



# DSGVO-konforme KI: Externe Lösungen für Ihr Unternehmen

11. KI-Stammtisch Weinheim,  
ISACA Germany Chapter

Referent: Peter Suhling

Herausgeber: suhling tooling GmbH

Hauptstraße 128, 69469 Weinheim,

suhling.biz, suhlingtooling.com

Autor: Peter Suhling

Version: 1.0

Vortrag am 13.11.2025

# Agenda



SUHLING  
TOOLING

## Vorstellung Referent

1. Überblick derzeitiger Künstliche Intelligenz (KI) Umsetzungsmöglichkeiten
2. Edge-Hardware (On-Device KI, komplett offline – auch im eigenen RZ/Edge)
3. Lokale „Desktop-KI“ (ohne Internet)
4. Self-Hosted LLM-Serving im eigenen Rechenzentrum (RZ)
5. On-Prem AI-Appliances / Private Cloud AI
6. EU-Managed SaaS (z. B. Langdock, Pryvet.ai)
7. EU-Souveräne Modell-APIs (Aleph Alpha, Mistral)
8. EU Data Boundary Cloud-Angebote (z. B. Microsoft, Azure)
9. Hyperscaler Foundation Models (AWS / Azure)
10. Lokale Wissensbots (z. B. PrivateGPT, OpenWebUI)
11. Praxisbeispiele & Vergleich
12. KI-Checkliste
13. Warum eine KI-Richtlinie
14. Fragen aus dem Plenum

# Vorstellung Referent Peter Suhling



SUHLING  
TOOLING

Zertifizierter **interner Auditor ISO 9000** ff. Qualitätsmanagement - Dekra

Zertifizierte Grundlagen im IT Service Management - TÜV SÜD

Zertifizierter Datenschutzbeauftragter DSB-TÜV - TÜV SÜD

Zertifizierter Datenschutzbeauftragter - udis Ulm

Zertifizierter **ISMS-Lead Auditor ISO 27001** - TÜV Nord

Akkreditierter **zertifizierter Datenschutzauditor** - DSZ - GDD und BvD

Revision ISO 9001:2015 und ISO 14001:2015 - TÜV SÜD

**CISA** - Certified Information Systems Auditor - ISACA

Akkreditierter **ISO 27001 Lead Auditor** - TÜV SÜD, sowie weitere Zert.-Stellen

Zertifizierter **KRITIS-Auditor** gemäß IT-Sicherheitskatalog nach § 11 (1a) EnWG - TÜV SÜD

Prüfungsvorsitzender des Prüfungsausschusses der Zusatzqualifikation  
Qualitätsmanagement für Kaufleute - IHK Karlsruhe

Menschenrechtsbeauftragter - Umweltinstitut

SzA-Prüfer (Systeme zur Angriffserkennung) – TÜV

Akkreditierter Compliance **Lead Auditor ISO 37301** – TÜV

Akkreditierter **Lead Auditor ISO 27001 Automotive** - TÜV SÜD

#suhlingtooling

CDPSE - Certified Data Privacy Solutions Engineer - ISACA

Zertifiziert nach der **Prüfverfahrenskompetenz § 8a BSI-Gesetz** - TÜV TRUST IT

TR Technical Reviewer Managementsysteme

Akkreditierter **ISO 9001 Lead Auditor** - TÜV SÜD

Zertifizierter Cyber Security Practitioner - ISACA

Zertifizierter anerkannter IT-Sachverständiger - BISG e.V.

IT-Compliance Manager - TÜV

Akkreditierter **TISAX Auditor** - TÜV SÜD

Zertifizierter interner + Lieferanten Auditor Arbeitsschutz ISO 45001 – ifg

CDPSE – Certified Data Protection Solutions Engineer – ISACA

Zertifizierter **ISO 9001 Lead Auditor** – Advisera

Zertifizierter **ISO 14001 Lead Auditor** – Advisera

Zertifizierter **ISO 45001 Lead Auditor** – Advisera

Bachelor Professional / geprüfter Fachwirt für Büro- und Projektorganisation - IHK

Zertifizierter KI-Compliance Beauftragter - TÜV

Zertifizierter KI Lead Auditor **ISO/IEC 42001** -Treccert

Akkreditierter KI Lead Auditor ISO/IEC 42001 – IAI, TÜV Austria

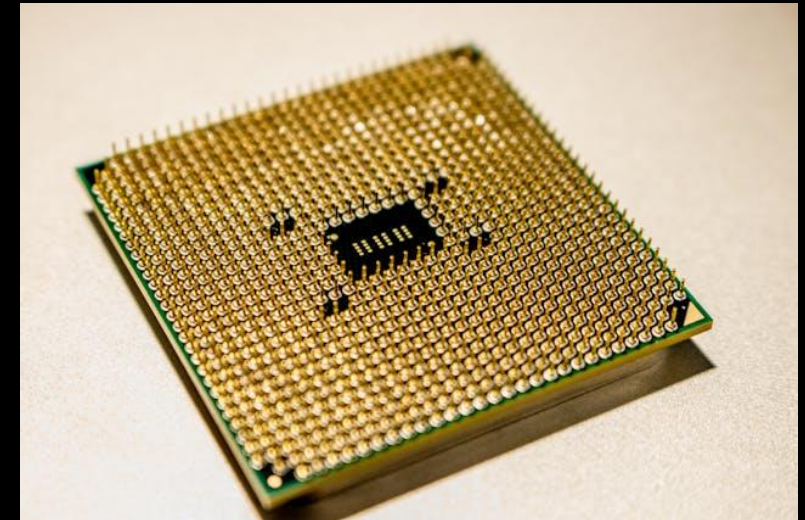
# 1. Überblick derzeitiger Künstliche Intelligenz (KI) Umsetzungsmöglichkeiten



SUHLING  
TOOLING

Wie kann eine KI heutzutage genutzt werden?

1. Hardware + Software auf dem eigenen Schreibtisch
2. Im eigenen Rechenzentrum in Deutschland
3. Im fremden Rechenzentrum in Deutschland
4. Im fremden Rechenzentrum in der EU
5. Im fremden Rechenzentrum außerhalb der EU



Und dabei ist auf Folgendes zu achten:

DSGVO compliant?

GeschGehG compliant?

Und IT SiG 2.0 (BSIG) compliant?



## 2. Edge-Hardware (On-Device KI, komplett offline – auch im eigenen RZ/Edge) (1)

Beispiel 1 für eine lokale Hardwarelösung:

NVIDIA Jetson Orin Nano: <https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-orin/nano-super-developer-kit/>

Google Coral Dev Board: <https://coral.ai/products/dev-board/>

Aus der Praxis: Qualitätskontrolle in der Produktion oder Videoanalysen am Band ohne Internetverbindung.



DSGVO compliant? ☒ Ja – keine Übermittlung an Dritte, lokale Verarbeitung (Art. 5 Abs. 1 DSGVO).

