WHITEPAPER

Datenschutz-Guide für Künstliche Intelligenz

Das müssen Unternehmen jetzt wissen

DATENSCHUTZ EXPERTE.DE
Ein Service der Proliance GmbH

Künstliche Intelligenz bietet Unternehmen viele Vorteile – die Frage ist: Wie lassen sich KI-Anwendungen, die Algorithmen und maschinelles Lernen implementieren, verantwortungsbewusst im Alltag nutzen? Und wie sicher sind sensible Daten in einer KI-geprägten Welt? Wir fassen wichtige Positionen von Datenschützern und ihre Empfehlungen zusammen und wagen einen Blick in die Zukunft.

1 Künstliche Intelligenz und der Datenschutz

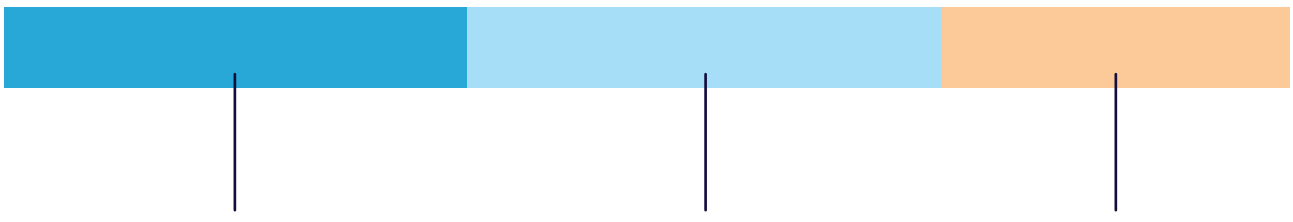
Seit Monaten beschäftigen sich Verbraucher, Unternehmen, Datenschützer und die Europäische Union mit Künstlicher Intelligenz (KI). Die Algorithmen, auf denen KI-Modelle basieren, werden immer besser darin, **menschliche Intelligenz zu simulieren** und Texte, Bilder, Videos oder sogar Stimmen zu generieren, die menschlichen Kreationen immer ähnlicher werden.

Unternehmen nutzen schon seit Jahren die Fähigkeiten von KI, um zum Beispiel Daten im Marketing einfacher zu analysieren oder Maschinenzustände zu überwachen und Wartungen vorausschauend zu planen. Mit der Veröffentlichung von ChatGPT hat die KI-Evolution einen Sprung nach vorn gemacht.

Seitdem wird immer deutlicher, welches Potenzial in KI-Modellen schlummert. Gleichzeitig zeigt sich, welche Gefahren von Algorithmen ausgehen, die in kurzer Zeit immer größere Datenmengen verarbeiten und Videos und Fotos kreieren können, die täuschend echt wirken.

Wie nutzen Unternehmen KI und was sind die Herausforderungen?

Das Institut für angewandte Arbeitswissenschaft (ifaa) hat 2022 eine Studie zum Stand des KI-Einsatzes in kleinen, mittleren und großen produzierenden Unternehmen und den sich daraus ergebenen Chancen und Herausforderungen durchgeführt.



36 %
gaben an, KI bereits zu nutzen

37 %
gaben an, dass KI in Planung ist

27 %
verneinten auch die Planung

Quelle: „ifaa-Studie: Künstliche Intelligenz in produzierenden Unternehmen“

36 Prozent der Befragten gaben an, KI bereits zu nutzen, weitere 37 Prozent planen den Einsatz bereits. Als Gründe nannten die KI-Befürworter unter anderem die Möglichkeit, den Fachkräfteengpässen entgegenzuwirken, Prozesse effizienter zu gestalten und ihren Angestellten mehr Zeit für interessante Arbeitsaufgaben zu geben.

Als wichtigsten Vertrauensfaktor für KI gaben 47 Prozent der Befragten menschliche Aufsicht und Kontrolle an. Darüber hinaus sorgen Zuverlässigkeit und Manipulationsfreiheit von KI-Systemen und der Schutz von personenbezogenen Daten dafür, dass Menschen in produzierenden Unternehmen einer KI vertrauen.

