

Risk Assessment Report

NKL Associates s.r.o. (XNXX.com)

Date of Creation	November 13, 2024
Version	01
Prepared by	David Hradecky, Compliance Officer
Approved on	November 13, 2024
Approved by	Robert Seifert, Statutory representative

Content

1.	Introduction	3
1.1	Purpose and Scope	3
1.2	Risk Management Framework	4
2.	Risk Identification	5
2.1	Methodology used for Risk Identification	5
2.2	Risk Categories and Risk Scenarios	7
2.3	Systemic Risks	10
3.	Risk Assessment	12
3.1	Risk Assessment Approach	12
3.2	Inherent Risk Assessment	12
3.3	Residual Risk Assessment	14
4.	Risk Assessment Results	15
4.1	Risk Assessment Overview	15
4.2	Mitigation measures in place	15
4.3	Residual Risk Assessment	16
4.4	Response Strategy	20
4.5	Risk Monitoring Procedures	22
5.	Conclusion	23
5.1	Summary of Findings	23
5.2	Overall Risk Profile	23
5.3	Recommendations	23
Annex 1	25

1. Introduction

1.1 Purpose and Scope

This report presents a risk assessment conducted by NKL Associates s.r.o., reg. ID 02330482, with registered seat at Krakovská 1366/25, Praha 1, 110 00, Czech Republic (also referred to as “NKL”), operator of the XNXX.com platform (also referred to as “Platform” or “XNXX”), which was designated as Very Large Online Platform (“VLOP”) in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (“Digital Services Act” or “DSA”).

NKL operates XNXX, which is an Internet platform hosting content created by third parties. This report aims at identifying, analysing and assessing, as comprehensively as possible, the risks associated with third parties’ non-compliance with XNXX Terms of Services (“TOS”) and NKL’s compliance with the requirements set forth by the DSA. The primary objective is to assess risks that may affect users, the community or the Platform’s compliance with the DSA including issues pertaining to the misuse by third parties of the Platform for distribution of illegal content, the Platform’s compliance with transparency requirements, content moderation, data privacy, risks to fundamental rights, civic discourse and electoral processes, public health and persons’ physical and mental well-being through the dissemination of content that promotes unhealthy or risky behaviours, misinformation about health, drug use, or encouraging self-harm, vulnerable groups such as minors, and victims of gender-based violence.

This report takes into consideration all elements related to our Platform’s operational, technical and procedural aspects. It includes content moderation processes, data management, user security measures, advertising integrity and compliance reporting mechanisms. The assessment evaluates these risks in terms of their likelihood and potential impact on the Platform’s operations, the Platform’s users and the Internet community as a whole.

The development of this risk assessment considers the Platform’s diverse user base, reflecting the complexities of different languages and regional contexts. The risk assessment approach is based on the principles of proportionality and the risk-based approach outlined in the DSA, ensuring that risk management strategies are appropriately tailored to address both global and cultural/region-specific challenges.

The different languages and regional contexts, including when specific to a Member State, are reflected particularly in content moderation, where the Platform’s content moderators are fluent in a broad range of languages, including German, French, Italian, English, Spanish, Polish, Russian, Slovak, and Czech, among others, enabling them to accurately assess and manage content across various regions. NKL employs a two-pronged approach to content moderation that combines the expertise of the Platform’s multilingual moderation team with reliable translation software, including Google Translate where necessary. While moderators handle content in their native languages, translation tools serve as supplementary resources for initial language support and to broaden coverage across languages not directly represented by the team.

The report comprises the following components to be read in conjunction with each other:

- The present Risk Assessment Report, which is the framework for understanding the concept of risk assessment, its methodology and developing strategy to risk mitigation.
- The Risk Register, including a risk assessment overview, that provides a comprehensive tool for documenting and tracking all identified risks, which are divided into 12 more general risk categories and further granulated into 83 specific risk scenarios; the Risk Register also provides a structured overview of the risk assessment results by systematically listing all measures in place, as well as those measures to implement where necessary, for each of the 83 risk scenarios identified.

The Risk Assessment Report and Risk Register are maintained in a manner that ensures easy accessibility for relevant internal stakeholders, as well as external auditors and regulators. NKL retains all supporting documents related to the risk assessment—including the Risk Register and any additional metadata, if applicable—for at least three years from the date

of the assessment. Risk assessment documentation is periodically reviewed and updated (at least annually) to reflect new risks, changes in operational practices, and shifts in regulatory requirements.

1.2 Risk Management Framework

The risk assessment process has been developed based on the principles outlined in ISO 31000: Risk Management, which provides an internationally recognised framework for establishing a comprehensive and effective risk management system. This standard provides a clear framework for identifying, assessing, handling and monitoring risks, irrespective of their nature, emphasising the need for stakeholder involvement and senior management participation.

One of the core principles of ISO 31000 is continuous improvement, which is essential to maintaining a flexible and adaptable risk management culture. Leadership plays a crucial role in this framework, ensuring that risk management is integrated into NKL's strategic decision-making process. Management takes an active role in NKL, committing time, resources and oversight to ensure that risk management measures are effectively implemented and aligned with business objectives. This active involvement demonstrates a solid commitment to creating a sustainable, risk-informed environment.

In addition to these principles, the ISO 31000 framework is closely aligned with the requirements set out in the DSA for VLOPs. Although the DSA does not prescribe a specific risk management standard, the objectives of ISO 31000 - active risk identification, risk mitigation and ongoing monitoring – are particularly relevant and closely align with the expectations of the regulator and of the enforcer. For example, the systematic approach encouraged by ISO 31000 promotes compliance with the DSA's requirements for transparency in content moderation, data reporting obligations, and addressing the risks associated with the distribution of illegal content.

ISO 31000 has been chosen as the basis for a risk assessment and management framework for several key reasons:

- ISO 31000 is an internationally recognised standard that provides a comprehensive and structured approach to risk management. It covers all aspects of the risk management process, from risk identification and assessment to risk handling, monitoring and communication, ensuring consistency and thoroughness across the organisation.
- Although the DSA does not explicitly require ISO 31000, the principles underpinning the standard are closely aligned with the DSA's regulatory objectives. ISO 31000 promotes proactive risk identification, the development of mitigation strategies, and a focus on continuous improvement, which are key elements of any effective risk management system that addresses Platform management, transparency, and content regulation under the DSA.
- One of the most valuable aspects of ISO 31000 is its flexibility. This framework allows us to tailor our risk management approach to the unique requirements of the Platform while remaining flexible in response to changing regulatory requirements. This adaptability is necessary to integrate DSA's specific obligations into a broader risk management strategy, ensuring that NKL remains compliant as the regulatory environment evolves.

Role of the Compliance Officer

The Compliance Officer has an essential role in the risk assessment process, ensuring NKL identifies, assesses, and manages risks effectively while complying with regulatory requirements and internal policies. The function is integral in each stage of the risk assessment.

The Compliance Officer actively collaborates to identify and assess various risk scenarios, formulating and advising on risk mitigation strategies, particularly monitoring the implementation and effectiveness of these strategies over time. The Compliance Officer documents the relevant findings and outputs. This documentation supports transparency and facilitates a proactive approach to risk management.

2. Risk Identification

2.1 Methodology used for Risk Identification

The methodology for identifying systemic risks on the Platform was diverse and as comprehensive as possible, as it combined both internal expertise from various teams within the Platform and external expertise from experts with valuable independent insight on content moderation, cybersecurity and compliance. Risk scenarios were identified through structured workshops based on the internal and external expertise as well as real-time data analysis and ongoing collaboration with external stakeholders.

Collaboration with key stakeholders

The Platform actively collaborates with non-governmental organisations (“NGOs”), such as OffLimits (NL) and Safer Internet Centres (“Safer IC”) CZ chapter, both of which have deep expertise on issues related to Non-Consensual Intimate Imagery (“NCII”) and Child Sexual Abuse Material (“CSAM”). Communication with these NGOs facilitated exchange of knowledge and information on risks the Platform could be exposed to, in particular those related to the upload of illegal material such as NCII and CSAM in violation of the Platform’s TOS. These interactions helped the Platform validate the risk management methodology and ensure that risks associated with the Platform are associated with relevant, effective measures, for example, via content moderation, reporting and child protection mechanisms.

As part of the collaboration, Safer IC has provided a view on the Platform's risk register and found that it provides a comprehensive categorising of potential risks listed in Article 34(1) of the DSA.

OffLimits also provided an expert overview of risks and recommended strategies to address potential issues that generally occur on adult content platforms, especially focused on preventing online child sexual abuse and minimizing illegal or harmful activities. Their key insights and suggested strategies include the following:

“Uploading and distributing illegal materials

There is a risk that users upload and distribute child sexual abuse materials (CSAM), or other illegal material (e.g., content with animals).

This risk can be reduced when uploader verification is used. Uploading illegal material will then be a risk for the users as they are committing an offense while their identity is known.

Uploading and distributing sexual content without consent

There is also a risk that users upload and distribute sexual images without the consent of the persons involved.