GeschGehG compliant? ☒ Ja – keine externen Datenflüsse, Geheimnisse verbleiben intern.

IT-SiG 2.0 (BSiG) compliant? ☒ Ja – Edge-Systeme können nach Stand der Technik gehärtet und isoliert betrieben werden (§ 8a Abs. 1 BSiG).



## 2. Edge-Hardware (On-Device KI, komplett offline – auch im eigenen RZ/Edge) (2)

Beispiel 2 für eine lokale Hardwarelösung:

Zuerst werden fünf Mac Studios mit M2 Ultra-Chips und je 64 GB RAM über einen 10-Gigabit-Ethernet-Switch oder Thunderbolt-Kabel verbunden, um ein Netzwerk für die Clusterbildung zu schaffen. Anschließend installiert man auf jedem Gerät Python, das MLX-Framework und die EXO-Software von Exolabs, inklusive einer Systemkonfiguration für optimierte Leistung. Zum Abschluss startet man EXO auf allen Maschinen, wodurch der Cluster automatisch gebildet wird und leistungsstarke AI-Modelle wie Llama 3.1 405B verteilt ausgeführt werden können, mit Demonstration der Token-Generierung und Ressourcennutzung.

DSGVO compliant? ☒ Ja – keine Übermittlung an Dritte, lokale Verarbeitung (Art. 5 Abs. 1 DSGVO).

GeschGehG compliant? ☒ Ja – keine externen Datenflüsse, Geheimnisse verbleiben intern.

IT-SiG 2.0 (BSiG) compliant? ☒ Ja – Edge-Systeme können nach Stand der Technik gehärtet und isoliert betrieben werden (§ 8a Abs. 1 BSiG).



# 3. Lokale Desktop-KI (Ollama / LM Studio) nur Software



SUHLING  
TOOLING

- Beispiele:

- Ollama: ...ist eine kostenlose, open-source Plattform, die es ermöglicht, leistungsstarke große Sprachmodelle wie Llama, Gemma oder Mistral lokal auf dem eigenen Computer auszuführen, sodass Nutzer KI-Funktionen wie Textgenerierung, Chat oder Programmierhilfe datenschutzfreundlich und ohne Cloud-Abhängigkeit nutzen können.

- Link: <https://ollama.com/>

- LM Studio: ... ist eine benutzerfreundliche Softwareanwendung, die es ermöglicht, große Sprachmodelle wie gpt-oss, Qwen3, Gemma3 oder DeepSeek lokal auf dem eigenen Computer auszuführen, sodass Nutzer KI-Funktionen privat, kostenlos und ohne Abhängigkeit von externen Servern nutzen können.

- Link: <https://lmstudio.ai/>

- Praxis: Juristen oder Entwickler nutzen lokale LLMs ohne Cloud-Verbindung.

- DSGVO compliant? ☒ Ja – Daten bleiben unter eigener Kontrolle (Art. 4 Nr. 7 DSGVO).

- GeschGehG compliant? ☒ Ja – kein Abfluss von Vertraulichkeitsinformationen.

- IT-SiG 2.0 (BSiG) compliant? ☒ Ja – System kann mit Endpoint-Security & Patch-Management nach Stand der Technik betrieben werden.



# 4. Self-Hosted LLM-Serving im eigenen Rechenzentrum (RZ)



SUHLING  
TOOLING

Beispiele:

**vLLM:** vLLM ist eine open-source Bibliothek, die eine hochdurchsatzfähige und speichereffiziente Inferenz- und Serving-Engine für große Sprachmodelle (LLMs) bereitstellt, sodass Entwickler Modelle wie Llama, Mixtral oder LLaVA effizient auf verschiedener Hardware ausführen und deployen können, mit fortschrittlichen Features wie PagedAttention, kontinuierlichem Batching und Unterstützung für Quantisierung sowie verteilte Inferenz

Link: <https://github.com/vllm-project/vllm>

**Hugging Face TGI:** Text Generation Inference (TGI) ist ein leistungsstarkes, open-source Toolkit von Hugging Face, das die Bereitstellung und das Serving von großen Sprachmodellen (LLMs) wie Llama, Falcon, StarCoder oder BLOOM ermöglicht, um hochperformante Textgenerierung in Produktionsumgebungen zu realisieren, mit fortschrittlichen Features wie Tensor-Parallelismus, kontinuierlichem Batching, Token-Streaming, Quantisierung und optimierten Inferenzmechanismen wie Flash Attention und Paged Attention.

Link: → <https://huggingface.co/docs/text-generation-inference>

Praxis: „CompanyGPT“ auf eigener Infrastruktur mit Qdrant oder Milvus zur Vektorsuche.



- DSGVO compliant? ☒ Ja, wenn Logs und Zugriffe protokolliert (Art. 32).
- GeschGehG compliant? ☒ Ja, durch Zugriffskontrolle und Netzwerksegmentierung.
- IT-SiG 2.0 (BSiG) compliant? ☒ Ja – eigene RZ-Systeme unterliegen direkter technischer Kontrolle und können BSI-Grundschutz folgen.

# 5. On-Prem AI-Appliances / Private Cloud AI



SUHLING  
TOOLING

Beispiele:

**NVIDIA DGX Platform:** Die NVIDIA DGX Platform ist eine vollständig integrierte, für Enterprise-KI entwickelte Plattform, die spezialisierte DGX-Hardware, eine optimierte AI-Software-Stack und Services zu einer einheitlichen Umgebung für Entwicklung, Training und Betrieb anspruchsvoller KI-Modelle kombiniert – on-premises, in der Cloud oder hybrid.

Link: <https://www.nvidia.com/en-us/data-center/dgx-platform/>

**HPE Private Cloud AI:** HPE Private Cloud AI ist eine von HPE und NVIDIA entwickelte, schlüsselfertige Private-Cloud-Plattform, mit der Unternehmen generative KI-Workloads sicher, skalierbar und datensouverän auf einer vollständig integrierten, GPU-beschleunigten Infrastruktur betreiben können.

Link: <https://www.hpe.com/us/en/newsroom/press-release/2024/09/hewlett-packard-enterprise-introduces-one-click-deploy-ai-applications-in-hpe-private-cloud-ai.html>



**Praxis:** Großunternehmen betreiben komplette KI-Fabriken intern oder in Colocation.

DSGVO compliant? ☒ Ja, wenn TOMs (Art. 32 DSGVO) und AVV intern geregelt sind.

GeschGehG compliant? ☒ Ja. On-Prem verhindert Abfluss geschäftskritischer Modelle und Daten.

# 6. EU-Managed SaaS Praxisbeispiele (1)



SUHLING  
TOOLING

Beispiele aus einer Vielzahl von Anbietern:

- Langdock,
- mein GPT,
- Cancom Enterprise AI Suite,
- Pryvet

# 6. EU-Managed SaaS Langdock (2)



Beispiele aus einer Vielzahl von Anbietern:

Langdock: Langdock ist eine in Europa gehostete All-in-One-KI-Plattform für Unternehmen, die leistungsstarke KI-Tools, Assistenten, Prozessautomatisierung und Integrationen bietet – alles modellunabhängig, datenschutzkonform und flexibel für individuelle Workflows einsetzbar.

