TechTarget | ComputerWeekly.de E-Guide

CW+ Content

KI und Datenschutz

In diesem E-Guide

In diesem E-Guide:

Die Nutzung von generativer KI hat in Unternehmen auf unterschiedlichsten Ebenen ganz selbstverständlich Einzug gehalten. Das ist mit erheblichen Risiken für die Datensicherheit und den Datenschutz verbunden. Daher sollten sich Unternehmen schon aus eigenem Interesse vorab mit den entsprechenden Maßnahmen auseinandersetzen, die auch durch die betroffenen Vorschriften und Gesetze eingefordert werden.

Im Falle der Datenschutz-Grundverordnung (DSGVO) müssen Unternehmen eine Datenschutz-Folgenabschätzung durchführen, wenn sie ein neues Projekt beginnen, das wahrscheinlich ein erhebliches Risiko für die personenbezogenen Daten von Personen darstellt. Sowohl DSGVO als auch der AI Act fordern eine Risikobestimmung vor der Nutzung eines KI-Dienstes.

In diesem E-Guide

Datenschutz: Was vor dem Einsatz von KI-Diensten zu tun ist

Oliver Schonschek, News Analyst

Vor dem Einsatz einer KI-Lösung muss nach Datenschutz-Grundverordnung eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Hinweise dafür liefern die Aufsichtsbehörden.

Umfragen zeigen regelmäßig, dass Unternehmen in Deutschland zwar große Vorteile in der Nutzung von Services mit KI (Künstlicher Intelligenz) sehen, aber von Bedenken hinsichtlich Datenschutz und Sicherheit zurückgehalten werden. Es sollte aber nicht übersehen werden, dass an vielen Stellen KI-Dienste „durch die Hintertür“ ins Unternehmen kommen könnten, über Cloud-Dienste, Security-Anwendungen, Office-Lösungen, Betriebssysteme oder auf Endgeräten.

Dabei besteht die Gefahr, dass KI-Dienste genutzt werden, ohne die rechtlichen Anforderungen zu erfüllen, die schon jetzt in der Datenschutz-Grundverordnung (DSGVO) zu finden sind und durch den AI Act hinzukommen.

Unter einer Datenschutz-Folgenabschätzung (DSFA) versteht man „eine für bestimmte Verarbeitungsvorgänge vorgeschriebene strukturierte Risikoanalyse. Sie dient einer Vorabbewertung bestimmter Verarbeitungsvorgänge, die ein

In diesem E-Guide

Verantwortlicher vornehmen möchte“, wie der Bundesdatenschutzbeauftragte 2024 erläutert hat.

Die Datenschutzkonferenz (DSK) hat schon vor mehreren Jahren eine „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist“ (PDF) veröffentlicht. Dort findet man auch den Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten, so dass vor dem Einsatz von KI also eine DSFA notwendig ist. Leider erfolgt aber oftmals keine solche DSFA, auch deshalb, weil es Unternehmen schwerfällt, die Risiken vor der Nutzung einer KI zu erfassen.

DSFA vor KI-Nutzung: Nicht einfach, aber Pflicht

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) (PDF) nennt neben der Verpflichtung auch die Vorteile einer solchen DSFA vor der Nutzung von KI-Diensten: Die Datenschutz-Folgenabschätzung ist nicht nur das (verpflichtende) Mittel der Wahl, hohen Risiken strukturiert und nachweislich in den Griff zu bekommen – sie dient auch dazu, mehr Vertrauen in den eigenen KI-Einsatz aufzubauen.

Wie aber lassen sich die Risiken einer KI bestimmen? Auch dazu hat das BayLDA wichtige Hinweise: Datenschutzrisiken für die Rechte und Freiheiten natürlicher Personen bei KI-Einsatz ergeben sich, wenn KI-spezifische Schutzziele nicht vollständig erfüllt werden. Beispiele derartiger Schutzziele sind

In diesem E-Guide

die Transparenz (Information der Betroffenen über Verwendung ihrer Daten beim Training von KI-Modellen; Prüfbarkeit im Sinne der Rechenschaftspflicht), die Verlässlichkeit (Schutz vor absichtlicher Manipulation; Umgang mit Halluzinationen bei Sprachmodellen) und die Fairness (Verhinderung unbeabsichtigter Diskriminierung oder Ungleichbehandlung durch die KI).

Es stellen sich also die Fragen, ob und wie sich solche Schutzziele bei Nutzung einer bestimmten KI-Lösung einhalten lassen, und was passieren kann, wenn dies nicht gelingt.

