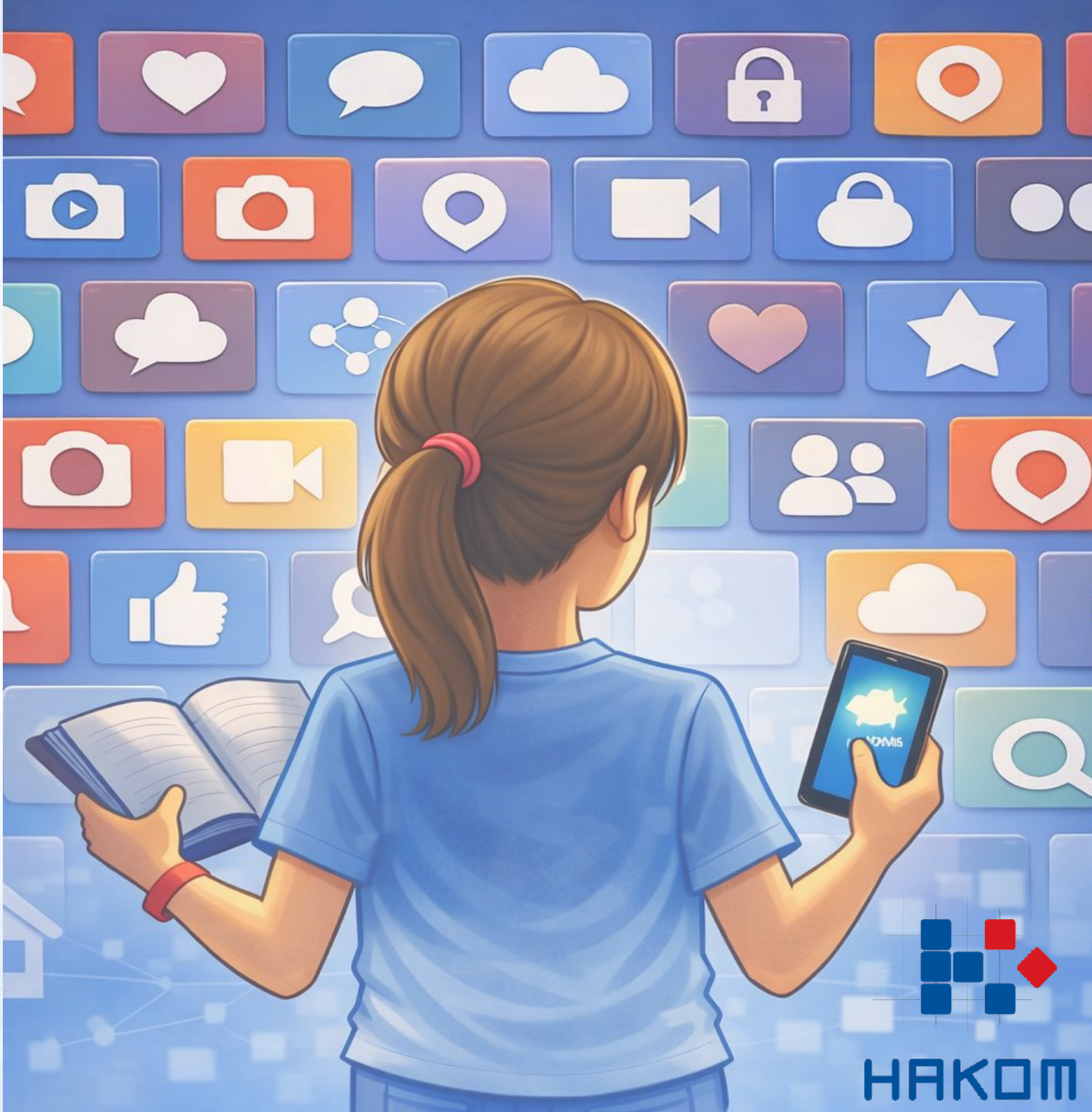
GUIDE FOR PROVIDERS OF ONLINE PLATFORMS: obligations, risks and recommended measures

Protection of minors
under the Digital Services Act

HAKOM

INTRODUCTION

Regulation (EU) 2022/2065 on a Single Market for Digital Services (hereinafter: Digital Services Act or DSA) establishes a harmonised set of rules for providers of intermediary services in the European Union, including **specific obligations for online platforms to protect users and fundamental rights, particularly where services are accessible to children and minors**[2]. The DSA requires online platforms accessible to minors to put in place **appropriate and proportionate measures** to ensure **a high level of privacy, safety and security of minors**, including by adapting their content moderation, advertising and recommender systems.