Link: <https://langdock.com/>

Während des Vortrags wird die Seite von Langdock gezeigt.

DSGVO compliant?  Grundsätzlich ja, da AV-Vertrag (Art. 28 DSGVO) und EU-Hosting vorhanden.

GeschGehG compliant?  Nur, wenn keine vertraulichen Inhalte in externe Modelle gegeben werden.

# 6. EU-Managed SaaS meinGPT (3)



Beispiele aus einer Vielzahl von Anbietern:

Mein GPT: meinGPT ist eine DSGVO-konforme KI-Plattform für Unternehmen und Teams, die den sicheren Einsatz verschiedenster KI-Modelle und Tools ermöglicht, individuelle Anwendungsfälle und Integrationen unterstützt und eine intuitive Einführung inklusive Workshops und On-Premise-Optionen bietet.

Link: <https://meingpt.com>

Während des Vortrags wird die Seite von meinGPT gezeigt.

DSGVO compliant?  Grundsätzlich ja, da AV-Vertrag (Art. 28 DSGVO) und EU-Hosting vorhanden.

GeschGehG compliant?  Nur, wenn keine vertraulichen Inhalte in externe Modelle gegeben werden.

# 6. EU-Managed SaaS Cancom (4)

Beispiele aus einer Vielzahl von Anbietern:

Die CANCOM Enterprise AI Suite ist für alle Anwendungsfälle, bei denen Standard-AI-Tools an ihre Grenzen stoßen. Sie bietet Unternehmen eine umfassende Plattform, um individuelle AI- und Advanced-Analytics-Lösungen zu realisieren. Dabei greifen wir auf ein bewährtes Framework zurück, das den Grundstein für all unsere AI-Projekte bildet. So unterstützen wir Sie von der ersten Idee bis zur produktiven Anwendung – angepasst an Ihre Infrastruktur- egal ob Cloud-, On-Premise- oder hybrid.

Link: <https://ai.cancom.de/enterprise-ai-suite/>

Während des Vortrags wird die Seite von Cancom gezeigt.

DSGVO compliant?  Grundsätzlich ja, da AV-Vertrag (Art. 28 DSGVO) und EU-Hosting vorhanden.

GeschGehG compliant?  Nur, wenn keine vertraulichen Inhalte in externe Modelle gegeben werden.

# 6. EU-Managed SaaS Pryvet (5)



SUHLING  
TOOLING

Beispiele aus einer Vielzahl von Anbietern:

Pryvet.ai ist eine KI-Plattform, die mittels Pseudonymisierung und strenger Datenschutzmechanismen Unternehmen den sicheren und DSGVO-konformen Einsatz moderner Large-Language-Models ermöglicht und sensible Daten effektiv schützt.

Link: <https://pryvet.ai/>

Vorstellung Pryvet durch Geschäftsführer Herrn Michael Witzenleiter!

DSGVO compliant?  Grundsätzlich ja, da AV-Vertrag (Art. 28 DSGVO) und EU-Hosting vorhanden.

GeschGehG compliant?  Nur, wenn keine vertraulichen Inhalte in externe Modelle gegeben werden.

# 7. EU-Souveräne Modell-APIs (Aleph Alpha, Mistral)



SUHLING  
TOOLING

Beispiele aus einer Vielzahl von Anbietern:

## **Aleph Alpha:**

Aleph Alpha bietet Unternehmen und öffentlichen Institutionen eine souveräne, transparente und erklärbare KI-Plattform mit individuellen, anpassbaren Lösungen für komplexe Wissensarbeit und höchste Anforderungen an Datenschutz, Datenhoheit und regulatorische Compliance.

Link: <https://aleph-alpha.com/>

## **Mistral AI:**

Mistral.ai ist ein französisches Unternehmen, das effiziente, leistungsstarke und modulare KI-Sprachmodelle und -Lösungen entwickelt, die sowohl offen verfügbar als auch für Unternehmen flexibel als API oder On-Premise nutzbar sind, mit Fokus auf Datensouveränität, Anpassungsfähigkeit und innovative Architekturansätze wie Mixtral.

Link: <https://mistral.ai/>

Praxis: APIs für eigene Anwendungen mit EU-Data Residency.

DSGVO compliant? ☒ Ja, wenn Nutzung innerhalb der EU bleibt und AVV vorliegt.

GeschGehG compliant? ☒ Bei gesicherten Schnittstellen und Verschlüsselung möglich.

# 8. EU Data Boundary Cloud-Angebote (z. B. Microsoft, Azure)



SUHLING  
TOOLING

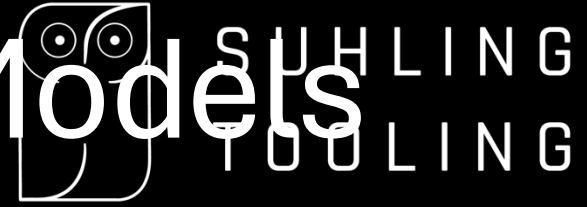
Beispiele:

- Microsoft EU Data Boundary: <https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb>
- Azure OpenAI (EU-Boundary): <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy>

Praxis: Nutzung von Copilot, SharePoint oder ChatGPT in EU-Clouds.

- DSGVO compliant?  Ja, da Microsoft Daten in der EU speichert (Art. 44 ff. DSGVO).  Jedoch möglicher Zugriff mittels Cloud Act.
- GeschGehG compliant?  Eingeschränkt – Microsoft hat administrativen Zugriff, daher Verschlüsselungspflicht.

# 9. Hyperscaler Foundation Models (AWS / Azure)



Beispiele:

**AWS Bedrock:** AWS Bedrock ist eine voll verwaltete Plattform von Amazon Web Services, die den einfachen, sicheren und skalierbaren Zugriff auf eine breite Auswahl leistungsstarker Foundation-Modelle verschiedener Anbieter ermöglicht, sodass Unternehmen generative KI-Anwendungen – wie Chatbots, Text-, Bild- oder Wissensdatenbank-Lösungen – mit eigenen Daten integrieren und ohne eigene Infrastruktur individuell anpassen und betreiben können.

Link: <https://aws.amazon.com/bedrock/>

**Azure OpenAI:** Azure OpenAI garantiert, dass Nutzerdaten wie Prompts, Ergebnisse und Trainingsdaten nicht zur Verbesserung der Modelle verwendet, nicht gespeichert oder für andere Kunden zugänglich gemacht werden, wodurch höchste Datenschutz- und Compliance-Anforderungen in der Microsoft Azure-Cloud erfüllt werden.

Link: <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy>

Praxis: Große Unternehmen binden generative KI in RAG-Workflows ein.