Aufsichtsbehörden geben Hinweise zu KI-Risiken

Die Datenschutzkonferenz (DSK) hatte schon vor Jahren die Schutzziele bei KI-Einsatz sowie mögliche Fragen zur Einhaltung des jeweiligen Schutzzieles im „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“ (PDF) veröffentlicht. Diese Fragen können bei der Risikobestimmung eine Hilfe sein.

Die Datenschutzkonferenz hat nun nochmals nachgelegt und eine Orientierungshilfe mit datenschutzrechtlichen Kriterien für die Auswahl und den datenschutzkonformen Einsatz von KI-Anwendungen veröffentlicht. Die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ (PDF) richtet sich an Unternehmen, Behörden und andere Organisationen. Im Sinne einer Checkliste dient das Papier als Leitfaden insbesondere für datenschutzrechtlich

In diesem E-Guide

Verantwortliche, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen. Die Orientierungshilfe wird künftig weiterentwickelt und an aktuelle Entwicklungen angepasst.

Ob Zweckbestimmung, Transparenzpflichten, Betroffenenrechte oder Richtigkeit von Ergebnissen: Die Orientierungshilfe erörtert – auch anhand von Beispielen – wichtige Kriterien entlang der Vorgaben der Datenschutz-Grundverordnung und zeigt Leitlinien für entsprechende Entscheidungen auf, so die DSK.

Prof. Dr. Dieter Kugelmann, Vorsitzender der Taskforce KI der DSK, erläuterte die Motivation für das Papier: „Wir wissen und erkennen an, dass Unternehmen und Behörden sich aktuell unter Hochdruck mit dem möglichen Einsatz von KI-Anwendungen auseinandersetzen. Allerdings sind in einem hochdynamischen Umfeld tragfähige Bewertungen schwierig“.

Zudem würden wesentliche Fragen zur Nutzung personenbezogener Daten für das Training von KI-Anwendungen von vielen Anbietern nicht transparent beantwortet. Andererseits sollten innovative Lösungen auch mittels KI möglich sein. „In dieser Situation möchten wir gerade kleine und mittlere Unternehmen sowie öffentliche Stellen nicht alleine lassen. Wir wollen ihnen ein Werkzeug an die Hand geben, um ihre Entscheidung informiert zu treffen und ihre datenschutzrechtliche Verantwortung bestmöglich wahrzunehmen“, so Prof. Kugelmann weiter.

In diesem E-Guide

Pflicht zur DSFA bleibt, trotz AI Act

Unternehmen sollten die von den Datenschutzaufsichtsbehörden angebotenen Orientierungshilfen nutzen, um die Risiken bei einer geplanten KI-Nutzung besser einschätzen zu können. Dies hilft ohne Zweifel bei der vorgeschriebenen DSFA. Diese wird auch in Zukunft Pflicht sein, auch mit dem AI Act der EU.

„Datenschutzregelungen wie die Datenschutz-Grundverordnung werden mit der KI-Verordnung nicht ersetzt, sondern gelten weiterhin“, betont die Datenschutzaufsicht von NRW. „KI-Anwendungen haben nicht immer mit personenbezogenen Daten zu tun. Wenn aber personenbezogene Daten bei KI-Anwendungen verarbeitet werden, muss das Datenschutzrecht eingehalten werden.“

Es ist also keine temporäre Aufgabe, sich mit den Datenrisiken vor KI-Nutzung zu befassen, sondern die Datenschutz-Folgenabschätzung bleibt als Aufgabe bestehen. Das gilt auch dann, wenn KI-Dienste quasi „durch die Hintertür“ ins Unternehmen kommen. Die Verantwortlichkeit für den Datenschutz besteht auch dann.

Das BayLDA hat dafür auch ein „Datenschutz-Risikomodell“ (PDF) erläutert: Festlegung und Dokumentation, welche der Schutzziele einer KI-Anwendung für das spezifische Szenario relevant sind. Datenschutzrisiken ergeben sich dann aus der Abweichung eines vollständigen Erreichens der jeweiligen Schutzziele.

In diesem E-Guide

Eine ausführliche Begründung, falls ein Schutzziel als nicht relevant angesehen wird, darf dann nicht fehlen.

An Hilfen für eine DSFA vor KI-Nutzung mangelt es also nicht, an der Umsetzung jedoch bisher schon.