The DSA applies without prejudice to Regulation (EU) 2016/679 on the protection of personal data (hereinafter: GDPR)[3] and the Directive on privacy and electronic communications (*e-Privacy*)[4], and is not a *lex specialis* derogating from them. Whenever compliance with DSA obligations relies on the processing of personal data, all GDPR requirements must be satisfied (legal basis, data minimisation, transparency, security, data subject rights, etc.).

To facilitate compliance with DSA obligations by online platforms established in the Republic of Croatia, **HAKOM**, in its capacity as the **Digital Services Coordinator** (DSC), has prepared this **Guide to obligations, risks and recommended measures** (hereinafter: the "Guide") for the prevention of risks related to harmful/illegal content, excessive use and addictive patterns, commercial exploitation, and risks to privacy and data security.

The Guide is **intended primarily for providers of online platforms whose services are accessible to minors**, irrespective of whether those services are directed exclusively at minors or are also used by the wider population. The Guide focuses on the protection of minors and does not elaborate on other DSA obligations not directly connected with that topic, including systemic risks unrelated to minors. This Guide is substantively linked to the measure proposed by HAKOM in the draft National Programme for Children and Young People in the Digital Environment for the period 2024 to 2026, and is also aligned with OECD recommendations on the protection of children in the digital environment. For transparency reasons, the Guide also sets out the obligations of very large online platforms (VLOPs)[5], even though such providers are currently not present in the Republic of Croatia.

1 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)
2 In this Guide, the terms "minor" and "child" mean persons under 18 years of age
3 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
4 DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
5 Very large online platform (VLOP)

This Guide covers key provisions of the DSA and the related European Commission Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065[6] (hereinafter: the Commission Guidelines), and contains practical steps that service providers can take independently to identify and mitigate risks to minors, improve transparency and increase the safety of the services they provide. It is important to stress that the Commission Guidelines assist in the application of Article 28(1) DSA and that following them may indicate compliance, but does not exclude the platform's obligation, on the basis of its own risk assessment, to take additional or different measures where necessary.

Pursuant to Article 7 of the Act on the Implementation of Regulation (EU) 2022/2065 (Official Gazette No 67/2025), **the competent authority for the application of Article 27** (Recommender system transparency) **and Article 28** (Online protection of minors) DSA is the **Croatian Personal Data Protection Agency** (AZOP)[7].

When implementing the recommended measures, due account should be taken of the **fundamental rights of children** under the Charter of Fundamental Rights of the European Union[8] (hereinafter: the Charter), including the right to respect for private and family life, protection of personal data and the rights of the child (Articles 7, 8 and 24 of the Charter).

DISCLAIMER
This document is for information and guidance purposes only and must not be interpreted as a legally binding act of HAKOM or as a substitute for the official interpretation or application of the DSA or other binding rules by the competent authorities. Providers of intermediary services are required to assess their own compliance with all applicable rules and, where necessary, seek expert legal advice.

6 Communication from the Commission - Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, adopted on 14 July 2025 and published in the Official Journal of the European Union on 10 October 2025
7 https://azop.hr/
8 Charter of Fundamental Rights of the European Union (2016/C 202/02)

Obligations, Risks and Recommended Measures for Providers of Online Platforms

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Online protection of minors **Art. 28(1)**	**Online platforms accessible to minors** *Exemption[9]: micro and small enterprises[10], unless they are VLOPs/VLOSEs (Art. 19).*	Put in place **appropriate and proportionate measures** to ensure a **high level of privacy, safety and security** of minors on their service. Note: a service is "accessible to minors"[11] where it is directed at minors, predominantly used by minors, or the provider is otherwise aware that some recipients of the service are minors.	**Reset the feed** and **reduce autoplay** and **infinite scroll** for child accounts as proportionate well-being measures; offer simple user settings, e.g. "Pause autoplay" and "Limit infinite scroll". **Commission Guidelines - recommended practices** ***Default "highest protection" settings*** • minors' profiles set to private • geolocation hidden/disabled by default • prevent downloading or taking screenshots of content posted by minors (where applicable) *Communications and groups* • one-step block/mute for minors • prevent adding minors to groups without explicit consent *Moderation and notices* • reporting tools adapted to minors • quick feedback on notice status and escalation • basic parental tools where relevant

