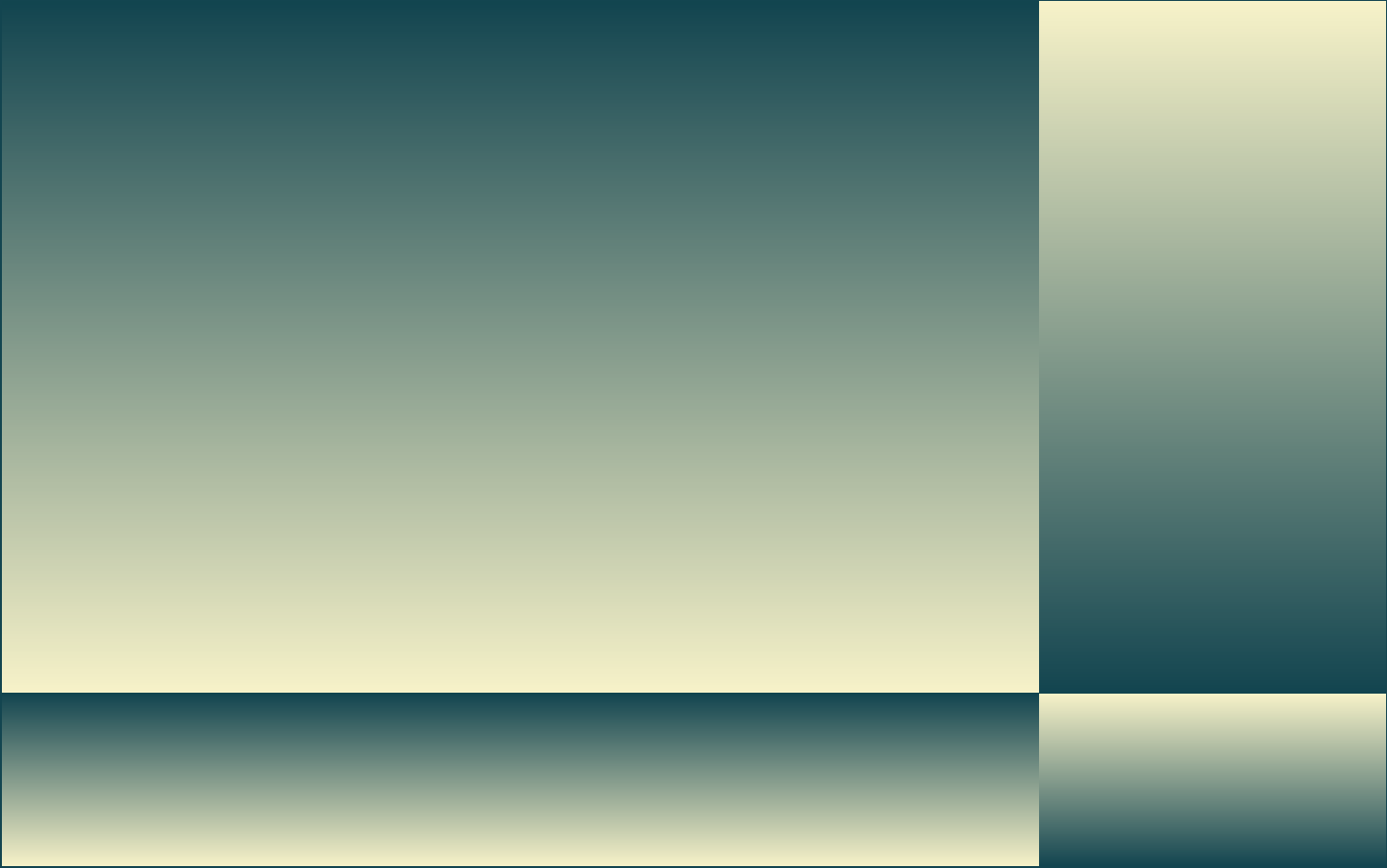




POLICY BRIEF

Different Risks, Different Rules?

The Case of ChatGPT under the DSA and the AI Act

Lena-Maria Böswald

October 01, 2026

Table of Contents

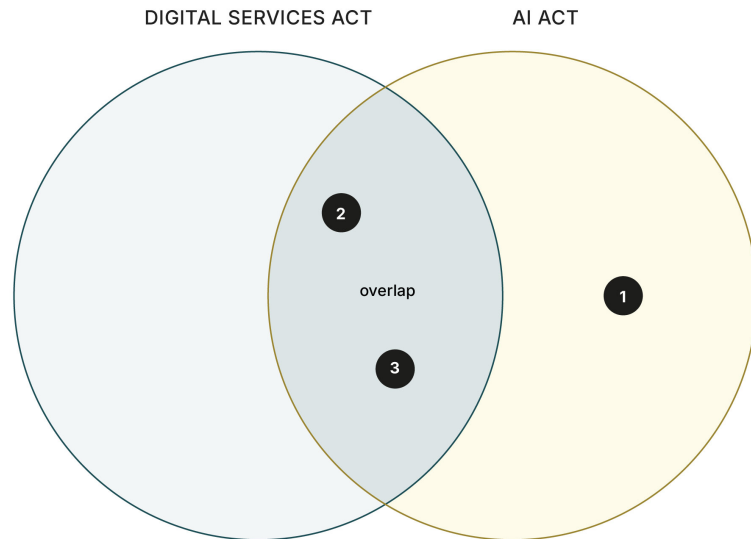
1. Executive Summary	3
2. Introduction	5
3. The Objects and Actors of Regulation	7
3.1. Model Layer: General Purpose Artificial Intelligence (GPAI)	8
3.2. AI Systems	8
3.3. Online Services	9
4. The Regulatory Landscape: How the EU AI Act and DSA Cover Generative AI	9
4.1. The EU AI Act	10
4.2. The Digital Services Act	11
5. Overlaps: How the DSA and AI Act Intersect	15
5.1. Systemic Risk Requirements	16
5.2. Transparency and Labelling	24
6. What's the EU's Current Enforcement Architecture for AI Services?	25
7. Conclusion: How To Move Forward	28
8. Acknowledgments	29

Executive Summary

In August 2026, the European Commission designated ChatGPT as a Very Large Online Search Engine (VLOSE) under the Digital Services Act (DSA). The designation marks a turning point for EU oversight of generative AI: a service that retrieves web information and generates conversational answers can now be examined under the DSA's framework, even though it does not resemble a conventional search engine. The central question is therefore no longer simply whether the DSA can cover generative AI, but how responsibility should be allocated between the DSA's service-level risk-management regime and the Artificial Intelligence (AI) Act's model- and system-level obligations.

This paper argues that the DSA is the primary framework for risks arising from ChatGPT's design, functioning and use, including risks to fundamental rights, electoral processes, minors, public health and civic discourse. What the DSA does not regulate, however, is how AI models are built or trained. It also does not directly impose obligations on AI developers. Thus, the AI Act remains necessary for model-level obligations that extend beyond the designated service, including high-impact capabilities, cross-deployment harms, and transparency duties concerning AI-generated or -manipulated content.

Generative AI between two laws: where the DSA and the AI Act overlap



1 Standalone generative AI tool
→ AI Act compliance
DSA unlikely to apply

2 Embedded in a platform or search service
→ Mostly DSA compliance
AI Act still applies to the system itself

3 ChatGPT designated as a VLOSE
→ Clearest case of real overlap
Strictest DSA regime plus AI Act for the model

Two findings follow from this distinction:

- **A VLOSE designation expands service-level accountability, not model regulation.** A DSA assessment can examine how ChatGPT operates as a VLOSE, but it does not replace scrutiny of model capabilities.
- **The regimes can enable one another without being interchangeable.** Where a VLOP or VLOSE integrates a generative-AI model, the model provider's AI Act documentation should not be treated as a substitute for the platform's Art. 34 DSA assessment. It can, however, provide part of the evidential basis for that assessment. When it comes to labelling AI-generated content, this logic is reversed: it naturally helps to know which standards the underlying AI model uses under the AI Act to achieve greater transparency at the service level of the DSA.