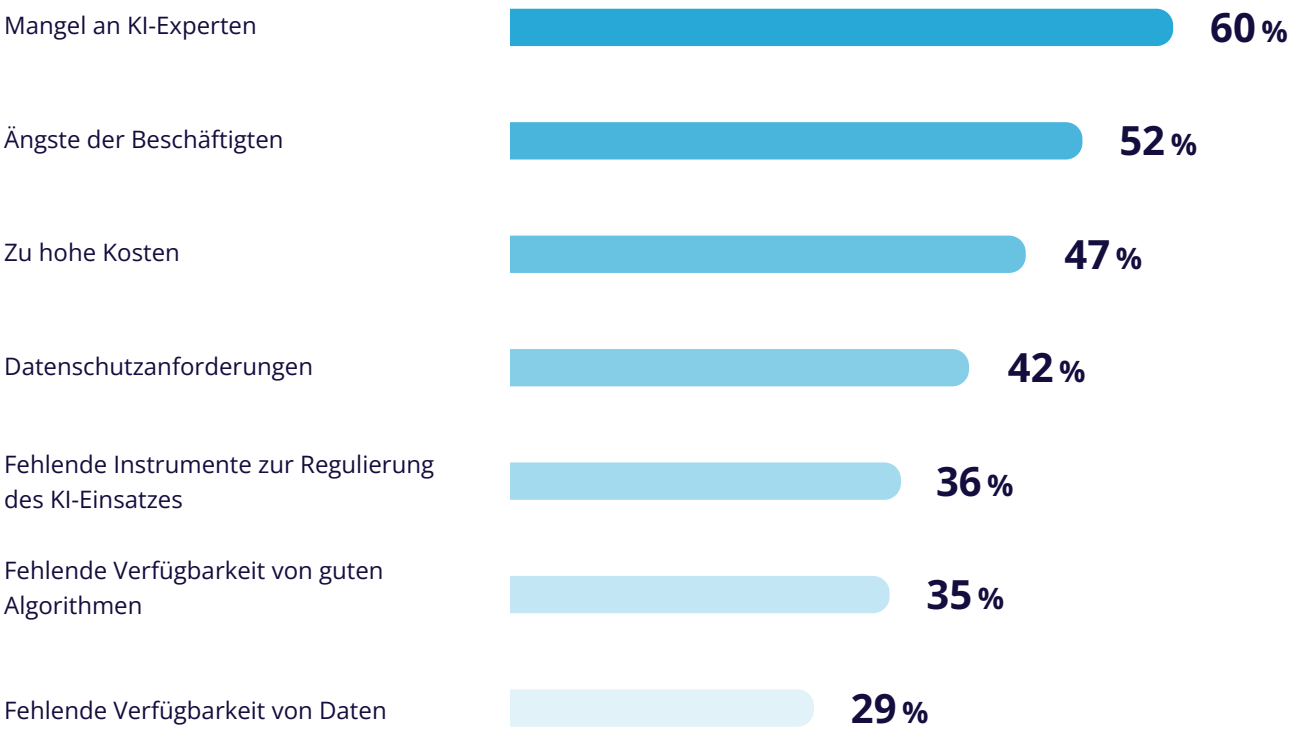
Der Datenschutz ist gleichzeitig allerdings auch eine der **Einstiegshürden** bei der Einführung von KI-Systemen. Denn neben einem Mangel an KI-Expertise, Ängsten der Beschäftigten und zu hohen Kosten sind für 42 Prozent der Befragten die Datenschutzanforderungen ein großes oder sehr großes Hindernis.

