

Annika Selzer, Jan Ole Berndt, Ingo J. Timm*

Einsatz KI-generierter Datenschutz-Schulungsmaterialien

Datenschutzrechtliche und betriebswirtschaftliche Perspektive

Unternehmen unterliegen der Pflicht, Mitarbeiter zum Datenschutzrecht zu schulen. Insbesondere für kleine Unternehmen ohne Datenschutzbeauftragten kann diese Pflicht zur Herausforderung werden, sodass Unternehmen z. T. auf KI-generierte Schulungsmaterialien zurückgreifen. Der Beitrag untersucht die datenschutzrechtliche Qualität und die betriebswirtschaftlichen Vorteile solcher Schulungsmaterialien.

1 Datenschutzschulungen in kleinen Unternehmen

Unternehmen sind grundsätzlich – unabhängig von ihrer Größe – dazu verpflichtet, die an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter regelmäßig¹ zum Datenschutzrecht

* Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Mi-



Dr. Annika Selzer,

Abteilungsleiterin „IT Law & Interdisciplinary Privacy Research“ am Fraunhofer SIT, Forschungsbereichs-koordinatorin „Legal Aspects of Privacy & IT Security“ in ATHENE.

E-Mail: Annika.Selzer@sit.fraunhofer.de

Dr. Jan Ole Berndt,

Stellv. Forschungsbereichsleiter für Kognitive Sozial-simulation am DFKI und Lehrbeauftragter an der Universität Trier.

E-Mail: jan_ole.berndt@dfki.de



Prof. Dr. Ingo J. Timm,

Lehrstuhl für Wirtschaftsinformatik I an der Universität Trier, Forschungsbereichsleiter für Kognitive Sozial-simulation am DFKI.

E-Mail: ingo.timm@dfki.de

zu schulen.² Diese Verpflichtung kann gerade für kleine Unternehmen ohne betrieblichen Datenschutzbeauftragten aufgrund begrenzter personeller und finanzieller Ressourcen eine erhebliche Herausforderung darstellen.³ Vor diesem Hintergrund greifen immer mehr kleine Unternehmen auf Schulungsmaterialien zurück, die sie von KI-Chatbots erstellen lassen.⁴ Bevorzugt werden hierbei von den kleinen Unternehmen i.d.R. Selbstlerneinheiten, da diese sowohl zeit- als auch ortsunabhängig bearbeitet werden können.

Aufgrund dieser Entwicklung untersucht der vorliegende Beitrag zunächst einen repräsentativen Querschnitt der Leistungsfähigkeit aktueller KIs im Bereich von *Grundlagen-Datenschutzschulung* für Mitarbeiter. Dies erfolgt über die Analyse von insgesamt neun exemplarischen Selbstlerneinheiten zum Datenschutz, die von drei verschiedenen KI-Chatbots erstellt wurden. Jeder der drei Chatbots generierte jeweils drei Schulungsinhalte zu den gleichen drei datenschutzrechtlichen Themen, die Teil von *Grundlagen-Mitarberschulungen zum Datenschutz* sein sollten. Um das Potenzial der Nutzung KI-generierter datenschutzrechtlicher Grundlagen-Schulungsinhalte in kleinen Unternehmen zu bewerten, wurden die neun Selbstlerneinheiten sodann aus datenschutzrechtlicher Sicht auf Korrektheit und Vollständigkeit überprüft sowie vor dem Hintergrund des risikobasierten Ansatzes – insbesondere in Bezug auf die Zeit- und Kostenersparnis im Vergleich mit traditionellen Schulungsmethoden – diskutiert.

nisterium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autoren wieder.

1 Martini in Paal/Pauly, DSGVO-BDSG, Art. 32 Rn. 66.

2 Aufgabe des betrieblichen Datenschutzbeauftragten, Art. 39 DSGVO.

3 Jandt in Kühling/Buchner, DSGVO-BDSG, Art. 32 Rn. 38.

4 Selzer/Kurchyna/Berndt/Timm, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten (upcoming).

2 KI-generierte Selbstlerneinheiten

Zur Umsetzung der Ziele des vorliegenden Beitrags wurden am 17. März 2025 drei führende KI-Chatbots – nämlich Copilot, Claude und ChatGPT – dazu aufgefordert, jeweils kurze Lerneinheiten für Mitarbeiter zu drei verschiedenen Datenschutz-Themen zu erstellen.⁵ Für die Aufforderung der KI-Chatbots wurde jeweils der exakt gleiche Text genutzt.