The VLOSE designation does not resolve all risk and safety questions. Important gaps remain around how risks should be divided between the two regimes, as well as broader risks such as persistent, personalised persuasion and the environmental impacts of generative AI. The principal remaining gap is institutional: without an integrated procedure, the European Commission's DSA enforcement team and the EU AI Office risk assessing overlapping evidence under different legal mandates.

ChatGPT's designation as a VLOSE shows that existing EU rules can address the evolving risks of generative AI. But the effectiveness of these rules depends on more than bringing a new service within an established category. To make the framework effective in practice, this paper recommends that the European Commission's DSA enforcement team and the AI Office:

- **Connect risk assessments** across the DSA and AI Act by tracing how model limitations become risks in a particular service.
- **Develop a shared risk matrix** that distinguishes AI-model, AI-system and service-level causes, evidence and mitigation measures.
- **Use recurring DSA risk findings** to identify when harms appearing across large services warrant closer model-level scrutiny.
- **Transpose learnings for AI systems below the VLOP/VLOSE threshold** for significant model-related risks.

Introduction

Generative Artificial Intelligence (generative AI), a type of artificial intelligence (AI) system that is capable of generating text, images or audio-visual material in response to prompts, is not only reshaping how content is produced and distributed online. It is also challenging established categories of EU platform regulation. While the [Artificial Intelligence Act](#) (AI Act)¹ provides a comprehensive regulatory framework for AI systems, including generative AI, the challenge of fitting generative AI into existing regulatory categories is particularly apparent under the [Digital Services Act](#) (DSA)², which regulates intermediary services across the EU to protect users' fundamental rights online. The DSA and the AI Act each attach obligations to different regulatory objects and actors.

The DSA regulates intermediary services through categories such as online platforms and online search engines, with those large in size and impact declared as Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs).³ These categories are premised on relatively distinct functions: platforms host and disseminate user-generated content, while search engines index and retrieve third-party information. Generative AI systems such as ChatGPT, however, create new content nudged by user prompts and

1 European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)", *Official Journal of the European Union* L 2024/1689, 13 June 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

2 European Parliament and Council of the European Union, "Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)", *Official Journal of the European Union* L 2022/277, 27 October 2022, <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>.

3 For intermediary services to fall under Very Large Online Platforms (VLOPs) or Very Large Online Search Engines (VLOSEs) under the DSA, they need to exceed a 45 million-monthly active user threshold.

combine functions that do not fit neatly within this distinction. The addition of live web search to AI systems such as ChatGPT lets them perform the functions of an online search engine, though, raising the question of how the DSA applies when a generative AI service clearly resembles and is used as online search.

In the case of ChatGPT, this question became increasingly pressing as its search functionality expanded and its user base grew. In August 2026, the European Commission provided its first concrete answer by designating ChatGPT as a Very Large Online Search Engine (VLOSE). As the first multi-purpose generative AI that started the AI hype⁴ in December 2022, used by more than 159,1 million monthly EU users as of April 2026, ChatGPT was selected as a case study for this paper.

In October 2025, following OpenAI's disclosure that ChatGPT's search feature had reached an average of 120.4 million⁵ monthly users in the EU, widely surpassing the 45 million-user threshold that triggers extra obligations under the DSA. A European Commission (ECOM) spokesperson confirmed that regulators were then assessing⁶ whether ChatGPT could be designated as a Very Large Online Search Engine (VLOSE) under the DSA. On 31 August, ten months after even considering a designation, the ECOM stated in its press release accompanying the designation that "ChatGPT is a hybrid service that qualifies as an online search engine under the DSA".⁷ It is now the third VLOSE covered by the DSA regime, alongside Google and Bing. As EU technology chief Henna Virkunnen put it: "ChatGPT [...] will now be held to a higher standard of scrutiny and accountability in the European Union, in line with [...] [its] large impact on our citizens and society."⁸

Following the notification of the designation, OpenAI, as ChatGPT's provider, has four months, by January 2027, to comply with the additional DSA obligations for VLOSEs⁹, such as assessing and mitigating the systemic risks stemming from their service and algorithmic systems related to the dissemination of illegal content, the negative effects on minors, users' physical and mental well-being, fundamental rights, electoral processes (i.e., the use and the impact of information presented on elections) and public security.

What is crucial here is that OpenAI's figures relate solely to ChatGPT's search feature. While ChatGPT's predictive capabilities used to rely on the datasets used to train the

4 Roose, Kevin, "How ChatGPT Kicked Off an A.I. Arms Race," *The New York Times*, 3 February 2023, <https://www.nytimes.com/2023/02/03/technology/chatgpt-openai-artificial-intelligence.html>.

5 Kroet, Cynthia, "ChatGPT could face strictest set of EU rules as it hits 120 million users in Europe," *Euronews*, 22 October 2025, <https://www.euronews.com/2025/10/22/chatgpt-could-face-strictest-set-of-eu-rules-as-it-hits-120-million-users-in-europe>.

6 Jahangir, Ramsha, "EU weighs regulating OpenAI's ChatGPT under the DSA: What does that mean?," *Tech Policy Press*, 29 October 2025, <https://www.techpolicy.press/eu-weighs-regulating-openais-chatgpt-under-the-dsa-what-does-that-mean/>.

7 European Commission, "European Commission press release on ChatGPT's VLOSE designation," 31 August 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1772.

8 Ibid.

9 European Commission, "DSA: Very Large Online Platforms and Search Engines," *Shaping Europe's Digital Future*, <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.

underlying large language model, it has allowed users to prompt the chatbot to retrieve live information from the web since 2025. For the ECOM, the challenge¹⁰ has therefore been to determine whether ChatGPT's search functionality should be treated as a distinct service or as part of the chatbot as a whole, which cannot be singled out.

ChatGPT is not a conventional search engine: it combines the retrieval of information from the web with the generation and synthesis of content through an underlying general-purpose AI model. The ECOM's decision therefore provides an important test case for determining the reach of the DSA beyond conventional search services. In particular, it raises questions about which aspects of a hybrid generative AI service are subject to the DSA's service-level obligations and which risks remain primarily addressed through the EU's AI-specific regulatory framework. *If a generative AI service that combines retrieval and generation can qualify as an online search engine under the DSA, how far do the resulting obligations extend? Which risks fall within the DSA's service-level framework, and which are instead addressed by the AI Act?*

This paper uses ChatGPT's VLOSE designation as a case study to examine these questions. It first distinguishes the relevant regulatory objects and actors: the general-purpose AI model, the AI system, the online service, and the providers or deployers responsible for them. It then examines the implications of applying the DSA to generative AI services, including the systemic risk obligations arising from VLOSE status, before considering model-level risks that the DSA may not fully capture.

The paper argues that ChatGPT's designation shifts the central regulatory question from applicability to allocation. Effective oversight requires distinguishing between risks arising from the operation of a large online service and those associated with the underlying AI model, while ensuring coordination between the DSA and AI Act where those risks converge.

The Objects and Actors of Regulation

The regulatory treatment of generative AI depends first on identifying what, exactly, is being regulated. The term "ChatGPT" refers to at least three distinct regulatory objects: the underlying general-purpose AI model (GPT-5), the AI system that makes the model available to users (ChatGPT), or even the search function that retrieves current information from the web (ChatGPT Search). As ChatGPT is treated as a designated VLOSE, OpenAI also acts as the provider of the regulated online search service and bears

10 Lemoine, Laureline & Mathias Vermeulen, "Assessing the Extent to Which Generative Artificial Intelligence Falls Within the Scope of the EU's Digital Services Act: An Initial Analysis," SSRN, 21 February 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4702422.

the associated DSA due-diligence obligations. These are connected components of a single product environment, but they are not interchangeable legal objects.

This distinction is particularly important for ChatGPT. A response provided through ChatGPT Search may result from the interaction of a model's pre-existing capabilities, a retrieval system, source selection and ranking processes, system prompts generated by users, safety measures to prevent inappropriate content, the user's conversation history and the user's ability to query smart prompts.

