August 2025 | Zum Datenschutz aufgefallen

Information zum (Weblink)
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in)*,

Datenschutz → einfach praktisch hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank(er), der Aufwand gering und mit (der) Sicherheit mehr Zeit gewonnen. Datenschutz schafft Vertrauen und ist eine Grundlage für nachhaltigen Erfolg.

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbstständige, Gewerbetreibende und KMU.

Sprechen wir!

Vielen Dank für Ihr Interesse

PS: Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist, oder kontaktieren Sie mich gerne.

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1a

Standard-Datenschutz-Modell
übersichtlich zusammengefasst
11 Seiten

Standard-Datenschutz-Modell
Datenschutzkonferenz DSK
78 Seiten

Datenschutz-Grundverordnung
auf dejure.org

Bundesdaten-schutzgesetz
auf dejure.org

Das SDM [*der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)*] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die technischen / organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Juristen und Informatiker für die Verantwortlichen und Datenschutzpraktiker zu finden. | Aktuell: SDM Version 3.1a (05/2025) Änderung Logo, einzelne grafische Darstellungen, keine inhaltlichen Änderungen | Letzter Maßnahmenkatalog 11/2021: Nr.51 „Zugriff auf Daten, Systeme und Prozesse regeln."

2. Zum Datenschutz

a) Künstliche Intelligenz (KI oder AI) und der Datenschutz

Es zeichnen sich steigenden Nutzerzahlen bei allen KI-Tools ab. Jedoch bietet die Nutzung nicht nur Vorteile (wie immer), sondern auch Nachteile. Die Integration in tägliche Arbeitsabläufe bieten das Potenzial für unbefugte Weitergabe, Missbrauch und Offenlegung von internen und/oder geschützten Firmendaten und personenbezogenen Daten. Im Blog von Incogni, laut Süddeutscher Zeitung ein automatisierter Service von Surfshark mit dem Ziel, persönliche Daten aus Datenbanken von Datenbrokern zu löschen[1], werden verschiedene KI-Modelle auf ihre Datenschutzfreundlichkeit und Fähigkeiten analysiert[2]. Zitat:

1 *Quelle Süddeutsche Zeitung: „Was ist der Datenlöschdienst Incogni?"*
2 *Quelle Incogni | blog: „Gen AI and LLM Data Privacy Ranking 2025.."*

„Obwohl diese Tools die Produktivität steigern können, sind sich die meisten Nutzer der komplexen Datenschutzprobleme hinter den Kulissen nicht bewusst.“

Einer Analyse unterzogen wurden ChatGPT von OpenAI, Meta AI, Gemini von Google, Copilot von Microsoft, Grok von xAI, Claude von Anthropic, Pi AI von Inflection AI, das französische Modell Le Chat von Mistral AI und das chinesische KI-Modell DeepSeek.

(1) Die vorderen Plätze:

Le Chat verletzt demnach am wenigsten die Privatsphäre seiner Nutzer. Das französische KI-Modell ist im Ranking dicht gefolgt von ChatGPT auf Platz zwei.

(2) Die hinteren Plätze:

Die hinteren Plätze in Bezug auf Datenschutz belegen die große Techkonzerne Google Gemini und Microsoft Copilot mit Schlusslicht Meta AI.

(3) Beispiel: Datenschutzrisiken von Microsoft 365 Copilot

In einem Fachbeitrag hat sich „Dr. Datenschutz“ (bzw. intersoft consulting services) damit auseinandergesetzt[3]. Die Kernpunkte:

- Die KI gestützte Assistenzfunktion ist gleich in die Office-Umgebung integriert, um durch Analyse die tägliche Arbeit zu erleichtern und wie ein Produktivitätsschub zu wirken.
- Neben der klassischen ChatGPT Funktion hat der Copilot zusätzlich Zugriff auf die Unternehmensdaten, mit der Möglichkeit Inhalte über verschiedene Anwendungen hinweg zu verarbeiten.
- Dabei ist die Entscheidungsfindung und die mögliche Verarbeitung zu Microsofts eigenen Zwecken intransparent. Durch die fehlende Transparenz ist es auch schwierig eine Rechtsgrundlage für die Verarbeitung nach DSGVO zu finden.
- Wird das Web-Plugin (Bing-API) aktiviert, wird mit den Inhalten auf das Web zugegriffen. Wie, warum und mit welchen Schutz bleibt intransparent.
- Copilot hat Zugriff auf alle Inhalte, auf die auch der Nutzer einen Zugriff hat (Mail, Kalender, Ordner, Dokumente u. ä.). Es fehlt also ein klar definiertes Berechtigungskonzept.

(4) KI-Trainingsdaten mit personenbezogenen Inhalten gefunden

T3n berichtet von sensiblen Daten im größten öffentlichen KI-Trainingsset[4]. Obwohl Forscher erst 01 % der Daten in einem der größten Open-Source-Trainingsdatensätze für KI-Bildgeneratoren untersuchen konnten, fanden sie Millionen von Bildern aus Reisepässen, Ausweisen, Kreditkarten, Geburtsurkunden und anderen Dokumenten, die personenbezogenen Daten enthalten. Zitat:

„Laut William Agnew, Postdoktorand im Bereich KI-Ethik an der Carnegie Mellon University und Mitautor der Studie, lässt sich daraus der (alte bekannte) *Schluss ziehen, dass ‚“alles, was man online stellt, gesammelt werden kann und wahrscheinlich auch schon gesammelt wurde’. Die Forschenden fanden Tausende Fälle nachweisbar korrekter Privatdokumente.“*