To prevent dissemination of sexual images without the consent of the persons involved, all persons visible on the images have to provide consent and should therefore be verified.

Insufficient content moderation

There is a risk that the platform fails to identify and remove illegal content when it is uploaded and distributed on the platform.

There should be sufficient content moderation to prevent illegal content being uploaded and distributed on the platform. A few strategies can help in this effort. There should be simple and effective reporting tools to help users report illegal content on the platform. Illegal content can then be removed. Secondly, platforms should work with Trusted Flaggers because they have experience in signaling and reporting illegal content. Reports from Trusted Flaggers should be followed up more quickly because they are more reliable than general users. Furthermore, an easy way to check regularly for known CSAM on the platform is to use the Hash Check Service. CSAM with known hashes will be detected and can be removed or prevented from being uploaded.

Exposure adult content to minors

There is a risk that minors access explicit adult content due to ineffective age verification systems. Exposure to adult content in young viewers may have a negative impact on mental health and sexual development, and poses a risk for developing addictive tendencies, risky sexual behaviors, and unhealthy attitudes.

To prevent young people from viewing explicit sexual material that might be harmful for the young viewer, there needs to be an age verification tool in place. A simple question based on self-validation is insufficient. However, privacy and security need to be considered when using more complex verification tools.

Searching for illegal material

There is a risk that users search for illegal content on the platform.

Scientific research shows that individuals can escalate on adult websites to extreme types of pornography. Through a process of desensitization, they can end up watching increasingly extreme and eventually also illegal material. To prevent this escalation process it is important to intervene early and make it impossible to search for illegal content on the platform. An approach which is being used more extensively and has been shown to be effective according to research, is the use of deterrence messages. Illegal search terms (and terms that suggest illegal material) can be banned on the platform. Whenever individuals are searching for these risky search terms a warning message can be displayed. Besides emphasizing the illegal and harmful aspects of this behavior, a referral to a helpline (such as Stop it Now) can be shown to users.

Gateway to illegal material

There is a risk that users click on links that direct them towards websites which contain illegal content.

Research conducted by Stop it Now on adult websites showed that it is possible to end up with illegal material using only 4 clicks. When a platform uses various deterrence strategies (as mentioned above) the risk is significantly reduced. Most risk seems to be related to pop-ups (advertisements) with links to various other adult websites. There is a chance that another website contains CSAM. It is therefore important to consider what advertisements are being used on the platform, and to which other platforms are being linked. This reduces the chance that the adult platform serves as a gateway to illegal material and also prevents the escalation process towards such content.”

Workshops

Workshops were held to identify risk categories and corresponding risk scenarios. Representatives from various departments participated in the risk identification, including:

- Leadership (on 7 November 2024)
- Legal and Compliance Department (on 4 November 2024)
- Content Moderation Department (on 23 October 2024 and 31 October 2024)
- Information Technology Department (on 1 November 2024)
- External expert (on 30 October 2024 and 8 November 2024)

The workshops were organised to encourage open communication, allowing participants to express their thoughts and concerns based on their experience and knowledge. This approach helped to identify nuanced risks that may have gone unnoticed with a more quantitative approach.

Discussions in the workshops revolved around specific risk categories. Appropriate risk scenarios were developed for each risk category. The participants collectively identified and assessed various plausible risk scenarios. In particular, these risk scenarios took into account the systemic risks related to the exercise of fundamental rights, civic discourse and electoral processes and public security, the proliferation of illegal content, minors' access to adult content, and data privacy and security risks (due to their sensitivity) as well as gender-based violence, the protection of public health and users' well-being.

Instead of relying solely on predefined indicators, the risk identification process was based on meaningful, open discussions. This approach resulted in a comprehensive assessment capable of adapting to the Platform's changing environment. Risk scenarios were identified based on multiple cases, allowing the participants to understand and capture the full range of potential risk events.

Whilst many of the risks identified are common to any platform, the risk identification process was focused on fulfilling DSA obligations, particularly the assessment of systemic risks under Article 34 of the DSA.

The workshops also identified areas with minimal risks to the Platform, such as the risk of negative impact on civil discourse or electoral processes. These risks were categorised as acceptable as they were not considered very significant to the nature of the Platform's services.

Corporate knowledge and know-how

The Platform's content moderation team has extensive practical experience dealing with sensitive and potentially illegal content. Their deep knowledge of Platform moderation processes, repeat offender behaviour, and typical cases formed the basis of the risk identification process. Their experience in dealing with content and issues related to detecting potential NCII and CSAM was beneficial to addressing the effectiveness with which such content is rejected and further dealt with.

Their understanding of user behaviour on the Platform and trends in flagged content contributed significantly to identifying risks such as the distribution of illegal content and privacy breaches.

The Platform's internal IT/IS experts contributed to the assessment of risks related to data protection and user privacy. Their views on Platform encryption protocols, two-factor authentication and data leakage mitigation measures were critical in identifying risks related to unauthorised access and misuse of data. The effectiveness of automated systems for detecting potentially illegal content (e.g. Thorn Safer, HIVE, Google Safety API) was analysed and evaluated to help mitigate content-related risks without compromising user privacy.

External experts' input

External legal and compliance experts were engaged to identify risks related to the Platform's compliance with the DSA. They ensured that the Platform's policies and moderation processes aligned with evolving legal standards, especially in protecting fundamental rights such as privacy, freedom of expression and child protection. Their recommendations also helped anticipate possible legal changes that could affect the Platform's operations.

In addition, external cybersecurity experts were engaged to participate in evaluation of the Platform's security measures and to identify vulnerabilities related to data leakage, algorithmic biases and potential cyber threats.

Monitoring the legal and regulatory framework

The Platform continuously monitored regulatory frameworks of the EU and the Member States applicable to the Platform's business to identify risks associated with non-compliance with legal requirements. This allowed the Platform to proactively respond to new legislative requirements and changes, ensuring that risk management practices are adapted to future regulatory environments.

It should be noted that the approach described above was also used to assess the identified risk scenarios and develop mitigation measures, as these processes are inherently linked.

2.2 Risk Categories and Risk Scenarios

Risk categories provide a basis for organising and analysing the different types of risks that online platforms hosting adult content, including XNXX may face. Each category represents a different problem area and covers different risk scenarios that arise for similar reasons. Risk categorisation also helps to prioritise and allocate resources for risk management effectively.

While risk category is a unifying container for risk scenarios, it should be noted that a risk scenario represents a hypothetical situation, plausible and relevant to the Platform, which, given its description, allows the assessors to effectively assess the likelihood of occurrence of such hypothetical situation (see Risk Register, column D) and its impact on the Platform (see Risk Register, column E). In addition, the mitigating measures already in place (see Risk Register, Column H) are also considered to estimate risk values (i.e., inherent risk and residual risk) for each scenario (for further details, see Section 3 below). These risk values express whether the potential for materializing is imminent and whether any (additional) measures shall be considered to decrease (especially) the likelihood of occurrence (see Section 4.3 below). Also, as indicated above, the NGOs feedback confirmed that the completeness of identified risk scenarios (and their categorization) is comprehensive per the DSA requirements.

Below we provide an overview of the 12 identified risk categories.

1. Dissemination of Illegal Content

This category addresses risks where Platform users are involved in uploading, sharing, or distributing content in violation of XNXX's TOS, such as, for instance, NCII, CSAM, copyrighted works without authorization, malware or phishing schemes, and other forms of harmful content, and the challenges for the Platform to detect such content through monitoring and remove it. The corresponding risk scenarios are listed as Risk Scenarios IDs IC-01 to 11 in the Risk Register.

2. Gender-Based Violence

This category involves risks related to content that glorifies, promotes, or trivializes violence against specific genders, particularly women and LGBTQ+ individuals. The Platform assesses the risks of allowing or encouraging such harmful narratives, as they contribute to societal harm and can lead to real-world violence. The risks might be amplified by algorithms that may unintentionally promote such content, or by limitations on the Platform's ability to adequately moderate it. The corresponding risk scenarios are listed as Risk Scenarios IDs GB-01 to 06 in the Risk Register.

3. Protection of Minors

The protection of minors encompasses risks related to minors' exposure to explicit, harmful, or inappropriate content. The Platform is intended exclusively for an adult audience but there are nonetheless risks that minors would access the content. The risks in this category are particularly concerning due to the unwarranted exposure to adult content or inappropriate material, alongside regulatory and legal consequences. The corresponding risk scenarios are listed as Risk Scenarios IDs PM-01 to 07 in the Risk Register.

4. Violations of Fundamental Rights

This category addresses risks in case of potential violation of users' fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the "Charter") such as, rights to human dignity, respect for private and family life, the protection of personal data, freedom of expression and information, non-discrimination and to high level of consumer protection. These risks arise from, amongst others, data breaches, misuse of personal data, discrimination, or the arbitrary removal of lawful content. The corresponding risk scenarios are listed as Risk Scenarios IDs FR-01 to 08 in the Risk Register.