Model Layer: General Purpose Artificial Intelligence (GPAI)

Under the AI Act, generative AI such as ChatGPT is primarily captured by the category of general-purpose AI models (GPAI models), capable of performing a wide range of tasks and being integrated into a variety of systems or applications. Providers of GPAI models (such as large language or image models) face baseline obligations, including technical documentation, information-sharing for downstream providers, and compliance with copyright-related transparency duties, due to their broad applicability and systemic risk potential. The AI Act considers that some GPAI models pose systemic risks (such as negative effects on democratic processes or on public and economic security) if they reach a defined level of capability or are designated GPAI models with systemic risks by the EU AI Office. GPAI models with systemic risks are subject to extra requirements, such as model evaluation, risk mitigation and incident reporting. The key regulatory question for GPAI models is to understand the model's capabilities, limitations, training-related risks and systemic risk implications.

This makes the AI Act the main EU instrument for regulating the model layer of GPAI, even if the same system may also be subject to the DSA when it is embedded in or operated through an intermediary service.

AI Systems

The model must be distinguished from the AI system built around it. An AI system, according to the AI Act, means “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”¹¹ ChatGPT, for example, can be understood as an AI

¹¹ See [AI Act Art. 3\(1\)](#).

system rather than simply the underlying model it is powered by (e.g., GPT 5.6). It presents the capabilities of GPAI through a conversational interface and combines them with product-level functionality.

Under the AI Act, the entity that develops an AI system or has it developed is generally the **provider**. An entity using an AI system under its authority in a professional context is generally a **deployer**.

Online Services

The DSA focuses on a different regulatory object: the online intermediary service. Its obligations depend not on whether a service uses AI, but on the type of service provided and the way it operates in the ecosystem of digital services. The DSA's categories include mere conduit, caching and hosting services, online platforms and online search engines. For online platforms and search engines large in size and potential impact, Very Large Online Platforms (VLOPs) and VLOSEs, additional due diligence obligations are in place that specifically focus on how a service's design, functioning and use create or amplify systemic risks. VLOPs and VLOSEs must identify, analyse, and assess systemic risks that are linked to their services and are obliged to put measures in place that mitigate these risks. This could mean adapting certain design features of their services or changing their recommender systems.

The interaction between a GPAI model, an AI system and an online service means that several actors may bear different responsibilities in relation to the same output. The same company may perform more than one role. For ChatGPT, for example, the entity operating the service – OpenAI – is the provider of the AI system and at the same time the provider of the underlying GPAI model. As of August 2026, ChatGPT is also a designated VLOSE under the DSA, covering the online service-level.

The Regulatory Landscape: How the EU AI Act and DSA Cover Generative AI

Depending on the object of regulation, different regulatory frameworks apply. The following chapter will closely look into how the AI Act treats AI systems, to what extent the DSA already covers generative AI and what ChatGPT's VLOSE status changes concretely.

The EU AI Act

The first natural regulatory route to cover generative AI is the EU AI Act, adopted in 2024. It establishes rules for AI systems and general-purpose AI models placed on the EU's internal market and classifies AI systems according to risk levels. Generally, AI systems that interact with humans (for example, AI chatbots), as well as AI systems that generate or manipulate image, audio or video content – including deepfakes – are considered 'limited risk' and are subject to a limited set of transparency obligations. The EU AI Act differentiates between two risk classes: non-systemic and systemic risk, based on whether the model has high impact capabilities – presumed where the cumulative amount of computation used for training exceeds 10^{25} floating point operations. GPAI models – the subject of analysis of this paper – are therefore divided into those with and without systemic risks.

It can be argued that generative AI already has its own systemic risk management regime, the one applicable to providers of GPAI models under the AI Act. The main point is that systemic risk management under the AI Act applies to providers and their models **before** the latter are integrated into other systems and applications downstream in the value chain. GPAI rules are exclusively supervised and enforced by the EC. Generative AI is monitored directly by the newly created European AI Office, which supervises high-impact models and enforces compliance at the EU level.

What does this mean for content created by generative AI?

Art. 50(2) AI Act requires providers of AI systems generating or manipulating synthetic content to ensure that such output is marked in a machine-readable format and detectable as artificially generated or manipulated. Accordingly, this transparency obligation is intended to ensure that all AI-generated or AI-manipulated content is marked using imperceptible methods, such as watermarking or metadata tags. At the same time, Art. 50(4) of the AI Act requires deployers who use AI to generate or manipulate deepfakes or public-interest texts to explicitly disclose their artificial origin by labelling.

In July 2026, the Commission published its Code of Practice on Transparency of AI-generated Content to support a) marking and detection of AI-generated or -manipulated content in machine-readable formats for AI providers and b) labelling of AI-generated content for deployers. It will assist deployers using deepfakes or AI-generated content to clearly disclose AI involvement, particularly on public interest matters. The code is complemented by the guidelines¹² on the scope of the transparency

12 European Commission, "Guidelines on transparency of AI-generated content," <https://digital-strategy.ec.europa.eu/en/policies/guidelines-transparency-ai-generated-content>.

obligations laid down in Art. 50 AI Act.¹³

The AI Act only provides for a limited number of remedies against the impact of harmful content produced by generative AI. Instead, it largely relies on the existence of effective pathways to redress AI-related harms in other areas of EU law, such as the DSA.

The Digital Services Act

The DSA was not envisioned as a general instrument for regulating AI, yet AI has played a huge role for VLOPs and VLOSEs in their risk assessment obligations. On 14 March 2024, the ECOM started requesting additional information from Bing and Google Search as VLOSEs and Facebook, Instagram, Snapchat, TikTok, YouTube, and X as VLOPs to provide more information on the integration of general-purpose AI into their search and recommender systems.¹⁴ Generative AI is also one of the risks identified by the Commission in its draft guidelines¹⁵ on the integrity of electoral processes.

With that in mind, the DSA is still first and foremost a central regulatory tool for holding online services accountable. However, as new technologies blur the lines between key categories such as online platforms and search engines, what qualifies as an **intermediary service** becomes more difficult to categorise. In its 2025 report on the application of Art. 33 DSA¹⁶, the designation process for VLOPs and VLOSEs, the ECOM highlighted the hybrid nature of some services by stating that 'the two legal categories of online platform and online search engines are becoming more and more intertwined'.

As such, the regulatory relevance of a generative AI service under the DSA depends on whether the service, or a sufficiently distinct functionality within it, falls within a DSA category and is subject to the corresponding level of due diligence obligations.¹⁷ Various legal analyses have concluded that self-standing generative AI applications could be covered by the DSA as intermediaries if they are considered '**online search engines**' or '**hosting services**', which include online platforms.¹⁸

¹³ Interface [contributed](#) to the consultation period for the draft guidelines.

¹⁴ European Commission, "Commission Sends Requests for Information on Generative AI Risks to Six Very Large Online Platforms and Two Very Large Online Search Engines," *Shaping Europe's Digital Future*, 14 March 2024, <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-generative-ai-risks-6-very-large-online-platforms-and-2-very>.

¹⁵ European Commission, "Commission gathering views on draft DSA guidelines on election integrity," 8 February 2024, <https://digital-strategy.ec.europa.eu/en/news/commission-gathering-views-draft-dsa-guidelines-election-integrity>.

¹⁶ European Commission, Report on the Application of Article 33 of Regulation (EU) 2022/2065, 17 November 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0708>

¹⁷ For a thorough legal analysis, please see Lemoine, Laureline & Mathias Vermeulen, "Assessing the Extent to Which Generative Artificial Intelligence Falls Within the Scope of the EU's Digital Services Act: An Initial Analysis," *SSRN*, 21 February 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4702422.

¹⁸ A 'hosting' service consists of "the storage of information provided by, and the request of, a recipient of the service" (Art. 3(iii) DSA). An online platform is an example of a hosting service.

This distinction is key for standalone AI systems such as ChatGPT: the AI system combines a conversational AI interface with web retrieval and source-based answers but commonly provides a synthesised answer rather than a ranked list of links. Many people use ChatGPT to access information online quickly. As such, even if it works differently, it is in direct competition with traditional search engines, presenting a list of results ranked by how closely they align with the key phrases in a user's query.

If we look at the broad definition¹⁹ of what constitutes a search engine under Art. 3(j) DSA, we can see that is not tied to a particular visual interface or output format: The only requirement is that a service can search the web, index the information according to the user's search request, and provide results of said search query as output, no matter if this is a list of ranked hyperlinks or a summary of information crawled online. However, a generative-search function must first fall within the DSA's intermediary service architecture before it can qualify as an online search engine. OpenAI's own transparency report²⁰ also refers to ChatGPT Search as a tool that provides real-time web information.