2.1 Datenschutzrecht

Zunächst erhielten alle drei KI-Chatbots den folgenden Arbeitsauftrag: „Bitte generiere eine textbasierte Selbstlerneinheit für Mitarbeiter mit maximal 1.000 Zeichen inkl. Leerzeichen zu der Frage ‚wen oder was schützt das Datenschutzrecht, so wie es in der Datenschutz-Grundverordnung geregelt wird?‘“ Nachfolgend werden die Ergebnisse dieses Arbeitsauftrags wiedergegeben.

Ergebnis 1

„Das Datenschutzrecht, wie es in der Datenschutz-Grundverordnung (DSGVO) geregelt wird, schützt die personenbezogenen Daten natürlicher Personen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören beispielsweise Name, Adresse, E-Mail-Adresse, Geburtsdatum, IP-Adresse und viele weitere Informationen, die eine Person direkt oder indirekt identifizieren können.

Die DSGVO zielt darauf ab, die Privatsphäre und die Grundrechte der betroffenen Personen zu schützen und gleichzeitig den freien Datenverkehr innerhalb der Europäischen Union zu gewährleisten. Sie legt fest, wie personenbezogene Daten erhoben, verarbeitet, gespeichert und weitergegeben werden dürfen. Unternehmen und Organisationen müssen sicherstellen, dass sie die Datenschutzprinzipien einhalten, wie z. B. Datenminimierung, Zweckbindung, Transparenz und Sicherheit der Datenverarbeitung.“⁶

Ergebnis 2

„Die Datenschutz-Grundverordnung (DSGVO) schützt natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten. Konkret:

Schutzgegenstand:

- ◆ Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- ◆ Nicht geschützt: Daten juristischer Personen (Unternehmen, Vereine) oder anonymisierte Daten
- ◆ Schutzbereich:
- ◆ Recht auf informationelle Selbstbestimmung
- ◆ Schutz der Privatsphäre
- ◆ Grundrechte und Grundfreiheiten natürlicher Personen

Betroffene Rechte:

- ◆ Auskunftsrecht
- ◆ Recht auf Berichtigung
- ◆ Recht auf Löschung („Vergessenwerden“)

⁵ Die Einschränkung auf kurze Lerneinheiten wurde gewählt, um die von den KI-Chatbots generierten Ergebnisse im vorliegenden Beitrag abdrucken zu können, ohne die Zeichenvorgaben an den Beitrag selbst zu überschreiten.

⁶ Erstellt von Copilot.

- ◆ Recht auf Einschränkung der Verarbeitung
- ◆ Recht auf Datenübertragbarkeit
- ◆ Widerspruchsrecht

Die DSGVO gilt für die Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter innerhalb der EU sowie für Datenverarbeitungen außerhalb der EU, wenn EU-Bürger betroffen sind oder Waren/Dienstleistungen in der EU angeboten werden.“⁷

Ergebnis 3

„Das Datenschutzrecht, geregelt durch die Datenschutz-Grundverordnung (DSGVO), schützt personenbezogene Daten von natürlichen Personen. Hierbei handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, wie Name, Adresse, E-Mail-Adresse, Geburtsdatum oder IP-Adresse.

Die DSGVO schützt also nicht nur die Privatsphäre der betroffenen Personen, sondern auch deren Rechte in Bezug auf die Verarbeitung ihrer Daten. Sie stellt sicher, dass personenbezogene Daten nur rechtmäßig, transparent und zweckgebunden erhoben und verarbeitet werden.

Besonders geschützt werden:

- ◆ Die Rechte der betroffenen Personen: Dazu gehören das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit.
- ◆ Vertraulichkeit und Sicherheit: Die DSGVO fordert, dass personenbezogene Daten vor unbefugtem Zugriff, Verlust oder Missbrauch geschützt werden.
- ◆ Ziel ist es, das Vertrauen in den Umgang mit personenbezogenen Daten zu stärken und die Grundrechte der betroffenen Personen zu wahren.“⁸

2.2 Datenschutz-Grundsätze

Danach erhielten alle drei KI-Chatbots folgenden Arbeitsauftrag: „Bitte generiere eine textbasierte Selbstlerneinheit für Mitarbeiter mit maximal 1.000 Zeichen inkl. Leerzeichen zu der Frage ‚was sind die wichtigsten Grundsätze des Datenschutzrechts nach Datenschutz-Grundverordnung?‘“ Nachfolgend werden die Ergebnisse dieses Arbeitsauftrags aufgezeigt.