For example, to manage risks related to **respect for private and family life**, the Platform identifies specific risk scenarios such as "Data breaches that expose user identities, viewing histories, and payment information, infringing on users' right to privacy" (FR-01), or "Users' browsing histories, including their viewing preferences for adult content, are sold to third parties, violating their right to privacy" (FR-02). Additionally, the Platform considers the risk of "Collecting data on users without sufficient consent, which is then shared with advertisers, infringing on the right to privacy" (FR-03).

Exposure or misuse of sensitive information could impact users' familial relationships. For example, if a data breach exposes a user's personal information, including viewing history or payment data, it could lead to unintended consequences for their family life, as it may affect the dynamics and trust within family relationships. Or, if family members share devices, ads or recommendations based on a user's browsing history, they could be visible to others, potentially revealing sensitive preferences or habits that the user did not intend to share within their family setting.

Furthermore, to manage risks related to **non-discrimination**, the Platform identifies scenarios such as "The terms of services disproportionately affect marginalized groups, leading to violations of the right to non-discrimination" (FR-04). This ensures that policies and practices do not unfairly impact specific groups.

Negative effects on **human dignity** have also been considered in risk scenarios such as "The distribution of degrading content, including explicit material that depicts exploitation or humiliation, violating the right to human dignity" (FR-05) and "Users post deepfakes or manipulated content that depict individuals in explicit scenarios without their consent, impacting their dignity" (FR-06).

To uphold **freedom of expression and information**, the Platform addresses risks such as "Overly strict content moderation that results in the removal of lawful adult content, infringing on creators' freedom of expression" (FR-07), as well as "Removing user-generated content arbitrarily without a proper appeal process, restricting the users' right to free speech" (FR-08). Specific risk scenarios related to the negative effects on the **protection of personal data** and the **rights of children** have been classified separately as the "Protection of Minor" and "Data Privacy and Protection Risks" categories.

Concerning the right to a high level of **consumer protection**, the Platform emphasizes that while it is an unpaid service relying on advertising rather than direct sales, the Platform has a responsibility to ensure consumer safety and transparency in data practices. This responsibility encompasses minimizing risks to user privacy, enabling user data protection rights, and implementing security measures that protect users from exploitation.

5. Public Health

Public health-related risks involve the dissemination of content that promotes unhealthy or risky behaviours, such as misinformation about health, drug use, or encouraging self-harm. The Platform does inherently consider the potential for impact on health that certain materials may have on users. These risks are associated with the promotion of unrealistic body standards or the spreading of content that encourages dangerous health practices. The corresponding risk scenarios are listed as Risk Scenarios IDs PH-01 to 05 in the Risk Register.

6. Civic and Electoral Impact

This category includes risks associated with the misuse of the Platform to spread misinformation about civic processes, elections, and political matters. It covers the Platform's role in shaping political discourse, mainly through content it promotes or limitations of the moderation procedures. Allowing extremist or misleading political content can erode democratic processes, destabilize social cohesion, and affect voter behaviour. The corresponding risk scenarios are listed as Risk Scenarios IDs CE-01 to 06 in the Risk Register.

7. Public Security Concerns

Public security risks relate to the misuse of the Platform by criminal organizations, extremist groups, or terrorists for purposes such as recruitment, exploitation, or inciting violence. The Platform might face challenges in moderating content that could compromise public safety. The corresponding risk scenarios are listed as Risk Scenarios IDs PS-01 to 04 in the Risk Register.

8. Data Privacy and Protection Risks

This category refers to risks involving collection, use, and protection of user data –specifically forbidden by the TOS. It includes issues such as unauthorized data collection, data breaches, insufficient user consent, and lack of transparency in data processing. The Platform implements robust security measures to protect sensitive user information from breaches or misuse. The corresponding risk scenarios are listed as Risk Scenarios IDs DP-01 to 08 in the Risk Register.

9. Recommender Systems and Algorithmic Risks

When implemented and applied, recommender systems pose risks by potentially promoting harmful, illegal, or inappropriate content based on user engagement patterns. These algorithms may prioritize sensational or controversial content, increasing its spread and visibility. Additionally, recommender systems that do not consider regional or cultural nuances may amplify harmful material in specific contexts. The corresponding risk scenarios are listed as Risk Scenarios IDs RS-01 to 07 in the Risk Register.

10. Advertising Integrity

This category encompasses risks associated with the Platform's advertising system. These include issues such as lack of transparency in ad targeting, and advertisements promoting harmful or dangerous products. The corresponding risk scenarios are listed as Risk Scenarios IDs AI-01 to 09 in the Risk Register.

11. TOS Obligations

Risks in this category arise from the challenges of ensuring that clear, accessible, and comprehensive terms of service (TOS) to users are provided at all times. The DSA requires the Platform to inform users of their rights and obligations, including how content is moderated or how complaints are handled. Regular updates to the TOS must be adequately communicated, ensuring users are fully informed about changes that may affect their experience on the Platform. The corresponding risk scenarios are listed as Risk Scenarios IDs TS-01 to 06 in the Risk Register.

12. Transparency and Reporting Obligations

This category includes risks that the transparency obligations regarding content moderation, algorithmic processes, or Platform data are not met. Incomplete or inaccurate transparency reports undermine regulatory compliance. Ensuring the Platform accurately discloses its actions and decisions, especially when responding to regulatory requests, is critical to

maintaining accountability. The corresponding risk scenarios are listed as Risk Scenarios IDs TR-01 to 06 in the Risk Register.

2.3 Systemic Risks

Specific risk scenarios address individual factors NKL considers as overarching systemic risk issues/concepts. Such foundational risk issues would include issues such as instances of dissemination of illegal content, violations of fundamental rights, gender-based violence, the protection of public health from risks involving for instance the dissemination of content that promotes unhealthy or risky behaviours, such as misinformation about health, drug use, or encouraging self-harm, the protection of minors, negative effects on civil discourse and electoral process, and public security. To do so, NKL's approach was to translate these high-level, broad concepts that are open to interpretation (including by the EU Courts and the European Court of Human Rights), such as "privacy and family life" or "human dignity," into specific risk scenarios that are clearly defined and addressed by specific responses/measures.

In examining systemic risks, particular attention was given to peer-reviewed studies (see Section 4 for seminal examples of the studies that were considered during the Risk Assessment) covering various aspects related to the dissemination of illegal content (such as CSAM and NCII), impacts on fundamental rights such as data privacy, children's rights, and effects on mental health and relationships. The studies were chosen to provide a comprehensive overview of the possible threats that platforms, users and society as a whole may face.

As an example, concerning the distribution of illegal content, studies conducted by international organisations such as the United Nations Office on Drugs and Crime ("UNODC") and ECPAT International were considered to provide insight into the distribution channels of child abuse material (see Section 4 for examples of the studies that were considered during the Risk Assessment). This data was important in determining the specifics of how platforms operate and in distinguishing between platforms that provide legitimate adult content and those that may serve as channels for the distribution of illegal material. Similar studies that were taken into account have also analysed the dynamics of the unauthorised distribution of intimate images, highlighting the key role of interpersonal factors in the occurrence and distribution of NCII.

Issues of child protection and restricting minors' access to adult material were considered in light of studies by UNICEF and others that have examined the impact of pornographic content on minors. Cybersecurity and data protection studies were used to analyse privacy risks. Studies such as Perry (2020), Wright (2015), (see Section 4 for examples of the studies that were considered during the Risk Assessment) and other meta-analyses were reviewed to analyse the impact of pornographic content on mental health and relationships.

The Platform's content moderation team focused on specific types of illegal content, such as CSAM and violence, that can threaten the safety and dignity of people - especially children. Assessing these risk scenarios and taking action to prevent harmful content from being uploaded and shared were more effective ways of responding to the relevant systematic risks.

Similarly, specific risk scenarios related to gender-based violence were identified. These included risk scenarios associated with content glorifying or trivialising violence against women or the LGBTQ+ community or insufficient moderation allowing users to post gender-offensive content.

In the area of protection of minors, specific scenarios were considered, such as minors gaining access to explicit content through third-party software (e.g. VPN). This enabled NKL to evaluate existing age verification methods and mechanisms and strengthen the protection of minors from inappropriate content.

In addition, risk scenarios related to civil discourse, elections and public safety were considered, even though based on XNXX's content moderation team's feedback the Platform is rarely used for political topics discussion, much less manipulation. Consideration was given to the possibility of the Platform being used to disseminate misleading election-related content and whether there are scenarios in which algorithms could inadvertently facilitate the dissemination of divisive or extremist political content. While the content moderation team rarely evidences any political topic to be present on the Platform, the potential impact could be noteworthy.

Risk scenarios have been identified in defence of fundamental rights regarding data leaks and the publication of fake or altered content (deepfakes) that portrays people in compromising situations without their consent. This harms individual human dignity, so focusing on these risks allows for more effective measures to be taken to protect data and users' rights.

The public health risks associated with content promoting unprotected sex or risky behaviour, as well as the dissemination of false or misleading health information, were also considered. Particular attention was given to content that promoted unrealistic standards of beauty or encouraged self-harm and unhealthy lifestyles.