9 The exemption for micro and small enterprises also applies during the 12-month period following the loss of that status, unless the provider has been designated as a VLOP (very large online platform) or a VLOSE (very large online search engine).
10 Micro and small enterprises as defined in Recommendation 2003/361/EC
11 Recital 71 DSA

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Online protection of minors **Art. 28(2)**	**Online platforms** *Exemption: micro and small enterprises[12], unless they are VLOPs/VLOSEs (Art. 19).*	**Prohibition on presenting advertisements on the interface based on profiling[13]** when the provider is **aware with reasonable certainty** that the recipient of the service (user) is a minor.	Examples of indicators that may contribute to reasonable certainty, depending on the context: • the user has entered their date of birth / age themselves, in combination with other relevant signals • the account was created through a "teen" onboarding flow • the platform activated "teen protections" on the basis of age estimation • parental controls / a family account identify the user as a minor **Example of ad transparency in relation to minors:** each advertisement clearly states who pays for it and why it is shown. **Commission Guidelines - recommended practices** *No profiled ads* • use contextual advertisements and clearly label them "Advertisement" *Commercial practices* • do not exploit children's lack of commercial literacy • introduce safeguards against inadvertent spending (e.g. in games - in-game currencies / loot boxes) and clear information on price and the consequences of purchase

12 See footnote 9.

13 As defined in Article 4(4) of Regulation (EU) 2016/679 (GDPR): "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling (in the context of Art. 28(2) DSA): personalisation based on monitoring and assessing the user's behaviour or preferences.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Online protection of minors **Art. 28(3)**	**Online platforms**	Compliance with Article 28 **does not oblige providers of online platforms to process additional personal data** in order to assess whether the recipient of the service is a minor.	The collection of additional data for age determination is not encouraged. When determining age, measures should be proportionate and aimed at protecting minors, while preserving privacy. The use of age assurance solutions that are accurate, reliable, robust, non-intrusive and non-discriminatory is recommended, together with clear information to the user/parent on how they work and what their effects are. **Commission Guidelines - recommended practices** • age estimation and age verification only where necessary (e.g. 18+ content such as pornography/gambling, or where required by national law) • when determining age, prefer device-based / on-device methods and approaches based on the EU Digital Identity Wallet (*EUDI Wallet*), with local on-device processing and anonymised tokens. At the same time, avoid storing additional personal data from the age assurance process, including biometric data, other than information on the user's age group • clearly explain to the user/parent how the solution works and what its effects are

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Online protection of minors **Art. 28(4)**	**Online platforms**	Take into account the European Commission Guidelines to support the implementation of Article 28(1).	The Commission Guidelines elaborate on Art. 28(1) DSA through thematic groups of measures (e.g. default privacy settings, recommender systems and feed management, communications and groups, design that encourages excessive use, commercial practices, moderation/notices and age assurance). Recommended practices from the Commission Guidelines and operational examples of implementation are included in column 4 of the table next to the relevant DSA provisions. **The Commission Guidelines were published in the Official Journal[14] of the EU on 10.10.2025.**
Risk assessment and mitigation of risks **Arts. 34 and 35**	**VLOP/VLOSE**	Platforms shall **conduct a systemic risk assessment at least once a year** and before introducing functionalities that may significantly affect those risks, such as a new recommender system, autoplay, or a generative AI smart assistant/chatbot, with the assessment being service-specific and proportionate to the risks.	Carry out testing and adaptation of algorithmic systems / recommender systems and advertising systems.

14 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202505519

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Risk assessment and mitigation of risks **Arts. 34 and 35 (continued)**	**VLOP/VLOSE**	→ The assessment includes analysis of whether, and in what way, intentional manipulation of the service and inauthentic use (e.g. coordinated behaviour, automated accounts) affect the identified risks, including effects on minors and the regional and linguistic specificities of those risks.	In practice, the risk assessment takes the following into account: **Intentional manipulation of the service:** attempts to systematically "game" the platform (e.g. coordinated campaigns, artificial suppression or "promotion" of certain topics). **Inauthentic use:** the use of automated accounts (bots), fake profiles, inauthentic engagement farming, coordinated networks of profiles, etc. **Effects on minors:** how such manipulation and inauthentic networks can increase risks for minors (e.g. heightened exposure to harmful narratives, grooming through fake profiles, coordinated harassment/cyberbullying, encouragement of risky challenges). **Regional and linguistic specificities:** the assessment must take account of language-specific features because patterns of abuse and risks differ by language, local context and market (moderation, bot detection, recommendations, advertising ecosystem).