**RAG= Retrieval-Augmented Generation (Retrieval-verstärkte Generierung):** Retrieval (Abruf): Das System durchsucht zunächst eine Wissensdatenbank oder Dokumentensammlung nach relevanten Informationen zur Anfrage

**Generation (Erzeugung):** Ein Large Language Model (LLM) nutzt diese abgerufenen Informationen, um eine Antwort zu generieren

DSGVO compliant?  Möglich, bei AVV und EU-Region-Restriktion.  Jedoch möglicher Zugriff mittels Cloud Act.

GeschGehG compliant?  Abhängig von Datenart – sensible Informationen sollten pseudonymisiert werden.

# 10. Lokale Wissensbots (z. B. PrivateGPT, OpenWebUI)



SUHLING  
TOOLING

Beispiele:

PrivateGPT: <https://github.com/zylon-ai/private-gpt>

OpenWebUI + Qdrant/Milvus: <https://openwebui.com/>

Praxis: Interner Q&A-Bot über Unternehmensrichtlinien und Verträge, offline.

DSGVO compliant? ☒ Ja. Keine externe Verarbeitung, lokale Logs kontrollierbar.

GeschGehG compliant? ☒ Ja. Daten verbleiben vollständig im internen System.



# 11. Praxisbeispiele & Vergleich

Beispiele:

Jetson / Coral: lokale Qualitätskontrolle

LM Studio: vertrauliche Vertragsanalyse

Langdock: interne Chatbots für Sales/Support

Pryvet.ai: KI mit Pseudonymisierung

M365 Copilot (EU Data Boundary): Büroarbeit mit EU-Residenz. Jedoch möglicher Zugriff mittels Cloud Act.

DSGVO compliant? ☒ Bei korrekter Implementierung aller genannten Optionen (Art. 25 Privacy by Design).

GeschGehG compliant? ☒ Wenn Zugriffskontrollen, Geheimhaltungsrichtlinien und Verschlüsselung dokumentiert sind.



# 12. KI- Checkliste

Fragen vor jedem KI-Projekt:

- Wo werden Daten verarbeitet? (DSGVO Art. 30, 28)
- Wer hat Zugriff? (Art. 32, GeschGehG § 2)
- Werden Geheimnisse technisch geschützt (Verschlüsselung, Isolierung)?
- Gibt es AV-Verträge und Datenklassifizierungen?
- ...

Diese Checkliste kann beliebig auf weitere zu prüfende Themen erweitert werden.

# 13. Warum eine KI-Richtlinie? (1)



SUHLING  
TOOLING

Jedes Unternehmen und jede Organisation sollte eine **KI-Richtlinie** erstellen und veröffentlichen, um die strengen Vorgaben der **EU-KI-Verordnung** (AI Act) zu erfüllen, denn Verstöße können mit bis zu 35 Millionen Euro oder 7% des weltweiten Jahresumsatzes geahndet werden. Sowohl die KI-Verordnung als auch die ISO/IEC 42001:2023, das **KI-Managementsystem** liefern praxisnahe Leitlinien, wie verantwortungsvolle und rechtssichere KI-Prozesse gestaltet und Compliance-Risiken sowie ethische und rechtliche Fallstricke systematisch vermieden werden können. Diese Standards/Gesetze dienen als roter Faden für Transparenz, Nachvollziehbarkeit, Risikomanagement und klare Zuständigkeiten beim Einsatz von KI.

Bei der ISO/IEC 42001:2023 bieten die Normabschnitte in harmonisierter High Level Structure (HLS) eine ideale, systematische Orientierung, sodass beim Aufbau einer KI-Richtlinie sämtliche relevanten Themenfelder – von Führung und Planung über Risikomanagement bis zur kontinuierlichen Verbesserung – strukturiert und vollständig abgedeckt werden.

# 13. Warum eine KI-Richtlinie? (2)



SUHLING  
TOOLING

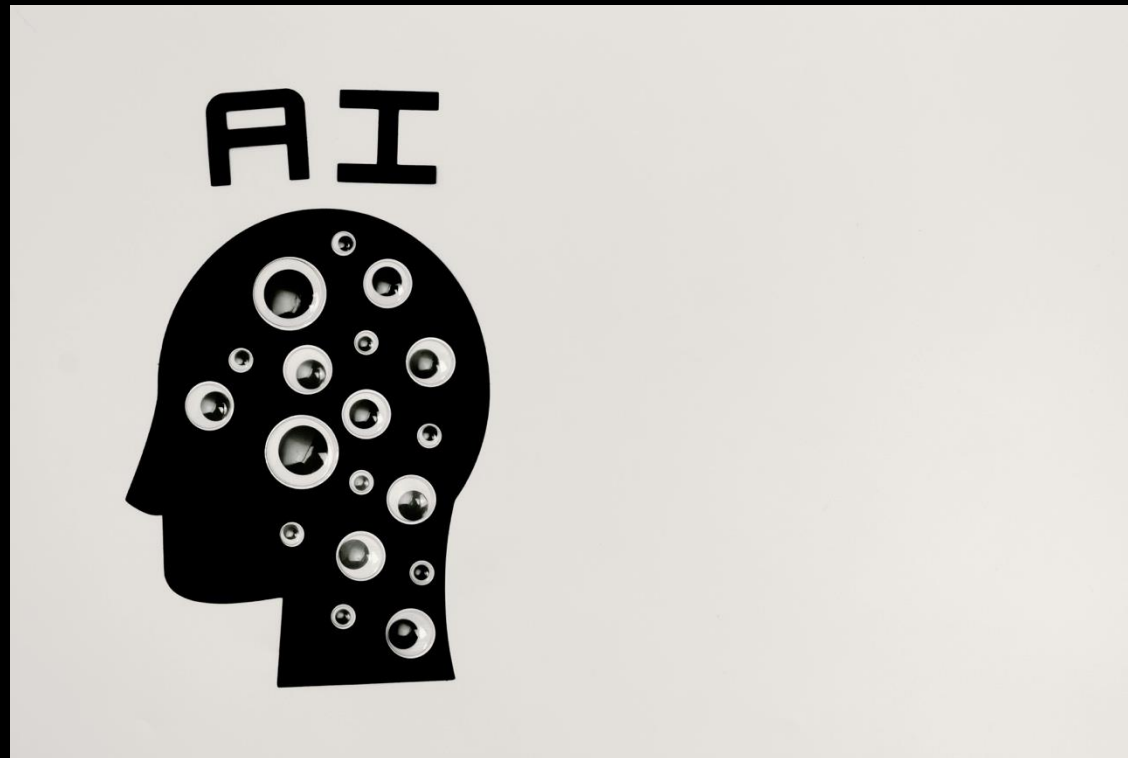
Liegt keine KI-Richtlinie vor, besteht die Gefahr, dass Beschäftigte aus Mangel an Vorgaben eigenständig KI-Tools mit privaten Konten und ohne Kontrolle nutzen. Dadurch entsteht **Schatten-IT, bzw. Schatten-KI**, bei der Unternehmensdaten unkontrolliert in externe Systeme gelangen können, was gravierende Risiken für Datenschutz, Informationssicherheit und Compliance nach sich zieht.