3. Risk Assessment

3.1 Risk Assessment Approach

The risk assessment process in this report follows the structure outlined in ISO 31000 and aims to identify and assess both inherent and residual risks systematically. Each identified risk scenario is analysed to understand its nature, sources and possible consequences.

Inherent risk is the level of risk that exists before applying any controls or mitigation strategies. Notably, the Platform since its creation – and well before any of the reporting requirements provided for by the DSA – has deployed and continues to deploy a host of mitigation efforts to address the inherent risks identified. We believe the Platform’s mitigation efforts have been and are effective, as reflected by the amount of residual risk that is left once the mitigation efforts have done their part. In particular, NKL has been aware of the important role it plays in the adult-content platform industry in fighting third party uploads of illegal content (e.g., CSAM, NCI and violence). Long before the adoption of the DSA, NKL has thus invested heavily, dedicated significant resources and built expertise to combat the distribution of such content deploying content moderation processes and practices that include advanced technology tools as well as human moderators with know-how and expertise in content moderation. To fight third parties’ upload and distribution of illegal content, NKL has also been collaborating for approximately a decade now with law enforcement agencies and officers. (See Paragraphs 4.1 – 4.5 which detail the risk management from identification to mitigation and Annex 1, containing risk scenarios that are associated with further actions to be carried out by NKL with the aim to continuously improve and further enhance the control environment, i.e., mitigation measures)).

For purposes of this report, each risk scenario is assessed based on a likelihood and an impact measurement. The risk level (low, medium, high) is then determined using a risk matrix.

Thereafter, strategies are developed to address each risk scenario to reduce the likelihood and impact to an acceptable level. Options include risk acceptance or mitigation. Once risk impact techniques have been implemented, the remaining risk (residual risk) is assessed.

Once inherent and residual risks have been identified, they are prioritised according to the severity and NKL's risk appetite. High-priority risks are those with “High” and “Medium” residual risk scores that exceed an acceptable threshold set by NKL (“Risk Management Policy”). For such risks, additional risk mitigation measures may be identified. Risks with “Low” residual risk scores are considered to have been sufficiently mitigated (i.e., respective measures and controls remain in place) and are within acceptable limits. For the sake of completeness, it should be noted that residual risks resulted only in “Medium” residual risk scores, as is evident from **Figure 3** below as well as the Risk Register.

3.2 Inherent Risk Assessment

An inherent risk assessment evaluates the potential risks to NKL without regard to existing controls or risk mitigation strategies. This assessment focuses on two main criteria: the likelihood of a risk event occurring and the potential impact of that event. Each criterion is scored on a scale of 1 to 5, with higher scores indicating greater likelihood or more severe impact.

The **likelihood** of a risk event is assessed using the following scale:

- **Rare (Score 1):** The risk event is highly improbable to take place within the next year considering no historical occurrences and robust preventative measures elsewhere.
- **Unlikely (Score 2):** The risk event has a low chance to take place within the next year, possibly due to rare instances or minimal vulnerabilities.

- **Possible (Score 3):** The risk event has a moderate chance of occurring within the next year, supported by occasional past occurrences and some identified vulnerabilities.
- **Likely (Score 4):** The risk event is expected to occur within the next year, indicated by frequent past instances and significant vulnerabilities.
- **Highly Likely (Score 5):** The risk event is almost certain to occur within the next year, with ongoing incidents or critical vulnerabilities present.

The potential **impact** of a risk event is evaluated on the following scale:

- **Insignificant (Score 1):** Minimal or no potential harm to users, society, or the organization. Regulatory action is unlikely, and any reputational impact would be immaterial.
- **Minor (Score 2):** Potential harm to users or society, such as exposure to inappropriate content or limited misinformation spread. The organization might face minor reputational damage or warnings from regulators.
- **Moderate (Score 3):** Notable potential for harm to users or society, including safety risks, privacy breaches, or erosion of trust. The organization could experience moderate reputational damage or regulatory investigations.
- **Major (Score 4):** Significant potential for widespread harm to users or society, such as extensive exposure to harmful content or manipulation of essential processes. The organization may face substantial reputational damage, operational suspensions, or significant fines.
- **Critical (Score 5):** Severe potential for extensive harm to users or society, including exploitation, psychological harm, or significant disruptions to societal functions. The organization could suffer severe reputational damage, loss of operational licenses, or complete shutdown.

Once the likelihood and impact are determined, the inherent risk value is calculated using the Risk Value Matrix (see **Figure 1** below). This matrix cross-references the likelihood score with the impact score to assign an overall risk value:

$$\text{Inherent Risk Score} = \text{Likelihood Score} \times \text{Impact Score}$$

Figure 1 – The Risk Value Matrix determines the categorisation of risk level

Risk Value Matrix		(x-axis: impact; y-axis: likelihood)				
		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Critical
1	Rare	1	2	3	4	5
2	Unlikely	2	4	6	8	10
3	Possible	3	6	9	12	15
4	Likely	4	8	12	16	20
5	Highly Likely	5	10	15	20	25

Source: NKL’s internal document – Risk Register

The color-coded risk values provide a visual representation of the risk level:

- **Low Risk (Green):** Risk values between 1 and 5 indicate a low level of inherent risk. The organization’s response strategy typically involves accepting these risks.
- **Medium Risk (Yellow):** Risk values between 6 and 15 represent medium level risks. For these risks, the organization focuses on reducing exposure through mitigation measures.
- **High Risk (Red):** Risk values between 16 and 25 indicate high inherent risk, requiring immediate attention and efforts to reduce or eliminate the risk through comprehensive strategies. For these risks, the organization focuses on reducing exposure through mitigation measures.

The details of inherent risk assessment for each of the 83 risk scenarios can be found in the Risk Register, columns “Risk Measurement” and “Inherent Risk.”

3.3 Residual Risk Assessment

Once the inherent risks were identified, a comprehensive assessment of the existing controls and risk mitigation measures relevant to each risk scenario was carried out. This assessment aimed at determining the residual risk, i.e., the level of risk remaining after applying controls.

Measure Effectivity Evaluation

The effectiveness of each control was systematically evaluated by examining several critical factors affecting its ability to mitigate risk effectively:

- The **strength of mitigation** refers to the extent to which the control reduces or eliminates the identified risk;
- The **frequency** with which controls are monitored, reviewed, or updated;
- The **historical effectiveness** of the measure in past cases or similar scenarios.

Further, each measure was categorised according to the assessment of its effectiveness:

Figure 2 – Effectiveness ratings for risk mitigation measures

Evaluation of Measures	Description
Low Effective	Measure that provide minimal risk reduction or have limited reliability. These measures may require improvement to effectively mitigate risk.
Moderately Effective	Measures that provide a reasonable degree of risk reduction but do not cover all aspects of risk. They may have limitations under certain conditions or require additional support measures.
Highly Effective	Measures that significantly reduce or eliminate risk. These controls have been proven over time and are reliable in various scenarios.

Residual Risk Determination

After assessing the effectiveness of measures, each risk scenario is scored in three categories of residual risk: Low Risk, Medium Risk and High Risk.

- **Low residual risk** score indicates that the risk has been sufficiently mitigated and is within acceptable limits, reflecting a high confidence level in existing measures.
- **Medium residual risk** score indicates that although the risk has been mitigated, there may still be a need for additional monitoring or implementation of further measures to ensure comprehensive risk mitigation.
- **High residual risk** score meant that the risk remained significant and required immediate and decisive action to reduce the potential impact further.

After assigning residual risk scores, risks are prioritised to focus on those requiring significant attention. First, residual risk levels are compared to identify risks with scores above the “Low Risk” threshold. This identifies which risks pose the greatest risk to NKL. By systematically assessing each residual risk, risks that remained significant despite existing controls were highlighted for further analysis.

Mitigation strategies were developed for the remaining prioritised risks, namely the “Medium” and “High” residual risks. These strategies aim to reduce or effectively manage risks, increasing NKL’s overall risk resilience. In developing these strategies, joint workshops were held with experts from relevant fields to ensure that the approaches were practical, effective and sustainable.

This prioritisation approach allowed resources to be effectively allocated to address the most significant risks, ensuring that the necessary resources were available for critical areas.

The details of residual risk assessment for each of the 83 risk scenarios can be found in the Risk Register, columns “Measures in Place”, “Inherent Risk”, “Response Strategy” and “Measures to Implement”.