In diesem E-Guide

Generative KI: Datenrisiken bei LLMs erkennen und minimieren

Oliver Schonschek, News Analyst

Bevor generative KI eingesetzt werden darf, steht eine Datenschutz-Folgeabschätzung an. Wie kann eine umfassende Datenschutz-Analyse beim Umgang mit LLMs in der Praxis aussehen?

Datenschutz wird häufig als einer der Gründe genannt, warum Unternehmen bei dem Einsatz von KI (künstlicher Intelligenz) und insbesondere von LLMs (Large Language Models) zögern. Es ist den Unternehmen zum Beispiel nicht klar, wie sich vertrauliches Firmenwissen sowie personenbezogene und andere zu schützende Daten vor ungewolltem Abfluss an Dritte schützen lassen.

Datenschützer warnen auch vor einer vorschnellen, unüberlegten Einführung von KI im Unternehmen, die Datenschutz-Grundverordnung (DSGVO) sieht den Bedarf einer Datenschutz-Folgenabschätzung (DSFA) vor Einführung von KI-Technologien (siehe auch Datenschutz: Was vor dem Einsatz von KI-Diensten zu tun ist).

Gleichzeitig möchte der Datenschutz aber den Einsatz moderner Technologien nicht verhindern, sondern vielmehr einen datenschutzgerechten Weg aufzeigen. So erklärt die Bundesdatenschutzbeauftragte (BfDI) Professor Dr. Louisa

In diesem E-Guide

Specht-Riemenschneider: „Damit datengetriebene Innovationen allen Menschen zu Gute kommen, ist es mir wichtig, Wege aufzuzeigen, die eine datenschutzkonforme Anwendung und die Umsetzung von Innovationen ermöglichen."

LLMs sind mit Datenrisiken verknüpft

LLMs sind hochkomplexe KI-Modelle zur Generierung von Texten. Sie werden mit großen Datenmengen trainiert, erklären die Mitglieder der Berlin Group, einer unabhängigen Gruppe von Expertinnen und Experten im Bereich des technologischen Datenschutzes unter Leitung der BfDI. Allein schon der Umstand, dass LLMs mit „großen Datenmengen" trainiert werden, zeigt, dass Unternehmen auch mit Risiken für den Datenschutz rechnen müssen, denn viele Daten haben direkten oder indirekten Personenbezug.

Zu den Herausforderungen für den Datenschutz zählt die Berlin Group gängige Praktiken wie wahlloses Datensammeln zum Erstellen der Trainingsdatensätze, unregelmäßige oder nicht vorhandene Prüfungen von Trainingsdaten und -ergebnissen, Black-Box-Algorithmen, die nicht überprüft oder erklärt werden können, und ein Mangel an technischem Wissen.

Data Scraping untergrabe die Kontrolle des Einzelnen über seine persönlichen Daten und nehme ihr oder ihm die Möglichkeit, die Verwendung der eigenen

In diesem E-Guide

Daten zu kontrollieren, insbesondere da Einzelpersonen häufig überhaupt nicht wüssten, dass ihre Daten von LLMs verwendet werden, so die Berlin Group.

Auch LLMs müssen sich an den Datenschutzprinzipien messen lassen

Um das Datenschutzniveau und die möglichen Datenrisiken bei LLMs prüfen zu können, müssen keine völlig neuartigen Datenschutzansätze gefunden werden, vielmehr gilt es, die aus der DSGVO bekannten Datenschutzprinzipien auch auf die LLMs anzuwenden. Genau das hat die Berlin Group in einer aktuellen Veröffentlichung zu LLMs (PDF) getan.

Im Folgenden werden die Hinweise der Berlin Group zusammengestellt, um aufzuzeigen, wie sich die Grundsätze des Datenschutzes auf LLMs anwenden lassen, als Grundlage der erforderlichen Datenschutz-Analyse oder Datenschutz-Folgenabschätzung:

Rechtsgrundlage: Die Entwickler und Betreiber generativer KI-Systeme, die personenbezogene Daten verarbeiten, müssen über eine gültige Rechtsgrundlage im Datenschutzrecht verfügen und auch im Einklang mit anderen geltenden Gesetzen (zum Beispiel Urheberrecht) sein. In Bezug auf Trainingsdaten für generative KI ist es wichtig zu beachten, dass öffentlich zugängliche personenbezogene Daten immer noch unter die Datenschutzgesetze fallen, so die Berlin Group.