Ergebnis 1

„Die Datenschutz-Grundverordnung (DSGVO) legt mehrere wesentliche Grundsätze fest, die den Umgang mit personenbezogenen Daten regeln. Diese Grundsätze sind:

- ◆ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in transparenter Weise verarbeitet werden.
- ◆ Zweckbindung: Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.
- ◆ Datenminimierung: Es dürfen nur solche Daten erhoben werden, die für die Zwecke der Verarbeitung notwendig sind.
- ◆ Richtigkeit: Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

⁷ Erstellt von Claude.

⁸ Erstellt von ChatGPT.

- ◆ Speicherbegrenzung: Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, notwendig ist.
- ◆ Integrität und Vertraulichkeit: Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung.⁹

Ergebnis 2

„Die Datenschutz-Grundverordnung (DSGVO) basiert auf sieben zentralen Grundsätzen:

- ◆ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Datenverarbeitung nur mit Rechtsgrundlage, fair und nachvollziehbar.
- ◆ Zweckbindung: Daten nur für festgelegte, eindeutige und legitime Zwecke erheben und verarbeiten.
- ◆ Datenminimierung: Nur Daten verarbeiten, die für den jeweiligen Zweck erforderlich sind.
- ◆ Richtigkeit: Personenbezogene Daten müssen sachlich richtig und aktuell sein.
- ◆ Speicherbegrenzung: Daten nur so lange speichern, wie für den Verarbeitungszweck nötig.
- ◆ Integrität und Vertraulichkeit: Angemessene Sicherheit gewährleisten, Schutz vor unbefugter Verarbeitung oder Verlust.
- ◆ Rechenschaftspflicht: Der Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen können.

Diese Grundsätze bilden das Fundament jeder datenschutzkonformen Verarbeitung personenbezogener Daten und müssen stets beachtet werden.“¹⁰

Ergebnis 3

„Die Datenschutz-Grundverordnung (DSGVO) regelt den Umgang mit personenbezogenen Daten in der EU und legt klare Grundsätze fest, die den Schutz der Privatsphäre der betroffenen Personen gewährleisten sollen. Die wichtigsten Grundsätze sind:

- ◆ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Daten müssen auf einer rechtmäßigen Grundlage verarbeitet werden, und die betroffenen Personen müssen über die Verarbeitung informiert werden.
- ◆ Zweckbindung: Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden.
- ◆ Datenminimierung: Es dürfen nur so viele Daten erhoben werden, wie für den jeweiligen Zweck notwendig sind.
- ◆ Richtigkeit: Personenbezogene Daten müssen korrekt und auf dem neuesten Stand sein.
- ◆ Speicherbegrenzung: Daten dürfen nur so lange aufbewahrt werden, wie es für den Verarbeitungszweck erforderlich ist.
- ◆ Integrität und Vertraulichkeit: Die Daten müssen vor unbefugtem Zugriff und Verlust geschützt werden.

Diese Grundsätze fördern den verantwortungsvollen Umgang mit personenbezogenen Daten und stärken die Rechte der betroffenen Personen.“¹¹

2.3 Clear-Desk-Prinzip

Abschließend erhielten alle drei KI-Chatbots folgenden Arbeitsauftrag: „Bitte generiere eine textbasierte Selbstlerneinheit für Mitarbeiter mit maximal 1.000 Zeichen inkl. Leerzeichen zu der Frage ‚was ist das Clear-Desk-Prinzip und wie wird es umgesetzt?‘“ Nachfolgend werden die Ergebnisse dieses Arbeitsauftrags aufgezeigt.

Ergebnis 1

„Was ist das Clear-Desk-Prinzip und wie wird es umgesetzt? Das Clear-Desk-Prinzip verpflichtet Mitarbeitende dazu, ihren Arbeitsplatz am Ende des Arbeitstags frei von sensiblen Informationen zu hinterlassen. Ziel ist es, Datenschutz und Informationssicherheit zu gewährleisten. Dokumente mit personenbezogenen oder vertraulichen Daten müssen sicher verstaut, Bildschirme gesperrt und mobile Datenträger weggeschlossen werden. Auch bei kurzer Abwesenheit gilt: keine offenliegenden Unterlagen! Die Umsetzung erfolgt durch klare interne Richtlinien, regelmäßige Schulungen und stichprobenartige Kontrollen. So wird das Risiko von Datenverlust oder unbefugtem Zugriff minimiert.“¹²

Ergebnis 2

„Was ist das Clear-Desk-Prinzip? Das Clear-Desk-Prinzip bedeutet: Arbeitsplatz immer aufgeräumt verlassen! Keine vertraulichen Dokumente, USB-Sticks oder sensible Informationen sollen offen herumliegen.