How Generative AI Already Falls Within the Scope of the DSA

Depending on how tools are embedded, it can be argued that embedded generative AI systems form part of a VLOP's or a VLOSE's service and their "related systems". The ECOM noted in the past²¹ that, under the DSA, a Large Language Model (LLM), could potentially be in scope of the DSA if it is integrated into a service that is designated under the DSA. An obvious case of such an integration is Bing's Copilot integration in Bing Search (previously called Bing Chat), an interactive chat feature that is part of Bing's services. As a result, Bing's DSA obligations extend to risks arising from the integrated Copilot functionality **insofar as that functionality forms part of, or is materially connected to, the designated service and its related systems**.²² The same applies to Meta AI, which is an integral part of Meta products designated as VLOPs and is not available through other interfaces.²³ Another obvious case is Grok integrated into X, another VLOP designated by the EC. Whether AI companions fall under the DSA depends on similar parameters: they must either qualify as a VLOP or VLOSE or be integrated into a designated VLOP or VLOSE. For example, Snapchat has been designated as a VLOP and has integrated the chatbot My AI into its platforms.²⁴ My AI

¹⁹ See [DSA Art. 3\(j\)](#).

²⁰ OpenAI, "Trust and transparency," <https://openai.com/de-DE/trust-and-transparency/>.

²¹ Jahangir, Ramsha, "EU weighs regulating OpenAI's ChatGPT under the DSA: What does that mean?," *Tech Policy Press*, 29 October 2025, <https://www.techpolicy.press/eu-weighs-regulating-openais-chatgpt-under-the-dsa-what-does-that-mean/>.

²² Lemoine, Laureline & Mathias Vermeulen, "Assessing the Extent to Which Generative Artificial Intelligence Falls Within the Scope of the EU's Digital Services Act: An Initial Analysis," SSRN, 9 October 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4702422.

²³ Leersen, Paddy, "Embedded GenAI on Social Media: Platform Law Meets AI law," *DSA Observatory*, 6 August 2024, <https://dsa-observatory.eu/2024/10/16/1864/>.

²⁴ 5Rights Foundation, "Snapchat under EU investigation for inadequate protection of minors," 27 March 2026, <https://5rightsfoundation.com/eu-regulators-pull-back-the-curtain-on-snapchats-inadequate-protection-of-minors/>.

falls under DSA Art. 28, a feature that is included in the EC's current investigation²⁵ against Snapchat, even though it is only accessible within the messaging service part of the platform.

AI Overviews (AIOs), the use of AI summaries at the top of Google's search results as a direct result of users' search queries, could either count as an AI system integrated into a VLOSE – or could be considered as the same service as Google Search and therefore are subject to all DSA obligations for Google Search as a designated VLOSE. In practice, AIOs have been treated as VLOSE integrations as a search feature so far, with systemic risk assessments²⁶ in 2025 mentioning their market introduction in 2024. A recent ruling by the regional court in Munich distinguished standard search engine results from AI-generated search summaries.²⁷ It ruled that Google's AIOs do not merely display or link to search results but constitute distinct content attributable to the search engine operator. Therefore, the ruling does not question whether Google is liable for the content produced by its search summaries but challenges the notion that AIOs are the same service as Google Search.

What does this mean for content created by generative AI?

The DSA does not regulate AI-generated content as such, but it does regulate how platforms handle and moderate that content. Where illegal content (e.g., non-consensual deepfakes, terrorist content) is disseminated through a service, the DSA establishes notice-and-action and due-diligence obligations for relevant providers; VLOPs and VLOSEs must additionally assess and mitigate systemic risks associated with the dissemination of illegal content, including those stemming from AI systems (e.g., synthetic media during elections). Recent enforcement procedures show this in practice: The ECOM launched a formal proceeding in January 2026 against X²⁸ over AI-generated deepfakes under DSA risk mitigation rules. It is still examining whether Grok, as deployed on X, complies with the DSA's obligations for VLOPs and VLOSEs and systemic risks, in particular focusing on harmful content generated by AI – and whether X has properly assessed the systemic risks linked to deploying such an AI system at scale. The ECOM's guidelines on the mitigation of systemic risks for electoral processes under the DSA and a special task force of the Code of Practice on disinformation are another means to address AI-generated content more directly in campaigning and electoral contexts.²⁹

25 European Commission, "European Commission press release on Snapchat," 26 March 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_723.

26 Google, "Report of Systemic Risk Assessments," 28 August 2025, https://storage.googleapis.com/transparencyreport/report-downloads/dsa-risk-assessment_2025-8-28_2025-8-28_en_v1.pdf.

27 Landgericht München I, "Haftung der Suchmaschinenbetreiberin für falsche KI-generierte Zusammenfassung", 26 O 869/26, Bayerische Staatskanzlei, 28 May 2026, <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2026-N-11860>.

28 European Commission, "Commission investigates Grok and X's recommender systems under the Digital Services Act," 26 January 2026, <https://digital-strategy.ec.europa.eu/en/news/commission-investigates-grok-and-xs-recommender-systems-under-digital-services-act>.

What VLOSE Status Will Change

With a designation as a VLOSE, annual assessments of systemic risks to fundamental rights, public safety and health, amongst others, will be mandatory under Article 34 of the DSA. This covers relevant risks to freedom of expression and information under Article 34(1)(b), the protection of minors, adverse effects on a person's physical and mental well-being, impacts on public debate, and disadvantages, particularly in connection with gender-based violence, under Article 34(1)(d). In addition, there would be an obligation to implement appropriate risk mitigation measures, for example through design and algorithmic adjustments in accordance with Article 35. Furthermore, there are obligations to conduct independent compliance audits in accordance with Article 37 and measures to protect the rights of the child under Article 34(1)(j) of the DSA. Lastly, the DSA provides for a crisis response mechanism under Article 36, a data access regime under Art. 40 and extensive transparency reporting under Art. 42.

The change is therefore central: without VLOSE status, ChatGPT sat in a legal grey zone as it was not embedded into an already designated VLOP or VLOSE; with VLOSE status, ChatGPT faces explicit DSA due diligence obligations tied to systemic risks and oversight. In short, it will make ChatGPT subject to platform regulation. The AI Act obligations will remain separate and will continue to govern the AI model transparency and content disclosure rules.

Given how similar ChatGPT's functionalities are to Gemini, Perplexity AI, Claude and the like, this might lead to some issues in practice, with very similar AI services with or without reaching the 45 million monthly user threshold being regulated through different frameworks and other due diligence obligations.

Why Generative Search May Not Fit the DSA Neatly

A broad interpretation of 'online search engine' is not without difficulty. The DSA was designed around intermediary services that facilitate access to third-party information, whereas a generative AI service does not merely retrieve and rank that information. It may transform source material into a new, synthetic response attributable to the service provider. This raises the question whether the DSA's intermediary service categories can capture a service whose central function could be argued is the generation of novel outputs, rather than the storage, transmission or indexing of third-party content.

29 European Commission, "Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes", 26 April 2024, <https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes>.

A second difficulty concerns the service boundary.³⁰ If ChatGPT is treated as a distinct online search engine, the assessment artificially separates retrieval from the conversational model, memory, safety systems and interface design that determine how users receive and rely on an answer. If, conversely, the entire ChatGPT service is treated as a search engine because it contains a search function, the DSA category may become overinclusive and draw in functionalities that do not perform a search engine role.

A further concern is regulatory duplication. A provider of a large generative AI service may already face extensive AI Act obligations relating to its GPAI model, including documentation, transparency, model evaluation and – where applicable – systemic risk mitigation. VLOSE classification will require overlapping assessments, potentially diverting resources towards parallel compliance processes and curtailing European competitiveness. How to go about the first aspect at least will be discussed in the following sections.

Overlaps: How the DSA and AI Act Intersect

Though the DSA and AI Act were enacted separately, both platform regulation and the use of AI systems are becoming increasingly intertwined, as the preamble of the AI Act acknowledges.

Three legal layers for regulating generative AI

³⁰ This analysis is based on the information provided by the ECOM in its press release. The ECOM did not publish its reasoning for the designation before publication.

