

Können KI-Chatbots zum Datenschutz schulen?

Eine vergleichende Untersuchung des Potenzials
von KI-Chatbots



AUTOREN

Alina Forina

Sarah Stummer

Impressum

Kontakt

Nationales Forschungszentrum für angewandte
Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

© Fraunhofer-Institut für
Sichere Informationstechnologie SIT,
Darmstadt, 2025

Hinweise

Die vorliegenden Ergebnisse sind im Rahmen des Fraunhofer Heilbronn Forschungs- und Innovationszentrums Cybersicherheit, das durch die Dieter Schwarz Stiftung gefördert wird, entstanden. Dieser Beitrag wurde zudem vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Inhalt

1. Problemstellung	7
2. Gang der Untersuchung	9
3. KI-generierte Schulungen.....	10
3.1 Claude Sonnet 4 (Anthropic, Anwendung: Claude).....	10
3.1.1 KI-generierter Inhalt.....	10
3.1.2 Bewertung	16
3.2 Command-a-03-2025 (Cohere, Anwendung: Cohere Playground)	22
3.2.1 KI-generierter Inhalt.....	22
3.2.2 Bewertung	25
3.3 DeepSeek V3 (DeepSeek AI, Anwendung: DeepSeek Chat)	28
3.3.1 KI-generierter Inhalt.....	28
3.3.2 Bewertung	31
3.4 Gemma 3n E2B (Google AI, Anwendung: Google AI Studio).....	34
3.4.1 KI-generierter Inhalt.....	34
3.4.1 Bewertung	37
3.5 GPT-4.1 (OpenAI, Anwendung: ChatGPT).....	42
3.5.1 KI-generierter Inhalt.....	42
3.5.2 Bewertung	44
3.6 Grok 3 (xAI, Anwendung: Grok Web-App)	49
3.6.1 KI-generierter Inhalt.....	49
3.6.2 Bewertung	51
3.7 LLaMA 4 (Meta AI, Anwendung: LLaMA Chat)	55
3.7.1 KI-generierter Inhalt.....	55
3.7.2 Bewertung	57
3.8 Mistral Medium 3 (Mistral AI, Anwendung: Le Chat).....	59
3.8.1 KI-generierter Inhalt.....	59
3.8.2 Bewertung	62
3.9 Qwen 3-235B-A22B-2507 (Alibaba DAMO Academy, Anwendung: Qwen Chat) 65	65
3.9.1 KI-generierter Inhalt.....	65
3.9.2 Bewertung	70
4. Gegenüberstellung der Schulungen	75
4.1 DSGVO-Relevanz.....	78

4.2 Kernbegriff „Personenbezogene Daten“	80
4.3 Kernbegriff „Verarbeitung“	82
4.4 Rollen im Datenschutzrecht	83
4.5 Grundsätze der Verarbeitung.....	86
4.6 Rechtsgrundlagen für die Verarbeitung.....	88
4.7 Rechte der betroffenen Person.....	90
4.8 Technische und organisatorische Maßnahmen	93
4.9 Datenschutzfolgenabschätzung	95
4.10 Meldepflichten bei Vorfällen	96
4.11 Verzeichnis von Verarbeitungstätigkeiten	98
4.12 Drittstaatenübermittlungen.....	100
4.13 Sanktionen bei Verstößen.....	101
4.14 Didaktische Qualität und Aufbau	103
5. Gesamtvergleich der Schulungen	104
5.1 Quantitative Auswertung.....	104
5.2 Qualitative Einordnung	106
6. Diskussion.....	107
6.1 Risikobasierter Ansatz und Qualitätsanforderungen nach DSGVO	107
6.2 Differenzierte Eignung nach Organisationsgröße und Risiko	108
7. Empfehlungen.....	110
8. Zusammenfassung	111
Anhang: Berechnung des Gesamtvergleichs.....	112
Literatur	114

1. Problemstellung

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet datenschutzrechtlich Verantwortliche dazu, angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Einhaltung datenschutzrechtlicher Vorgaben sicherzustellen.¹ Ein zentraler Bestandteil der organisatorischen Maßnahmen zur Umsetzung und Sicherstellung der Datenschutzgrundsätze ist die regelmäßige Schulung der Beschäftigten im Datenschutz.² Datenschutzschulungen helfen den Mitarbeitern eines Unternehmens, sich in ihrer täglichen Arbeit datenschutzkonform zu verhalten, denn nur wenn Mitarbeiter die konkreten Anforderungen im Umgang mit personenbezogenen Daten kennen, ist zu erwarten, dass sie gesetzeskonform und im Einklang mit unternehmensinternen Richtlinien handeln.³ Inhaltlich sollten Datenschutzschulungen regelmäßig sowohl die grundlegenden rechtlichen Prinzipien als auch die konkreten Anforderungen im jeweiligen Tätigkeitsbereich der Mitarbeiter abdecken. In der Regel erfolgt dies durch ein gestuftes Schulungskonzept: Eine allgemeine Basisschulung vermittelt zunächst allen Beschäftigten die zentralen Inhalte des Datenschutzrechts. Darauf aufbauend folgen zielgruppenspezifische Schulungen, die auf die besonderen Aufgaben und Verantwortlichkeiten einzelner Rollen – etwa im Personalwesen, in der IT-Administration oder in der Forschung und Entwicklung – sowie auf die individuellen Gegebenheiten des Unternehmens abgestimmt sind.⁴

Die Verpflichtung zur Durchführung datenschutzrechtlicher Schulungen von Mitarbeitern gilt unabhängig von der Unternehmensgröße – sie betrifft sowohl Kleinstbetriebe als auch Großkonzerne. Die konkrete Ausgestaltung und Intensität der Schulungen richtet sich jedoch nicht primär nach der Unternehmensgröße, sondern nach dem Risiko, das mit den jeweiligen Datenverarbeitungsprozessen im Unternehmen verbunden ist.⁵ Gemäß dem risikobasierten Ansatz der DSGVO (Art. 24, 25 und 32 DSGVO) sind bei der Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen neben dem Stand der Technik sowie der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung, insbesondere auch die Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Diese Kriterien verdeutlichen, dass Unternehmen nicht verpflichtet sind, sämtliche verfügbaren Schulungsmaßnahmen umzusetzen.⁶ Entscheidend ist vielmehr, dass die Maßnahmen dazu geeignet sind sicherzustellen, dass die Vorgaben der DSGVO umgesetzt werden, und dem konkreten Risiko angemessen sind. Dabei steht stets der Schutz der betroffenen Personen im Vordergrund. Kostenüberlegungen können berücksichtigt werden, dürfen aber nicht dazu führen, dass vollständig auf Schulungen verzichtet wird.⁷