Warum ist es wichtig?

- ◆ Schutz vor Datendiebstahl
- ◆ Verhinderung von unbefugten Einblicken
- ◆ Compliance mit Datenschutzgesetzen
- ◆ Schutz von Geschäftsgeheimnissen

Umsetzung:

- ◆ Dokumente wegschließen (Schreibtischschublade/Schrank)
- ◆ Bildschirm sperren bei Abwesenheit
- ◆ USB-Sticks entfernen und sicher verwahren
- ◆ Notizzettel mit sensiblen Daten entsorgen/wegräumen
- ◆ Telefonate nicht mithören lassen
- ◆ Am Arbeitseende: komplette Aufräumung

Merksatz:

„Was andere nicht sehen sollen, gehört nicht auf den Schreibtisch!“

Tipp: Machen Sie das Clear-Desk-Prinzip zur Routine – Ihre Daten und die des Unternehmens sind es wert!“¹³

Ergebnis 3

„Das Clear-Desk-Prinzip bedeutet, dass Arbeitsplätze am Ende des Arbeitstages frei von vertraulichen Unterlagen, Notizen oder Datenträgern sein müssen. Ziel ist der Schutz sensibler Informationen und die Förderung von Ordnung und Effizienz.

So setzen Sie das Prinzip um:

- ◆ Verstauen Sie Unterlagen in abschließbaren Schränken.
- ◆ Schalten Sie Computerbildschirme aus oder sperren Sie diese.
- ◆ Entfernen Sie USB-Sticks oder externe Speichermedien.

9 Erstellt von Copilot.

10 Erstellt von Claude.

11 Erstellt von ChatGPT.

12 Erstellt von Copilot.

13 Erstellt von Claude.

- ◆ Notizen mit vertraulichen Informationen gehören ins Archiv oder in den Schredder.¹⁴

3 Bewertung der KI-generierten Inhalte

Nachfolgend werden die neun Selbstlerneinheiten aus datenschutzrechtlicher Sicht auf Korrektheit und Vollständigkeit¹⁵ sowie vor dem Hintergrund des risikobasierten Ansatzes auf die Vorteile des Generierens und Einsetzens KI-gestützter Schulungsinhalte diskutiert.

3.1 Datenschutzrechtliche Sicht

Die Analyse der KI-generierten Grundlagen-Schulungsinhalte zeigt ein insgesamt gutes Qualitätsniveau.

Bei den Selbstlerneinheiten zum **Datenschutzrecht** weisen Ergebnis 1 und 3 Ungenauigkeiten bezüglich des Schutzgegenstandes auf (korrekterweise Schutz natürlicher Personen, nicht ihrer Daten). Ergebnis 2 liefert hier präzisere Formulierungen mit guter Abgrenzung von relevanten und nicht relevanten Daten, nennt jedoch keine Beispiele für personenbezogene Daten, was jedoch für das Verständnis als essenziell erachtet wird.

Ergebnis 2 enthält zudem eine nicht unbedingt notwendige Auflistung zum Schutzbereich und erwähnt das deutsche Grundrecht auf informationelle Selbstbestimmung, das im DSGVO-Kontext eine untergeordnete Rolle spielt. Die Datenschutz-Grundsätze werden in Ergebnis 2 nicht erwähnt; stattdessen werden Betroffenenrechte aufgelistet. Ergebnis 3 enthält sowohl Grundprinzipien als auch Betroffenenrechte, mit einer kleinen Ungenauigkeit bei der Nennung der Ziele bezüglich des zu stärkenden Vertrauens.

Alle Selbstlerneinheiten zu den **Datenschutz-Grundsätzen** orientieren sich am Verordnungstext mit sinnvollen Kürzungen und Vereinfachungen. In den Ergebnissen 1 und 3 fehlt der Grundsatz der Rechenschaftspflicht. Positiv zu vermerken ist, dass die Ergebnisse 2 und 3 die Bedeutung der Grundsätze abschließend hervorheben, um deren Wichtigkeit zu betonen.