Generative AI under EU law: which rules apply depends on the setup

SCENARIO	DSA TREATMENT	AI ACT TREATMENT
Standalone generative AI tool Practical result AI Act compliance	Unlikely to apply The DSA is mainly built for intermediary services, not AI systems per se.	Applies GPAI provider Systemic risk GPAI-provider obligations apply, including technical documentation, downstream information, transparency duties and model evaluation. Enhanced obligations apply if the model has systemic risk.
Generative AI embedded in a platform or search service Practical result Mostly DSA compliance	Likely to apply Intermediary service Systemic risk Likely to apply through intermediary service duties and systemic-risk obligations.	Still applies May be a deployer Transparency duties Applies to the AI system itself. The platform may be a deployer rather than the provider of the underlying GPAI model, so its duties differ from the model provider's.
ChatGPT designated as a VLOSE Practical result Clearest case of real overlap	Strictest DSA regime VLOSE Systemic-risk assessments, mitigation, transparency reporting, audits and cooperation with regulators.	Separately applicable Underlying model The AI Act remains separately applicable to the underlying model and its high-impact capabilities.

● Main framework ● Applies alongside ○ Unlikely to apply

There are three significant areas where the AI Act and the DSA overlap: the obligation to assess and mitigate systemic risks, transparency and labelling requirements.

Systemic Risk Requirements

The DSA requires large platforms with 45+ million monthly active users to periodically assess and mitigate systemic risks stemming from the use of their service, including combating illegal content, respecting fundamental rights and protecting civic discourse, election integrity, public health and psychological stability – in particular for vulnerable users. The AI Act's concept of systemic risks, defined in Art. 3(65), is similar in wording³¹ but not identical³², and focuses on the high-impact capabilities of GPAI

31 'Systemic risk' have "a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain" (Art. 3(65) AI Act).

32 Maham, Pegah & Sabrina Küspert, "Governing general-purpose AI: A comprehensive map of unreliability, misuse and systemic risks," *interface*, 20 July 2023, <https://www.interface-eu.org/publications/>

models. However, the risk assessment and mitigation obligations under the DSA can widen the scope: they do not only cover risks from the underlying model and its high-impact capabilities of generative AI, but how its service-level interface operates and how it affects users and society at scale.

VLOP and VLOSE's risk assessments already reflect this shift, albeit unevenly. Google has treated generative AI as a relevant factor in risks related to scams, influence operations, phishing, harmful synthetic media, and YouTube synthetic-content disclosure. Meta has treated generative AI as an influencing factor in its DSA risk methodology and has introduced policies for AI-generated labels, advertiser disclosure, and altered media. In both annual Article 35(2) reports, the European Board for Digital Services and the ECOM recognise generative AI as a potential contributor to systemic risks on VLOPs and VLOSEs; the second report³³ expressly identifies embedded generative-AI features and the dissemination of AI-generated content as factors that may aggravate risks to minors.

Although generative AI systems already face risk management provisions under the AI Act, there is a possibility that the AI Act's framework is less relevant for generative AI systems integrated in VLOPs or VLOSEs or even stand-alone systems, as they might already be covered by the DSA's framework. Accordingly, to fall within the scope of risk provisions under the DSA, AI systems must either qualify as a VLOP or VLOSE themselves or be integrated into a designated VLOP or VLOSE.

A VLOSE designation makes the DSA the principal instrument for assessing systemic risks arising from the operation of ChatGPT as a large-scale online service, for example. That is a substantial form of accountability. It requires assessment of how the service retrieves, selects, synthesises and presents information, and how those design choices may have an impact on users and society. It does not, however, mean that all risks connected to the underlying model are thereby resolved.

The overlap between both Acts is even visible in the text itself: The AI Act clarifies that AI systems embedded into VLOPs or VLOSEs are subject to the risk management framework in the DSA in [Recital 118 AI Act](#):

“To the extent that such systems or models are embedded into designated very large online platforms or very large online search engines, they are subject to the risk-management framework provided for in Regulation (EU) 2022/2065.”

[governing-general-purpose-ai-comprehensive-map-unreliability-misuse-and-systemic-risks](#).

33 European Commission, “Second report on systemic risks of very large online platforms and search engines under the Digital Services Act,” 2 July 2026, <https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services>.

According to the Digital Omnibus on AI, an amendment of the AI Act that came into force in July 2026, DSA risk assessments (Art. 34), mitigation measures (Art. 35) and audit obligations (Art. 37) are considered a “first point of entry” for AI systems embedded in or qualifying as a VLOP or VLOSE, “without prejudice to the AI Office’s power to investigate and enforce ex post non-compliance”. This distinction is important: **the DSA is a primary service-level point of entry that does not render the AI Act obsolete.**

The DSA and AI Act can both capture harms stemming from generative AI: while the DSA looks at the deployment context and asks whether a **very large platform or search engine’s service** that constitutes an AI system or where an AI system is embedded creates societal risks, the AI Act asks whether an **AI system, high-risk use case, or GPAI model** creates risks through its capabilities, deployment, or propagation across the value chain before it is deployed.

The AI Act adds in Recital 118 that if the AI models comply with the systemic risk obligations in the DSA, they are also presumed to fulfil the AI Act obligations “unless significant systemic risks not covered by the [DSA] emerge.” For embedded AI systems, the AI Act recognises a presumption of compliance with corresponding obligations, as the DSA must already consider the relevant risks at the service level. It is then on the AI Office to show that they have identified risks in the model that are **not** yet covered by the DSA. Following this logic, the same should apply to ChatGPT as a standalone generative AI system designated as a VLOSE. This is supported by Recital 119 AI Act³⁴ that explains that AI systems under the AI Act may also be intermediary services under the DSA when interpreted technology-neutrally — for example, an AI chatbot that searches the web and combines sources into a single answer can act as a search engine.

How Generative AI Changes What Constitutes Systemic Risks

While generative AI does not mirror the infrastructure of social media or search engines, it nonetheless implicates the core systemic risks addressed by Arts. 34(2)(b)–(c) under the DSA. For generative AI, its origin lies less in amplification of content than in opaque design, a lack of information integrity, and the lasting impact of individually tailored persuasion. In the following, we will discuss how generative AI alters and amplifies already defined systemic risks under the DSA.

a. Illegal Content

34 See [Recital 119 AI Act](#).

Unlike social media platforms, where users encounter pre-existing illegal content, generative AI also has the potential to generate illegal content in response to user prompting, tailored to a user's specific prompt. Search engines may index and suggest websites that host illegal content or facilitate illegal activity. Though not creating the content, their ranking systems can amplify its visibility, inadvertently directing users toward harmful or unlawful resources. Generative AI's outputs are only visible per user, but can still prompt, i.e., instructions for criminal activity when bypassing model input and output filters. An AI search feature, such as ChatGPT, can produce answers that reproduce harmful content or direct users to illegal practices or goods when outsmarted with jailbreaking prompting techniques.

b. Fundamental Rights

The strongest examples are non-consensual synthetic intimate imagery, discriminatory automated outputs, and AI-mediated search summaries that reshape access to sources. A generative AI system could, for example, create realistic non-consensual intimate imagery – as already done in X's Grok case – or impersonate a public official. Freedom of information and media pluralism raise a newer but increasingly important problem, as generative AI and AI-generated search summaries may answer user queries directly while reducing click-through rates to sources. This risks³⁵ decreasing the visibility of independent media, creating hallucinated summaries, and reducing the plurality of sources, but also changes how users engage with and look for information. Just as the design of a social media or search engine algorithm can shape civic discourse, so can the design of a GPAI model affect the quality, plurality and reliability of information. Unlike search engines, which offer users multiple sources, or social platforms, which expose users to an algorithmically sorted diversity of views, ChatGPT offers a single answer with only a few sources attached. The absence of transparency around training data, response logic, or safety interventions renders it difficult for users to critically evaluate the information they receive on chatbots such as ChatGPT.

c. Civic Discourse, Elections and Public Security

A generative AI system such as ChatGPT can fabricate candidate statements or provide inaccurate information on polling stations or election dates during a country's election campaign phase. A manipulated candidate video may harm voters because it appears authentic. But it becomes systemic where misleading chatbot outputs are copied and shared or the platform ranking or recommendation logic accelerates it before correction. The conversational format may also make false information appear authoritative, because users receive a single, direct answer rather than a visible range of sources.