Die praktische Umsetzung von risikoadäquaten Schulungsmaßnahmen stellt für viele Unternehmen jedoch eine erhebliche Herausforderung dar. Kleine und mittlere Unternehmen verfügen häufig nicht über ausreichendes internes Fachwissen, finanzielle Ressourcen oder zeitliche Kapazitäten, um selbst risikoadäquate Schulungsmaßnahmen

¹ Vgl. Art. 24, 25, 32 DSGVO.

² Hartung, in: Kühling/Buchner, DSGVO/BDSG, Art. 25 Rdnr. 16, Art. 32 Rdnr. 38; Martini, in: Paal/Pauly, DSGVO/BDSG, Art. 25 Rdnr. 10; Mantz, in: Sydow/Marsch, DSGVO/BDSG, Art. 25 Rdnr. 60; Nolte/Werkmeister, in: Gola/Heckmann, DSGVO/BDSG, Art. 25 Rdnr. 17.

³ Günthner/Krohm, in: Bürkle, Compliance in Versicherungsunternehmen, § 14. Rdnr. 52; Drewes, in: Besgen, Rechtshandbuch Leitende Angestellte, Geschäftsführer und Vorstände, Teil 6 Rdnr. 131.

⁴ Günthner/Krohm, in: Bürkle, Compliance in Versicherungsunternehmen, § 14. Rdnr. 52; Drewes, in: Besgen, Rechtshandbuch Leitende Angestellte, Geschäftsführer und Vorstände, Teil 6 Rdnr. 131.

⁵ Petri/Stief, in: Simitis/Hornung/Specker gen. Döhmann, DSGVO/BDSG, Art. 24 Rdnr. 9.

⁶ Jandt, in: Kühling/Buchner, DSGVO/BDSG, Art. 32 Rdnr. 7 ff.

⁷ Jandt, in: Kühling/Buchner, DSGVO/BDSG, Art. 32 Rdnr. 11.

zu entwickeln und angemessen umzusetzen.⁸ Aber auch größere Unternehmen dürften oftmals vor der Herausforderung stehen, Datenschutzschulungen effizient zu skalieren und unternehmensweit einheitlich umzusetzen. Neben unterschiedlichen Standorten, Sprachen und Systemen, können insbesondere auch die Vielzahl von Mitarbeitern, deren verschiedenen Schulungsständen und Tätigkeitsprofile sowie der hohe Aufwand für Koordination, Aktualisierung und Qualitätssicherung die effiziente Skalierung und unternehmensweite praktische Umsetzung von Datenschutzschulungen erschweren.

Vor diesem Hintergrund rückt der Einsatz von KI-Modellen, insbesondere sogenannter KI-Chatbots, die ohne oder mit minimalem menschlichen Aufwand Selbstlernseinheiten zum Datenschutz generieren können, zunehmend in den Fokus. Die automatisierte Erstellung von Schulungsinhalten durch KI-Modelle verspricht auf den ersten Blick eine erhebliche Kosten- und Zeitsparnis, sowohl für kleine Unternehmen, die regelmäßig keine eigene Datenschutzabteilung unterhalten und auf externe Schulungsangebote angewiesen wären, als auch für größere Organisationen mit hohem Schulungsbedarf. Gleichzeitig wirft der Einsatz von KI-Modellen zur Erstellung von Schulungsunterlagen eine Reihe grundlegender Fragen auf: Welche inhaltliche Qualität weisen KI-generierte Schulungsmaterialien auf? Und kann das KI-basierte Generieren von Lerninhalten tatsächlich als angemessene Umsetzung der gesetzlichen Pflicht zur Schulung von Mitarbeitern im Sinne der DSGVO gelten?

Erste Untersuchungen zum didaktischen und inhaltlichen Potenzial von KI-generierten Schulungseinheiten liefern bereits wertvolle Einblicke in die grundsätzlichen Chancen und Grenzen des Einsatzes von KI-Modellen im Kontext datenschutzrechtlicher Weiterbildung.⁹ Sie zeigen, dass KI-generierte Inhalte grundsätzlich in der Lage sind, zentrale datenschutzrechtliche Informationen richtig darzustellen, zugleich jedoch auch einzelne Unklarheiten, Unschärfen oder punktuelle Fehler aufweisen können. Die vorliegende Untersuchung knüpft an diese bestehenden Untersuchungen und Erkenntnisse an und erweitert diese um einen breiteren methodischen Ansatz, um zusätzliche Erkenntnisse darüber zu gewinnen, ob KI-generierte Schulungsinhalte den datenschutzrechtlichen Anforderungen genügen können. Ziel dieser Untersuchung ist es, die Qualität von durch KI-Modellen generierten Schulungsinhalten systematisch zu analysieren und zu bewerten. Im Mittelpunkt steht die Frage, inwieweit das KI-basierte Generieren solcher Inhalte als angemessene Umsetzung der datenschutzrechtlichen Schulungspflicht betrachtet werden kann. Dafür wird in Kapitel 2 zunächst das methodische Vorgehen der Untersuchung erläutert. Kapitel 3 stellt sodann die von den KI-Modellen erstellten Schulungseinheiten vor. Innerhalb des Kapitels 3 erfolgt eine Bewertung der von den KI-Modellen erstellten Schulungseinheiten im Hinblick auf ihre datenschutzrechtliche Richtigkeit, Vollständigkeit und Verständlichkeit. In Kapitel 4 werden die KI-generierten Schulungsinhalte hinsichtlich zentraler Qualitätskriterien miteinander verglichen. In Kapitel 5 folgt sodann ein Gesamtvergleich. Kapitel 6 diskutiert sodann, welche Schwachstellen die KI-generierten Schulungsinhalte aufweisen, welches Potenzial sie haben und inwieweit sowie ggf. unter welchen Voraussetzungen sie geeignet sein können, die datenschutzrechtliche Schulungspflicht angemessen umzusetzen. Kapitel 7 formuliert auf dieser Grundlage Empfehlungen für den gezielten und verantwortungsvollen Einsatz von KI-generierten Schulungsinhalten, bevor Kapitel 8 die wesentlichen Ergebnisse zusammenfasst.