In diesem E-Guide

Zweckbindung: Die Entwickler und Betreiber von LLMs und generativen KI-Systemen, die personenbezogene Daten verarbeiten, müssen sicherstellen, dass diese Daten für bestimmte explizite und legitime Zwecke verarbeitet werden. Darüber hinaus müssen sie sicherstellen, dass sie die Daten nicht über die berechtigten Erwartungen des Einzelnen hinaus oder für unvereinbare Zwecke verarbeiten.

Datenminimierung: Die Entwickler und Betreiber von LLMs und anderen generativen KI-Systemen, die personenbezogene Daten verarbeiten, sollten die Verarbeitung auf das für ihren Zweck „Notwendige“ beschränken. Die frühzeitige Einschränkung des Vorkommens oder der Verarbeitung personenbezogener Daten ist ein wichtiger Schritt zum Schutz der Rechte der betroffenen Personen. Zu diesem Zweck sollten Entwickler bestrebt sein, bei allen Vorkommen personenbezogener Daten in ihren Datensätzen eine Datenminimierung anzuwenden.

Transparenz: Die Entwickler und Betreiber von LLMs und anderen generativen KI-Systemen, die personenbezogene Daten verarbeiten, müssen Transparenzmaßnahmen umsetzen, und zwar insbesondere in Bezug auf betroffene Personen, denen eine Reihe von Informationsrechten zustehen. Dazu sollten Informationen darüber gehören, was, wie, wann und warum personenbezogene Daten im Trainingsprozess des Systems erfasst und verwendet werden, einschließlich der Quellen der Trainingsdaten, der Vor- und

In diesem E-Guide

Nachverarbeitungsmaßnahmen zur Entfernung personenbezogener Daten und der Zuverlässigkeit der Vorhersage des generierten Textes.

Sicherheit: Die Entwickler und Bereitsteller von LLMs und anderen generativen KI-Systemen, die personenbezogene Daten verarbeiten, müssen Sicherheitsmaßnahmen implementieren. Die Daten müssen während der Speicherung, Entwicklung, aber auch während der Nachbereitstellung sicher aufbewahrt werden, um komplexen Sicherheitsproblemen Rechnung zu tragen.

Rechenschaftspflicht: Die Entwickler und Betreiber von LLMs und anderen generativen KI-Systemen, die personenbezogene Daten verarbeiten, sollten sicherstellen, dass sie die Einhaltung des Datenschutzes nachweisen können.

Genauigkeit: Die Entwickler und Betreiber von LLMs und anderen generativen KI-Systemen müssen sicherstellen, dass die von ihnen verarbeiteten personenbezogenen Daten so genau, vollständig und aktuell sind, wie es für die Zwecke, für die sie verwendet werden sollen, erforderlich ist. Dies gilt insbesondere für personenbezogene Daten, die zum Trainieren von LLMs oder generativen KI-Modellen verwendet werden. Um dieses Prinzip zu unterstützen, sollten Entwickler und Bereitsteller über einen Prozess verfügen, mit dem ihr LLM- oder generatives KI-System aktualisiert werden kann (zum Beispiel durch Verfeinerung oder Neutraining des Modells).

In diesem E-Guide

LLMs: Die Einhaltung des Datenschutzes muss sichergestellt werden

Die Berlin Group beschreibt auch eine Reihe von Maßnahmen zur Gewährleistung dieser Prinzipien des Datenschutzes. Dazu gehören das Kuratieren der Datenquellen, die Vorverarbeitung (Entfernen vertraulicher Daten) und Differential Privacy.

Nur wenn alle Grundprinzipien des Datenschutzes gewahrt werden und entsprechende technisch-organisatorischen Maßnahmen ergriffen werden, kann eine Datenschutz-Analyse zu dem Ergebnis kommen, dass ein LLM datenschutzgerecht eingesetzt werden kann. Abweichungen von den Datenschutzprinzipien bedeuten ein Datenrisiko, also eine mögliche Verletzung des Datenschutzes.

Das Papier der Berlin Group enthält auch Beispiele für LLM-Anwendungen und entsprechende Maßnahmen, um die Prinzipien des Datenschutzes einzuhalten, und ist deshalb ein wertvoller Baustein auf dem Weg zu einem Datenschutzkonzept für die Nutzung von LLMs im Unternehmen.

In diesem E-Guide

Datenschutz und KI-VO: Die Rolle der Aufsichtsbehörden

Oliver Schonschek, News Analyst

Die KI-Verordnung (KI-VO) ist am 1. August 2024 in Kraft getreten. Unternehmen suchen Unterstützung bei der Umsetzung. Die nationale Aufsicht bei KI ist aber komplex.