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Risk assessment and mitigation of risks **Arts. 34 and 35 (continued)**	**VLOP/VLOSE**		**Operational examples of implementation** *Governance* • appoint a Child Safety Lead • introduce CIRA (*Critical Information Risk Assessment*) / DPIA (*Data Protection Impact Assessment*) workflows into product development • conduct periodic reviews of features affecting well-being (e.g. feed, notifications, autoplay, chatbots) *Measurement* • define key performance indicators (*KPIs*), e.g. time for removing high-risk content, share of child accounts with maximum protections, share of non-profiled recommendations/ads, number of unwanted contacts prevented, break metrics and DND (*Do Not Disturb / Do Not Display*) • connect KPIs and mitigations with annual systemic risk assessments and risk-mitigation measures, and take into account the findings of annual DSA reports on risks and best practices.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Risk assessment **Art. 34**	**VLOP/VLOSE**	**Platforms shall analyse in particular:** → whether the design of the app (e.g. infinite scroll, notifications, recommender algorithms) may adversely affect minors → whether minors are exposed to illegal and/or harmful content (e.g. violence, hate speech, pornographic content, disinformation, addictive content) → whether there is a risk of interference with privacy, misuse of personal data or advertising based on profiling directed at minors (e.g. excessive tracking, inappropriate processing of children's data, location tracking) → the effects on public health, minors, and serious negative consequences for the physical and mental well-being of minors **Platforms must examine in particular the impact of:** → their recommender algorithms (what children see, how long they stay on the platform, spiral recommendation of sensitive topics) → **content moderation** (SLA[15] timeframes for removal of illegal and/or harmful content) → **advertisements** (whether they are shown to children and whether they are appropriate)	Example: if the algorithm recommends content that encourages self-harm, extreme dieting or violence, this constitutes a serious systemic risk that the platform must mitigate (and, where applicable, also remove the content in accordance with its moderation rules and risk assessment). Note: presenting advertisements to minors based on profiling is prohibited where the provider is aware with reasonable certainty that the user is a minor (Art. 28(2) DSA). Measures to protect minors should ensure a high level of privacy; geolocation and behavioural tracking present heightened risks and should therefore be limited and disabled by default where possible (Art. 28(1) DSA; Commission Guidelines - risk-based approach). Example: rabbit-hole effects, sleep disruption/loneliness, encouragement of risky challenges, gender-based violence and cyberbullying.

