repository of advertisements presented on their interface and accessible via a specific section of the interface; ▪ The repository provided a search and filter functionality supporting multicriteria queries; ▪ The repository was also accessible via API; ▪ The information remained available for the entire display duration of the ad and for at least one year after its last presentation; ▪ No personal data of the recipients to whom the ad was or could have been presented was included in the repository; ▪ Reasonable efforts were made to ensure the accuracy and completeness of the published information.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's advertisement repository, including its public availability, multicriteria search and filter functionality, API accessibility, required retention period, exclusion of recipients' personal data, and measures supporting the accuracy and completeness of published information.

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 Ad Repository - Xvideos.com.
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:	**Audit criteria:**	**Materiality threshold:**
Article 39.2	Throughout the period, in all material respects: ▪ The provider included in the advertisement repository all information required: – 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's advertisement repository content, including the availability of required information on advertisement subject, advertiser, display period, targeting parameters, and aggregated recipient reach by Member State.

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. This data is accessible within the Ad Detail screen under the “Impression for country” field, which presents both numerical ranges and percentage shares per location.

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.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 39.3	Throughout the period, in all material respects: ▪ 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).	N/A

Audit procedures, results and information relied upon:

1. Reviewed the updated advertising status report and verified that the provider implemented the previously planned remediation measures for the advertisement repository. The report states that the implementation of a dedicated filter allowing users to display only removed advertisements was completed. The repository now includes a checkbox labelled “Show only Removed Ads”, which enables users to search specifically for removed advertisements.
2. Verified that, for removed advertisements, the advertisement creative is no longer displayed. The updated repository replaces the creative with placeholder wording such as “Hidden for removed ads” in the results grid and displays a removal notice stating that the content was removed because it did not follow the provider’s advertising standards.
3. Verified that the previously identified issue concerning the continued display of advertiser identity has been addressed. The updated report confirms that advertiser identity details are hidden for removed advertisements. In the removed-ad detail modal, the advertiser identity is displayed as “Hidden for removed ads”, and the Advertiser Name filter is disabled when the removed-ads filter is active.
4. Verified that information about the payer and beneficiary of removed advertisements is also hidden. The updated screenshots show the fields “Paid by” and “On behalf of” populated with “Hidden for removed ads” for removed advertisements, which addresses the requirement to exclude payer and beneficiary information from repository entries for removed or disabled advertisements.
5. Reviewed whether alternative information is displayed for removed advertisements. The updated repository displays a removal reason both on the removed-ad card and in the ad detail view, for example: “This content was removed because it didn’t follow our advertising standards.” This provides a visible statement explaining the removal of the advertisement.
6. Reviewed additional repository functionality. The updated repository includes audience-selection information for advertisements, including whether the advertisement was intended for specific recipient groups and, where applicable, the main targeting parameters used for inclusion or exclusion. The report confirms that this information is displayed independently of the availability of the advertisement creative and may remain available even where the advertisement content has been removed.
7. Assessed the status of the previously recommended implementation measures. The recommendation to remove or anonymise advertiser identity for removed advertisements was implemented. The recommendation to include a removal reason was also implemented through the display of a visible removal reason.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 40.1	Throughout the period, in all material respects: ▪ Access to data necessary to monitor and assess compliance with Regulation (EU) 2022/2065 was provided, at the reasoned request of the DSC of establishment or the EC, within the period specified in the request.	N/A

Audit procedures, results and information relied upon:

1. Conducted interviews with the Compliance Officer to assess awareness of obligations under Article 40 DSA and readiness to respond to competent authority requests. The interviewed personnel confirmed that regulatory data-access and information requests are coordinated by the Compliance Office, with support from Legal, Regulation, IT and other relevant operational teams.
2. Reviewed the *Compliance Statute*, version MD-S-002, approved on 05.01.2026. The document establishes the Compliance Office as the function responsible for coordinating formal responses to official orders or information requests and confirms that the Compliance Officer has unrestricted access to company data and information relevant to compliance matters.
3. Reviewed Section *8.3 Data Access and Scrutiny* of the Compliance Statute. The section sets out a formal procedure for handling requests from the DSC or the EC. It requires that requests be received in written form, logged with the date of receipt, requesting authority, nature and scope of the request, and the specified deadline. It further requires WGCZ to respond to reasoned requests within the timeframe specified.
4. Verified that the procedure includes internal review and allocation steps. The Compliance Officer performs a preliminary assessment of scope, urgency and applicable legal obligations; Legal Team reviews the request for legal sufficiency and regulatory consistency; Senior Management is notified and provides oversight approval; and the request is assigned to the relevant operational owner, such as Content Moderation, Notice and Complaint, or IT teams.
5. Verified that the Compliance Statute includes safeguards for proportionality, confidentiality and secure disclosure. Data provided must be limited to what is necessary to monitor and assess DSA compliance, including platform usage data, moderation metrics, risk mitigation measures and other compliance-relevant datasets. Requests are subject to legal and security review, and data access is provided only through secure technical means, while protecting GDPR rights, trade secrets and confidential business information.
6. Reviewed evidence of EC information requests and related correspondence during the examination period. The requests concerned DSA compliance matters, including systemic risk assessment, mitigation measures, supporting documentation, recommender / algorithmic transparency, and related governance topics. The audit team reviewed the procedural handling, internal coordination and submission evidence at a high level, without assessing or reproducing the confidential substantive content of the responses.
7. Conducted inquiries with the Compliance Officer, Legal Team and Regulatory Director. They confirmed that EC requests were handled through cross-functional coordination involving Compliance, Legal, Regulation, IT and relevant operational teams. They also confirmed that the provider remains in dialogue with the EC, is considering how to respond to the EC's preliminary findings and intends to comply with applicable DSA requirements.
8. Assessed the implementation status of the previously recommended measure. The recommendation to formalise a process for receiving and responding to regulator data-access requests was implemented through the Compliance Statute, which now documents

request intake, logging, legal review, internal assignment, response coordination, secure disclosure and escalation.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 40.3.	Throughout the period, in all material respects: ▪ The provider was able, upon request by the EC or the DSC, to explain the design, logic, functioning, and testing of its algorithmic systems, including recommender systems.	N/A

Audit procedures, results and information relied upon:

1. Examined internal materials describing the architecture, design, logic and functioning of the platform's recommender systems, including the Recommender System Guideline, version MD-G-001, dated 01.03.2026.
2. Confirmed that the previously recommended implementation measure was conducted. The earlier recommendation to develop the recommender system process mapping into a formal explanatory document was addressed through the Recommender System Guideline, which documents recommender entry points, ranking parameters, user controls, non-profiling options, governance responsibilities and regulatory scrutiny arrangements.
3. Reviewed the Guideline's description of the main recommender entry points, including homepage recommendations, search-bar recommendations, and related / suggested videos. The document also includes visual process charts showing recommendation flows and decision points.
4. Verified that the Guideline explains the main ranking parameters, including primary category, country and optional viewing history. It further explains that the system does not apply fixed numerical weights but uses multi-step logic and aggregated behavioural signals.
5. Reviewed governance and testing responsibilities. The Guideline assigns the IT Team responsibility for technical development, implementation, testing, maintenance, model validation, checks for accuracy, bias and unintended ranking outcomes, and logging changes to algorithmic logic and configuration parameters.
6. Reviewed the regulatory scrutiny section of the Guideline. It states that, upon reasoned request by the DSC or EC, access can be provided to the Guideline and additional information necessary to assess the recommender system, including its design, logic, functioning and testing.
7. Conducted inquiries with the Compliance Officer and IT team. They confirmed that both teams coordinate responses to regulatory information requests and are prepared to provide algorithmic explanations where requested.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 40.4. - 40.7	Throughout the period, in all material respects: ▪ Upon a reasoned request from the DSC of establishment, the provider provided access to data to vetted researchers meeting the requirements of Article 40(8), within the period specified in the request. ▪ The data access was provided solely for research contributing to the detection, identification and understanding of systemic risks under Article 34(1), or to the assessment of the adequacy, efficiency and impact of mitigation measures under Article 35.	N/A

	▪ Where the provider considered that it could not provide the requested data because it did not have access to the data, or because access would create significant security, confidentiality or trade-secret risks, it had a process to request amendment of the request within 15 days and propose alternative means of access. ▪ The provider was able to facilitate access through appropriate interfaces, including controlled databases or APIs, as specified in the request.	