„Die nationale Aufsicht bei Fragen Künstlicher Intelligenz ist aufgrund der sektoralen Zuständigkeiten und der föderalen Aufteilung komplex. Wer die KI-Governance in Deutschland übernehmen soll, ist offen“, so lautete es aus dem Digitalausschuss des Deutschen Bundestages. Eine genaue Klärung der Aufsicht ist aber notwendig, denn die KI-Verordnung (KI-VO) ist am 1. August 2024 in Kraft getreten, die Fristen zur Umsetzung laufen.

Als Unternehmen muss man wissen, welche Behörde und Aufsicht wann zuständig ist und auch Beratung und Unterstützung anbieten könnte. Das gilt ganz besonders für KI-Systeme, die als mit hohem Risiko behaftet klassifiziert werden. Das umfasst etwa KI-Systeme, die in Produkten wie Funkanlagen oder Fahrzeugen eingesetzt werden, aber auch solche KI- Systeme, die zur biometrischen Fernidentifizierung oder bei der Prüfung von Asylanträgen zum Einsatz kommen, erläuterte der Bundesdatenschutzbeauftragte.

In diesem E-Guide

Für solche Hochrisiko-KI- Systeme gelten spezifische Anforderungen, beispielsweise an die Qualität der verwendeten Daten, die Genauigkeit, die Robustheit und die Cybersicherheit. Zusätzlich muss es für Hochrisiko-KI-Systeme eine technische Dokumentation, eine Protokollierungsfunktion und ein Risikomanagement geben. Weitere Anforderungen sind Transparenz und menschliche Aufsicht.

Doch auch wer KI-Systeme mit etwas geringerem Risiko einsetzen will, hat Informations- und Aufklärungsbedarf und möchte wissen, welche Behörde denn nun ansprechbar ist und womöglich eine Prüfung vornehmen möchte.

Die Datenschutzaufsicht hat Aufgaben nach KI-Verordnung

Bereits jetzt steht fest, dass den Datenschutzaufsichtsbehörden die Marktüberwachung für weite Teile des Hochrisiko-Katalogs an KI-Systemen übertragen wird, das sieht die KI-Verordnung vor, wie zum Beispiel der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit deutlich macht.

In den Sektoren der Strafverfolgung, Justizverwaltung und Migrationskontrolle sowie bei KI, die Wahlen beeinflusst, sind demnach die Datenschutzbehörden als Marktüberwachungsbehörden gesetzt (Art. 74 Abs. 8 KI-VO). Das gilt nicht nur für die Behörden, die solche Systeme einsetzen, sondern beispielsweise

In diesem E-Guide

auch für Softwareunternehmen, Cloud-Dienste und Sicherheitsunternehmen, die für diese Sektoren KI-Systeme anbieten, in bestehende Systeme integrieren oder sie vertreiben. Die Marktüberwachungskompetenz erstreckt sich auf die gesamte Wertschöpfungskette.

In anderen Bereichen sind noch keine derartigen Festlegungen zur Aufsicht getroffen: Bis zum 2. August 2025 müssen die Mitgliedstaaten aber ein Durchführungsgesetz erlassen, in dem unter anderem allgemeine Marktüberwachungsbehörden für die Durchsetzung der KI-VO benannt werden.

Die KI-VO sieht vor, dass die zuständigen Behörden ständig über eine ausreichende Zahl von Mitarbeitenden verfügen, deren Kompetenzen und Fachkenntnisse ein umfassendes Verständnis der KI-Technologien und insbesondere der relevanten Vorgaben aus dem Daten- und Produktsicherheitsrecht umfassen. Da könnten sich Synergien anbieten, zwischen Datenschutz-Grundverordnung und KI-Verordnung, wenn es um die Aufsicht geht.

Mögliche, nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hält es in einem Positionspapier (PDF) für sinnvoll, aufgrund der langjährigen Erfahrung im Bereich der Beratung, Beschwerdebearbeitung und Kooperation auf nationaler wie europäischer Ebene grundsätzlich die Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden nach der KI-VO zu benennen. Ausgenommen seien einzelne Sektoren wie etwa der Finanzsektor oder die kritische Infrastruktur.

Mit dieser Konzeption könnten Doppelstrukturen und zusätzlicher Bürokratieaufwand vermieden werden, so die DSK. Die Datenschutzaufsichtsbehörden hätten ohnehin in allen Fällen, in denen KI-Systeme personenbezogene Daten verarbeiten, die Aufsicht nach der Datenschutz-Grundverordnung. Nur durch die Zuständigkeit der Datenschutzaufsichtsbehörden nach KI-VO werde eine Beratung und Aufsicht aus einer Hand möglich.