42%

gaben Datenschutzanforderungen als großes oder sehr großes Hindernis für die Einführung von KI an

Quelle: „ifaa-Studie: Künstliche Intelligenz in produzierenden Unternehmen"

Die größten Hindernisse für die Einführung von KI-Systemen



Quelle: „ifaa-Studie: Künstliche Intelligenz in produzierenden Unternehmen"

2 Das sagen Datenschützer zum KI-Einsatz in Unternehmen

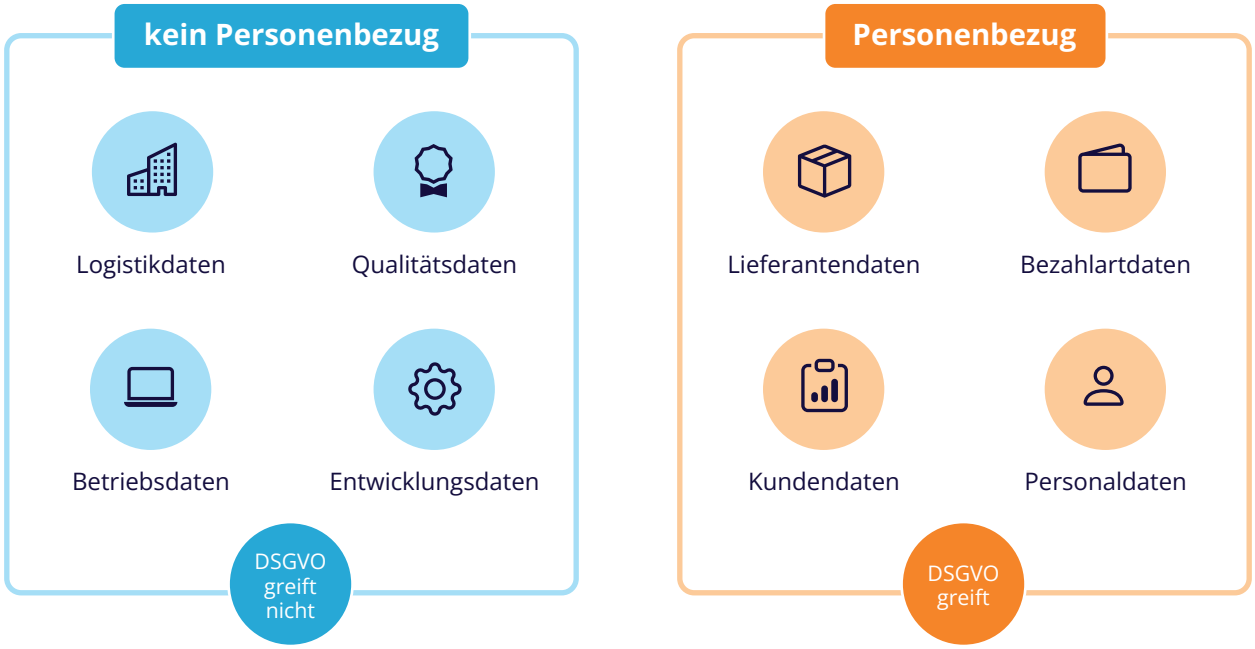
Datenschützer in ganz Europa beschäftigen sich schon seit einiger Zeit mit den datenschutzrechtlichen Aspekten von Künstlicher Intelligenz. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg (LfDI BW) hat Ende 2023 ein **Diskussionspapier** veröffentlicht, das Unternehmen beim Einsatz von KI unterstützen soll.

Das Papier vermittelt Überblickswissen zu Rechtsgrundlagen und bietet Leitfragen für die rechtliche Bewertung von Einsatzszenarien. Neben Vorgaben der DSGVO wurde auch die EU-Verordnung zur Festlegung von Vorschriften für Künstliche Intelligenz (KI-Verordnung oder englisch AI Act) berücksichtigt.

Wann sind Daten personenbezogen?

Um datenschutzrechtlich relevante Vorgänge im Zusammenhang mit KI bewerten zu können, müssen Unternehmen unter anderem klären, ob die in KI-Systemen verarbeiteten Daten einen **Personenbezug** haben.

Mit der Frage, welche Daten personenbezogen und damit besonders sensibel sind und welche Daten unbedenklich in KI-Systemen genutzt werden können, hat sich auch die Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik der Plattform Lernende Systeme in ihrem Whitepaper „Datenschatz für KI nutzen, Datenschutz mit KI wahren“ beschäftigt.