⁸ Enzmann/Selzer/Stummer, EuDIR 2025, 270 (270).

⁹ Enzmann/Selzer/Stummer, EuDIR 2025, 270 (270 ff.); Selzer/Kurchyna/Berndt/Timm, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten, 53 (53 ff.); Selzer/Berndt/Timm, DuD 2025, 539 (539 ff.).

2. Gang der Untersuchung

Bisherige Untersuchungen beschränkten sich jeweils auf die Analyse von Schulungsinhalten, die von drei unterschiedlichen KI-Modellen (OpenAIs ChatGPT, Anthropic's Claude und Microsofts Copilot) generiert wurden. Dabei verwendeten sie eine enge Zeichenbegrenzung (maximal 1.000 Zeichen inkl. Leerzeichen¹⁰ bzw. maximal 2.500 Zeichen inkl. Leerzeichen¹¹) und gaben ein klar umrissenes Themenfeld vor („Was ist aus Sicht der DSGVO bei dem Einsatz KI-basierter Chatbots zu beachten?“; „Was sind personenbezogene, pseudonyme und anonyme Daten; wie lassen sich die Begriffe voneinander abgrenzen und welche Relevanz haben sie für das Datenschutzrecht?“; „wen oder was schützt das Datenschutzrecht, so wie es in der Datenschutz-Grundverordnung geregelt wird?“; „was sind die wichtigsten Grundsätze des Datenschutzrechts nach Datenschutz-Grundverordnung?“; „was ist das Clean-Desk-Prinzip und wie wird es umgesetzt?“).

Die vorliegende Untersuchung geht über diesen Ansatz hinaus und vergleicht erstmals die generierten Schulungsunterlagen von neun unterschiedlichen KI-Modellen. Dabei wird auf eine Zeichenbeschränkung verzichtet. Zudem wird der thematische Fokus erweitert: Anstelle der Erstellung einer kompakten Selbstlerneinheit zu einem spezifischen Thema der DSGVO wird in dieser Untersuchung die Generierung einer umfassenden Schulung zu den Grundlagen des Datenschutzrechts verlangt. Darüber hinaus werden nicht nur kleinere Unternehmen, sondern Organisationen jeglicher Größe in den Blick genommen. Auf diese Weise soll eine umfassendere Beurteilungsgrundlage für den praktischen Einsatz KI-generierter Schulungsinhalte in unterschiedlich strukturierten Organisationen geschaffen werden.

Zur Umsetzung der Ziele des vorliegenden Beitrags wurden am 29. und 30.07.2025 neun führende KI-Modelle (Large Language Models, LLMs) – Claude Sonnet 4 (Anthropic, Anwendung: Claude), Command-a-03-2025 (Cohere, Anwendung: Cohere Playground), DeepSeek V3 (DeepSeek AI, Anwendung: DeepSeek Chat), Gemma 3n E2B (Google AI, Anwendung: Gemma AI Studio), GPT-4.1 (OpenAI, Anwendung: ChatGPT), Grok 3 (xAI, Anwendung: Grok Web-App), LLaMA 4 (Meta AI, Anwendung: LLaMA Chat), Mistral Medium 3 (Mistral AI, Anwendung: Le Chat), Qwen 3-235B-A22B-2507 (Alibaba DAMO Academy, Anwendung: Qwen Chat) – mit jeweils dem exakt gleich lautenden Arbeitsauftrag dazu aufgefordert, für Personen, die in einer Organisation eine neue Arbeitsstelle antreten, eine umfangreiche Schulung zu den Grundlagen des Datenschutzrechts zu erstellen. Bei der Auswahl der KI-Modelle wurde darauf geachtet, dass diese wiederum nicht selbst auf eine (ältere) Version eines bereits genannten KI-Modells zurückgreifen, um eine Doppelung zu vermeiden.¹² Außerdem wurde darauf

¹⁰ Selzer/Kurchyna/Berndt/Timm, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten, 53 (54); Selzer/Berndt/Timm, DuD 2025, 539.

¹¹ Enzmann/Selzer/Stummer, EuDIR 2025, 270 (271).

¹² Es gilt hier zu beachten, dass die meisten KI-Chatbots auf dem Markt – zumindest im Hintergrund – auf große Sprachmodelle (Large Language Models, LLMs) wie GPT-4 (OpenAI), Claude (Anthropic), Gemma (Google), Mistral oder LLaMA (Meta) zurückgreifen. Völlig eigenständig entwickelte, kostenfrei nutzbare KI-Chatbots ohne Zeichenbegrenzung und ohne Rückgriff auf bestehende LLMs sind selten. Es gibt keine vollständige Garantie, dass ein KI-Chatbot nicht direkt oder indirekt auf ein anderes genanntes LLM zurückgreift, da viele Plattformen Modelle kombinieren oder deren Herkunft nicht transparent offenlegen. Selbst bei eigenständigen LLMs kann eine Überschneidung in Trainingsdaten oder Architektur bestehen, was eine klare Abgrenzung zusätzlich erschwert. Die Auswahl der in dieser Arbeit betrachteten KI-Chatbots erfolgte auf Grundlage öffentlich zugänglicher Informationen und wurde mit größtmöglicher Sorgfalt hinsichtlich ihrer Eigenständigkeit und Unabhängigkeit sowie des Angebots der Textgenerierung in deutscher Sprache getroffen.

geachtet, dass die KI-Modelle kostenlos nutzbar sind und keine harte Zeichenbegrenzung aufweisen.¹³

Der Arbeitsauftrag an die KI-Modelle lautete:

« Bitte generiere eine textbasierte Selbstlerneinheit in deutscher Sprache für Personen, die in einer Organisation eine neue Arbeitsstelle antreten und von der Organisation umfangreich zu den Grundlagen des Datenschutzrechts geschult werden müssen. Bitte gehe hierbei davon aus, dass für die Organisation, in der die Person anfängt zu arbeiten, nur die Datenschutz-Grundverordnung Anwendung findet. Die Person soll neben theoretischen Grundlagen auch über die praktische Relevanz der DSGVO-Anforderungen geschult werden und Tipps zur Umsetzung dieser erhalten. Die Schulung soll für alle neuen Mitarbeiter gleich sein, unabhängig von Geschlecht, Alter, Bildungsstand und Tätigkeitsfeld, wobei in der Regel davon ausgegangen werden darf, dass keine Person unter 16 Jahre alt ist. »

Für die Erstellung der Datenschutzschulung wurden bei allen neun eingesetzten KI-Modellen ausschließlich die frei verfügbaren Standardversionen verwendet (mit Anmeldung, jedoch ohne kostenpflichtiges Abonnement). Auf spezielle Modi wie „Deep Research“ oder „Think“ wurde bewusst verzichtet, da sich diese je nach Anbieter stark in Funktionsweise, Verfügbarkeit und Kosten unterscheiden und zudem nicht von allen Modellen angeboten werden. So stellen etwa Gemma oder LLaMA solche Modi überhaupt nicht zur Verfügung. Die Nutzung der Standardversionen gewährleistet daher, dass alle Modelle unter vergleichbaren Bedingungen eingesetzt wurden und die Ergebnisse objektiv nebeneinander bewertet werden können.

3. KI-generierte Schulungen

Die von den KI-Modellen erstellten Schulungseinheiten werden im Folgenden jeweils dargestellt und hinsichtlich deren Themenschwerpunkte, Umfang und didaktischer Aufbereitung bewertet. Die Formatierung der KI-generierten Inhalte wurde hinsichtlich Schriftgröße und Schriftart an diese Studie angepasst; Fettdruck, Aufzählungen, Trennstriche und Symbole wurden hingegen originalgetreu aus der Quelle übernommen.

3.1 Claude Sonnet 4 (Anthropic, Anwendung: Claude)

3.1.1 KI-generierter Inhalt¹⁴

DSGVO-Schulung für neue Mitarbeiter Grundlagen des Datenschutzrechts in der Praxis

Lernziele dieser Schulung

Nach Abschluss dieser Schulung können Sie:

- Die wichtigsten Grundlagen der DSGVO erklären
- Personenbezogene Daten in Ihrem Arbeitsalltag erkennen

¹³ Hinweis zur Zeichenbegrenzung: Die meisten kostenlosen KI-Chatbots begrenzen aus Performance- und Kostengründen die Länge der vom Modell generierten Antworten – nicht, weil das jeweilige Sprachmodell technisch nicht dazu in der Lage wäre, längere Antworten zu generieren, sondern aufgrund der durch die längere Generierung entstehenden Serverkosten.

¹⁴ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell Claude Sonnet 4 über Claude generiert.

- Datenschutzrechtliche Anforderungen praktisch umsetzen
 - Datenschutzverletzungen vermeiden
 - Im Zweifelsfall richtig handeln
-

1. Was ist die DSGVO und warum ist sie wichtig?

Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO ist seit dem 25. Mai 2018 in der gesamten Europäischen Union gültig. Sie regelt, wie Organisationen mit personenbezogenen Daten umgehen müssen. Das Ziel ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten.

Warum betrifft mich das?

Jeder Mitarbeiter in unserer Organisation verarbeitet in irgendeiner Form personenbezogene Daten - sei es von Kunden, Kollegen oder Geschäftspartnern. Verstöße gegen die DSGVO können zu hohen Bußgeldern führen und das Vertrauen in unser Unternehmen beschädigen.

2. Grundbegriffe der DSGVO

2.1 Personenbezogene Daten

Definition: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Beispiele aus der Praxis:

- **Direkte Identifikatoren:** Name, Anschrift, E-Mail-Adresse, Telefonnummer
- **Indirekte Identifikatoren:** IP-Adresse, Kundennummer, Personalnummer
- **Besondere Kategorien:** Gesundheitsdaten, politische Meinungen, religiöse Überzeugungen

 **Praxistipp:** Im Zweifelsfall behandeln Sie Informationen als personenbezogen, wenn Sie damit eine Person identifizieren könnten.

2.2 Verarbeitung

Definition: Jeder Vorgang im Zusammenhang mit personenbezogenen Daten.

Beispiele:

- Erheben (sammeln)
- Speichern
- Verwenden
- Übermitteln
- Löschen
- Archivieren

2.3 Verantwortlicher

Unsere Organisation ist **Verantwortlicher** für die Datenverarbeitung. Das bedeutet, wir entscheiden über Zweck und Mittel der Verarbeitung und sind für die Einhaltung der DSGVO verantwortlich.

3. Die Grundsätze der DSGVO

3.1 Rechtmäßigkeit der Verarbeitung

Was bedeutet das? Jede Verarbeitung personenbezogener Daten braucht eine **Rechtsgrundlage**.

Die wichtigsten Rechtsgrundlagen:

1. **Einwilligung** der betroffenen Person
2. **Vertragserfüllung** (z.B. Kundendaten zur Auftragsabwicklung)
3. **Rechtliche Verpflichtung** (z.B. Aufbewahrungspflichten)
4. **Berechtigte Interessen** (z.B. Videoüberwachung zur Sicherheit)

Praktische Umsetzung:

- Prüfen Sie vor jeder Datenverarbeitung: "Auf welcher Rechtsgrundlage tue ich das?"
- Dokumentieren Sie die Rechtsgrundlage

- Bei Unsicherheit: Fragen Sie den Datenschutzbeauftragten

3.2 Zweckbindung

Was bedeutet das? Daten dürfen nur für den ursprünglich festgelegten Zweck verwendet werden.

Beispiel:

- Richtig: Kundendaten aus einem Kaufvertrag für die Rechnungsstellung verwenden
- Falsch: Dieselben Daten für Werbung verwenden (ohne separate Einwilligung)

Praktische Umsetzung:

- Verwenden Sie Daten nur für den ursprünglichen Zweck
- Neue Zwecke erfordern neue Rechtsgrundlagen
- Informieren Sie betroffene Personen über Zweckänderungen

3.3 Datenminimierung

Was bedeutet das? Verarbeiten Sie nur die Daten, die für den Zweck tatsächlich erforderlich sind.