# 14. Fragen aus dem Plenum



SUHLING  
TOOLING

Ihre Fragen bitte!



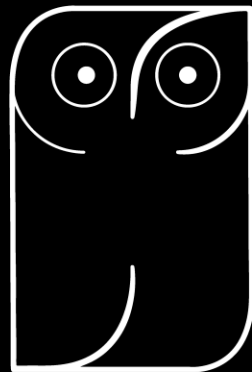


SUHLING  
TOOLING

# Vielen Dank!



@petersuhling



SUHLING  
TOOLING

# Urheberrechtshinweise



SUHLING  
TOOLING

Diese Unterlagen sind als Begleitmaterial zum Vortrag „DSGVO-konforme KI: Externe Lösungen für Ihr Unternehmen“ von suhling tooling GmbH, Peter Suhling gedacht und nicht zum Selbststudium geeignet.

Diese Unterlagen dienen ausschließlich des persönlichen Gebrauch der Vortragsteilnehmer. Alle Rechte an den Unterlagen, einschließlich der Übersetzung in fremde Sprachen bleiben dem Verfasser vorbehalten. Kein Teil dieses Werkes darf ohne schriftliche Genehmigung des Verfassers in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© Peter Suhling, Weinheim, suhling tooling GmbH, 2025

# Quellen

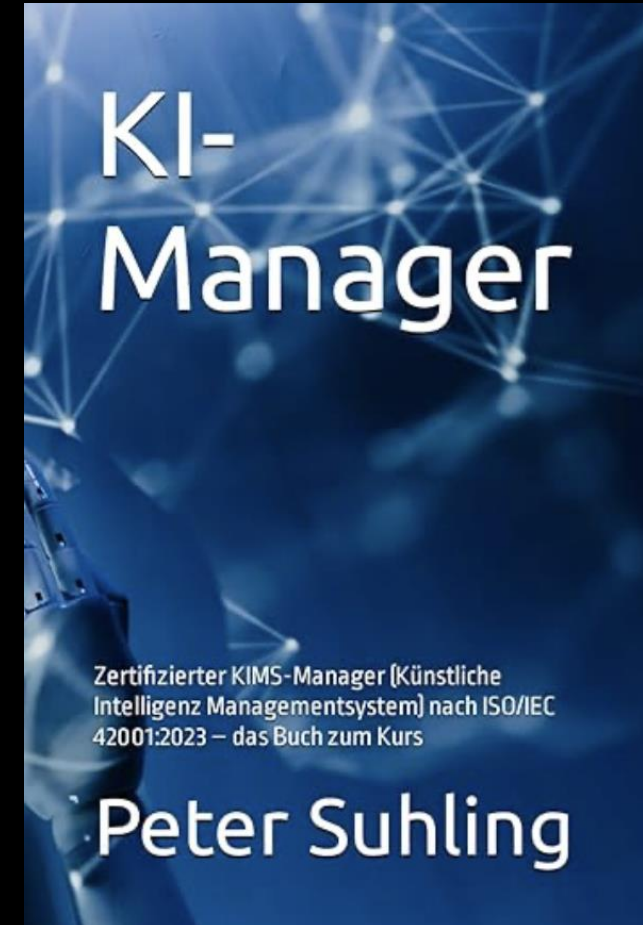


SUHLING  
TOOLING

- DSGVO, <https://dsgvo-gesetz.de>
- BDSG, <https://dsgvo-gesetz.de/bdsg/>
- KI-Verordnung (KIVO): <https://ai-act-law.eu/de/>
- ISO-Standards: <https://www.iso.org/home.html>
- Fortbildungen: <https://www.isaca.org>
- Bilderquellen: unplash, pexels, pixabay

# KI-Buchtipp, KI-Kurse

- Buch KI-Manager: <https://amzn.eu/d/1uLkd8w>
- Kurse zum Thema:





SUHLING  
TOOLING

# Lecture in englisch



SUHLING  
TOOLING

# GDPR-compliant AI: External solutions for your company

11th AI Regulars' Table Weinheim,  
ISACA Germany Chapter

Speaker: Peter Suhling

Publisher: suhling tooling GmbH

Hauptstraße 128, 69469 Weinheim,  
suhling.biz, suhlingtooling.com

Author: Peter Suhling

Version: 1.0

Lecture on 13 November 2025

# Agenda



SUHLING  
TOOLING

## Speaker introduction

1. Overview of current artificial intelligence (AI) implementation options
2. Edge hardware (on-device AI, completely offline – also in your own data centre/edge)
3. Local "desktop AI" (without internet)
4. Self-hosted LLM serving in your own data centre
5. On-prem AI appliances / private cloud AI
6. EU-managed SaaS (e.g. Langdock, Pryvet.ai)
7. EU-sovereign model APIs (Aleph Alpha, Mistral)
8. EU data boundary cloud offerings (e.g. Microsoft, Azure)
9. Hyperscaler foundation models (AWS / Azure)
10. Local knowledge bots (e.g. PrivateGPT, OpenWebUI)
11. Practical examples & comparison
12. AI checklist
13. Why an AI policy?
14. Questions from the floor

# Introduction Speaker Peter Suhling

Certified internal auditor ISO 9000 ff. Quality management - Dekra

Certified fundamentals in IT service management - TÜV SÜD

Certified data protection officer DSB-TÜV - TÜV SÜD

Certified data protection officer - udis Ulm

Certified ISMS Lead Auditor ISO 27001 – TÜV it/TÜV Nord

Accredited Certified Data Protection Auditor – DSZ – GDD and BvD

Revision ISO 9001:2015 and ISO 14001:2015 – TÜV SÜD

CISA - Certified Information Systems Auditor - ISACA

Accredited ISO 27001 Lead Auditor - TÜV SÜD, as well as other certification bodies

Certified KRITIS Auditor in accordance with the IT Security Catalogue pursuant to Section 11 (1a) EnWG - TÜV SÜD

Examination Chair of the Examination Board for the Additional Qualification in Quality Management for Business People - IHK Karlsruhe

Human Rights Officer - Environmental Institute

SzA Examiner (Attack Detection Systems) – TÜV

Accredited Compliance Lead Auditor ISO 37301 – TÜV

Accredited Lead Auditor ISO 27001 Automotive - TÜV SÜD  
#suhlingtooling



SUHLING  
TOOLING

**CDPSE** - Certified Data Privacy Solutions Engineer - ISACA

Certified according to the test procedure competence § 8a BSI Act - TÜV TRUST IT

TR Technical Reviewer Management Systems

Accredited ISO 9001 Lead Auditor - TÜV SÜD

Certified Cyber Security Practitioner - ISACA

Certified recognised IT expert - BISG e.V.