4. Risk Assessment Results

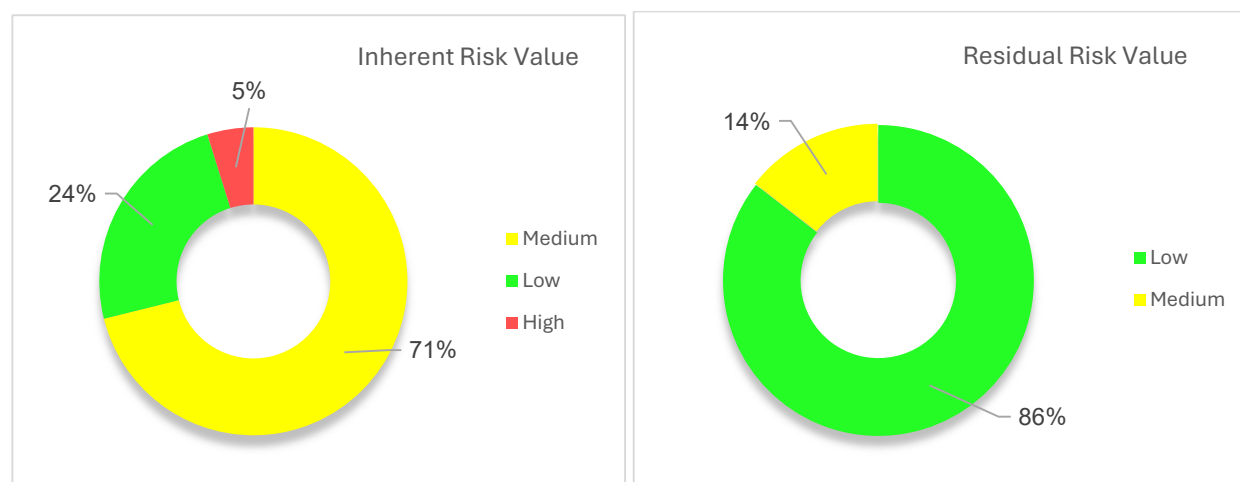
4.1 Risk Assessment Overview

The risk assessment thoroughly examined risk scenarios across key risk categories, assessing both inherent and residual risks to determine the organization's level of exposure accurately. The inherent risk assessment identified 83 different risk scenarios spread across 12 risk categories listed in Section 2.2 above.

As a result of the inherent risk assessment, it was found that NKL faced predominantly medium to low levels of inherent risk: 59 risk scenarios (71%) were rated as medium, and 20 risk scenarios (24%) were low. The high inherent risk was minimal and accounted for only 4 risk scenarios (5%) of the assessed scenarios. This distribution mainly reflects an environment of moderate inherent risk with limited exposure to high risks.

In the next step, residual risk was assessed, considering existing controls and risk mitigation strategies, which demonstrated a significant risk reduction. 71 risk scenarios (86%) were rated as low residual risk, while 12 scenarios (14%) remained at a medium risk level, emphasizing the effectiveness of existing controls in addressing and mitigating inherent risks.

Figure 3 – Comparison of inherent and residual risk assessment results



Source: NKL's internal document – Risk Register, RA Dashboard

4.2 Mitigation measures in place

The Platform since its creation - and well before the reporting requirements provided for by the DSA - has deployed and continues to deploy a host of mitigation efforts to address the inherent risks identified. All these measures are listed in Column "Measures in Place" in the Risk Register for each of the 83 risk scenarios.¹ NKL believes the Platform's mitigation efforts have been and are effective, as reflected by the amount of residual risk that is left once the mitigation efforts have done their part.

¹ The Compliance Officer is currently preparing a documentation further detailing these measures in place with regard to each of the [83] scenarios. This preparation is an ongoing effort that is in process and will be updated in the next iteration.

Mitigation measures are associated with specific risk scenarios identified in the Platform's Risk Register. The effectiveness of each mitigation measure in preventing or reducing the likelihood of its corresponding risk scenario materializing is discussed and evaluated during the risk assessment workshops.

This evaluation leads to the determination of residual risk values, which represent the level of risk remaining after the mitigation measures have been applied. The residual risk values are crucial for informing the Platform's overall risk management strategies.

4.3 Residual Risk Assessment

The residual risk assessment phase identified 12 risk scenarios that, after the implementation of risk mitigation measures, have a risk level higher than “Low Risk” threshold, i.e., Medium residual risk (see **Figure 4** below). The affected risk categories are the following:

- Protection of Minors (5 risk scenarios)
- Gender-Based Violence (1 risk scenario)
- Public Health (3 risk scenarios)
- Transparency and Reporting Obligations (3 risk scenarios)

Figure 4 – Overview of risks requiring additional measures to be implemented

ID	Risk Category	Risk Scenario	Risk Measurement		Inherent Risk		Measures in Place	Residual Risk Value
			Likelihood	Impact	Score	Value		
GB-05	Gender-Based Violence	Dissemination of harmful stereotypes contributing to gender inequality	Possible	Moderate	9	Medium	<ul style="list-style-type: none"> -TOS prohibitions -Several mechanisms to identify and prevent the distribution of harmful or illegal content, including (i) algorithmic content verification systems such as the Hve classification system and (ii) digital fingerprinting for known illegal material, as well as (iii) trained team of content moderators' reviewing flagged content and consequent removal of any material that violates the TOS, and (iv) mechanisms for user reporting of inappropriate content facilitate closer monitoring- -Ongoing in-depth review of studies and research papers on the impact of violent content (gender-based violence, non-consensual sexual act, physical aggression etc.) 	Medium
PM-01	Protection of Minors	Minors access explicit adult content	Highly Likely	Major	20	High	<ul style="list-style-type: none"> -Warnings about adult content -Self-validation -Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) -RTA label -Terms of Service - Point 3 - Child content -Parental controls direct link to instructions security measures and parental controls setup including deployment of filters -Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users 	Medium
PM-02	Protection of Minors	Minors bypass age verification systems by using fake identities, or sharing adult credentials	Likely	Major	16	High	<ul style="list-style-type: none"> -Warnings about adult content -Self-validation -Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) -RTA label -Terms of Service - Point 3 - Child content -Parental controls direct link to instructions security measures and parental controls setup including deployment of filters -Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users 	Medium
PM-03	Protection of Minors	Minors bypass age verification systems by using third-party software or techniques (such as VPNs or proxy servers)	Likely	Major	16	High	<ul style="list-style-type: none"> -Warnings about adult content -Self-validation -Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) -RTA label -Terms of Service - Point 3 - Child content -Parental controls direct link to instructions security measures and parental controls setup including deployment of filters -Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users 	Medium
PM-06	Protection of Minors	Distribution of content with prohibited material (e.g., violent or exploitative content involving minors)	Likely	Major	16	High	<ul style="list-style-type: none"> -TOS prohibitions -Deployment of technology and human moderations such as: <ul style="list-style-type: none"> -internal fingerprint check -hive classification (violence, weapons) -user reports and moderation team -user account verification procedure -Cooperation with law enforcement agencies to fight the distribution of any such content -In-depth review of studies and research papers on the impact of dissemination of CSAM 	Medium
PM-07	Protection of Minors	Exposure to adult content may negatively affect minors' physical and mental health, potentially fostering addiction or unhealthy attitudes	Possible	Major	12	Medium	<ul style="list-style-type: none"> - Warnings about adult content -Self-validation -Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) -RTA label -Terms of Service - Point 3 - Child content -Parental controls direct link to instructions security measures and parental controls setup including deployment of filters -Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users -In-depth review of studies and research papers on the impact of adult content 	Medium
PH-01	Public Health	Content promoting unprotected sex or risky behaviours without disclaimers	Likely	Minor	8	Medium	<ul style="list-style-type: none"> -Co-operation with NGO - OffLimits -In-depth review of studies and research papers on the impact of adult content on the public health 	Medium
PH-03	Public Health	Content promoting unrealistic or unhealthy body standards	Likely	Minor	8	Medium	<ul style="list-style-type: none"> -Co-operation with NGO - OffLimits -In-depth review of studies and research papers on the impact of adult content on the public health 	Medium
PH-05	Public Health	Content that may encourage self-harm or unhealthy lifestyles	Unlikely	Moderate	6	Medium	<ul style="list-style-type: none"> -Co-operation with NGO - OffLimits -In-depth review of studies and research papers on the impact of adult content on public health -user reports and moderation team (self-harm) 	Medium
TR-03	Transparency and Reporting Obligations	The platform inaccurately reports the average monthly number of active recipients of the service	Possible	Moderate	9	Medium	<ul style="list-style-type: none"> -Use of an acceptable calculation methodology based on available data and common practice 	Medium
TR-04	Transparency and Reporting Obligations	Inadequate disclosure of algorithmic decision-making processes	Possible	Major	12	Medium	<ul style="list-style-type: none"> -Compliance Officer nomination -Resources allocated to secure compliance with DSA requirements -Process/procedural changes and updates to reflect DSA requirements -Algorithmic definitions and application subject to regular Compliance audits -Close internal cooperation in case of any changes with algorithms should they become more complex (currently basic - see above) 	Medium
TR-05	Transparency and Reporting Obligations	Non-compliance with regulatory requests for platform data	Unlikely	Major	8	Medium	<ul style="list-style-type: none"> -Compliance Officer nomination -Resources allocated to secure compliance with DSA requirements -Process/procedural changes and updates to reflect DSA requirements -Maintenance of required databases -Regular reporting to Authorities in the required form and structure 	Medium

Source: NKL's internal document – Risk Register

Protection of Minors

(i) Risk of accessing explicit content

A significant portion of the assessed risks is related to the protection of minors, primarily due to the high likelihood and potential impact of minors accessing explicit content. The identified risk scenarios involve minors circumventing age verification systems through various methods or being exposed to inappropriate content, resulting in consistently classifying the risk assessment as high.