Die Datenschutzkonferenz empfiehlt, als Marktüberwachungsbehörden nach der KI-VO den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie die Landesdatenschutzbehörden zu benennen.

Der BfDI sollte nach Vorstellungen der Datenschutzkonferenz Deutschland im Europäischen Ausschuss für KI vertreten.

Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, erläuterte: „Die Marktüberwachung für KI-Verfahren erfordert Expertise und den Willen sowie die Fähigkeit zur Kooperation. Die Datenschutzaufsichtsbehörden bringen diese Kompetenzen mit. Eine übergreifende Aufsicht bedeutet für die Verantwortlichen, dass sie einheitliche Ansprechpartner haben. Dies entspricht dem Wunsch der Wirtschaft nach einer Antwort auf ihre Fragen“. Man wolle Marktüberwachung und Datenschutzaufsicht für KI-Verfahren aus einer Hand gewährleisten und stehe für diese Zukunftsaufgabe bereit.

Europäischer Datenschutzausschuss empfiehlt ebenfalls einheitliche Aufsicht

Die stellvertretende Vorsitzende des EDSA, Irene Loizidou Nicolaidou, sagte: „Die Datenschutzbehörden sollten bei der Durchsetzung des KI-Gesetzes eine wichtige Rolle spielen, da die meisten KI-Systeme die Verarbeitung personenbezogener Daten beinhalten. Ich bin fest davon überzeugt, dass die Datenschutzbehörden aufgrund ihrer völligen Unabhängigkeit und ihres tiefen Verständnisses der Risiken der KI für die Grundrechte aufgrund ihrer vorhandenen Erfahrung für diese Rolle geeignet sind.“

In diesem E-Guide

Entsprechend empfiehlt der Europäische Datenschutzausschuss (EDSA): Die Mitgliedstaaten sollten in Erwägung ziehen, Datenschutzbehörden auch für andere Hochrisiko-KI-Systeme als Marktaufsichtsbehörden zu ernennen und dabei die Ansichten der nationalen Datenschutzbehörden zu berücksichtigen, insbesondere dann, wenn diese Hochrisiko-KI-Systeme in Sektoren eingesetzt werden, in denen wahrscheinlich die Rechte und Freiheiten natürlicher Personen im Hinblick auf die Verarbeitung personenbezogener Daten beeinträchtigt werden.

Nun bleibt abzuwarten, ob die möglichen Synergien zwischen Datenschutz-Grundverordnung und KI-Verordnung zum Tragen kommen. Unabhängig davon ist aber klar, dass die DSGVO auch bei KI-Systemen vollständig zum Tragen kommt, ganz gleich, wer die allgemeine Marktaufsicht nach KI-VO umsetzen wird.

In diesem E-Guide

Impressum:

Dies ist eine Publikation von ComputerWeekly.de

Michael Eckert | *Editorial Director*
Malte Jeschke | *Senior Online Editor*
Ulrike Riess-Marchive | *Senior Online Editor*
Tobias Servaty-Wendehost | *Senior Online Editor*
Julia Reber | *Junior Online Editor*
Becky Wrigley & Gardis Cramer von Laue | *Production Editors*
Brent Boswell | *Herausgeber*
Brent.Boswell@informatechtarget.co

Hauptsitz:
Informa TechTarget, 275 Grove Street, Newton, MA 02466
www.techtarget.com

Deutsche Redaktion:
TechTarget Germany GmbH
c/o RPI-Roehm, Elsenheimerstr. 7, D-80687 München
E-Mail: webmaster@de.techtarget.com
www.techtarget.de

In diesem E-Guide

Erhalten Sie mehr exklusive Inhalte von CW+

Als Mitglied erhalten Sie Zugriff auf unser CW+—Angebot—eine Auswahl von freien Inhalten, Trainingsmaterialien und exklusiven Möglichkeiten, die speziell von unseren Partnern und unseren Seiten bereitgestellt wurden.

CW+—Angebote bieten kostenlose Inhalte, die nur für unsere Mitglieder zur Verfügung gestellt werden.

Nutzen Sie die Vorteile Ihrer Mitgliedschaft in vollem Umfang und besuchen Sie

http://www.computerweekly.de/ehandbooks

Bilder: stock.adobe.com Titel image: nassim/Adobe