IT Compliance Manager – TÜV

Accredited TISAX Auditor – TÜV SÜD

Certified Internal + Supplier Auditor Occupational Health and Safety ISO 45001 – ifg

CDPSE – Certified Data Protection Solutions Engineer – ISACA

Certified ISO 9001 Lead Auditor – Advisera

Certified ISO 14001 Lead Auditor – Advisera

Certified ISO 45001 Lead Auditor – Advisera

Bachelor Professional / Certified Specialist in Office and Project Organisation – IHK

Certified AI Compliance Officer – TÜV

Certified AI Lead Auditor ISO/IEC 42001 – Treccert

Accredited AI Lead Auditor ISO/IEC 42001 – IAI, TÜV Austria



# 1. Overview of current artificial intelligence (AI) implementation options

How can AI be used today?

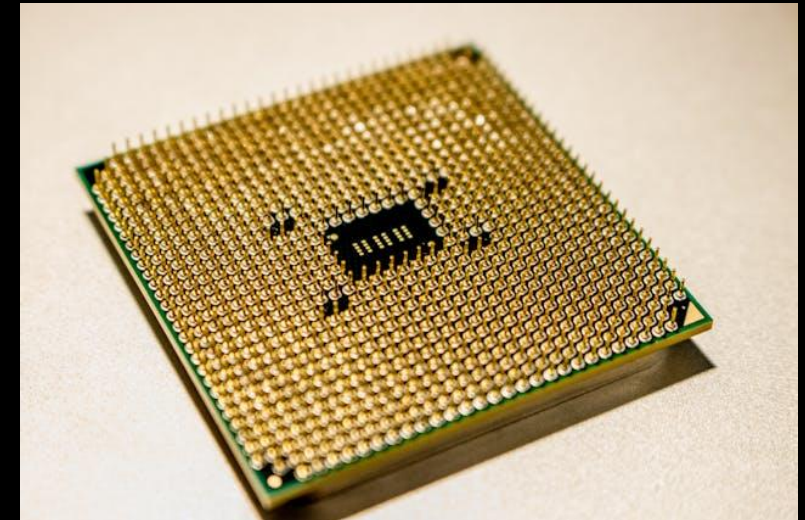
Hardware + software on your own desk

In your own data centre in Germany

In a third-party data centre in Germany

In a third-party data centre in the EU

In a third-party data centre outside the EU



And the following must be taken into account:

GDPR compliant?

GeschGehG compliant?

And IT SiG 2.0 (BSiG) compliant?



## 2. Edge hardware (on-device AI, completely offline – also in your own data centre/edge) (1)

Example 1 for a local hardware solution:

NVIDIA Jetson Orin Nano: <https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-orin/nano-super-developer-kit/>

Google Coral Dev Board: <https://coral.ai/products/dev-board/>

From practice: Quality control in production or video analysis on the assembly line without an internet connection.



GDPR compliant? ☒ Yes – no transfer to third parties, local processing (Art. 5(1) GDPR).

GeschGehG compliant? ☒ Yes – no external data flows, secrets remain internal.

IT-SiG 2.0 (BSiG) compliant? ☒ Yes – edge systems can be hardened and operated in isolation in accordance with the state of the art (Section 8a (1) BSiG).



## 2. Edge hardware (on-device AI, completely offline – also in your own data centre/edge)

Example 2 for a local hardware solution:

First, five Mac Studios with M2 Ultra chips and 64 GB RAM each are connected via a 10 Gigabit Ethernet switch or Thunderbolt cables to create a network for clustering. Next, Python, the MLX framework and Exolabs' EXO software are installed on each device, including a system configuration for optimised performance. Finally, EXO is launched on all machines, automatically forming the cluster and enabling powerful AI models such as Llama 3.1 405B to be run in parallel, demonstrating token generation and resource utilisation.

GDPR compliant? ☒ Yes – no transfer to third parties, local processing (Art. 5(1) GDPR).

GeschGehG compliant? ☒ Yes – no external data flows, secrets remain internal.

IT-SiG 2.0 (BSiG) compliant? ☒ Yes – edge systems can be hardened and operated in isolation in accordance with the state of the art (Section 8a(1) BSiG).



# 3. Local desktop AI (Ollama LM Studio) software only



SUHLING  
TOOLING

Examples:

Ollama: ...is a free, open-source platform that allows powerful large language models such as Llama, Gemma or Mistral to be run locally on your own computer, enabling users to utilise AI functions such as text generation, chat or programming assistance in a privacy-friendly manner and without cloud dependency.

Link: <https://ollama.com/>

LM Studio: ... is a user-friendly software application that allows large language models such as gpt-oss, Qwen3, Gemma3 or DeepSeek to be run locally on your own computer, enabling users to utilise AI functions privately, free of charge and without dependence on external servers.

Link: <https://lmstudio.ai/>

Practice: Lawyers or developers use local LLMs without a cloud connection.

GDPR compliant? ☒ Yes – data remains under your own control (Art. 4 No. 7 GDPR).

GeschGehG compliant? ☒ Yes – no leakage of confidential information.

IT-SiG 2.0 (BSIG) compliant? ☒ Yes – system can be operated with state-of-the-art endpoint security & patch management.



# 4. Self-Hosted LLM-Serving in our own data centre



## Examples:

**vLLM:** vLLM is an open-source library that provides a high-throughput and memory-efficient inference and serving engine for large language models (LLMs), enabling developers to efficiently run and deploy models such as Llama, Mixtral, or LLaVA on various hardware, with advanced features such as PagedAttention, continuous batching, support for quantisation, and distributed inference.

Link: <https://github.com/vllm-project/vllm>

**Hugging Face TGI:** Text Generation Inference (TGI) is a powerful, open-source toolkit from Hugging Face that enables the deployment and serving of large language models (LLMs) such as Llama, Falcon, StarCoder, or BLOOM to achieve high-performance text generation in production environments, with advanced features such as tensor parallelism, continuous batching, token streaming, quantisation, and optimised inference mechanisms such as Flash Attention and Paged Attention.

Link: → <https://huggingface.co/docs/text-generation-inference>



Practice: "CompanyGPT" on your own infrastructure with Qdrant or Milvus for vector search.

GDPR compliant? ☒ Yes, if logs and accesses are logged (Art. 32).

GeschGehG compliant? ☒ Yes, through access control and network segmentation.

IT-SiG 2.0 (BSIG) compliant? ☒ Yes – own data centre systems are subject to direct technical control and can follow BSI basic protection



# 5. On-Prem AI-Appliances / Private Cloud AI



SUHLING  
TOOLING

Examples:

**NVIDIA DGX Platform:** The NVIDIA DGX Platform is a fully integrated platform designed for enterprise AI that combines specialised DGX hardware, an optimised AI software stack and services into a unified environment for developing, training and operating sophisticated AI models – on-premises, in the cloud or hybrid.