Beispiele:

- Richtig: Für Newsletter-Versand nur E-Mail-Adresse erfragen
- Falsch: Zusätzlich Geburtsdatum, Telefonnummer und Adresse verlangen

Praktische Umsetzung:

- Hinterfragen Sie: "Brauche ich diese Information wirklich?"
- Verwenden Sie nur Pflichtfelder, wenn die Daten zwingend erforderlich sind
- Prüfen Sie regelmäßig, ob alle gespeicherten Daten noch benötigt werden

3.4 Richtigkeit

Was bedeutet das? Personenbezogene Daten müssen sachlich richtig und aktuell sein.

Praktische Umsetzung:

- Korrigieren Sie falsche Daten umgehend
- Löschen Sie unrichtige Daten, wenn eine Berichtigung nicht möglich ist
- Ermöglichen Sie betroffenen Personen die Berichtigung ihrer Daten

3.5 Speicherbegrenzung

Was bedeutet das? Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.

Praktische Umsetzung:

- Beachten Sie Aufbewahrungsfristen (z.B. 10 Jahre für Rechnungen)
- Löschen Sie Daten nach Ablauf der Fristen
- Prüfen Sie regelmäßig Ihre Datenbestände auf veraltete Informationen

3.6 Integrität und Vertraulichkeit

Was bedeutet das? Daten müssen vor unbefugtem Zugriff, Verlust oder Zerstörung geschützt werden.

Praktische Umsetzung:

- Verwenden Sie sichere Passwörter
- Sperren Sie Ihren Bildschirm beim Verlassen des Arbeitsplatzes
- Verschicken Sie vertrauliche Daten nur verschlüsselt
- Melden Sie Sicherheitsvorfälle sofort

4. Betroffenenrechte - Was müssen Sie wissen?

Betroffene Personen haben verschiedene Rechte bezüglich ihrer Daten. Diese Anfragen können bei Ihnen eingehen:

4.1 Auskunftsrecht

Was bedeutet das? Personen können fragen: "Welche Daten haben Sie über mich gespeichert?"

Ihr Vorgehen:

3. KI-generierte Schulungen

1. Leiten Sie die Anfrage an den Datenschutzbeauftragten weiter
2. Sammeln Sie keine Daten selbst zusammen
3. Antwortfrist: 1 Monat

4.2 Recht auf Berichtigung

Was bedeutet das? Personen können verlangen, dass falsche Daten korrigiert werden.

Ihr Vorgehen:

- Prüfen Sie die Richtigkeit der Angaben
- Korrigieren Sie falsche Daten unverzüglich
- Informieren Sie andere Stellen, an die die Daten weitergegeben wurden

4.3 Recht auf Löschung ("Recht auf Vergessenwerden")

Was bedeutet das? Personen können unter bestimmten Umständen die Löschung ihrer Daten verlangen.

Ihr Vorgehen:

- Prüfen Sie, ob eine Löschpflicht besteht
- Beachten Sie Aufbewahrungspflichten (z.B. steuerrechtliche Vorgaben)
- Bei Unsicherheit: Rücksprache mit dem Datenschutzbeauftragten

4.4 Weitere Rechte

- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch gegen die Verarbeitung

 **Wichtig:** Alle Betroffenenanfragen müssen innerhalb eines Monats beantwortet werden!

5. Technische und organisatorische Maßnahmen (TOM)

5.1 Was sind TOM?

Maßnahmen zum Schutz personenbezogener Daten vor unbefugtem Zugriff, Verlust oder Missbrauch.

5.2 Ihre Rolle bei der Umsetzung

Zutrittskontrolle:

- Lassen Sie keine unbefugten Personen an Ihren Arbeitsplatz
- Verwenden Sie Zugangskarten ordnungsgemäß
- Melden Sie verdächtige Personen

Zugangskontrolle:

- Verwenden Sie nur Ihre eigenen Zugangsdaten
- Geben Sie Passwörter niemals weiter
- Melden Sie sich nach Arbeitsende ab

Zugriffskontrolle:

- Greifen Sie nur auf die Daten zu, die Sie für Ihre Arbeit benötigen
- Öffnen Sie keine vertraulichen Dokumente aus Neugier
- Respektieren Sie Berechtigungsstrukturen

Weitergabekontrolle:

- Verschicken Sie personenbezogene Daten nur verschlüsselt
- Prüfen Sie Empfänger vor dem Versand
- Nutzen Sie sichere Kommunikationswege

Eingabekontrolle:

- Dokumentieren Sie, wer welche Daten eingegeben hat
- Verwenden Sie Versionskontrolle bei wichtigen Dokumenten

Auftragkskontrolle:

- Bei externen Dienstleistern: Prüfen Sie Datenschutzvereinbarungen
- Geben Sie nur die notwendigen Daten weiter

Verfügbarkeitskontrolle:

- Erstellen Sie regelmäßig Backups

- Melden Sie Systemausfälle sofort
- Schützen Sie Daten vor versehentlicher Löschung

Trennbarkeit:

- Trennen Sie Daten unterschiedlicher Zwecke
- Vermischen Sie nicht private und geschäftliche Daten

6. Datenschutzverletzungen erkennen und melden

6.1 Was ist eine Datenschutzverletzung?

Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt.

Beispiele:

- Versehentlicher Versand einer E-Mail an falsche Empfänger
- Verlust eines USB-Sticks mit Kundendaten
- Hackerangriff auf das System
- Diebstahl eines Laptops mit personenbezogenen Daten

6.2 Ihre Meldepflicht

Zeitfrist: Melden Sie Datenschutzverletzungen **unverzüglich** (spätestens innerhalb von 72 Stunden) an:

1. Ihren direkten Vorgesetzten
2. Den Datenschutzbeauftragten
3. Die IT-Abteilung (bei technischen Problemen)

⚠️ **Wichtig:** Auch vermeintlich kleine Vorfälle können schwerwiegende Folgen haben.

Melden Sie im Zweifel!