Audit procedures, results and information relied upon:

1. Conducted interviews with the Compliance Officer to assess readiness to respond to vetted researcher data-access requests under Article 40.4-40.7. The provider confirmed that no formal reasoned request for access to data by vetted researchers had been received during the examination period.
2. Considered the current regulatory context in the Czech Republic. The ČTÚ publicly states that it is currently unable to process requests for granting vetted researcher status. It also explains that applications must be submitted through the DSA Data Access Portal and that the final decision on access is made by the coordinator of establishment, with the provider having the right to object.
3. Reviewed the provider's public DSA Data Access page: https://info.xvideos.net/dsa-data-access. The page explains that data access is available only following a valid reasoned request issued by the relevant DSC, identifies a dedicated contact point for vetted researchers, refers to the official DSA Data Access Portal, and explains that the portal is used for information exchange but is not itself a data-access modality.
4. Reviewed the provider's DSA Data Catalogue: https://info.xvideos.net/dsa-data-catalogue. The catalogue describes available data assets, their research purpose, data fields, format and update frequency. The datasets include, among others, video, studio and model databases, deleted-video feed, search APIs, home exposure data, pseudonymised user interaction data, search term statistics, notices review, content moderation data and advertising moderation data.
5. Assessed alignment with Delegated Regulation (EU) 2025/2050[1]. The delegated regulation requires a harmonised data-access process, use of the DSA Data Access Portal, publication of information relevant to the data-access process, and availability of DSA data catalogues describing data assets relevant to systemic-risk research and assessment of mitigation measures.
6. Verified that the provider has published suggested access modalities. The DSA Data Access page identifies three indicative modalities: aggregated export for low-sensitivity data, guarded API access for medium-sensitivity data, and secure processing environment for highly sensitive data. This is aligned with the delegated regulation's expectation that providers publish suggested access modalities proportionate to data sensitivity, while the DSC remains responsible for determining the final modality.
7. Reviewed the Compliance Policy and Compliance Statute. The Compliance Policy refers to data access for researchers and states that access is subject to privacy and confidentiality safeguards and DSC approval. The Compliance Statute sets out a process for written request intake, logging, legal review, assignment to operational owners, secure disclosure,

[1] Commission Delegated Regulation (EU) 2025/2050 of 1 July 2025 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

proportionality review and protection of personal data, trade secrets and confidential information.