Quelle: Whitepaper „Datenschutz für KI nutzen, Datenschutz mit KI wahren“ - Plattform Lernende Systeme

Wann werden personenbezogene Daten verarbeitet?

Beim Datenschutz in KI-Systemen spielt neben der Art der Daten auch der **Zeitpunkt der Datenverarbeitung** eine Rolle. Laut LfDI BW gibt es fünf mögliche Phasen der Datenverarbeitung bei KI-Systemen, die datenschutzrechtlich unterschiedlich zu bewerten sind:

- Sammeln von Trainingsdaten
- Verarbeiten von Daten für das KI-Training
- Bereitstellen von KI-Anwendungen
- Nutzen von KI-Anwendungen
- Nutzen von KI-Ergebnissen

Die Schwierigkeit für Unternehmen besteht laut der Plattform Lernende Systeme darin, dass bei der Erhebung von Daten oft noch nicht klar ist, **welche Datenpunkte** konkret verwendet werden sollen. Ohne einen festgelegten Zweck zum Zeitpunkt der Erhebung ist es für Unternehmen schwierig, eine datenschutzkonforme und zulässige Verarbeitung von personenbezogenen Daten bei der weiteren Nutzung der KI sicherzustellen.

Wer ist für den Datenschutz verantwortlich?

Da Unternehmen in der Regel KI-Modelle von Drittanbietern nutzen, ist außerdem die **Verantwortlichkeit für den Datenschutz** zu klären.

Dabei könnte

- eine **Auftragsverarbeitung** vorliegen, wenn der Drittanbieter eines KI-Systems personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen innerhalb seines Systems verarbeitet und diese nicht für eigene Zwecke wie bspw. das Training oder die Weiterentwicklung der KI selbst nutzt
- eine **gemeinsame Verantwortung** vorliegen, wenn gemeinsame Zwecke an der Verarbeitung verfolgt und die Mittel hierfür (zum Beispiel das System) gemeinsam festgelegt werden

Welche Art der Verantwortlichkeit beim Einsatz eines KI-Systems vorliegt ist jedoch grundsätzlich im Einzelfall zu bewerten und kann nicht pauschal von einem System auf das andere übertragen werden.

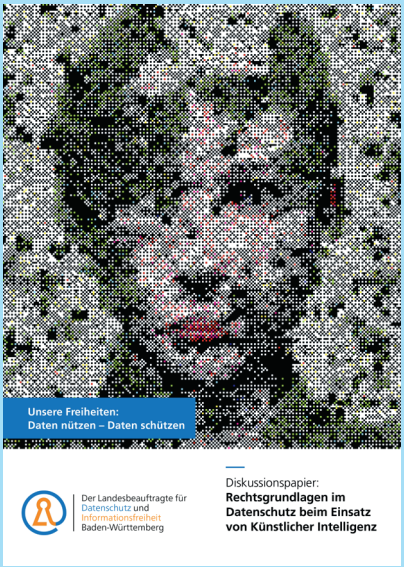
Auf welche Rechtsgrundlage kann sich der Verantwortliche stützen?

Will ein Unternehmen personenbezogene Daten in einer KI-Anwendung verarbeiten, so wird eine entsprechende **Rechtsgrundlage** hierfür benötigt.

- Eine **Einwilligung** käme als Rechtsgrundlage in Frage. Zu beachten wäre, dass diese jederzeit widerrufbar ist und eine Verarbeitung somit leicht einstellbar sein muss.
- Die **Vertragsdurchführung** käme gerade in solchen Konstellationen in Frage, in welchen die Nutzung der KI klarer Vertragsbestandteil oder als Mittel zur Erfüllung vertraglicher Zwecke festgelegt wurde (zum Beispiel 24/7-Kundensupport). Jedoch deckt diese Rechtsgrundlage allein oftmals nicht alle Nutzungszwecke ab.
- Eine weitere Option wäre das **berechtigte Interesse** an der Datenverarbeitung, welches zum Beispiel besteht, wenn es um die Optimierung von internen Prozessen mithilfe von KI geht. Wichtig ist es, die Interessen der Betroffenen mit denen des Unternehmens vorsichtig abzuwägen und hierbei sowohl den Umfang als auch die Notwendigkeit der Verarbeitung zur Erreichung der Interessen zu berücksichtigen.