Bei den Selbstlerneinheiten zum **Clear-Desk-Prinzip** schränkt die Erklärung des Ergebnisses 1 zunächst falsch ein, dass das Clear-Desk-Prinzip nur am Ende eines Arbeitstages Anwendung findet, was im weiteren Verlauf der Selbstlerneinheit jedoch korrigiert wird, indem erwähnt wird, dass es auch bei kürzeren Abwesenheiten greift. Auch Ergebnis 2 könnte durch die Formulierung einer „komplette[n] Aufräumung“ am Arbeitende zumindest die Folgefrage auslösen, inwiefern sich die Umsetzung des Prinzips bei kürzeren und längeren Abwesenheiten unterscheiden soll. Ergebnis 3 geht nur auf die Anwendung des Prinzips am Ende eines Arbeitstages ein und lässt somit unerwähnt, dass das Prinzip (in abgestufter Form) auch bei kürzeren Abwesenheiten greifen soll.

Nach der hier vertretenen Meinung würde das Lesen keiner der Selbstlerneinheiten zu einem falschen Verständnis der für das Datenschutzrecht relevanten Daten, der wichtigsten Regelungs-

inhalte und der Handlungsempfehlungen zu einem in der täglichen Arbeit besonders wichtigen Prinzip führen, sondern wäre im Gegenteil dazu geeignet, kleinen Unternehmen, in denen keine eigene Datenschutzexpertise vorhanden ist und die finanziellen Ressourcen den Einkauf solcher Ressourcen erschweren, einen soliden Erstüberblick über diese Themen zu verschaffen. Gleichwohl ist anzumerken, dass der Umfang der hier betrachteten Selbstlerneinheiten bewusst sehr klein gewählt wurde, um den Zeichenvorgaben des vorliegenden Beitrags entsprechen zu können; daher ist die Aussagekraft zur inhaltlichen Qualität und Vollständigkeit beschränkt. Sollten kleine Unternehmen KI-generierte Selbstlerneinheiten zur Grundlagenvermittlung bei Mitarbeitern einsetzen, scheint eine längere Selbstlerneinheit erforderlich zu sein.¹⁶

3.2 Diskussion

Die DSGVO verfolgt einen sogenannten risikobasierten Ansatz. Dieser ist darauf ausgerichtet, die Höhe des Risikos für die Rechte und Freiheiten betroffener Personen unmittelbar mit der Art und dem Umfang der zu treffenden Schutzmaßnahmen (und den für die Umsetzung dieser Maßnahmen anfallenden Kosten) zu verknüpfen. Dies bedeutet, dass technische und organisatorische Maßnahmen proportional zum Risikopotenzial der Datenverarbeitung gestaltet werden müssen.

Die untersuchten Selbstlerneinheiten zeigen, dass KI-generierte Schulungsmaterialien trotz einiger Ungenauigkeiten einen substantiellen Mehrwert für Unternehmen ohne eigene Datenschutzexpertise bieten können. Im Sinne des risikobasierten Ansatzes ermöglichen sie eine kostengünstige Risikominimierung, indem sie grundlegendes Datenschutzwissen vermitteln. Insbesondere bei begrenzten finanziellen Ressourcen stellen sie eine praktikable Lösung dar, um Mitarbeiter grundlegend für datenschutzrechtliche Fragestellungen zu sensibilisieren.

Allerdings zeigen sich neben dieser Stärke auch Grenzen der KI-Generierung: Prägnante Darstellungen stehen neben terminologischen Unschärfen, grundlegende Erklärungen neben punktuellen Auslassungen.

Vor diesem Hintergrund können KI-generierte Schulungsmaterialien insbesondere – aber aufgrund der eben genannten inhaltlichen Einschränkungen vermutlich auch nur – für Kleinstunternehmen mit einem nach dem risikobasierten Ansatz als gering eingestuften Datenverarbeitungsrisiko einen wertvollen Orientierungsrahmen schaffen. Die Verhältnismäßigkeit zwischen Schulungsaufwand und Risikominderung ist dabei entscheidend. Jedoch sollten auch KI-generierte Schulungsmaterialien den spezifischen Kontext des Unternehmens berücksichtigen.