8. Assessed implementation of the planned measures. The provider has implemented a practical readiness framework through the public DSA Data Access page, public Data Catalogue, proposed access modalities, dedicated contact point, and internal governance under the Compliance Policy and Compliance Statute. The mechanism has not yet been tested through an actual vetted researcher request due to the absence of a processed reasoned request.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 40.12.	Throughout the period, in all material respects: ▪ The provider gave access without undue delay to publicly accessible data, including, where technically possible, real-time data, to researchers who comply with Article 40(8)(b), (c), (d) and (e); ▪ The data was made available solely for research contributing to the detection, identification and understanding of systemic risks in the Union under Article 34(1); ▪ The provider had appropriate safeguards to ensure that data access is proportionate, secure and limited to the stated research purpose; ▪ The provider limited Article 40(12) access to data publicly accessible in the platform's online interface.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the provider's public DSA Data Access page and DSA Data Catalogue. The Data Access page provides information for researchers and regulatory authorities, identifies a contact point, refers to the DSA Data Access Portal, and explains that data access is available for research on systemic risks and mitigation measures. The Data Catalogue describes available datasets, research purposes, data fields, formats and update frequencies, including CSV/JSON datasets and live API-based access where available.
2. Verified that the Data Catalogue includes datasets relevant to systemic-risk research, including video metadata, studio and model metadata, deleted-video feed, search APIs, home-exposure data, pseudonymised user interaction data, search-term statistics, notices review, content moderation data and advertising moderation data. The catalogue also distinguishes update frequencies, including live access for certain APIs and regular CSV/JSON exports for other datasets.
3. Reviewed the Compliance Due Diligence Form for Qualified Researcher under Article 40(12) DSA. The form sets out a structured process for verifying requester identity, research purpose, systemic-risk relevance, independence from commercial interests, funding disclosure, data-security and confidentiality safeguards, personal-data protection, necessity and proportionality, and whether the requested data is publicly accessible in the platform interface.
4. Reviewed two Article 40(12) data-access requests received by the provider or related platform operator. The requests concerned research into systemic risks on adult platforms, including protection of minors, gender-based violence, dissemination of illegal content, and fundamental-rights impacts. The requests also included information on researcher affiliation, funding, research purpose, requested datasets, preferred access format and data-protection safeguards.
5. Reviewed the provider's handling of the requests submitted by an independent researcher. The provider prepared dataset instructions mapping each requested field to its availability status: publicly available, not collected, or not publicly available. The mapping also identified the relevant export files and fields to be provided, including video metadata, comments, gallery data, uploader/profile metadata and certain public content-publication fields
6. Verified that the provider applied the Article 40(12) public-access limitation. Data not publicly accessible in the online interface, such as content rejection dates, content removal dates, uploader account approval dates and uploader account termination dates, was identified as not available under Article 40(12) and more appropriately handled, where applicable, under Article 40(4). Data not collected by the platform, such as certain separate category or description fields, was also identified as unavailable.
7. Reviewed the provider's request for methodological guidance to the ČTÚ concerning Article 40(12). The request specifically asked how to assess non-vetted researcher requests, verify Article 40(8)(b)-(e) conditions, define public accessibility, handle non-public or deleted data, and determine whether dataset transfers are required beyond public-interface access. The Office stated that, although it is the designated DSC, it is not competent for supervision of VLOP obligations under Chapter III, Section 5 DSA and directed the provider to contact the EC for this matter. This confirms that the provider sought supervisory guidance and that, in practice, the national route for this specific VLOP issue was not available.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 41.1.	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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the Compliance Officer Appointment dated 22 March 2024, confirming the appointment of Mr. David Hradecký as Compliance Officer, effective from the same date. The appointment was made by the Board of Directors and gave him responsibility for leading the Compliance Office and overseeing the compliance programme.
2. Verified that the appointment document grants the Compliance Officer unrestricted access to company records, data and information, decision-making authority for the compliance programme, direct reporting to the Board of Directors, authority to cooperate with function leaders and regulators, and discretion to request and allocate compliance resources.
3. Inspected the Compliance Policy and Compliance Statute, both approved on 05.01.2026. These documents confirm the existence of an independent Compliance Office, led by the Compliance Officer, operating separately from operational units and with direct access to Senior Management. They also define the Compliance Officer's responsibilities for DSA oversight, risk monitoring, policy alignment, training, regulatory cooperation and escalation.
4. Reviewed the Compliance Statute's provisions on independence, authority and resources. The Statute confirms that the Compliance Officer may access records, request resources, design and update policies, conduct investigations, report significant compliance matters and recommend corrective measures. Senior Management is responsible for ensuring independence, access to information and adequate personnel, financial and technical resources.
5. Reviewed the Leadership Declaration on Compliance and Commitment, which confirms senior-level commitment to DSA compliance, user protection, transparency and continuous improvement.
6. Reviewed supporting information on the Compliance Officer's professional qualifications, including experience in governance, risk and compliance, ISO compliance management systems, regulatory compliance and DSA-related compliance support.
7. Confirmed through interviews and documentation review that no adverse changes to the compliance function's structure, mandate, independence or reporting lines were identified 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:	Audit criteria:	Materiality threshold:
Article 41.2.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the provider's DSA-related Compliance Officer function, including its appointment, reporting line and independence, which remain unchanged.

1. Reviewed the Compliance Officer Appointment dated 22 March 2024, confirming the appointment of Mr. David Hradecký as Compliance Officer, effective from the same date. The appointment was made by the Board of Directors and entrusted him with leading the Compliance Office and overseeing the compliance programme.
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. Inspected the Compliance Policy and Compliance Statute, both approved on 05.01.2026. These documents define the Compliance Office as an independent function led by the Compliance Officer, operating separately from operational units and with direct access to Senior Management. They also set out responsibilities for DSA oversight, systemic-risk monitoring, policy alignment, regulatory cooperation, escalation and training.
4. Reviewed the Compliance Statute's provisions on independence and authority. The Statute confirms that the Compliance Officer may escalate compliance risks, access records, request resources, design and update policies, conduct investigations, report significant compliance matters and recommend corrective measures. Senior Management is responsible for ensuring independence, access to information and adequate resources.
5. Confirmed through interviews and documentation review that the Compliance Officer remained in role during the examination period and that no removal or reassignment occurred. Management further confirmed that any removal would require formal approval by the management body.