Link: <https://www.nvidia.com/en-us/data-center/dgx-platform/>

**HPE Private Cloud AI:** HPE Private Cloud AI is a turnkey private cloud platform developed by HPE and NVIDIA that enables organisations to run generative AI workloads securely, scalably, and with data sovereignty on a fully integrated, GPU-accelerated infrastructure.

Link: <https://www.hpe.com/us/en/newsroom/press-release/2024/09/hewlett-packard-enterprise-introduces-one-click-deploy-ai-applications-in-hpe-private-cloud-ai.html>



Practice: Large enterprises operate complete AI factories internally

GDPR compliant? ☒ Yes, if TOMs (Art. 32 GDPR) and AVV are regulated internally.

GeschGehG compliant? ☒ Yes. On-premises prevents the outflow of business-critical models and data.

# 6. EU-Managed SaaS practical examples (1)



SUHLING  
TOOLING

Examples from a variety of providers:

- Langdock,
- my GPT,
- Cancom Enterprise AI Suite,
- Pryvet

# 6. EU-Managed SaaS Langdock (2)



Examples from a variety of providers:

Langdock: Langdock is a European-hosted all-in-one AI platform for businesses that offers powerful AI tools, assistants, process automation and integrations – all model-independent, data protection-compliant and flexible for use in individual workflows.

Link: <https://langdock.com/>

The Langdock website will be shown during the presentation.

GDPR compliant?  Basically yes, as there is an AV contract (Art. 28 GDPR) and EU hosting.

GeschGehG compliant?  Only if no confidential content is entered into external models.

# 6. EU-Managed SaaS meinGPT (3)



Examples from a variety of providers:

My GPT: meinGPT is a GDPR-compliant AI platform for companies and teams that enables the secure use of a wide variety of AI models and tools, supports individual use cases and integrations, and offers an intuitive introduction including workshops and on-premise options.

Link: <https://meingpt.com>

The meinGPT website will be shown during the presentation.

GDPR compliant?  Basically yes, as there is an AV contract (Art. 28 GDPR) and EU hosting.

GeschGehG compliant?  Only if no confidential content is entered into external models.

# 6. EU-Managed SaaS Cancom (4)



Examples from a variety of providers:

The CANCOM Enterprise AI Suite is designed for all use cases where standard AI tools reach their limits. It offers companies a comprehensive platform for implementing customised AI and advanced analytics solutions. We use a proven framework that forms the basis for all our AI projects. We support you from the initial idea to the productive application – adapted to your infrastructure, whether cloud, on-premise or hybrid.

Link: <https://ai.cancom.de/enterprise-ai-suite/>

The Cancom website will be shown during the presentation.

GDPR compliant?  Basically yes, as there is an AV contract (Art. 28 GDPR) and EU hosting.

GeschGehG compliant?  Only if no confidential content is entered into external models.

# 6. EU-Managed SaaS Pryvet (5)



Examples from a variety of providers:

Pryvet.ai is an AI platform that uses pseudonymisation and strict data protection mechanisms to enable companies to use modern large language models securely and in compliance with the GDPR, effectively protecting sensitive data.

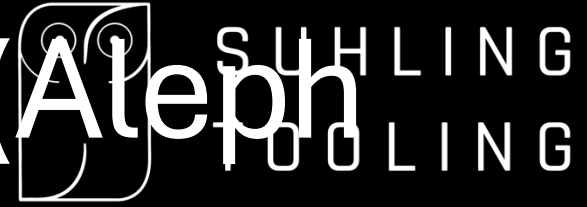
Link: <https://pryvet.ai/>

Presentation of Pryvet by Managing Director Mr Michael Witzel!

GDPR compliant?  Basically yes, as there is an AV contract (Art. 28 GDPR) and EU hosting.

GeschGehG compliant?  Only if no confidential content is entered into external models.

# 7. EU sovereign model APIs (Aleph Alpha, Mistral)



Examples from a variety of providers:

**Aleph Alpha:** Aleph Alpha offers companies and public institutions a sovereign, transparent and explainable AI platform with individual, customisable solutions for complex knowledge work and the highest requirements for data protection, data sovereignty and regulatory compliance.

Link: <https://aleph-alpha.com/>

**Mistral AI:** Mistral.ai is a French company that develops efficient, powerful and modular AI language models and solutions that are both openly available and flexible for companies to use as APIs or on-premise, with a focus on data sovereignty, adaptability and innovative architectural approaches such as Mixtral.

Link: <https://mistral.ai/>

Practice: APIs for own applications with EU data residency.

GDPR compliant? ☒ Yes, if use remains within the EU and an AVV is in place.

GeschGehG compliant? ☒ Possible with secure interfaces and encryption.

# 8. EU Data Boundary cloud offerings (i.e. Microsoft, Azure)



SUHLING  
TOOLING

Examples:

Microsoft EU Data Boundary: <https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb>

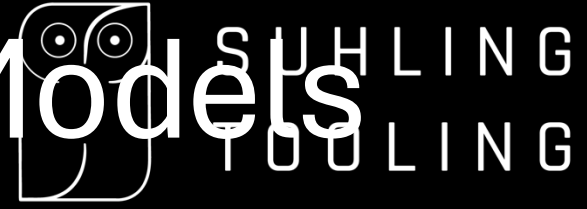
Azure OpenAI (EU Boundary): <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy>

Practice: Use of Copilot, SharePoint or ChatGPT in EU clouds.

GDPR compliant?  Yes, as Microsoft stores data in the EU (Art. 44 ff. GDPR).  However, access is possible via the Cloud Act.

GeschGehG compliant?  Limited – Microsoft has administrative access, therefore encryption is mandatory.

# 9. Hyperscaler Foundation Models (AWS / Azure)



Examples:

**AWS Bedrock:** AWS Bedrock is a fully managed platform from Amazon Web Services that provides easy, secure and scalable access to a wide range of powerful foundation models from various providers, enabling companies to integrate generative AI applications – such as chatbots, text, image or knowledge base solutions – with their own data and customise and operate them without their own infrastructure.

Link: <https://aws.amazon.com/bedrock/>

**Azure OpenAI:** Azure OpenAI guarantees that user data such as prompts, results and training data will not be used to improve the models, stored or made accessible to other customers, thereby meeting the highest data protection and compliance requirements in the Microsoft Azure cloud.

Link: <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy>

Practice: Large companies integrate generative AI into RAG workflows.

**RAG = Retrieval-Augmented Generation:** Retrieval: The system first searches a knowledge database or document collection for information relevant to the query.

Generation: A large language model (LLM) uses this retrieved information to generate a response.

GDPR compliant?  Possible, with AVV and EU region restriction.  However, access is possible via the Cloud Act.

GeschGehG compliant?  Depends on the type of data – sensitive information should be pseudonymised.  
#suhlingtooling [www.suhlingtooling.com](http://www.suhlingtooling.com)

# 10. Local knowledge bots (e.g. PrivateGPT, OpenWebUI)



SUHLING  
TOOLING

Examples:

PrivateGPT: <https://github.com/zylon-ai/private-gpt>

OpenWebUI + Qdrant/Milvus: <https://openwebui.com/>

Practice: Internal Q&A bot about company policies and contracts, offline.