Wirtschaftlich bietet dieser Ansatz Kleinstunternehmen die Möglichkeit, den eigenen Mitarbeitenden Datenschutzwissen zu vermitteln, ohne nennenswerte finanzielle Ressourcen zu binden. Hierbei wird der Grundsatz des risikobasierten Ansatzes umgesetzt, Schutzmaßnahmen proportional zum Risikopotenzial zu gestalten. Der Mehrwert KI-generierter Selbstlerneinheiten liegt somit in der Schaffung eines Grundbewusstseins für datenschutzrechtliche Fragestellungen.

¹⁴ Erstellt von ChatGPT.

¹⁵ Die Prüfung auf Vollständigkeit bezieht sich auf die Benennung der aus der hier vertretenen Sicht wichtigsten, aufgrund der für den Beitrag gewählten Zeichenbegrenzung der Selbstlerneinheiten zu erwartenden Inhalte der Lerneinheit, nicht jedoch auf deren Ausführlichkeit (bspw. wurde überprüft, ob in der Selbstlerneinheit zu den Datenschutz-Grundsätzen alle in Art. 5 DSGVO verankerten Grundsätze benannt, nicht aber, ob diese ausführlich genug erläutert wurden).

¹⁶ Diese sollten wiederum in weiteren Forschungsarbeiten datenschutzrechtlich auf inhaltliche Qualität und Vollständigkeit überprüft werden.

3.3 Einschränkungen

Die Bewertung und Diskussion basiert auf bewusst knapp gehaltenen Selbstlerneinheiten. Um umfassendere Aussagen zur Qualität KI-generierter Schulungsmaterialien treffen zu können, sollten weiterführende Studien durchgeführt werden.

4 Fazit

Die vorliegende Untersuchung konzentrierte sich auf KI-generierte Selbstlerneinheiten zum Datenschutzrecht zu ausgewählten Themen, die Bestandteil von Grundlagen-Mitarbeiterschulungen zum Datenschutz sein sollten. Die Analyse der Schulungsmaterialien zeigt die Potenziale und Grenzen KI-generierter Inhalte im Kontext des risikobasierten Datenschutzansatzes.

Der Vergleich der drei jeweils drei KI-generierten Selbstlerneinheiten mit dem gleichen Arbeitsauftrag zeigt, dass es empfeh-

lenswert sein kann, unterschiedliche KI-Chatsbots mit der Erstellung der gleichen Selbstlerneinheit zu beauftragen und

- ◆ zum einen die Ergebnisse miteinander zu vergleichen, um sicherzustellen, dass die Schulungsinhalte vollständig sind (dies hätte z. B. hinsichtlich der Datenschutz-Grundsätze verhindert, dass der Grundsatz der Rechenschaftspflicht unerwähnt bleibt)

- ◆ zum anderen die Ergebnisse mit den tatsächlichen Gegebenheiten des (kleinen) Unternehmens abzugleichen und ggf. anzupassen (gibt es in dem Unternehmen z. B. die Anweisungen, keine vertraulichen Informationen auf Notizzettel zu notieren, müsste die Handlungsempfehlung hierzu angepasst werden).

Die Entwicklung KI-generierter Schulungsmaterialien markiert somit zwar einen bedeutsamen Schritt in der Digitalisierung betrieblicher Weiterbildung, kann die menschliche Expertise jedoch (zumindest bisher) nicht ersetzen.

Künstliche Intelligenz



U. Barthelmeß, U. Furbach
Künstliche Intelligenz aus ungewohnten Perspektiven
 Ein Rundgang mit Bergson, Proust und Nabokov
 2019, X, 190 S. 18 Abb., 10 Abb. in Farbe. Brosch.
 € (D) 29,99 | € (A) 30,83 | *CHF 33.50
 ISBN 978-3-658-24569-6
 € 22,99 | *CHF 26.50
 ISBN 978-3-658-24570-2 (eBook)



C. Beierle, G. Kern-Isberner
Methoden wissensbasierter Systeme
 Grundlagen, Algorithmen, Anwendungen
 6., überarb. Aufl. 2019, XVIII, 564 S. 165 Abb.
 Mit Online-Extras. Brosch.
 € (D) 39,99 | € (A) 41,11 | *CHF 44.50
 ISBN 978-3-658-27083-4
 € 29,99 | *CHF 35.50
 ISBN 978-3-658-27084-1 (eBook)

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar |
 Kostenloser Versand für Printbücher weltweit

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich. * : unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Jetzt bestellen auf springer.com/informatik oder in der Buchhandlung

Part of **SPRINGER NATURE**