Das ist die andere Seite der KI-Modelle. Ich denke, die Nutzung schützt nicht vor der Verletzung von Schutzrechten Dritter (z. B. Daten- oder Urheberrechtsschutz u. ä.). Genauso könnten eigen Daten von Dritten fälschlicherweise verwendet werden.

b) Einsatz von KI im Unternehmen

Laut einer Ifo – Studie aus Juni 2025[5] setzten deutsche Firmen zunehmend auf KI. In 41 % der Unternehmen ist KI bereits im Einsatz. 19 % planen den Einsatz in den kommenden Monaten. Laut einer GOLEM-Studie[6] schaffen allerdings nur wenige Firmen die mit KI gesetzten Ziele (z. B. Umsatzwachstum) zu erreichen. Das liegt laut Studie weniger an der Qualität der Tools noch an den regulatorischen Beschränkungen. Es ist vielmehr die Art und Weise wie die Integration erfolgt.

3 *Quelle. Dr. Datenschutz. „Datenschutzrisiken von Copilot für Microsoft 365“*
4 *Quelle t3n: „Forscher finden sensible Daten in einem der größten öffentlichen KI-Trainingssets“*
5 *Quelle Ifo Institut „Unternehmen setzten immer stärker auf künstliche Intelligenz“*
6 *Quelle GOLEM: „KI-Millionen verpuffen“*

Kontraproduktiv ist der Studie nach, dass mehr als die Hälfte des KI-Budgets in den Unternehmen in Sales- und Marketing-Tools gesteckt werde. Dabei ergebe sich der größte Gewinn, wenn einfache Bürotätigkeiten automatisiert würden. Damit ließen sich externe Dienstleistungen und Agenturen einsparen, interne Prozesse verschlanken und mehr Zeit für den Vertrieb gewinnen.

(1) Fazit einer Studie:

Unternehmen sollten eher auf extern entwickelte KI-Tools von darauf spezialisierten Anbietern setzen, als auf selbst entwickelte Lösungen. Bei Ersteren lag die Erfolgsquote immerhin bei 2/3, bei Letzteren nur bei 1/3.

(2) Die bessere, europäische Antwort zu KI

Und das es Europa sogar besser kann, zeigt der FOCUS-Online in seinem Artikel „KI-Wettstreit“[7]. Ich zitiere:

(2.1) Wer ist Mistral

„Sie nennen sich die französische Antwort auf OpenAI. Doch Mistral AI ist mehr als das: Es ist der Beweis, dass Europa im KI-Rennen nicht nur mitspielen, sondern die Regeln neu schreiben kann. Von null auf demnächst zehn Milliarden Dollar Bewertung innerhalb von zwei Jahren lautet ihre Bilanz. Fast 400 Mitarbeiter. Frankreichs beliebteste KI-App.“

(2.2) Was ist Mistral

„Während Konkurrent OpenAI seine Modelle wie ein Staatsgeheimnis hütet, macht Mistral das genaue Gegenteil: Opern-Source-first nennt sich die Methode. Viele Mistral-KI-Modelle sind frei verfügbar, was eine Kampfansage an die Geheimniskrämer im Silicon Valley ist und gleichzeitig eine Strategie, um Entwickler und Kunden, die es hassen, nicht eingeweiht zu sein, auf die eigene Seite zu ziehen.“

(2.3) Datenschutz statt Datenklau

„Die Franzosen bauen unter der strengen EU-Regulierung eine souveräne KI-Infrastruktur auf. Ihr Versprechen: Europäische Daten bleiben in Europa. Die Strategie zahlt sich aus.“

Neben der interessanten Information zu Mistral sollte dies nur ein Hinweis sein, sich beim ersten Einsatz von KI an einen externen Dienstleister zu wenden, auch wenn es am Anfang etwas teurer ist, gespart wird dann am langen Ende.

3. Zur Datensicherheit

a) BSI zu KI Systemen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) leistet Grundlagenforschung und entwickelt bedarfsorientierte wie praxisnahe Anforderungen, Prüfkriterien und Prüfmethodologien, um den Einsatz von KI zum Wohle der Allgemeinheit sicher zu gestalten. Ausführliche Informationen finden Sie auf der Webseite des BSI, die in der Fußleiste verlinkt ist[8].

Enthalten ist auch ein Kriterienkatalog für vertrauenswürdige KI-Systeme im Finanzsektor, der auch zur Orientierung in anderen Sektoren dienen kann und sich an der KI – Verordnung der EU orientiert. Weiter interessant sind auch die Qualitätskriterien für Trainingsdaten im KI – Lebenszyklus.

Ich muss allerdings gestehen diese Dokumente nicht alle selbst gelesen zu haben, sondern mich auf die Empfehlung eines IT-Spezialisten dabei verlasse.

4. Zu angrenzenden Themen

a) Paypal aber sicher[9]

In dem verlinkten Beitrag wird auf die aktuellen Probleme (Datenleck, Lastschriftenblockade) von Paypal eingegangen. Zu den Schutzmaßnahmen gehört – genau – 2-Faktor-Authentisierung beim Login, dann „klappt es auch problemlos mit dem bezahlen. 😉

Bei Bedarf, einfach mal sprechen!

7 Quelle FOCUS-Online: „KI-Wettstreit: Mistral vs. OpenAI: Wie drei europäische Forscher das Silicon Valley herausfordern!“
8 Quelle BSI: „Künstliche Intelligenz“
9 Quelle tagesschau.de: „Wie sicher ist PayPal als Zahlungsmethode?“