Nevertheless, the residual risk is moderate (“Medium”) due to risk control mechanisms. The Platform is intended **exclusively** for an adult audience and NKL does not permit minors to use its service. In particular, the Platform indicates on its landing page and TOS that it specifically restricts the viewing of content to those aged 18 or above by (a) warning users that the site is for adults only and (b) requiring users to acknowledge they are 18 or older before accessing the site. The Platform has an age assurance system in the form of a disclaimer about adult content and a feature requiring users to confirm they are of legal age. Further to that the Platform is rated with the “Restricted to Adult” (“**RTA**”) label. The RTA label was created by the Association of Sites Advocating Child Protection (“**ASACP**”) to better enable parental filtering and demonstrate the commitment of those using this rating to help parents and guardians ensure minors do not view age-inappropriate content. Additionally, the Platform also points users to a dedicated section on its interface on “parental control” and provides detailed guidance on how to activate safe mode in search engines, as well as guidance for parents on website, app, and game restrictions, time limits, methods to review recent activity, control of app-installs and so forth. In addition to all this the Platform has been investing significant resources to find suitable additional means to prevent minors from accessing the Websites, considering parental education and enhanced filtering and advocating device level age verification and other ways to address any such risks, in full respect of privacy and security, which need to be considered when considering the deployment of more complex verification tools.

Additionally, NKL consistently monitors the status quo of existing age verification tools and methods and has invested and continues to invest significant resources in participating in public expert discussion aimed at finding suitable methods that will offer optimal solutions, especially such that will not encourage users to instead visit other websites with lower or no regulation or oversight (as above). Currently, the issue with website-based age verification remains unresolved, as there is no such approach that addresses the problem effectively (meaning that (1) website-based age verification (1) fails to meaningfully restrict minors’ access to adult content online while also risking to push minors to poorly or non-moderated websites with riskier, harmful illegal content, or the Dark Web and (2) poses significant privacy, safety and security risks to users).

(ii) CSAM

Separately and apart from the risk of bypassing current age verification measures, this report also assesses risk of CSAM distribution. In this regard several studies on content distribution methods have been considered to identify the potential dangers of using the Platform to for these purposes.

The UNODC² study indicates that CSAM is primarily distributed through non-commercial channels, such as peer-to-peer networks, encrypted private networks, and the dark web, rather than mainstream adult content platforms. Huikuri (2023)³ emphasizes that anonymity is vital for CSAM consumers, making cloud-based peer-to-peer platforms challenging to monitor, as they often lack activity oversight. Emerging technologies like live streaming, along with dark web and peer-to-peer networks, are identified as major distribution channels in ECPAT International's 2018 report⁴ on online CSAM trends.

Adult content platforms, such as NKL, are not major distribution channels for CSAM due to strict content moderation policies, regulatory compliance, and user identification requirements, all of which NKL has in place and requires. These factors distinguish legal adult content providers, such as XNXX, from platforms intentionally used to distribute illegal

² United Nations Office on Drugs and Crime. Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children. Vienna, 2015

³ Huikuri, S. (2023). Users of Online Child Sexual Abuse material. Journal of Police and Criminal Psychology, 38(4), 904–913.

⁴ ECPAT International. (2018). Trends in Online Child Sexual Abuse Material. Bangkok: ECPAT International (April 2018)

content. Research by Gannon et al. (2023)⁵ notes that CSAM is far more prevalent on the dark web, with studies showing a higher concentration of CSAM-related sites compared to the clearnet.

In this regard, the Platform deploys several mechanisms to identify and prevent the distribution of any such content. These mechanisms include algorithmic content verification systems such as the Hive classification system and digital fingerprinting technologies that detect known illegal material. In addition, a trained team of content moderators reviews flagged content and removes any material that violates the TOS. Mechanisms for user reporting of inappropriate content further facilitate monitoring.

Further risk analysis links CSAM production to specific motivations, often unrelated to adult content platforms. Salter and Wong (2023)⁶ reveal that a substantial portion of CSAM production comes from unhealthy, dysfunctional family environments driven by commercial interests, which is distinct from the operational goals of adult content sites that focus on entertaining consenting adult audiences.

Gender-based violence

Gender-based violence and the potential dissemination of non-consensual or exploitative content are recognised as extremely risky, given their societal implications and the Platform's zero-tolerance policy for such content. This risk assessment recognises both the direct threat posed by harmful content and the broader implications related to the reinforcement of stereotypes, gender inequality and the prevalence of violence against women.

This is yet another instance where the Platform utilises several mechanisms to identify and prevent the distribution of harmful or illegal content, including algorithmic content verification systems such as the Hive classification system and digital fingerprinting for known illegal material. In addition, a trained team of content moderators' reviews flagged content and removes any material that violates the TOS, and mechanisms for user reporting of inappropriate content facilitate closer monitoring.

Also, NKL has scrutinised the impact of adult content on the formation of gender stereotypes and gender-based violence per se. At this point, research findings are mixed and require more in-depth study. For this reason, NKL is actively establishing cooperation with various NGOs that deal with this issue to explore the associated risks and possible control measures fully.

The research on the impact of pornography on gender-based violence reveals mixed and inconclusive findings. Lim et al. (2015)⁷ noted that, while pornography often portrays violence against women, studies on its influence on real-life violence yield inconsistent results. Some studies suggest that violent pornography may foster attitudes that support violence against women, while others propose it might act as a cathartic outlet, reducing aggressive tendencies. Additionally, pornography has been linked to decreased relationship satisfaction in heterosexual couples, though it may also offer benefits like reduced sexual anxiety.

Wright et al. (2015)⁸ conducted a meta-analysis linking pornography use with sexual aggression and attitudes supporting sexual violence, though they emphasized that not all users exhibit aggressive behaviour, as multiple factors contribute to sexual aggression. The World Health Organization ("WHO")⁹ notes that risk factors for gender-based violence include societal acceptance of violence, gender inequality, and individual traits, with pornography being a potential but non-determinative contributor.

Mestre-Bach et al. (2023)¹⁰ observed inconsistent associations between pornography use and violence, particularly with violent content, and noted that individual predispositions play a significant role in shaping attitudes related to sexual

⁵ Gannon, C., Blokland, A. A., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie*, 17(4), 353–365.

⁶ Salter, M., & Wong, T. (2023). Parental production of Child sexual abuse material: A critical review. *Trauma, Violence, & Abuse*, 25(3), 1826–1837

⁷ Lim, M. S., Carrotte, E. R., & Hellard, M. E. (2015). The impact of pornography on gender-based violence, sexual health and well-being: What do we know? *Journal of Epidemiology and Community Health*, 70(1), 3–5

⁸ Wright, P. J., Tokunaga, R. S., & Kraus, A. (2015). A meta-analysis of pornography consumption and actual acts of sexual aggression in general population studies. *Journal of Communication*, 66(1), 183–205

⁹ World Health Organization: WHO. (2024, March 25). Violence against women

¹⁰ Mestre-Bach, G., Villena-Moya, A., & Chiclana-Actis, C. (2023). Pornography use and violence: A systematic review of the last 20 years. *Trauma, Violence, & Abuse*, 25(2), 1088–1112

violence. Lastly, Fisher et al. (2013)¹¹ found limited support for a direct link between pornography and sexual violence. Observational data suggested that greater access to pornography might not increase sexual crime rates and may even reduce child sexual abuse cases in some contexts, pointing to personality traits as potentially more influential factors.

Public Health

The Platform has evaluated the risks associated with adult content concerning potentially promoting risky behaviour, unhealthy body standards, or self-harm. While these risks are deemed lower than those related to underage access and gender-based violence, NKL recognizes their significance and the importance of managing them.

Although NKL has tools to monitor content contextually, fully mitigating these systemic risks remains challenging. Nevertheless, the platform has comprehensively reviewed relevant research on these issues. To better monitor and address these risks, the Platform actively collaborates with NGOs and continuously analyses emerging studies to develop effective solutions. NKL remains committed to neither ignoring nor accepting these risks.

The studies collectively suggest a complex and nuanced relationship between pornography use, sexual behaviours, and psychological outcomes. Sinković et al. (2013)¹² found no direct link between pornography use and risky sexual behaviours, highlighting that other factors, such as sensation seeking or early exposure to sexual media, may influence sexual aggressiveness more directly. Stefanska et al. (2022)¹³ found that taboo sexual fantasies are rare, with consensual fantasies being far more common. Research also indicates that pornography use does not directly lead to adverse mental health outcomes like depression, with individual personality traits and attitudes significantly moderating its effects. Willoughby et al. (2014)¹⁴ found that heavy pornography use does not necessarily reflect social isolation or lack of real sexual experiences but may represent a broader openness to sexual exploration. Bóthe et al. (2020)¹⁵ emphasized that high-frequency pornography use isn't inherently problematic, though low-frequency use might correlate with depression if users feel moral conflict. Overall, these findings suggest that the effects of pornography on behaviour and mental health are shaped by personal beliefs, contextual factors, and individual differences rather than frequency of use alone.