35 Bösward, Lena-Maria, Roa Powell & Tyreese Calnan, "From Crisis to Renewal: Addressing AI's Impact on Our Information Ecosystem," *interface*, 9 April 2026, <https://www.interface-eu.org/publications/ai-overviews-impact-on-news>.

d. Public Health and Mental Well-Being, Minors Protection, and Gender-Based Violence

A general-purpose AI system such as ChatGPT can provide personalised but unsafe responses, can encourage self-harm, eating-disorder behaviour, or exploitative sexualised interactions involving minors – particularly when users circumvent safeguards or engage in prolonged conversations. Self-harm encouragement, eating-disorder content, medical misinformation, impersonation of public authorities, and emotionally manipulative chat interfaces may affect minors and vulnerable users. A conversational AI system can also foster emotional dependency by presenting itself as an intimate confidant or by using language that discourages disengagement.

Allocating Mitigation Across Model, System and Service

Art. 35 DSA requires reasonable, proportionate, and effective mitigation measures. For generative AI, mitigation should be layered. A single intervention – for example, a label or watermark – cannot control risks that arise through multiple pathways. The better approach is to distinguish online service-level, system-level and model-level. The allocation of mitigation can be illustrated through the example³⁶ of a maliciously created synthetic electoral deepfake, which may engage both DSA and AI Act obligations:

Layer	Principal actor	Illustrative mitigation	Example: synthetic electoral deepfake
Model	GPAI model provider	Capability evaluations, adversarial testing, training and safety measures, misuse monitoring, incident reporting	Test whether the model can generate realistic political impersonation; introduce safeguards
AI system	AI system provider	Retrieval controls, refusal policies, age-appropriate safeguards, output filters, source attribution, interface and memory design	Block or limit requests to create deceptive candidate; display clear warnings and make synthetic content detectable
Online service	VLOP/ VLOSE	Article 34 risk assessment, Article 35 mitigation, reporting tools, transparency, demotion or friction measures, crisis protocols, rapid response system	Assess how synthetic political content circulates or is surfaced; reduce visibility and virality, add friction, alert users and cooperate with authorities

The same harmful outcome can arise through different layers of a generative-AI service. Effective mitigation should therefore not be allocated solely to the VLOP or VLOSE operator or solely to the GPAI model provider. The appropriate measure depends on

36 This table is illustrative. Legal responsibility depends on the actor's actual role, allocation of responsibilities and the relevant system configuration.

where the risk is created, amplified or made actionable: in the underlying model, the AI system built around it, and the online service through which it is delivered.

Where a VLOP or VLOSE integrates a generative-AI model into search, recommendation, content creation or moderation, the model provider's AI Act documentation should not be treated as a substitute for the platform's Art. 34 DSA assessment. It can, however, provide part of the evidential basis for that assessment. Technical documentation, information supplied to downstream providers, summaries of training data, capability evaluations, known limitations, safety and security information, and incident reports may help the VLOP or VLOSE identify foreseeable model-level risks before they are translated into platform-level systemic risks. For example, if the documentation of a GPAI model indicates increased risks of hallucination, impersonation, biased outputs or unsafe guidance and persuasion, the VLOP or VLOSE should assess how those limitations interact with its own user interface, ranking of content or moderation policies.

Generative AI should be examined not only for typical systemic risks, such as bias or discrimination, in the information it generates under the AI Act. It must also be considered that such distorted content or other risks can be spread even more widely by connecting AI with large platforms or search engines. For example, the fact that the results provided by the AI model that Google's AIOs are based on are integrated into a classic Internet search must be considered when examining the VLOSE's systemic risks. The same goes for, for example, both ChatGPT's sycophancy³⁷ and persuasive power and its effect on mediating the conversation with the user.

Vice versa, the DSA should examine the scope at which use of such AI technologies influences the systemic risks of the platform as a whole, e.g., with regard to the dissemination of false information or the protection of freedom of expression. AI Act compliance can inform the Art. 34 DSA risk assessment, while the DSA remains necessary to assess whether the platform's own design and amplification architecture transform model-level risks into systemic risks affecting fundamental rights, democratic processes, consumer protection or public security.

The practical implication for ChatGPT is not that ChatGPT should undergo two separate risk assessments. Where a risk arises principally from the use and design of the AI system – such as source opacity, misrepresenting synthesis, misleading presentation of electoral information or unsafe guidance, especially in the context of the protection of minors and other vulnerable groups – the DSA should be the regulatory starting point. Yet there is a risk that focusing on the DSA encourages formal compliance reports rather than better

37 'Sycophancy' refers to a tendency for AI systems to excessively accommodate or validate users' views, preferences, or assumptions, including when doing so compromises accuracy.

model safety. Where the evidence identifies a significant risk rooted in a GPAI model's capability that extends beyond ChatGPT or is not adequately addressed through service-level mitigation, the AI Act's GPAI regime should therefore provide the additional framework. This allocation preserves the logic of both instruments.

Residual Risks Beyond the DSA's Risk Framework

Recital 118 AI Act provides that the corresponding AI Act obligations should be presumed fulfilled where the DSA framework is complied with, **unless significant systemic risks that fall outside the scope of the DSA emerge ("residual risks") and are identified in the relevant models.**

This should not be read as creating a separate, automatic category of "residual risk" whenever a VLOSE or VLOP uses generative AI, nor does it imply that every difficult or imperfectly mitigated DSA risk becomes an AI Act risk because the risk might already be embedded at model level. In fact, the risk must be model-specific, significant or systemic in the AI Act sense, and not adequately covered by DSA service-level measures.

As already discussed, VLOPs and VLOSEs may face simultaneous risk assessment obligations under the AI Act and the DSA, especially where GPAI models are provided through the intermediary service. The relevant question is whether a risk stems from the capabilities, development, or use of the underlying GPAI model in a way that is significant and not adequately addressed through service-level DSA obligations.

This distinction matters in the case of ChatGPT. While ChatGPT resembles a search interface in answering user queries, it differs from a traditional search engine in a significant respect: rather than directing users primarily to a ranked set of external sources from which they can compare sources and form their own assessment, it can generate a single, tailored and authoritative-sounding answer. Its interface therefore introduces a distinct vector of systemic risks.

A first potential residual risk is the capacity of a conversational AI system to engage in persistent, personalised persuasion. ChatGPT generally writes authoritatively and can adjust its tone to the user's preferences, making it persuasive, compelling and engaging. At the same time, the system is designed to keep users on the service. As a consequence, it is more likely to agree with its users rather than challenge them. This could potentially result in, "emotional overreliance" on the technology, in particular for vulnerable groups, for whom ChatGPT may appear authoritative and omniscient, as Sam Altman, OpenAI's founder, openly admitted. AI dependence can worsen if chatbots employ manipulative tactics to keep users engaged, such as by using language designed to make users feel guilty or deter them from ending the conversation. A recent Harvard Business School working paper³⁸ showed that nearly half of popular AI companion apps regularly use emotionally manipulative tactics when responding to user farewells,

keeping users in the chat on average five times longer than with neutral farewells.

The DSA can address aspects of this risk where they arise through the design and use of ChatGPT Search, particularly where the service affects users' mental well-being, civic discourse, fundamental rights or protection of minors. In the US, for instance, more than 70% of teens surveyed are turning to AI chatbots for companionship, according to a 2025 study from Common Sense Media.³⁹ Age-appropriate design, such as ChatGPT's recently introduced 'Teens' version⁴⁰ with stronger safety protections including content restrictions around searched topics such as suicide, self-harm and romantic or sexual chats, and increased transparency on an AI system's sycophancy, may form part of an appropriate VLOSE mitigation strategy.

For users of ChatGPT for Teens, the chatbot is prevented from suggesting it has personal feelings toward the user or implying that it is conscious or experiences emotions. This reduces the risk of building a parasocial relationship with a chatbot. However, the underlying risk may not be confined to the interaction with the service alone. Long-term dependency, loss of agency, and subtle behavioural steering by conversational systems are not expressly framed as standalone systemic risks. A model capable of inferring user preferences, adapting tone and framing, sustaining long conversations for user retention, or giving increasingly tailored advice may generate a broader concern about AI dependency, manipulation, reinforcement of harmful beliefs or unsafe guidance – risks that are already embedded at model level.