Insgesamt stellt Art. 6 Abs. 1 Buchst. f DS-GVO aufgrund des offenen Tatbestands für die meisten Verarbeitungsprozesse im KI-Kontext eine besonders geeignete Rechtsgrundlage dar. Aufgrund der obligatorischen Interessenabwägung kann die Norm allerdings nur bedingt eine Rechtssicherheit vermitteln, da es stets erforderlich sein wird, den konkreten Einzelfall umfassend zu bewerten.

Quelle: Whitepaper „Datenschutz für KI nutzen, Datenschutz mit KI wahren" - Plattform Lernende Systeme



Das ganze Diskussionspapier lesen

3 Hilfreiche Checklisten von Datenschutzbeauftragten

Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit hat eine **Checkliste für den Einsatz von Chatbots** wie ChatGPT, Luminous oder Gemini veröffentlicht. war sind die Tools in vielen Einrichtungen bereits Teil des Arbeitsalltags geworden, allerdings fehlen oft verbindliche Nutzungsvorgaben.

Datenschutzrisiken ergeben sich unter anderem aus der Tatsache, dass viele Sprachmodelle in einer Cloud betrieben werden und von mehreren Unternehmen genutzt werden. Damit besteht die Gefahr, dass Geschäftsgeheimnisse an die Öffentlichkeit geraten. Ein weiteres Risiko sei die unzulässige Verarbeitung personenbezogener Daten. Die Checkliste aus Hamburg soll Unternehmen und Behörden als Leitfaden zur datenschutzkonformen Nutzung von Chatbots dienen.