Conclusion:	
Positive – In our opinion, the provider complied with the specified requirements during the examination period, in all material respects.	
Recommendations on specific measures: N/A	**Recommended timeframe to implement specific measures:** N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 41.3.	Throughout the period, in all material respects, the designated compliance officer(s): ▪ Cooperated with the DSC (DSC) and the EC; ▪ Ensured systemic risks (Art. 34) were identified, reported, and mitigated through reasonable, proportionate, and effective measures (Art. 35); ▪ Organised and supervised activities related to the independent audit (Art. 37); ▪ Informed and advised management and staff about relevant DSA obligations; ▪ Monitored the provider's compliance with DSA obligations; ▪ Where applicable, monitored compliance with commitments under codes of conduct (Art. 45–46) or crisis protocols (Art. 48).	N/A

Audit procedures, results and information relied upon:

1. Reviewed the Compliance Officer Appointment dated 22 March 2024, confirming that Mr. David Hradecký was appointed as Compliance Officer and entrusted with leading the Compliance Office, overseeing the compliance programme, reporting to the Board of Directors, cooperating with regulatory bodies, and accessing information necessary for compliance activities.
2. Inspected the Compliance Statute and Compliance Policy, both approved on 05.01.2026. These documents confirm that the Compliance Officer is responsible for overseeing DSA implementation, monitoring compliance, managing systemic risk assessment and mitigation activities, coordinating with external stakeholders, and managing responses to official orders or information requests.
3. Reviewed the provider's regulatory cooperation framework. The Compliance Statute assigns the Compliance Office responsibility for coordinating responses to requests from the EC and DSCs, including intake, logging, legal review, assignment to operational owners, secure disclosure, and escalation where necessary.
4. Reviewed high-level evidence of EC information requests and related correspondence. The audit team reviewed procedural handling, internal coordination and submission evidence, without assessing or reproducing the confidential substantive content of the responses. The evidence supports that the Compliance Officer and relevant teams cooperated with the EC in practice.
5. Reviewed the Compliance Officer's role in systemic risk management. The Compliance Statute and Policy state that the Compliance Officer conducts systemic risk assessments,

manages the Risk Register and Mitigation Measures Register, monitors mitigation measures, and reports compliance matters to Senior Management.

6. Reviewed responsibilities relating to independent audits. The Compliance Policy states that the provider undergoes annual independent compliance audits under Article 37 DSA and that the provider cooperates with auditors by granting access to relevant data, premises and operational records. The Compliance Statute also assigns the Compliance Officer responsibility for internal DSA audits, follow-up corrective actions and external compliance audits.
7. Reviewed evidence of advisory, training and internal communication responsibilities. The Compliance Policy states that the Compliance Officer facilitates compliance training, provides guidance and support on compliance matters, and ensures that policies and procedures remain aligned with DSA obligations. The Compliance Statute further confirms regular cross-functional coordination with Legal, Content Moderation and IT teams.
8. Reviewed information provided by the Compliance Team regarding the implementation of a dedicated DSA compliance SharePoint environment. The Compliance Officer explained that this environment is used as a central workspace for monitoring, coordination and management of DSA compliance activities, including document storage, task tracking, compliance follow-up and audit-related coordination. The solution uses Microsoft tools, including SharePoint, Planner and related Microsoft web-based functionalities.
9. Reviewed information provided by the Compliance Team regarding the implementation of a DSA training management environment using the same Microsoft tools. The Compliance Team confirmed that training materials have been made available to relevant personnel, including materials covering general DSA compliance and systemic risk assessment. The team also confirmed that more specific team-level DSA trainings are planned for May 2026, tailored to the responsibilities of individual teams.
10. Assessed these tools and training arrangements against Article 41(3). The DSA Microsoft-based workspace supports the Compliance Officer's ability to monitor DSA compliance, coordinate implementation activities, track follow-up actions and supervise audit-related tasks. The training environment and training materials support the Compliance Officer's responsibility to inform and advise management and staff on relevant DSA obligations.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 41.4.	Throughout the period, in all material respects: ▪ The name and contact details of the head of compliance were formally communicated to the EC; ▪ If applicable, the same communication was prepared for the DSC (DSC) of the Member State of establishment.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related Compliance Officer notification arrangements, which remain unchanged.

1. Reviewed internal appointment records for the Compliance Officer (Mr. David Hradecký), including internal decision logs and organizational chart references.
2. Interviewed management, who confirmed that the contact information for the Compliance Officer was transmitted to the EC shortly after appointment;
3. Assessed contextual legal constraints in the Czech Republic:
    - As of the audit period, the ČTÚ had been designated as the future DSC, but did not yet exercise formal supervisory powers, as the national adaptation law had not been enacted;
    - Therefore, while the DSC of establishment was nominally identified, no official communication channel or operational intake procedure was available during the audit period.