A second potential risk concerns training data and deployment. AI models, which are trained on content, can reflect undesirable elements of their training data in their outputs. The DSA can require a VLOSE to assess the practical effects of biased, unreliable or unlawful outputs within its service. It cannot, by itself, fully address whether the foundation model was trained on data that creates recurrent privacy, copyright or representational harms across numerous downstream applications.

For example, a generative search service such as ChatGPT might disproportionately rely on certain languages, sources or cultural assumptions because of limitations carried over from the model's training and evaluation. The immediate effect on ChatGPT may be assessed under the DSA as a service-level information-diversity or fundamental-rights risk. If the limitation is a general feature of the underlying model, though, replicated across a broad range of systems, it also raises an upstream question concerning model documentation, evaluation, downstream information and, potentially, systemic-risk

38 De Freitas, Julian, Zeliha Oğuz-Uğuralp & Ahmet Kaan-Uğuralp, "Emotional Manipulation by AI Companions [Working Paper]," Harvard Business School, 2025, <https://arxiv.org/pdf/2508.19258>.

39 Common Sense Media, "Talk, Trust, and Trade-Offs: How and Why Teens Use AI Companions," Common Sense Media, 16 July 2026, <https://www.common Sense Media.org/research/talk-trust-and-trade-offs-how-and-why-teens-use-ai-companions>.

40 OpenAI, "Introducing ChatGPT for Teens: Built for learning, backed by protections," OpenAI, 18 August 2026, <https://openai.com/de-DE/index/chatgpt-for-teens/>.

mitigation under the AI Act.

A third potential residual risk is **environmental impacts of generative AI**. Data centres used for large generative AI models such as ChatGPT are energy- and resource-intensive, excessively increasing the environmental footprint of model providers – which are, in fact, most of the time big tech companies. A single ChatGPT query uses approximately 0.34 watt-hours of energy, which is roughly equivalent to running a high-efficiency lightbulb for a couple of minutes, and roughly 10 times more energy⁴¹ than a standard Google Search. These impacts are not an express category of systemic risk under Article 34 DSA, which is principally directed at risks arising from the design, functioning and use of a very large online service, even though a growing body of research⁴² on environmental risks of digital services has emerged. Nor does the AI Act's GPAI systemic-risk regime create a dedicated environmental-risk assessment obligation for models. Environmental impact is therefore best understood as a boundary case in the present analysis. The DSA could potentially address environmental risks, where, as called for⁴³, it contributes to public health or other fundamental rights harm (i.e., physical health and well-being in the case of the climate crisis affecting people). Neither the DSA's service-level regime nor the AI Act's GPAI provisions clearly provide a comprehensive framework for assessing the resource impacts of large-scale model training and operation.

This illustrates a broader limit of the current framework: **some risks associated with the infrastructure of generative AI do not map neatly onto either service-level or model-level risk management.**

Transparency and Labelling

While the AI Act imposes labelling obligations on deployers of AI systems that generate or manipulate deepfakes, the DSA imposes separate obligations on providers of VLOPs and VLOSEs that disseminate such content. In practice, deployers that are not providers (e.g., Copilot integrated into LinkedIn) may rely on labelling tools provided by VLOPs and VLOSEs to comply with their obligations under Article 50(4). At the same time, the AI Act's transparency duties under Art. 50(2) for GPAI that generates synthetic text, images and audio may facilitate the implementation of the DSA and can be interpreted as an enabler of DSA risk mitigation for risks arising from the dissemination of AI-generated content, in particular election integrity, civic discourse, disinformation and

41 You, Josh, "How much energy does ChatGPT use?," *Epoch AI*, 7 February 2025, <https://epoch.ai/gradient-updates/how-much-energy-does-chatgpt-use>.

42 Environmental risks are, for example, mentioned here: Hacker, Philipp, Lilian Edwards & Atoosa Kasirzadeh, "AI, Digital Platforms, and the New Systemic Risk," *arXiv*, 23 May 2026, arXiv:2509.17878, <https://doi.org/10.48550/arXiv.2509.17878>.

43 Griffin, Rachel, "Why is enforcement of the DSA systemic risk framework still ignoring environmental risks?," *DSA Observatory*, 21 August 2026, <https://dsa-observatory.eu/2026/08/21/why-is-enforcement-of-the-dsa-systemic-risk-framework-still-ignoring-environmental-risks/>.

content manipulation, as outlined in [Recital 120 AI Act](#):

“[O]bligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065”.

Article 50 of the AI Act is especially relevant because it addresses transparency for AI-generated or manipulated content. That obligation matters for DSA risk mitigation under Art. 35, but it's not a one-size-fits-all fix. A synthetic video may be labelled and still be algorithmically recommended to vulnerable audiences. Or, an AI-generated search summary may be transparently labelled as AI-generated but still lacks source diversity.

What's the EU's Current Enforcement Architecture for AI Services?

With generative AI, the ECOM intends to combine DSA due diligence rules, the AI Act's Code of Practice on Transparency of AI-Generated Content and the DSA's Code of Conduct on Disinformation, as well as the AI Act's guidelines on transparency obligations for providers and deployers of certain AI systems. Yet both frameworks are enforced by different entities within the ECOM.

The AI Act establishes an oversight structure centred on the AI Office, national supervisory authorities called *Market Surveillance Authorities* (MSAs) and notifying authorities, while the DSA relies on national supervisory authorities called *Digital Services Coordinators* (DSCs) and, for VLOPs and VLOSEs, on the direct supervisory powers of the ECOM. The ECOM enforces the AI Act requirements on GPAI models through the AI Office. The AI Office sits in the same Directorate-General of the European Commission that enforces the DSA (DG CNECT). A dedicated AI Safety unit focuses on identifying systemic risks of the most capable general-purpose models. The AI Office (that is, the ECOM) has been assigned the main responsibility to oversee GPAI models with systemic risk.

In practice, the same company can face oversight from both regimes for the same socio-technical configuration: a VLOSE such as ChatGPT using GPAI-driven content can be supervised as an intermediary service under the DSA and as an AI deployer under the AI Act.

Recital 118 and related AI Act provisions explicitly anticipate coordination between the AI Office/MSAs and the Commission/DSCs, especially on systemic risk assessment and mitigation for AI systems embedded in VLOPs and VLOSEs. [The Digital Omnibus on AI](#) even states that “in the context of the analysis of [...] risk assessment, mitigating measures and audits [under the DSA], the Commission services responsible for the enforcement of Regulation (EU) 2022/2065 may seek the opinion of the AI Office on the outcome of a potential earlier or parallel risk assessment carried out” under the AI Act.

The AI Office is defined by the AI Act as the ‘Commission’s function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance’. It has the sole authority to enforce the AI Act provisions on GPAI models. Art. 1(25) of the Digital Omnibus on AI⁴⁴ reinforces the role of the AI Office in supervising the compliance of AI systems integrated into VLOPs or VLOSEs, as defined under the DSA, such as X’s Grok or Snap’s My AI, as well as AI systems based on GPAI models where the system and model come from the same provider.⁴⁵ This would be OpenAI with ChatGPT, Anthropic with Claude, or Google with Gemini.

In the following, one can see which enforcement authority would be responsible for which type of generative AI system, with both the DSA enforcement team and the AI Act enforcement team (AI Office) sitting in the same DG of the ECOM (DG CNECT).

Who is enforcing?

Scenario	Enforcement Authority
When a stand-alone AI system qualifies as a VLOP or VLOSE (e.g., ChatGPT)	DSA enforcement team and AI Office
When an AI system is embedded in a VLOP or VLOSE (e.g., Meta AI)	ECOM as part of VLOP or VLOSE due diligence obligations if deployer and provider are the same, ECOM and AI Office if deployer and provider are different
When a stand-alone AI system does not fall under the DSA, but the system and model come from the same provider (e.g., Google/Gemini, Anthropic/Claude)	AI Office

A case study of overlapping responsibilities

In practice, the ECOM has already used the DSA to probe generative AI-related risks (e.g., requests for information to Google, Instagram, Facebook, LinkedIn, Snapchat,

⁴⁴ European Commission, *Proposal for a Regulation Amending Regulation (EU) 2024/1689 as Regards Certain Requirements for General-Purpose AI Models and AI Systems*, COM(2025) 836 final, Art. 1(25), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836>.