15 Service Level Agreement

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Risk assessment **Art. 34 (continued)**	**VLOP/VLOSE**	→ **the way data are collected and used** (e.g. monitoring minors' behaviour, data retention periods) → **the applicable terms and conditions and their enforcement** (whether the content of the terms and conditions and their enforcement negatively affect minors and their rights) → **interface design** (whether it may encourage addictive behaviour or peer pressure) **Platforms must in particular consider the effects on:** → **Art. 24** (rights of the child) of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter) → **Art. 7** (respect for private and family life) and **Art. 8** (protection of personal data) of the Charter **Accountability and supervision** Platforms must preserve supporting documents relating to risk assessments for at least 3 years after the assessments have been carried out. The European Commission and the Digital Services Coordinators of the Member States may request documents relating to the assessments and verify whether measures for the protection of children have actually been implemented.	It is not enough for terms and conditions merely to be legally correct; they must also be explained in language understandable to children and minors. If minors do not understand the rules and their consequences, that may increase risks. The systemic risk assessment also covers effects on fundamental rights, including the rights of the child, privacy and protection of personal data, and the physical and mental well-being of minors, in accordance with Art. 34 DSA. → A child has the right to such protection and care as is necessary for their well-being. In all actions relating to children, the child's best interests must be a primary consideration → Platforms must consider the effects on the rights to privacy and confidentiality of communications, as well as the right to the protection of personal data, including risks arising from the excessive collection, use or sharing of children's data, particularly in the absence of a lawful basis and appropriate safeguards. Mitigation of identified risks is carried out under Art. 35 DSA.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Mitigation of risks **Art. 35**	**VLOP/VLOSE**	**Put in place reasonable, proportionate and effective measures to mitigate identified risks,** tailored to the specific systemic risks identified in the assessment under Art. 34 DSA, with particular consideration for the impact of those measures on fundamental rights.	Example: compile a risk/measure list risk: excessive time spent by minors on the platform; measure: switch off autoplay for child accounts, introduce a **break reminder** after 20 minutes and a quiet night mode from 22:00 to 7:00.
		→ **adapt the design, features or functions of the service, including online interfaces**	Example: set a private profile for minors by default; hide precise location; limit infinite scroll; reduce gamification; add an "**Are you sure?**" message before public sharing; **prohibit downloading or taking screenshots** of content posted by minors in order to prevent the unwanted distribution of sexualised or intimate content and sextortion; and set minimum requirements for parental control tools. Prohibit **adding minors to groups without explicit consent**; limit the visibility of children's profiles; give minors greater control over their own feeds and empower them to block and/or mute any user.
		→ **define the terms and conditions and ensure their enforcement**	
		→ **strengthen moderation and the response to notices**	Example: set an **SLA** - highly harmful content is removed **on average in < 24 h**; a 24/7 emergency contact point; a **Report/Block button** visible in every post/message; and allow the use of the Croatian language.
		→ **adapt algorithms (e.g. recommender systems)**	When changing an algorithm, carry out an **A/B test**[16] and check the impact on minors (e.g. time spent, exposure to risky topics).

16 An A/B test (split test) is a method of comparing two versions (A and B) of a website, advertisement or email in order to determine which performs better.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Mitigation of risks **Art. 35 (continued)**	**VLOP/VLOSE**	→ **adapt the advertising system**	**No profiled ads for minors; allow only contextual ads; block risky categories** (alcohol, gambling, "crash diets", etc.). **Example of age-appropriate explanation:** "Why am I seeing this ad?" and limit frequency (*frequency cap*). **Disable by default** features that contribute to excessive use, such as streaks, disappearing content, read receipts, autoplay or push notifications; remove **manipulative/persuasive design** elements aimed primarily at engagement; and introduce **safeguards around AI** smart assistants **(chatbots)** integrated into platforms. **Ensure that the lack of commercial literacy of minors is not exploited** and that they are not exposed to commercial practices that may be manipulative, lead to unwanted expenditure or addictive behaviour, including the use of certain **virtual currency** or loot boxes.
		→ **strengthen internal processes and resources**	Appoint a **person responsible for child protection**; review, on a quarterly basis, designs affecting children; maintain an **evidence log** - what was done and why; and designate emergency contacts.
		→ **cooperate with trusted flaggers and certified out-of-court dispute settlement bodies** (*ODS*)	Agree a **priority channel** with trusted flaggers and, where applicable and where accepted/contracted, implement the outcomes of ODS proceedings without delay.