Conclusion:

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

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

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 41.5.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the Risk Management Guideline (MD_G_01_Risk Management Guideline_V2), which designates the management body as responsible for validating systemic risks and approving mitigation resource allocation. The guideline also references periodic engagement of leadership in risk-related decisions. This is consistent with the 2026 Risk Assessment Report, which states that the risk assessment follows ISO 31000 principles, involves top management and relevant stakeholders, and that Senior Management is responsible for strategic oversight, final accountability, approval of risk-management documentation, review of the annual systemic-risk assessment, and allocation of resources for mitigation, monitoring and follow-up.

2. Reviewed the Compliance Statute, approved on 05.01.2026. The Statute defines the Compliance Office as an independent function led by the Compliance Officer, operating separately from operational units and with direct access to Senior Management. It also confirms that Senior Management is responsible for ensuring the independence of the Compliance Officer, access to necessary information, and adequate personnel, financial and technical resources.
3. Inspected the Compliance Policy, approved on 05.01.2026. The Policy sets out the governance and compliance oversight framework, including the Compliance Officer's role in monitoring systemic risks, mitigation measures, DSA compliance, regulatory cooperation, training and guidance.
4. Reviewed the division of responsibilities across the Compliance Office, Senior Management, Legal and Regulation, and line function leaders. The Compliance Statute confirms that Senior Management approves compliance documentation and oversees systemic risk governance, while line function leaders are responsible for embedding compliance requirements into day-to-day operational workflows.
5. Reviewed the Leadership Declaration on Compliance and Commitment, which confirms senior-level commitment to DSA compliance, transparency, user protection, integrity and continuous improvement.
6. Reviewed governance arrangements related to systemic risk management. The Compliance Statute and Compliance Policy confirm that the Compliance Officer manages the Risk Register and Mitigation Measures Register, while Senior Management remains responsible for sound management of systemic risks and for allocating resources to the compliance management system.
7. Reviewed information provided by the Compliance Team regarding the implementation of a dedicated DSA compliance web using Microsoft tools, including SharePoint, Planner and related web-based functionalities. The environment supports monitoring, coordination, task tracking, document management and audit-related follow-up for DSA compliance activities.
8. Conducted interviews and reviewed governance information confirming that the compliance function had direct access to Senior Management, compliance and risk reporting were integrated into management-level review processes, no adverse changes to the Compliance Officer's mandate or reporting line were identified, and no active conflicts of interest were disclosed 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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 41.6.	Throughout the period, in all material respects: ▪ The management body approved and reviewed, at least annually, the strategies and policies for identifying, managing, monitoring, and mitigating systemic risks under Article 34 DSA.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the Risk Management Guideline (MD_G_01 Risk Management Guideline_V2), which designates the management body as responsible for validating systemic risks and approving mitigation resource allocation. The guideline also references periodic leadership engagement in risk-related decisions.
2. Reviewed the Compliance Policy, approved on 05.01.2026. The Policy confirms that systemic risk assessments are conducted at least annually and additionally where significant changes occur. It also states that mitigation strategies are documented in the Mitigation Measures Register and refined based on regulatory guidance and independent audits.
3. Reviewed the Compliance Statute, approved on 05.01.2026. The Statute assigns Senior Management responsibility for approving compliance documentation, integrating compliance requirements into business and risk-management processes, ensuring sound management of systemic risks, and allocating adequate resources.
4. Reviewed versioned compliance documentation, including the Risk Assessment Report, Risk Register, Mitigation Measures Register, Compliance Policy and Compliance Statute, which support management-level oversight of systemic-risk strategies and mitigation measures.
5. Reviewed information from the Compliance Team regarding the dedicated DSA compliance web, using Microsoft tools such as SharePoint and Planner, which supports monitoring, task tracking, document management and audit follow-up.
6. Reviewed information provided by the Compliance Team regarding the dedicated DSA compliance web, using Microsoft tools such as SharePoint, Planner and related web-based functionalities. The environment supports monitoring, task tracking, document management, audit follow-up and coordination of DSA compliance activities.
7. Conducted interviews with the Compliance Officer and senior managers. They confirmed that systemic risk assessment outputs, mitigation strategies and compliance priorities were discussed with management through planning sessions, risk briefings and compliance updates.
8. Noted that a standalone board approval log specific to systemic-risk strategies was not separately identified. However, approval and review were evidenced through the risk governance framework, annual risk assessment documentation, versioned compliance documents and management-level oversight processes.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 41.7.	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.	N/A

Audit procedures, results and information relied upon:

No changes were identified since the previous review of the DSA-related resourcing of systemic risk mitigation, which remains unchanged.