6.3 Erste Hilfe bei Datenschutzverletzungen

1. **Sofortmaßnahmen:** Stoppen Sie die weitere Verletzung (z.B. E-Mail zurückrufen)
2. **Dokumentation:** Notieren Sie sich alle Details zum Vorfall
3. **Meldung:** Informieren Sie unverzüglich die zuständigen Stellen
4. **Keine Panik:** Jeder macht Fehler - wichtig ist die schnelle Reaktion

7. Praktische Tipps für den Arbeitsalltag

7.1 E-Mail-Verkehr

Do's:

- Verwenden Sie BCC bei Massen-E-Mails
- Verschlüsseln Sie vertrauliche Inhalte
- Prüfen Sie Empfänger vor dem Versand
- Nutzen Sie aussagekräftige Betreffzeilen

Don'ts:

- Keine personenbezogenen Daten in CC, wenn nicht nötig
- Keine automatischen Weiterleitungen an private E-Mail-Adressen
- Keine Verwendung unsicherer E-Mail-Dienste für geschäftliche Zwecke

7.2 Arbeitsplatz-Sicherheit

Clean Desk Policy:

- Räumen Sie Ihren Schreibtisch am Ende des Arbeitstages auf
- Lassen Sie keine vertraulichen Dokumente offen liegen
- Sperren Sie Ihren Bildschirm beim Verlassen des Platzes
- Entsorgen Sie Dokumente mit personenbezogenen Daten im Reißwolf

7.3 Mobile Arbeitsgeräte

- Verwenden Sie Gerätesperren (PIN, Passwort, Biometrie)
- Installieren Sie nur genehmigte Apps
- Nutzen Sie VPN-Verbindungen für den Zugriff auf Firmendaten
- Melden Sie Verlust oder Diebstahl sofort

7.4 Umgang mit Besuchern und Kunden

- Führen Sie vertrauliche Gespräche in geschlossenen Räumen
- Drehen Sie Bildschirme so, dass Unbefugte nicht mitlesen können
- Geben Sie keine Informationen über andere Personen preis
- Überprüfen Sie die Identität bei telefonischen Anfragen

8. Häufige Fragen und Antworten

Q: Darf ich Kundendaten für eigene Zwecke nutzen? A: Nein, Kundendaten dürfen nur für die vereinbarten Geschäftszwecke verwendet werden.

Q: Was mache ich, wenn ein Kunde die Löschung seiner Daten verlangt? A: Leiten Sie die Anfrage an den Datenschutzbeauftragten weiter und löschen Sie nichts eigenmächtig.

Q: Darf ich personenbezogene Daten mit nach Hause nehmen? A: Nur mit ausdrücklicher Genehmigung und unter Einhaltung der Sicherheitsmaßnahmen.

Q: Wie lange darf ich E-Mails aufbewahren? A: Das hängt vom Inhalt ab. Geschäftliche E-Mails unterliegen oft Aufbewahrungspflichten, private sollten regelmäßig gelöscht werden.

Q: Was ist, wenn ich unsicher bin, ob ich eine Information weitergeben darf? A: Fragen Sie lieber einmal zu viel nach. Wenden Sie sich an Ihren Vorgesetzten oder den Datenschutzbeauftragten.

9. Wichtige Kontakte

Datenschutzbeauftragter:

- Name: [Hier Namen einfügen]
- E-Mail: [Hier E-Mail einfügen]
- Telefon: [Hier Telefonnummer einfügen]

IT-Support bei technischen Problemen:

- E-Mail: [Hier E-Mail einfügen]
- Telefon: [Hier Telefonnummer einfügen]

Geschäftsführung bei schwerwiegenden Vorfällen:

- E-Mail: [Hier E-Mail einfügen]
- Telefon: [Hier Telefonnummer einfügen]

10. Selbsttest: Haben Sie alles verstanden?

Szenario 1: Sie erhalten eine E-Mail von einer Person, die behauptet, ein Kunde zu sein und Auskunft über seine gespeicherten Daten möchte. Was tun Sie?

- Ich sende die Daten sofort zu
- Ich prüfe die Identität und leite die Anfrage an den Datenschutzbeauftragten weiter
- Ich ignoriere die E-Mail

Szenario 2: Sie versenden versehentlich eine E-Mail mit Kundendaten an den falschen Empfänger. Was tun Sie?

- Ich hoffe, dass es niemand bemerkt
- Ich rufe die E-Mail zurück und melde den Vorfall sofort
- Ich bitte den falschen Empfänger, die E-Mail zu löschen

Szenario 3: Ein Kollege möchte von Ihnen die Telefonnummer eines Kunden für private Zwecke. Was tun Sie?

- Ich gebe die Nummer weiter, da es nur ein Kollege ist
- Ich lehne ab, da dies nicht erlaubt ist
- Ich frage erst den Kunden um Erlaubnis

Lösungen:

1. Richtig: Identität prüfen und an Datenschutzbeauftragten weiterleiten
2. Richtig: E-Mail zurückrufen und Vorfall melden
3. Richtig: Ablehnen, da nicht erlaubt

11. Abschluss und Verpflichtung

Mit dieser Schulung haben Sie die wichtigsten Grundlagen des Datenschutzes kennengelernt. Datenschutz ist eine **Gemeinschaftsaufgabe** und jeder Mitarbeiter trägt Verantwortung.

Ihre Verpflichtung:

- Ich verpflichte mich, die Datenschutzbestimmungen einzuhalten
- Ich werde bei Unsicherheiten nachfragen
- Ich melde Datenschutzverletzungen unverzüglich
- Ich behandle personenbezogene Daten vertraulich

Denken Sie daran:

- Im Zweifelsfall: Fragen Sie nach!
- Lieber einmal zu vorsichtig als einmal zu nachlässig
- Datenschutz schützt Menschen - und damit auch Sie selbst

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen zur Schulung oder zum Datenschutz wenden Sie sich jederzeit an den Datenschutzbeauftragten.