Transparency and Reporting Obligation

Transparency is one of the essential requirements under the DSA, which obliges platforms to publish accurate and timely transparency reports and to develop clear and transparent TOS. NKL has appointed a compliance officer and continues to follow the adopted strategy and is implementing measures to further improve the transparency of relevant processes and reports.

4.4 Response Strategy

NKL has adopted specific response strategies tailored to the residual risk scores that align with the risk management strategy. These strategies provide an integrated approach to managing potential risks.

For risk scenarios categorised as “**Low**” residual risk, the risk is **accepted** as the chosen response strategy. This decision is based on evaluation of existing controls that have been deemed sufficient to reduce the risk to an acceptable level. Acceptance does not mean neglect; rather, it represents a calculated decision that ongoing monitoring of controls is deemed necessary to ensure their continued effectiveness over time. A risk acceptance strategy builds on the following:

- Continuous monitoring of the environment surrounding the low-risk scenario to identify any changes in the risk landscape;

¹¹ Fisher, W. A., Kohut, T., Di Gioacchino, L. A., & Fedoroff, P. (2013). Pornography, sex crime, and paraphilia. *Current Psychiatry Reports*, 15(6).

¹² Sinković, M., Štulhofer, A., & Božić, J. (2013). Revisiting the association between pornography use and risky sexual behaviors: The role of early exposure to pornography and sexual sensation seeking. *Journal of Sex Research*, 50(7), 633–641

¹³ Stefanska, E. B., Longpré, N., & Rogerson, H. (2022). Relationship between atypical sexual fantasies, behavior, and pornography consumption. *CrimRxiv*

¹⁴ Willoughby, B. J., Carroll, J. S., Nelson, L. J., & Padilla-Walker, L. M. (2014). Associations between relational sexual behaviour, pornography use, and pornography acceptance among US college students. *Culture, Health & Sexuality*, 16(9), 1052–1069

¹⁵ Bóthe, B., Tóth-Király, I., Potenza, M. N., Orosz, G., & Demetrovics, Z. (2020). High-frequency pornography use may not always be problematic. *The Journal of Sexual Medicine*, 17(4), 793–811.

- Proactive adjustment, i.e. when weaknesses or changes in the operating environment arise, appropriate action will be taken, such as strengthening existing or implementing new mitigation measures;
- Even if the residual risk is deemed acceptable, regular review of the measures put in place ensures that decisions align with the changing regulatory and operational environment.

The strategy chosen for risk scenarios that fall under "**Medium**" or "**High**" residual risk is to **reduce** the risk through mitigation efforts. Based on the results of the risk assessment, 13 risk scenarios with a residual risk level of "Medium" were identified, which, despite the existing measures, require an integrated approach to ensure their effective management. This process entails the design, development, and implementation of new measures, or the enhancement of existing ones, to more effectively address elevated risk levels. For each of these 13 risk scenarios, the measures to implement to mitigate residual risks have been identified and outlined in the Risk Register (provided as **Annex 1**). Key mitigation measures include:

Table 1 - Residual risk mitigation strategies

Strategy Area	Description
Collaboration with NGOs and experts on online protection of minors	<p>Liaison with reputable NGOs to fund and implement programs aimed at raising awareness about the importance of online safety and security for minors. These programs focus on educating minors and their parents or guardians on risks associated with internet use and how to mitigate them.</p> <p>Engage experts on age verification and minor protection to ensure that the NKL's risk mitigation strategies consider the latest best practices and innovative solutions. This collaboration would help fine-tune policies that affect vulnerable groups.</p>
Strengthening age verification and protection mechanisms	<p>Assessing current status of tools for purposes of protecting minors, including in addition to self-validation, parental control and filtering, such as device level age verification tools, particularly to ensure an effective protection of minors, without jeopardizing fundamental rights, privacy rights and the safety of the users, and the continuity of the business operations. This includes evaluating solutions that integrate seamlessly into operating systems, thus offering more robust and standardized protection mechanisms.</p> <p>Support the promotion and implementation of parent filtering and device level age verification tools that effectively protect minors without jeopardizing fundamental rights, privacy rights and the safety of the users, by advocating and continuing to invest in more effective tools. Monitor the industry recent developments of solutions that effectively prevent underage access and respect fundamental freedom and privacy as well as safety as well as business considerations, such as operational efficiency.</p>
Raising awareness and educating the public	<p>Continue content development aimed at raising awareness of online safety. This content should be geared towards educating minors about risks, providing guardians with resources to protect their children, and offering general advice on online security measures. This initiative also supports compliance and broader social responsibility goals.</p>
Compliance management and auditing	<p>Continued implementation of the CMS ensuring it aligns with the latest regulatory requirements under the DSA and other relevant regulations. The CMS should be designed to manage and mitigate risks related to content moderation, user privacy, and illegal content dissemination.</p> <p>External audits of CMS assess the system's effectiveness in managing compliance risks, identifying gaps, and recommending improvements. It helps ensure that internal processes are robust and meet the requirements set by authorities.</p> <p>Ongoing compliance audits evaluate the adherence to internal policies and external regulatory frameworks. These audits are essential for identifying potential non-compliance areas and implementing timely corrective actions.</p>
Data Management for Reporting and Compliance	<p>Develop a standardized user-counting methodology, supported by regulators, which incorporates insights from public and regulatory consultations to ensure accuracy in reporting.</p>
Content Moderation	<p>Internal audit of content moderation processes and procedures</p>

4.5 Risk Monitoring Procedures

Continuous monitoring of key measures and processes is integral to the risk management strategy. Both accepted and mitigated risks are continuously monitored and evaluated. This continuous oversight ensures that risk mitigation efforts remain effective and that any changes in risk levels or new vulnerabilities are promptly addressed. The risk monitoring process is carried out through a combination of ongoing activities and periodic reviews.

Ongoing monitoring includes the following activities:

- Attending conferences, and reviewing market research to stay updated on new risks and challenges,
- Analysing data from operational systems, such as user activity logs, incident reports, and compliance audits, to identify potential risk indicators,
- Monitoring regulatory changes in relevant legislation, such as DSA, GDPR, or other regulations, that may impact NKL's risk landscape and adjusting internal processes accordingly,
- Encouraging employees to report risks by conducting regular workshops and maintaining an open communication channel for potential risk concerns,
- Evaluating the performance of existing tools and procedures such as automated content monitoring tools, user reporting systems, data security measures and user verification tools.
- Training for the moderation team to ensure they remain equipped to handle new types of content risks and moderation challenges.

Periodic reviews include the following activities:

- Risk Reduction (Medium and High) – gradual implementation of measures to decrease residual risks to levels that allow for accepting the risk as is, while continuing to apply the measures and controls in place,
- Comprehensive reviews of risk scenarios and the measures in place to ensure that the results of the assessment are up to date and that there have been no significant changes requiring new measures,
- Independent external audits at least once a year to assess compliance with regulatory requirements such as DSA, evaluate the effectiveness of allocated resources and determine if any processes need to be updated,
- Annual review of publicly available legal documents such as terms of service (TOS), privacy policies and cookie policies to ensure they are up-to-date and compliant with regulatory changes,
- Periodic assessment of NKL's risk register, incorporating risk indicators and updating risk maps to reflect any newly identified risks or changes to existing risks,
- Enhanced assessments of resource utilisation and moderation processes to ensure effective use of resources.

5. Conclusion

5.1 Summary of Findings

The risk assessment for NKL identifies and evaluates risks across 83 scenarios in 12 categories. The inherent risk assessment found that NKL faces mainly medium (71%) and low (24%) levels of inherent risk, with only a small portion (5%) classified as high risk. After applying risk mitigation measures, residual risks were notably reduced, with 86% of scenarios rated as low and 14% as medium, underscoring the effectiveness of NKL's controls.

After mitigation, 12 scenarios across four categories retained an average level of risk requiring further action. These four affected risk categories are: Protection of Minors (five scenarios highlighted the risk of minors accessing explicit content, although existing controls mitigate this risk), Public Health, Gender-based violence, and Transparency and reporting obligations.

NKL's risk management strategy emphasises continuous monitoring and proactive adjustment of established control measures. For scenarios with low residual risk, NKL accepts the risk through continuous monitoring. Despite the implementation of existing risk controls, NKL actively monitors medium residual risk scenarios, recognising that these risks require constant vigilance, improvement and the search for advanced technical solutions. The approach to medium residual risk reflects NKL's commitment to actively mitigating risk rather than simply accepting the level of risk.

For this purpose, NKL intends to implement relevant measures, such as co-operation with NGOs, research into proper, efficient, suitable systems to prevent minors' access to the Platform, implementation of a compliance management system and auditing of content moderation processes. NKL actively monitors arising risks and invests in ongoing improvement, including finding technical solutions to thoroughly mitigate risks and ensure compliance.