1. Reviewed the Risk Management Guideline (MD_G_01_Risk Management Guideline_V2), 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, approved on 05.01.2026, 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:	Recommended timeframe to implement specific measures:
N/A	N/A

Obligation:	Audit criteria:	Materiality threshold:
Article 42.1.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

No material changes were identified since the previous review in relation to the provider's biannual transparency reporting under Article 42(1) DSA. The reporting cadence, publication timelines, governance process, and public accessibility of the transparency reports remain unchanged and continue to support the positive assessment.

1. Reviewed transparency reports published by the provider for:
    - January–June 2025 (first reporting period); and
    - July–December 2025 (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:	**Recommended timeframe to implement specific measures:**
N/A	N/A

Obligation:	**Audit criteria:**	**Materiality threshold:**
Article 42.2.	Throughout the period, in all material respects: ▪ 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.	N/A

Audit procedures, results and information relied upon:

1. Reviewed the provider's public mandatory information page and confirmed that the transparency reports for January-June 2025 and July-December 2025 are publicly accessible via the provider's official website.
2. Reviewed the July-December 2025 Transparency Report, published in a structured machine-readable CSV format. The report package contains separate data tables covering report identification, average monthly active recipients, government orders, notices, own-initiative moderation, complaints, automated means, human resources, and qualitative disclosures.
3. Confirmed continued semi-annual publication of transparency reports. The reviewed package identifies a publication date of 28 February 2026 and refers to the previous report published on 29 August 2025, demonstrating publication more frequently than annually.
4. Reviewed the human resources disclosures. The report provides the number of moderators using FTE / headcount methodology and discloses 44 internal moderators, 9 external moderators, and 53 total moderators with sufficient linguistic expertise. Linguistic expertise is further broken down by language, including cs, de, en, es, fr, it, pl and sk.
5. Reviewed the qualitative disclosures on moderator qualifications, training and support. The report states that moderators are expected to have advanced English proficiency, strong PC skills, experience-based suitability for adult-content moderation, and access to ongoing training. Training is provided by the Head of Moderation and experienced moderators, using mentorship, supervision, feedback and practical exposure to moderation cases.
6. Reviewed disclosures on moderator support. The report describes operational support through Q&A materials, group communication tools, consultation channels, and well-being measures, including ergonomic workstations, subsidised fitness / wellness access, confidential consultation options, flexible working arrangements and regular breaks.
7. Reviewed disclosures on automated means and accuracy indicators. The report provides tool-specific information on the purpose and performance of automated moderation tools, including Vercury, Hive, Google SafetyNet API, Safer, and keyword matching. It includes available accuracy, precision, recall or error-rate information for selected tools and distinguishes between automated measures and measures involving human review.
8. Confirmed that the report was published in English, which is an official language of the EU.
9. Assessed the implementation status of prior recommendations. The provider addressed several prior audit recommendations by publishing the report in machine-readable format, improving structured disclosures on moderation resources, expanding information on automated moderation tools, and distinguishing between law-based and TOS-based enforcement. However, language-specific accuracy information remains more developed for automated tools and high-volume categories than for all EU language groups.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 42.3.	Throughout the period, in all material respects: ▪ The provider included in its biannual transparency reports the average number of monthly recipients of the service; ▪ This data was broken down by each EU Member State, as required under Article 42(3) and in alignment with Article 24(2) DSA.	N/A

Audit procedures, results and information relied upon:

No material changes were identified since the previous review regarding Article 42(3) DSA. The provider continues to report average monthly active recipients per EU Member State, and the assessment remains positive.

1. The January-June 2025 and July-December 2025 transparency reports 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.
2. 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.

Conclusion:

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

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

Obligation:	Audit criteria:	Materiality threshold:
Article 42.4	Throughout the period, in all material respects: ▪ The provider transmitted to the DSC of establishment and the EC, without undue delay: – a report setting out the results of the risk assessment; – the specific mitigation measures put in place; – the audit report; – the audit implementation report; – information about the consultations conducted in support of the risk assessments and design of the risk mitigation measures (if applicable); ▪ The provider made these information publicly available within three months of receiving the audit report.	N/A

Audit procedures, results and information relied upon:

No material changes were identified since the previous review regarding Article 42(4) DSA transmission and publication obligations. The prior assessment remains unchanged and continues to support a positive conclusion.