Diese Schulung wurde erstellt für [Name der Organisation] und entspricht dem Stand der DSGVO. Letzte Aktualisierung: [Datum einfügen]

3.1.2 Bewertung

Die von Claude Sonnet 4 generierte Datenschutzschulung überzeugt insgesamt durch einen gut strukturierten Aufbau, eine klare Sprache sowie durch anschauliche Beispiele und praxisnahe Umsetzungshinweise. Besonders hervorzuheben sind die Übersichtlichkeit, die motivierenden Lernziele, die Verwendung von Icons zur besseren Lesbarkeit sowie die realitätsnahen Beispiele, etwa zum E-Mail-Versand oder zur Clean-Desk-Policy. Die Schulung ist insgesamt logisch aufgebaut und deckt zentrale Inhalte der DSGVO – darunter die datenschutzrechtlichen Grundbegriffe, die Grundsätze der Verarbeitung, die Betroffenenrechte sowie technische und organisatorische Maßnahmen – ab. Die Inhalte sind übersichtlich und verständlich aufbereitet und scheinen insbesondere für neue Mitarbeiter mit wenig Vorkenntnissen geeignet. Gleichwohl weist die Schulung auch inhaltliche und rechtliche Defizite auf. Übergeordnet ist festzustellen, dass die Schulung die Begriffe „personenbezogene Daten“ und „Daten“ synonym zu verwenden scheint, was zu Missverständnissen führen könnte. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

1. Was ist die DSGVO und warum ist sie wichtig? Die Datenschutz-Grundverordnung (DSGVO)

Positiv hervorzuheben ist, dass zunächst der zeitliche und sachliche Anwendungsbereich der DSGVO – wenn auch nur oberflächlich – angesprochen wird. Es fehlt jedoch ein Hinweis auf den räumlichen Anwendungsbereich der DSGVO. Ebenso wird das Ziel der DSGVO, die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen, richtig genannt. Positiv zu vermerken ist auch, dass die Mitarbeitenden direkt mit der Frage „Warum betrifft mich das?“ adressiert werden, was zur Stärkung ihres Verantwortungsbewusstseins beitragen kann. Die Zielgruppe („neue Mitarbeiter“) wird klar benannt.

2. Grundbegriffe der DSGVO

Die Definition der „personenbezogenen Daten“ (Art. 4 Nr. 1 DSGVO) ist zwar grundsätzlich richtig, es fehlt jedoch eine Erläuterung des Unterschieds zwischen den

3. KI-generierte Schulungen

Begriffen identifiziert und identifizierbar. Da es für die Fähigkeit Informationen als personenbezogene Daten einzuordnen zentral ist zu verstehen, wann eine natürliche Person identifizierbar ist, könnte die fehlende Erläuterung zu einem mangelnden Verständnis und einer mangelnden Umsetzung in der Praxis führen. Zudem kann der Mitarbeitende nur durch eine solche Erläuterung verstehen, wieso im Weiteren zwischen direkten und indirekten Identifikatoren unterschieden wird. Auch die Unterscheidung zwischen personenbezogenen, anonymen und pseudonymen Daten fehlt. Zu einem mangelnden Verständnis kann zudem der Umstand führen, dass der Begriff der „natürlichen Personen“ nicht erläutert wird. Insbesondere bei Mitarbeitenden mit wenig juristischen Vorkenntnissen kann nicht vorausgesetzt werden, dass sie den Begriff der natürlichen Person kennen.

Grundsätzlich positiv hervorzuheben sind die getroffenen Beispiele für direkte Identifikatoren, indirekte Identifikatoren und besondere Kategorien. Es fehlt jedoch eine Erläuterung, was unter besonderen Kategorien (Art. 9 Abs. 1 DSGVO) zu verstehen ist und welche erhöhten Anforderungen für deren Verarbeitung gelten. Zudem könnte die diesbezügliche Aufzählung beim Mitarbeitenden den Eindruck der Vollständigkeit erwecken (mangels „z. B.“), obwohl nur einige Beispiele aus Art. 9 Abs. 1 DSGVO genannt werden. Es wäre dem Verständnis weiterhin zuträglich gewesen, Beispiele für personenbezogene Daten aufzulisten, die in den verschiedenen Unternehmensbereichen typischerweise vorkommen. So hätte beispielsweise erläutert werden können, dass im Personalwesen etwa Bewerbungsunterlagen, Gehaltsdaten oder Krankmeldungen, im Marketing Kundendaten aus Befragungen, Interessenprofile oder Newsletter-Abonnements, im IT-Bereich IP-Adressen, Zugangsdaten und Kommunikationsinhalte und im Veranstaltungsmanagement Teilnehmerlisten, Foto- und Videoaufnahmen oder Angaben zu Essenspräferenzen verarbeitet werden können. Solche praxisnahen Beispiele tragen wesentlich dazu bei, einen Bezug zur praktischen Arbeit herzustellen, das Konzept der personenbezogenen Daten greifbarer zu machen und die Sensibilität im Umgang mit ihnen zu stärken.

Die Definition des Begriffs „Verarbeitung“ (Art. 4 Nr. 2 DSGVO) ist zwar knapp, aber präzise und zutreffend sowie durch die beispielhafte Aufzählung für Verarbeitungsvorgänge gut verständlich.

Bei der Darstellung der Rolle des „Verantwortlichen“ (Art. 4 Nr. 7 DSGVO) wird zutreffend auf die Steuerung von Zweck und Mittel der Datenverarbeitung verwiesen. Die Formulierungen „unsere Organisation ist Verantwortlicher“ und „wir entscheiden über Zweck und Mittel der Verarbeitung“ könnten durch ihre Absolutheit jedoch zu Missverständnissen führen. So ist es durchaus möglich, dass eine Organisation auch als Auftragsverarbeiter (Art. 28 DSGVO) tätig wird und sodann gerade nicht über die Zwecke und Mittel der Verarbeitung entscheidet. Es hätte hier also eine Abgrenzung zu Auftragsverarbeiteuren und gemeinsam Verantwortlichen (Art. 26 DSGVO) ergänzt werden können. Insbesondere in größeren Organisationen wäre zudem eine Differenzierung zwischen den verschiedenen unternehmensinternen Rollen hilfreich – auch um die Verantwortlichkeiten und die Aufgabenverteilung im Datenschutz besser nachvollziehen zu können. Zwar unterscheiden sich Rollen und Aufgabenbereiche je nach Organisation, es hätten jedoch (wie auch an anderen Stellen) Platzhalter für organisationsspezifische Konkretisierungen vorgesehen werden können.

