

LLMs, Chatbots und KI-Agenten unter der DSA-Lupe – Blinder Fleck oder volles Risiko?

**Nathalie Koch, LL.M. (UC Law San
Francisco) – Taylor Wessing**

Richard Gläser – Taylor Wessing

Herbstakademie 2026

Agenda

1. DSA im Überblick: Regelungszweck, Adressaten und Pflichten
2. Einordnung von KI-Anwendungen: LLM, Chatbot und KI-Agenten
3. Diskussion
4. Q&A

1. DSA im Überblick

1.1 Regelungszweck

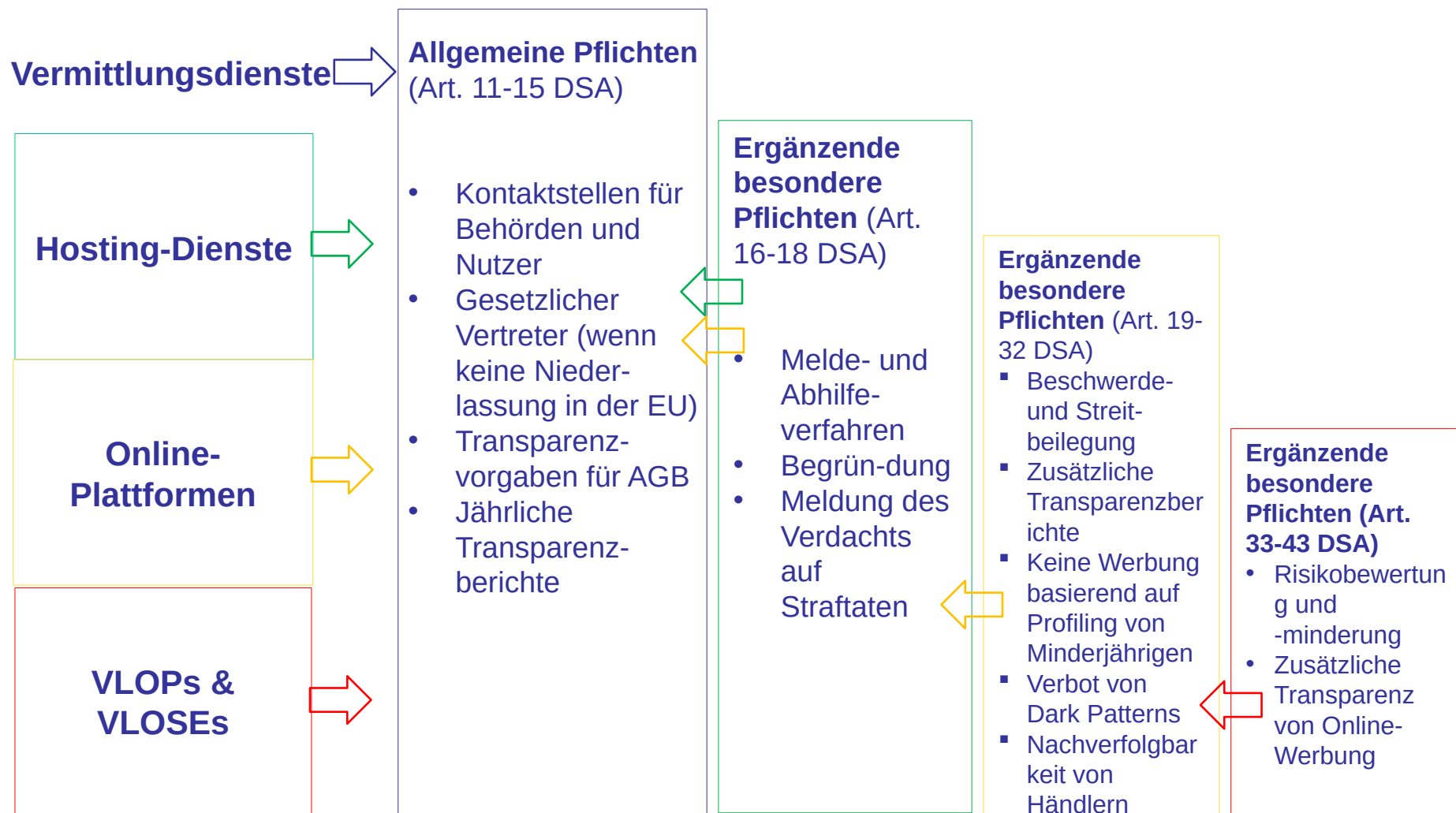
- ▶ Verordnung (EU) 2022/2065 vom 19. Oktober 2022
- ▶ Vollständige Anwendbarkeit seit dem **17. Februar 2024**
- ▶ Vollharmonisierende EU-Verordnung für digitale Vermittlungsdienste
- ▶ Schaffung eines sicheren und vertrauenswürdigen digitalen Raumes, Schutz von Nutzerrechten, Transparenz bei Moderation und Werbung, und Bekämpfung illegaler Inhalte, irreführender Werbung und Dark Patterns