1. Inquired Compliance Team to gain an understanding of the internal processes and timelines for transmitting risk-related documentation to the EC and the DSC.
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.

Conclusion:

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

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

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

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

29-32	The provider does not enable recipients of the service to conclude distance contracts with traders. Consequently, the obligations under Articles 29 to 32 do not apply to the provider during the examination period.
33	Article 33 does not impose a specific obligation on the provider. Therefore, it is not applicable and considered within the scope of the audit.
35.2-35.3	Articles 35(2) and 35(3) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
36.2-36.11	Articles 36(2), 36(3), 36(4), 36(5), 36(6), 36(7), 36(8), 36(9), 36(10), and 36(11) do not impose specific obligations on the provider. Therefore, they are not applicable and considered within the scope of the audit.
37.1	The audit was conducted as the provider's first independent audit in accordance with the specified requirements under Article 37. Therefore, the obligations under Article 37(1) were not applicable during the examination period.
37.2	The access conditions, cooperation measures, and any limitations or constraints encountered during the audit were formally addressed in Sections 7 ("Access and Cooperation") and 8 ("Limitations and Disclaimers") of the audit report.
37.3-37.5	Articles 37(3), 37(4), and 37(5) set requirements for the independent auditing organization. Assessing compliance with these provisions would constitute a self-audit by the auditing organization itself. Therefore, they are applicable and considered within the scope of the audit.
37.6	The audit was conducted as the provider's first independent audit in accordance with the specified requirements under Article 37. No audit report or audit implementation report had yet been submitted to the EC. 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.
40.13	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.)	21 April 2025 – 23 April 2026
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 2025 (fieldwork commenced)	21 March 2026 (fieldwork completion / "as-of" date for findings)

Section B: Auditing organization

1. Name(s) of organization(s) constituting the auditing organization:
CERTICOM s.r.o. (Commercial Register no. 35 987 211) – accredited conformity-assessment and assurance provider according to standard ISO /IEC 17021-1:2015 – together with its accredited certification body CERTICOM, Pod Donátom 907/5, 965 01 Žiar nad Hronom, Slovak Republic.
2. Information about the auditing team of the auditing organization:
Ing. Marián Illovský (lead auditor)
3. Auditors' qualification:
a. Overview of the professional qualifications of the individuals who performed the audit, including domains of expertise, certifications, as applicable:
Marián Illovský, a lead auditor, graduated from the University of Economics in Bratislava's Faculty of Economic Informatics, Department of Operational Research and Econometrics. With over two decades of experience in auditing and information security management, Marián has held various roles. Between 2004 and 2019, he served as the head of the internal IT audit unit at POŠTOVÁ BANKA in Bratislava, Slovakia, where he was responsible for developing the bank's IT audit function. From 2008 to 2022, he worked for EUROGIRO in Copenhagen, Denmark, as a member of the Security group. His role involved auditing all members worldwide. Since 2014, Marián has been a freelancer specialising in auditing of IT, IS, OT and cybersecurity. Additionally, from 2011, he has been an external expert and assessor for ISO 27001 for the Slovak National Accreditation Service in Bratislava, Slovakia. He has continued his work with ISO 20000-1, ISO 22301 and eIDAS. Furthermore, since 2017, he has also been an external expert and assessor for eIDAS at the Public Institute Slovenian Accreditation in Ljubljana, Slovenia. Marián holds several certifications, including Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Data Privacy Solution Engineer (CDPSE), Certified Information Security Manager (CISM), Certified cybersecurity auditor (Slovak certification), Certified cybersecurity manager (Slovak certification) and Global Industrial Cyber Security Professional (GICSP).
b. Documents attesting that the auditing organisation fulfils the requirements laid down in Article 37(3), point (b) of Regulation (EU) 2022/2065 have been attached as an annex to this report:
- Certificate of accreditation to carry out certification of quality management systems according to the ISO 9001:2015 No. : Q-003 - Certificate of accreditation to carry out certification of environmental management systems according to the ISO 14001:2015 No. : R-005, - Certificate of accreditation to carry out certification of occupational health and safety management system in accordance with requirements of standard ISO 45001:2018, No.: R-015

- Certificate of accreditation to carry out certification of Information Security Management System according to the ISO/IEC 27001:2022 No.: R-153 - Certificate of accreditation to carry out certification of anti-bribery management system in accordance with requirements of standard ISO 37001:2025 No.: R-136 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
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 EC, 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:	23 April 2026	**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 2025 to 23 April 2026, 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