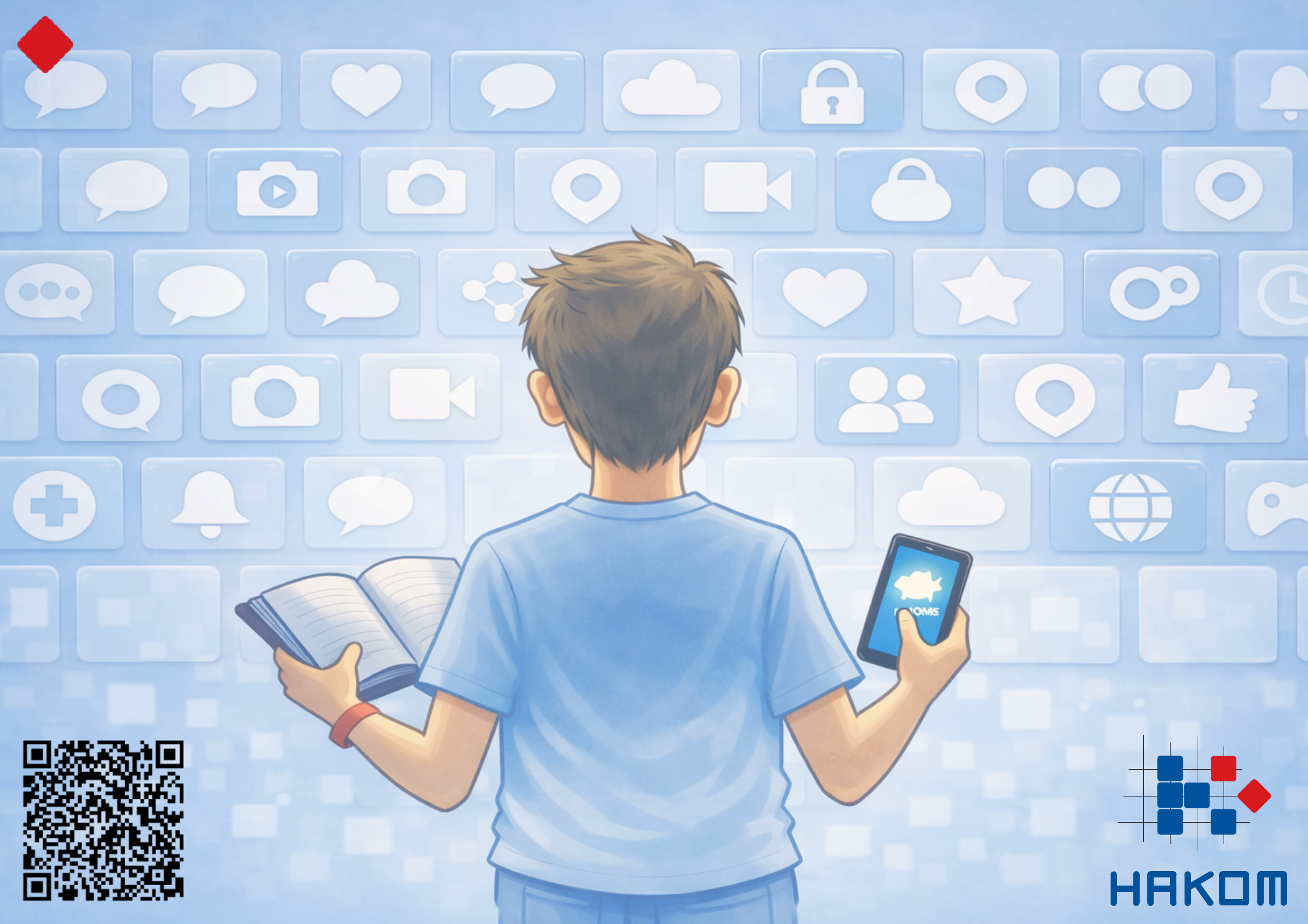
DSA provision	Type of provider	Prescribed obligations	Recommended measures
Mitigation of risks **Art. 35 (continued)**	**VLOP/VLOSE**	→ **initiate or adjust cooperation with other providers through codes of conduct and crisis protocols**	Where appropriate, participate in the drafting of **codes of conduct** and comply with them and, where applicable, also participate in relevant crisis protocols. Establish an **internal plan for rapid response** to trends encouraging dangerous challenges among children - e.g. a weight-loss challenge.
		→ **better informing users through the interface**	Introduce an in-app **safety centre** (FAQ for children/parents), **"Why am I seeing this"** next to recommendations/ads, **timers/break reminders** and easily accessible help numbers/helplines.
		→ **special measures for minors**	Apply proportionate **age assurance** measures without accumulating data; ensure **parental tools** (*family pairing*); introduce a simple **panic/report** feature in chat and quick links to assistance. For communications and groups, build block/mute/report into communication flows; prevent being added to groups without consent; and limit contact from unknown users.
		→ **labelling AI-generated/manipulated content ("deepfakes")**	Require creators to label AI content; add a visible label and allow users to **report** suspicious content easily; consider automatic **watermarking**.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Mitigation of risks **Art. 35 (continued)**	**VLOP/VLOSE**		**Check the annual reports** under Art. 35(2) DSA, **published by the European Board for Digital Services in cooperation with the Commission,** and compare them with your own risk assessments, transparency reports and existing measures **(mini gap analysis)**; where improvements are needed, apply good practices, for example by adding new measures and timelines. If the Commission issues new guidelines, **implement the recommended steps without delay** and add them to your "risk -> measure" list. **Follow recommendations of other EU bodies and "best practices".**
Recommender system transparency **Arts. 27 and 38**	Art. 27 **Online platforms that use recommender systems** *Exemption: micro and small enterprises, unless they are VLOPs/VLOSEs (Art. 19)* Art. 38 **VLOP/VLOSE**	Recommender systems (for all online platforms that use them) → in the terms and conditions, set out in clear and intelligible language the main parameters of the recommender systems and the options through which users can modify or influence those main parameters	It is desirable to consult minors, guardians and experts when testing/adapting recommender systems. The main parameters must explain why something is suggested and must include at least: (a) the criteria that are most significant and (b) the reasons for their relative importance. **Parental PIN / locking of settings.** Allow the choice of recommender system to be locked and personalisation to be switched off, without introducing additional processing of personal data solely for age purposes.