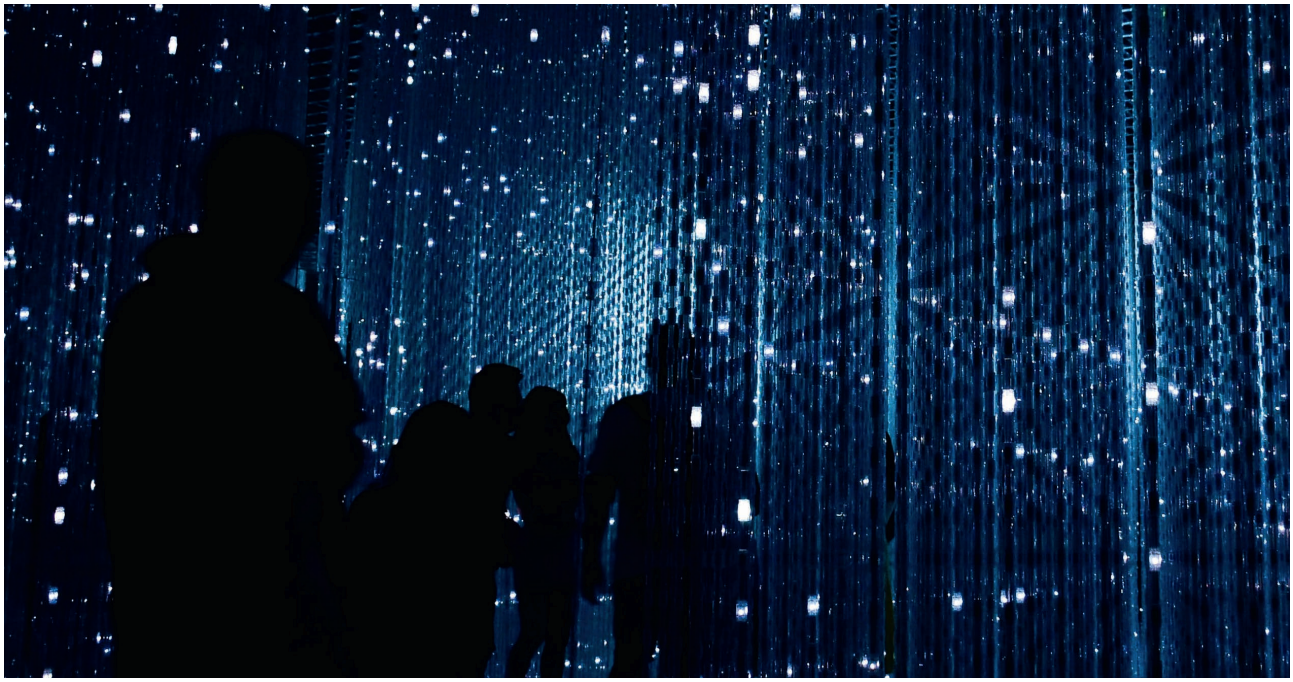
Lese-Tipp: Zur Checkliste aus Hamburg

Eine besonders **umfangreiche Checkliste für KI** hat das Bayerische Landesamt für Datenschutz (BayLDA) veröffentlicht. Nach einer allgemeinen Einordnung des KI-Themas finden Unternehmen eine Checkliste für das Training von KI-Modellen, die Bewertung von KI-Risiken und für den Einsatz einer KI-Anwendung.

Lese-Tipp: Zur BayLDA-Checkliste

Auszug aus der BayLDA-Checkliste: Risikomodell erstellen

Laut dem BayLDA müssen sich Unternehmen, die personenbezogene Daten für die Erstellung von KIModellen oder in KI-Anwendungen verwenden, der datenschutzrechtlichen Risiken bewusst sein und entsprechende Maßnahmen ergreifen, um diese Risiken einzudämmen.



Diese Maßnahmen sind im Sinne der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO durch eine geeignete Dokumentation nachzuweisen. KI-Risiken spielen außerdem Bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA) nach Art. 35 DS-GVO eine Rolle.

Um Datenschutzrisiken in einer KI-Anwendung zu minimieren, sollten Unternehmen folgende Schritte beachten:

1

Legen Sie fest, welche Schutzziele für das spezifische Einsatzszenario der KI relevant sind, und dokumentieren Sie Ihre Entscheidung.

2

Identifizieren Sie Datenschutzrisiken, indem Sie feststellen, ob die Schutzziele vollständig erreicht werden („Datenschutz-Risikomodell“).

3

Erklären Sie ausführlich, warum ein Schutzziel als nicht relevant angesehen wird. Hierbei dienen z.B. die Ethik-Richtlinien für vertrauenswürdige KI der Europäischen Kommission als Orientierung.

Als Beispiele nennt das BayLDA folgende Schutzziele:

„Fairness“ im Sinne, dass keine unvertretbaren Risiken in Bezug auf Diskriminierung oder Ungleichbehandlung vorhanden sind.

„Autonomie und Kontrolle“ im Sinne, dass Eingriffsmöglichkeiten in den Betrieb einer KI-Anwendung existieren bzw. Entscheidungen mit Rechtswirkung nicht ohne menschliche Kontrolle erfolgen.

„Transparenz“ im Sinne, dass zum einen die Betroffenen über deren Verwendung personenbezogener Daten beim Training von KI-Modellen informiert werden als auch derart, dass KI-Modelle und KI-Anwendungen prüfbar im Sinne der Rechenschaftspflicht sein müssen. Ebenfalls auch, dass KI-Anwendungen für Betroffene in der Interaktion als solche erkannt werden müssen (z. B. ChatBots oder Anpassung von Audiosignalen zur Imitation eines Sprechers).

„Verlässlichkeit“ im Sinne, dass ein KI-Modell bzw. eine KI-Anwendung zum einen seinen beabsichtigten Zweck innerhalb tolerierbaren Fehlergrenzen erfüllt als auch, dass diese vor absichtlichen Manipulationen (sog. Adversial Angriffe bspw. mittels Prompt-Injection bei Großen Sprachmodellen oder Störung bei der Erkennung von Verkehrsschilderung durch spezielle „Aufkleber“) geschützt sind. (...)