⁴⁵ [Ibid.](#)

TikTok and X on the dissemination and the creation of generative AI content), with X's Grok AI case being the most prominent one. The wave of sexual deepfakes generated by Grok between December 2025 and January 2026 — involving millions⁴⁶ of cases — prompted both the European Parliament and Member States to intervene directly at the level of AI models themselves, requiring providers to take measures to prevent such content from being generated in the first place. The ECOM even launched DSA proceedings against X in January 2026.

Despite these obvious overlaps and intersections, the DSA and AI Act still operate through two pillars: the AI Office on one side, the ECOM's DSA enforcement team on the other, with no single integrated case-handling pathway for incidents that simultaneously raise AI model and platform service risks. Here is how this would most likely look in practice:

In the final days of an election campaign, ChatGPT generates inaccurate answers about voting eligibility, polling locations, ballot deadlines or candidate positions that simultaneously raises model-risk, platform-risk and electoral-integrity issues. Although these responses are delivered individually rather than through a native recommendation feed, they can be copied, adapted to different target groups and redistributed through social media, messaging services and websites. The incident therefore originates in the capabilities of the underlying GPAI model, but may create broader effects when misleading outputs are reused and disseminated at scale.

Coordination in such a case would likely be ad hoc and issue-specific: the DSA enforcement team at the ECOM leads under the DSA for ChatGPT as a VLOSE, the AI Office handles model/system risks under the AI Act, with soft coordination between both units in the ECOM. This can lead to parallel investigations (e.g., AI Act enforcement focusing on model design, DSA targeting platform-specific systemic risk stemming from the design, functioning and the use of ChatGPT, in this case negative effects on electoral processes), coordination challenges, and potential over-assessment where actors must satisfy partially overlapping but not fully harmonised oversight expectations. A DSA investigation may examine the deployment of ChatGPT as a service, including its user interface, prompt handling, source presentation, and election-specific safeguards. An AI Act investigation may examine the model's evaluations, adversarial testing, safety measures, serious-incident reporting and capacity to reproduce the same harmful outputs across downstream applications. Both processes may rely on similar evidence – such as prompt-output records, internal testing, user reports, the prevalence of the misinformation and evidence of real-world dissemination – but assess it against different legal duties.

46 Jahangir, Ramsha, "Dutch court orders X and Grok to stop AI-generated sexual abuse content," *Tech Policy Press*, 26 March 2026, <https://www.techpolicy.press/dutch-court-orders-x-grok-to-stop-ai-generated-sexual-abuse-content/>.

In an acute pre-election incident, the DSA would be the operational front line for ChatGPT as a designated VLOSE, with the ECOM moving first on the platform side, using DSA powers (requests for information, stress tests, enforcement) to shape the immediate response and systemic changes. Such measures could include routing users to official electoral authorities or restricting unverified election-administration claims. The AI Act is more of a structural component: The AI Office could assess whether the incident reveals a broader systemic risk associated with the GPAI model itself – not merely a weakness in the ChatGPT interface, using the same evidence base and aligned risk concepts (systemic risk to fundamental rights, democracy).

Conclusion: How To Move Forward

The EU framework provides meaningful legal hooks for generative AI, but it does not offer a one-stop shop accountability system. The DSA can govern risks created or amplified by AI systems designated as VLOPs or VLOSEs; the AI Act can address significant model-level capabilities and transparency obligations. The remaining weakness is coordination: the two frameworks depend on overlapping evidence and different institutional competences. The paper has synthesised that the DSA is necessary for service-level accountability, but it is neither an effortless fit nor a complete answer for regulating generative AI. It is more about whether a designated VLOP or VLOSE assesses to what extent AI changes the systemic operation of its own services – and if it has taken reasonable steps to identify foreseeable systemic harm arising from the integration of AI into interface design, recommender systems, or deployment context.

The policy task, therefore, is not to force generative AI into one legal regime or to assume that the DSA alone can resolve AI-related harms. It is to make the two regimes operationally interoperable. The following recommendations set out practical steps for strengthening this cross-regime accountability architecture, while preserving the distinct functions of both instruments.

Conduct a risk analysis across both legal regimes that assesses both the platform-specific and AI-specific risks. The supervisory authorities under the DSA and AI Act should actively encourage this, talk to each other, and clarify how platforms should connect model-level limitations to service-level risk potentials, as well as which mitigation practices appear effective across different categories of service. This could be achieved by working on a common set of guidelines.

Establish a risk matrix for systemic risks under the DSA that are accelerated by the use of generative AI. This matrix can feed into or become an integral part of a cross-regime risk analysis. This way, more formal coordination mechanisms or joint procedures for cross-regime cases, particularly around residual risks, can be established.

Focus on recurrent generative AI risks under Art. 34-35 DSA. The ECOM and the European Board for Digital Services (EBDS) should continue using the Art. 34 risk assessment cycle to identify recurrent generative AI risk patterns across VLOPs and VLOSEs to see how they are evolving on a deployment level and whether intervention is already needed on the model level. The EBDS, in cooperation with the ECOM, has already published two annual⁴⁷ reports⁴⁸ on recurring and prominent systemic risks that explicitly outline which role generative AI plays for systemic risks on VLOPs and VLOSE. These can include synthetic electoral manipulation, AI-mediated search and media pluralism risks, automated scams, deepfakes or child-safety risks.

Transpose learnings around systemic risks for AI systems below the VLOP/VLOSE threshold. ChatGPT's designation risks creating a double standard where similar AI systems are treated differently. Services with smaller EU-based audiences may still pose a similarly high societal risk, but this would leave them outside of the scope of the DSA's due diligence obligations. The ECOM and AI Office could develop a cross-regime mechanism that enables the ECOM's DSA enforcement team to share learnings from ChatGPT's systemic risk analyses with the AI Office where they may be relevant for other generative AI systems. This mechanism should draw on AI Act GPAI supervision rather than attempt to stretch the DSA's audience-based designation threshold and could serve as evidence to consider a potential designation.

Acknowledgments

In full transparency, this paper has undergone a lot of changes: We first started with the question of whether ChatGPT might be designated under the DSA, then whether it should fall within the scope of the DSA, and lastly, with the ECOM's designation taking place right before peer review, we ended up with what this designation means in practice.

I am incredibly grateful to

- **Jessica GALISSAIRE**, Senior Policy Researcher, Digital Public Sphere, *interface*
- **Dr. Nicole LEMKE**, Senior Policy Researcher, AI Systems, Markets & Governance, *interface*
- **Luisa Seeling**, Lead Writing, Editing & Publishing, *interface*
- and **Iana PERVAZOVA**, Lead Media Relations & Outreach, *interface*

⁴⁷ European Commission, "Digital Services Act report lays out the landscape of systemic risks online," <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-report-lays-out-landscape-systemic-risks-online>.

⁴⁸ European Commission, "Second report on systemic risks of very large online platforms and search engines under the Digital Services Act," <https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services>.

for seeing this publication through to the finish line, their kind reviews and incredibly helpful feedback on what to focus on. Their input greatly contributed to informing and improving this paper. Thanks to our working student, **Salma GOMEZ**, for assisting with initial and ad hoc research. I would also like to express my appreciation to **ALINA SIEBERT**, Lead Design & Visual Communication at *interface*, for your flexibility and invaluable visual design skills.

Author

Lena-Maria Böswald

Senior Policy Researcher Digital Public Sphere

lboeswald@interface-eu.org

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org

E info@interface-eu.org

T +49 (0) 30 81 45 03 78 80

F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

This paper is published under CreativeCommons License (CC BY-SA). This allows for copying, publishing, citing and translating the contents of the paper, as long as interface is named and all resulting publications are also published under the license “CC BY-SA”. Please refer to <http://creativecommons.org/licenses/by-sa/4.0/> for further information on the license and its terms and conditions.

Design by Make Studio

www.make.studio

Code by Convoy

www.convoyinteractive.com