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Recommender system transparency **Arts. 27 and 38 (continued)**	Art. 27 **Online platforms that use recommender systems** *Exemption: micro and small enterprises, unless they are VLOPs/VLOSEs (Art. 19)* Art. 38 **VLOP/VLOSE**	→ where several ranking options exist (e.g. chronological/personalised), ensure a function that allows the user to choose and change the option at any time, directly and easily accessible where content is prioritised (e.g. in the feed itself) → only for VLOPs/VLOSEs - provide at least one option for each of their recommender systems that is not based on profiling as defined in Art. 4(4) of Regulation (EU) 2016/679[17]	In the feed itself, offer a clear toggle: **Chronological / Non-profiled / Personalised** + a short explanation (one tap to change the feed). **Default for minors: a non-profiled feed, where appropriate in light of the risk assessment and the design of the service.** For accounts where there is reasonable certainty that the users are minors, the default option should be **non-profiled**, while still allowing it to be changed.
Online interface design and organisation **Art. 25**	**Online platforms** *Exemption: micro and small enterprises, unless they are VLOPs/VLOSEs (Art. 19).*	**Deceptive or manipulative patterns** are prohibited where they materially distort or impair recipients' ability to make free and informed decisions. → Such practice[18] includes, inter alia: • unfair design choices that steer the recipient towards actions that benefit the provider of the online platform and may not be in the recipient's interest • presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory or other elements when the recipient of the service is asked to make a decision	No **"dark patterns"**. Options (especially the non-profiled option) must be presented with **equal prominence**. While the non-profiled option is active, do not use signals collected in that mode for future profiled recommendations, unless there is a separate clear legal basis and an informed user choice. For minors, by default reduce incentives for excessive use such as streaks, read receipts, ephemeral content and aggressive notifications, and offer simple controls such as breaks and a Do Not Disturb (DND) / nighttime window.

17 Article 4(4) GDPR: "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
18 Recital 67 DSA

DSA provision	Type of provider	Prescribed obligations	Recommended measures
Online interface design and organisation **Art. 25 (continued)**	**Online platforms** *Exemption: micro and small enterprises, unless they are VLOPs/VLOSEs (Art. 19).*		Minors face risks arising from excessive use of online platforms, including in the context of gambling and video games. The integration of chatbots into online platforms may further exacerbate existing risks and create new risks that may negatively affect minors' privacy, safety and protection. It is recommended that elements of privacy, safety and protection of minors be built into the design of products and services from the development phase onwards, e.g. by designing services in a way that is consistent with minors' developmental, cognitive and emotional needs. Carry out a periodic analysis of interface design at least once a year, or whenever there is a significant change in design, or when it becomes known that the design affects other relevant circumstances (rights of minors, level of risk, safety or privacy).
Additional online advertising transparency **Art. 39**	**VLOP/VLOSE** displaying advertisements	An advertisement repository is mandatory for VLOPs/VLOSEs that display advertisements.	Ensure advertising transparency and, where applicable, set up and maintain an advertisement repository containing the relevant information.
Standards and codes of conduct **Arts. 44 and 45**	Relevant service providers and other stakeholders at Union level; particularly relevant for VLOPs/VLOSEs in the context of risk management	Standards and codes of conduct are voluntary instruments supporting the proper application of DSA obligations.	Where appropriate, participate in the development of standards and codes of conduct **addressing the protection of minors**, especially in relation to age verification, interface design and protection against profiling in advertising. Monitor and, where appropriate, apply relevant standards and codes of conduct related to the protection of minors.


HAKOM