1.2 Adressaten

- ▶ Der DSA gilt sowohl für B2B- als auch für B2C-Anbieter von **digitalen Vermittlungsdiensten (Intermediäre)**
- ▶ Vermittlungsdienste:
 - ▶ Reine Durchleitungsdienste – Bsp. Internetzugangsprovider, VPN-Dienste, Domain-Registrare, DNS-Resolver, VoIP
 - ▶ Caching-Dienste - alleinige Betreiben von Netzwerken zur Bereitstellung von Inhalten, Reverse-Proxys oder Proxys zur Anpassung von Inhalten
 - ▶ Hosting-Dienste – Bsp. Cloud-Computing-Dienste, Web-Hosting-Dienste, oder Dienste, die den Online Austausch von Informationen und Inhalten ermöglichen
 - ▶ Online Plattformen – Bsp. Soziale Netzwerke und Online Marktplätze
 - ▶ Sehr große Online Plattformen (VLOP) und Online-Suchmaschinen (VLOSE)

1.3 Abgestufter Pflichtenkatalog



2. Einordnung von KI-Anwendungen: LLM, Chatbot und KI-Agenten



2.1 Large Language Models (LLMs)

- ▶ **Funktionsweise:** statistische Sprachmodelle, die Output ausgehend von Wahrscheinlichkeiten erstellt
- ▶ **Einordnung:** Regelmäßig keine Vermittlungsdienste nach dem DSA
 - Übermittlung von Informationen, die durch Nutzer bereitgestellt werden?
 - Dauerhafte Speicherung von Inhalten?
 - Vergleich mit den vom DSA benannten Beispielen
- ▶ **Phänomen der Memorisierung von Trainingsdaten als Speicherung?**
 - Hintergrund: GEMA-Urteile des LG München
 - Übertragbarkeit im Kontext des DSAs – Online-Plattform?

2.2 Chatbots

► Funktionsweise und Anwendungsformen:

Statisches LLM plus damit verknüpfte Chat-Applikation

Chat-Applikation speichert jedenfalls idR Prompts und
Konversationsverläufe

► Chatbots als Hosting oder Online-Suchmaschine

- Speicherung von Prompts oder Konversationsverläufen?
- Hochladen von bestimmten Datenbanken (retrieval augmented generation)?
- Möglichkeit einer Echtzeit-Suche?
- Maßgeblich: Bestimmung von "**allen Webseiten**"



2.3 KI-Agenten

▶ Funktionsweise und Unterschiede zum "Chatbot":

Mehrstufige Handlungsabläufe und Kombination von Anwendungen

Mehrere Arbeitsschritte: Planung, Ausführung, Revision

Sehr viele Praxisbeispiele denkbar

▶ Kategorisierung im Rahmen des DSA

Eigene Kategorisierung unmöglich

Abhängigkeit von anderen Diensten

3. Diskussion ausgewählter Problemfelder

- ▶ Bestimmung von "allen Webseiten"
- ▶ Memorisierung von Trainingsdaten als "Speicherung"
- ▶ Konsequenzen einer Einordnung als VLOSE

4. Q&A