GDPR compliant? ☒ Yes. No external processing, local logs controllable.

GeschGehG compliant? ☒ Yes. Data remains entirely within the internal system.

# 11. Practical examples & comparison



SUHLING  
TOOLING

Beispiele:

Jetson / Coral: lokale Qualitätskontrolle

LM Studio: vertrauliche Vertragsanalyse

Langdock: interne Chatbots für Sales/Support

Pryvet.ai: KI mit Pseudonymisierung

M365 Copilot (EU Data Boundary): Büroarbeit mit EU-Residenz. Jedoch möglicher Zugriff mittels Cloud Act.

DSGVO compliant? ☒ Bei korrekter Implementierung aller genannten Optionen (Art. 25 Privacy by Design).

GeschGehG compliant? ☒ Wenn Zugriffskontrollen, Geheimhaltungsrichtlinien und Verschlüsselung dokumentiert sind.



# 12. AI- Checkliste

Questions to ask before every AI project:

Where is the data processed? (GDPR Art. 30, 28)

Who has access? (Art. 32, GeschGehG § 2)

Are secrets technically protected (encryption, isolation)?

Are there AV contracts and data classifications?...

This checklist can be expanded as desired to include additional topics to be reviewed.



# 13. Why an AI-Policy? (1)

Every company and organisation should create and publish an AI policy in order to comply with the strict requirements of the EU AI Regulation (AI Act), as violations can be punished with fines of up to €35 million or 7% of global annual turnover. Both the AI Regulation and ISO/IEC 42001:2023, the AI management system, provide practical guidelines on how to design responsible and legally compliant AI processes and systematically avoid compliance risks and ethical and legal pitfalls. These standards/laws serve as a common thread for transparency, traceability, risk management and clear responsibilities when using AI.

In ISO/IEC 42001:2023, the standard sections in a harmonised High Level Structure (HLS) offer ideal, systematic guidance so that all relevant topics – from leadership and planning to risk management and continuous improvement – are covered in a structured and comprehensive manner when developing an AI policy.



# 13. Why an AI-Policy? (2)

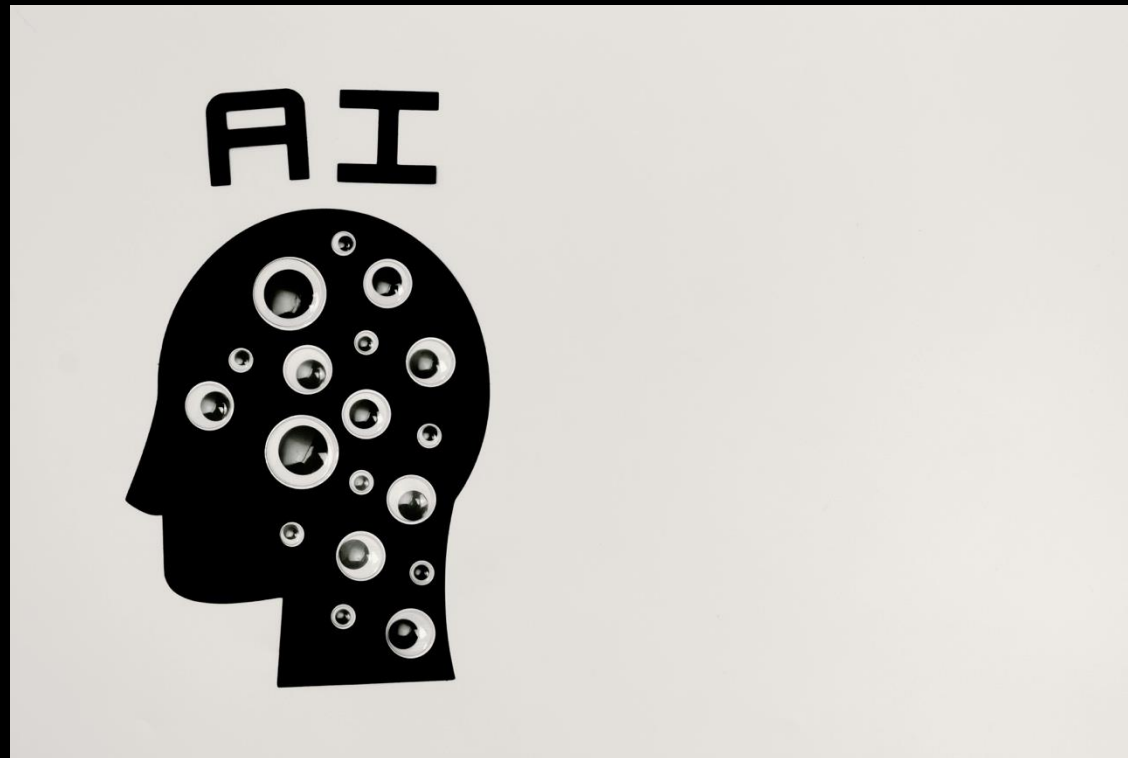
If there is no AI policy in place, there is a risk that employees will use AI tools independently with private accounts and without supervision due to a lack of guidelines. This creates shadow IT or shadow AI, where company data can enter external systems unchecked, posing serious risks to data protection, information security and compliance.



SUHLING  
TOOLING

# 14. Questions from the floor

Ihre Fragen bitte!



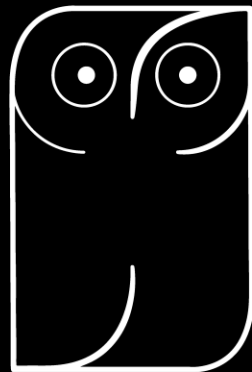


SUHLING  
TOOLING

# Thank you!



@petersuhling



SUHLING  
TOOLING

# Urheberrechtshinweise



SUHLING  
TOOLING

These documents are intended as accompanying material for the presentation "GDPR-compliant AI: External solutions for your company" by suhling tooling GmbH, Peter Suhling, and are not suitable for self-study.

These documents are for the personal use of the presentation participants only. All rights to the documents, including translation into foreign languages, remain with the author. No part of this work may be reproduced or processed, duplicated or distributed in any form (photocopy, microfilm or any other method), including for teaching purposes, without the written permission of the author.

© Peter Suhling, Weinheim, suhling tooling GmbH, 2025

# Quellen



SUHLING  
TOOLING

- GDPR, <https://dsgvo-gesetz.de>
- BDSG, <https://dsgvo-gesetz.de/bdsg/>
- AI Regulation (KIVO): <https://ai-act-law.eu/de/>
- ISO standards: <https://www.iso.org/home.html>
- Training courses: <https://www.isaca.org>
- Image sources: unplash, pexels, pixabay

# AI book recommendation, AI courses

- Book KI-Manager: <https://amzn.eu/d/1uLkd8w>
- Courses on the topic :