5.2 Overall Risk Profile

Overall, NKL exhibits a moderate exposure to inherent risks, with an average risk score of 8. The current controls effectively reduce most scenarios to low residual risk, evidencing the robustness of the existing mitigation strategies. However, certain high-priority risks demand continuous monitoring and further mitigation efforts, especially in categories like Protection of Minors, which involves challenges in order to deploy effective mechanisms that do not chill fundamental freedoms, privacy rights and safety and the complexity of user behaviour in circumventing restrictions. This moderate-to-low risk profile reflects a controlled yet vigilant approach, emphasizing NKL's proactive risk management.

5.3 Recommendations

Participate in finding effective age verification measures that adequately address protection of minors

It has been NKL's practice to participate in public discussions and consultations on age verification measures, and NKL will continue to engage in, and contribute to broad public discourse to advance the discussion on the prevention of minors' access to adult content alongside engagement with governments and regulators, and on the technologies that can effectively safeguard minors. The focus should be on developing solutions that effectively prevent underage access to adult content across the whole ecosystem while preventing the issue to shift towards less controlled environments and, which also takes into consideration users' privacy and safety. NKL's commitment to child safety requires ongoing monitoring of technological advancements and regulatory updates to ensure compliance with the developing practices in privacy-preserving methods that fulfil this purpose.

Increase collaboration with reputable NGOs

NKL's ongoing collaboration with NGOs and industry experts in protection of minors, gender-based violence prevention, and public health is important. By collaborating with organizations with expertise in these areas, NKL will be able to contribute to, and also make use of the latest trends and issues. In addition, regular consultations with non-governmental organizations and consumer advocacy groups can provide both the sides with valuable feedback on risk prevention strategies and focused risk management practices.

Monitor regulatory changes

In a rapidly changing regulatory landscape, particularly under the DSA, NKL will seek to stay ahead of potential legislative changes by closely monitoring legislative developments at both EU and national levels.

Annex 1

Action Plan

The action plan details the specific controls and measures currently in place, as well as additional mitigation strategies planned for implementation. The focus is on addressing risks with a residual score of "Medium" or "High" as identified in the residual risk assessment (see **Figure 4** above).

Risk Category	Risk Scenario	Controls & Measures in place	Additional Measures in the process of being implemented and/or to be implemented
Gender-Based Violence	Dissemination of harmful stereotypes contributing to gender inequality	<ul style="list-style-type: none"> - TOS prohibitions - Several mechanisms to identify and prevent the distribution of harmful or illegal content, including (i) algorithmic content verification systems such as the Hive classification system and (ii) digital fingerprinting for known illegal material, as well as (iii) trained team of content moderators' reviewing flagged content and consequent removal of any material that violates the TOS, and (iv) mechanisms for user reporting of inappropriate content facilitate closer monitoring- - Ongoing in-depth review of studies and research papers on the impact of violent content (gender-based violence, non-consensual sexual act, physical aggression etc.) 	<ul style="list-style-type: none"> - Networking with experts and NGOs focusing on the health and social impacts of adult content
Protection of Minors	Minors access explicit adult content	<ul style="list-style-type: none"> - Warnings about adult content - Self-validation - Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) - RTA label - Terms of Service - Point 3 - Child content - Parental controls direct link to instructions security measures and parental controls setup including deployment of filters - Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy 	<ul style="list-style-type: none"> - Continue to closely monitor the latest developments in the field of prevention of minors' access to adult platforms (including consultations, legislative initiatives, best practices in the sector) and actively participate to dialogue with a view to contribute to the discussion in order to achieve an acceptable, sufficient balance between effective protection of minors and the fundamental freedoms and rights and safety of all; - Support the development and raising awareness of effective methods, such as those integrated into the operating system of individual devices; - Collaboration with NGOs and experts on online protection of minors;

rights as well as the safety of all users

Protection of Minors	Minors bypass age verification systems by using fake identities, or sharing adult credentials	<ul style="list-style-type: none"> - Warnings about adult content - Self-validation - Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) - RTA label - Terms of Service - Point 3 - Child content - Parental controls direct link to instructions security measures and parental controls setup including deployment of filters - Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users 	<ul style="list-style-type: none"> - Continue to closely monitor the latest developments in the field of prevention of minors' access to adult platforms (including consultations, legislative initiatives, best practices in the sector) and actively participate to dialogue with a view to contribute to the discussion in order to achieve an acceptable, sufficient balance between effective protection of minors and the fundamental freedoms and rights and safety of all; - Support the development and raising awareness of effective methods, such as those integrated into the operating system of individual devices; - Collaboration with NGOs and experts on online protection of minors;
Protection of Minors	Minors bypass age verification systems by using third-party software or techniques (such as VPNs or proxy servers)	<ul style="list-style-type: none"> - Warnings about adult content - Self-validation - Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) - RTA label - Terms of Service - Point 3 - Child content - Parental controls direct link to instructions security measures and parental controls setup including deployment of filters - Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users 	<ul style="list-style-type: none"> - Continue to closely monitor the latest developments in the field of prevention of minors' access to adult platforms (including consultations, legislative initiatives, best practices in the sector) and actively participate to dialogue with a view to contribute to the discussion in order to achieve an acceptable, sufficient balance between effective protection of minors and the fundamental freedoms and rights and safety of all; - Support the development and raising awareness of effective methods, such as those integrated into the operating system of individual devices; - Collaboration with NGOs and experts on online protection of minors;
Protection of Minors	Distribution of content with prohibited material (e.g., violent or exploitative content involving minors)	<ul style="list-style-type: none"> - TOS prohibitions - Deployment of technology and human moderations such as: - internal fingerprint check 	<ul style="list-style-type: none"> - Internal audit of content moderation processes and procedures in 1Q 2025

- hive classification (violence, weapons)
- user reports and moderation team
- user account verification procedure
- -Cooperation with law enforcement agencies to fight the distribution of any such content
- In-depth review of studies and research papers on the impact of dissemination of CSAM

Protection of Minors	Exposure to adult content may negatively affect minors' physical and mental health, potentially fostering addiction or unhealthy attitudes	<ul style="list-style-type: none"> - Warnings about adult content - Self-validation - Providing guidelines and on-line support for guardians and parents for protection of minors (sub-site dedicated to awareness and caution) - RTA label - Terms of Service - Point 3 - Child content - Parental controls direct link to instructions security measures and parental controls setup including deployment of filters - Ongoing in-depth assessment of additional measures such as device level age verifications tools that allow to preserve the fundamental freedoms and privacy rights as well as the safety of all users - In-depth review of studies and research papers on the impact of adult content 	<ul style="list-style-type: none"> - Closely monitor the latest developments in the field of prevention of minors' access to adult platforms (including consultations, legislative initiatives, best practices in the sector) and actively participate to dialogue with a view to contribute to the discussion in order to achieve an acceptable, sufficient balance between effective protection of minors and the fundamental freedoms and rights and safety of all; - Support the development and raising awareness of effective methods, such as those integrated into the operating system of individual devices; - Collaboration with NGOs and experts on online protection of minors;
Public Health	Content promoting unprotected sex or risky behaviours without disclaimers	<ul style="list-style-type: none"> - Co-operation with NGO – OffLimits - In-depth review of studies and research papers on the impact of adult content on the public health 	<ul style="list-style-type: none"> - Networking with experts and NGOs focusing on the health and social impacts of adult content
Public Health	Content promoting unrealistic or unhealthy body standards	<ul style="list-style-type: none"> - Co-operation with NGO - OffLimits - In-depth review of studies and research papers on the impact of adult content on the public health 	<ul style="list-style-type: none"> - Networking with experts and NGOs focusing on the health and social impacts of adult content
Public Health	Content that may encourage self-harm or unhealthy lifestyles	<ul style="list-style-type: none"> - Co-operation with NGO - Offlimits - In-depth review of studies and research papers on the impact of adult content on public health 	<ul style="list-style-type: none"> - Networking with experts and NGOs focusing on the health and social impacts of adult content

- user reports and moderation team (self-harm)

Transparency and Reporting Obligations	The platform inaccurately reports the average monthly number of active recipients of the service	- Use of an acceptable calculation methodology based on available data and common practice	- Develop a standardized methodology for counting users based on available data and resources, which is supported by regulators and incorporates input from public discussions and regulatory consultations
Transparency and Reporting Obligations	Inadequate disclosure of algorithmic decision-making processes	<ul style="list-style-type: none"> - Compliance Officer nomination - Resources allocated to secure compliance with DSA requirements - Process/procedural changes and updates to reflect DSA requirements - Algorithmic definitions and application subject to regular Compliance audits - Close internal cooperation in case of any changes with algorithms should they become more complex (currently basic - see above) 	<ul style="list-style-type: none"> - Continued implementation of Compliance Management System focusing on DSA and other regulations - External audit of CMS in 2025 - Performance of compliance audits 1H 2025
Transparency and Reporting Obligations	Non-compliance with regulatory requests for platform data	<ul style="list-style-type: none"> - Compliance Officer nomination - Resources allocated to secure compliance with DSA requirements - Process/procedural changes and updates to reflect DSA requirements - Maintenance of required databases - Regular reporting to Authorities in the required form and structure 	<ul style="list-style-type: none"> - Continued implementation of Compliance Management System focusing on DSA and other regulations - External audit of CMS in 2025 - Performance of compliance audits 1H 2025