„Sicherheit“ in dem Sinne, dass ungewollte technische Störungen („Safety“ wie Hardwarefehler aufgrund ungenügendem Arbeitsspeicher), aber vor allem unbefugte Zugriffe/Änderungen („Security“ wie die Manipulation von Trainingsdaten bei der KI-Modellerzeugung oder Manipulation von „Filtern“, die als Zensurmechanismus missbraucht werden können) wirksam verhindert werden können.

„Datenschutz“ im Sinne, dass neben einer Rechtsgrundlage für das Erzeugen von KI-Modellen und dem Betrieb/dem Einsatz von KI-Anwendungen auch die Betroffenenrechte sowie weiteren Compliance-Anforderungen der DS-GVO umgesetzt werden müssen. (...)“

Quelle: Direkt zitiert aus der Checkliste „Datenschutzkonforme Künstliche Intelligenz - Checkliste mit Prüfkriterien nach DS-GVO“ des Bayerischen Landesamtes für Datenschutzaufsicht

4 Ansätze aus Wirtschaft und Forschung für mehr Datenschutz bei KI

Mit der Frage, wie KI-Systeme datenschutzkonform in Unternehmen genutzt werden können, beschäftigen sich nicht nur Datenschutzverantwortliche, sondern auch Vertreter von Wirtschaft und Forschung.

Erste Ansätze bestehen bereits.

Dazu gehören:

- die **Anonymisierung und Pseudonymisierung** von Daten. Damit wird verhindert, dass Personen anhand von Daten identifiziert werden können. Allerdings leidet die Datenqualität unter diesen Maßnahmen. Zudem ist für Unternehmen unklar, bis zu welchem Grad sie eine Anonymisierung vornehmen müssen. Bei der Pseudonymisierung ist außerdem nicht gewährleistet, dass Personen nicht mehr identifizierbar sind.
- das **Privacy-Preserving Machine Learning (PPML)**. PPML ist eine Möglichkeit, den Datenschutz in KI-Systemen zu vereinfachen. Darunter fasst man Techniken zusammen, die Algorithmen datenschutzfreundlicher gestalten und den Datenschutz bereits in der Designphase von KI-Anwendungen sicherstellen sollen (Stichwort: Privacy by Design). Allerdings fehlt laut der Plattform Lernende Systeme bisher die rechtliche Anerkennung von technischen Instrumenten für mehr Privatsphäre.

Fazit: Auf dem Laufenden bleiben und datenschutzrechtliche Unterstützung suchen

Bis es verbindliche Vorgaben für den Einsatz von KI-Systemen in Unternehmen gibt oder der Datenschutz von Anfang an in KI-Modelle integriert werden kann, sollten Unternehmen sich **an den Einschätzungen der Datenschutzbeauftragten der Bundesländer orientieren** und die Entwicklungen rund um den Datenschutz beim Einsatz künstlicher Intelligenz **aufmerksam verfolgen**.

Wenn Sie KI-Systeme schon jetzt möglichst DSGVO-konform in Ihrem Unternehmen nutzen möchten, ist ein **(externer) Datenschutzbeauftragter (DSB)** Ihr wichtigster Ansprechpartner. Ein DSB kann Sie dabei unterstützen, von den Vorteilen von KI profitieren zu können, ohne DSGVO-Verstöße zu riskieren.

Sie haben Fragen?
Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung zum Datenschutz Management in Ihrem Unternehmen und dem Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de

Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist Ihr Partner im Datenschutz.
Wir glauben, dass Datenschutz nicht teuer und komplex sein muss. Mit unseren auf KMU zugeschnittenen Lösungen beraten wir Sie als externer Datenschutzbeauftragter. Alternativ unterstützen wir sowohl interne oder externe Datenschutzbeauftragte mit unserer smarten SaaS-Plattform Proliance 360. So lässt sich Datenschutz einfach & pragmatisch umsetzen. Wir sind ein junges Münchner Unternehmen mit mehr als 70 Mitarbeitern und helfen bereits über 2.000 Unternehmen, die Herausforderungen der DSGVO zu meistern. Sprechen Sie uns gerne an.