3. Die Grundsätze der DSGVO

Im Abschnitt zu den Grundsätzen der DSGVO (Art. 5 DSGVO) wird das Vorliegen einer Rechtsgrundlage zutreffend als zentrale Voraussetzung der Rechtmäßigkeit einer Verarbeitung personenbezogener Daten beschrieben. Das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ wird nicht genannt. Positiv ist jedoch, dass es aus der Formulierung „Jede Verarbeitung personenbezogener Daten braucht eine

Rechtsgrundlage“ indirekt hervorgeht. Jedoch bleibt es bei einer sehr allgemein gehaltenen und unvollständigen Aufzählung der Rechtsgrundlagen, ohne inhaltliche Erläuterung. Positiv hervorzuheben sind grundsätzlich die genannten Beispiele. Eine Einordnung und nähere Erläuterung wären jedoch besonders bei der Einwilligung und dem berechtigten Interesse geboten gewesen. Bei der Einwilligung fehlen jegliche Hinweise auf deren Voraussetzungen nach Art. 7 DSGVO. Zudem wird – anders als bei den anderen Rechtsgrundlagen, die aufgelistet werden – kein Beispiel genannt, in dem die Einwilligung als Rechtsgrundlage in Betracht kommt. Das könnte in Kombination mit der Erwähnung an erster Stelle den Eindruck erwecken, dass die Einwilligung für sehr viele Verarbeitungen die Rechtsgrundlage der Wahl ist, obwohl die Einwilligung in der Praxis nur dann eingeholt werden sollte, wenn keine andere Rechtsgrundlage in Frage kommt.¹⁵ Beim berechtigten Interesse fehlt jeder Hinweis auf die vorzunehmende Interessenabwägung und deren Anforderungen – ein in der Praxis besonders fehleranfälliger Punkt. Das dort gewählte Beispiel zur Videoüberwachung ist zu absolut, da es ohne rechtliche Relativierung oder Kontextualisierung erfolgt.¹⁶ Positiv hervorzuheben sind die Hinweise zur praktischen Umsetzung der Rechtmäßigkeit der Verarbeitung. Auffällig ist jedoch, dass hier bei Unsicherheiten auf den Datenschutzbeauftragten verwiesen wird, welchen es in einigen Organisationen jedoch gar nicht gibt und gemäß Art. 38 DSGVO (bzw. § 38 BDSG) auch nicht geben muss.

Es wird nicht auf die (Teil-)Grundsätze des „Treu und Glaubens“ und der „Transparenz“ eingegangen. Insbesondere Letzteres ist für die praktische Umsetzung des Datenschutzes relevant, so dass hier bereits auf die Informationspflichten (Art. 13, 14 DSGVO) des Verantwortlichen hätte hingewiesen werden können.

Der Abschnitt zur Zweckbindung gibt den Grundsatz der „Zweckbindung“ nicht vollständig wieder. Die Aussage, dass Daten ausschließlich für den ursprünglich festgelegten Zweck verwendet werden dürfen, ist zwar nicht falsch, greift jedoch zu kurz, da eine Weiterverarbeitung nach Art. 5 Abs. 1 lit. b DSGVO zulässig sein kann, wenn die Weiterverarbeitung nicht in einer Weise erfolgt, die mit dem ursprünglichen Verarbeitungszweck unvereinbar ist, insbesondere unter den in Art. 6 Abs. 4 DSGVO bestimmten Voraussetzungen. Ebenso ist das aufgeführte Beispiel zu absolut. So können Kundendaten unter den Voraussetzungen des § 7 UWG auch zu Werbezwecken eingesetzt werden. Dies folgt implizit auch aus Erwägungsgrund 47 DSGVO. Die Tipps zur praktischen Umsetzung sind hier jedoch gut gewählt.

Der Grundsatz der „Datenminimierung“ wird knapp und verständlich dargestellt. Die gewählten Beispiele und Hinweise zur praktischen Umsetzung sind richtig, hilfreich und praxisrelevant.

Der Grundsatz der „Richtigkeit“ wird im Wesentlichen zutreffend dargestellt. Im Zusammenhang mit der Aktualität von personenbezogenen Daten fehlt jedoch der Zusatz „erforderlichenfalls“, so wie es auch in Art. 5 Abs. 1 lit. d DSGVO vorgesehen ist. Dieser Begriff verdeutlicht, dass personenbezogene Daten nur dann aktualisiert werden müssen, wenn dies im Einzelfall auch erforderlich ist. Mangels des Zusatzes könnte der Eindruck entstehen, dass personenbezogene Daten immer aktualisiert werden müssen.¹⁷ Eine weitere Ungenauigkeit enthält die Schulung in den Hinweisen zur praktischen Umsetzung. Dass unrichtige Daten gelöscht werden sollen, wenn keine Berichtigung möglich ist, ist weder aus datenschutzrechtlicher Sicht erforderlich noch aus praktischer

¹⁵ EDSA, Leitlinien 05/2020, Rdnr. 122.

¹⁶ Selbst die Intensität des Grundrechtseingriffs durch Videoüberwachungen kann nicht pauschal festgelegt werden, sondern hängt von mehrere Abwägungsfaktoren wie der Größe des überwachten Bereichs, Zahl der überwachten Personen, Nutzungszweck der Videoüberwachung ab, vgl. EDSA, Leitlinien 3/2019, Rdnr. 22, 34.

¹⁷ Heberlein, in: Ehmann/Selmayr, DSGVO, Art. 5 Rdnr. 32; Reimer, in: Sydow/Marsch, Art. 5 Rdnr. 40.

3. KI-generierte Schulungen

Sicht immer sinnvoll. So kann in bestimmten Fällen auch kein Anspruch auf Berichtigung bestehen. Zudem muss gemäß Art. 17 DSGVO nicht immer eine Löschung unrichtiger Daten erfolgen, in bestimmten Fällen kommt stattdessen auch eine Einschränkung der Verarbeitung in Frage.¹⁸

Der Grundsatz der „Speicherbegrenzung“ wird zwar nur oberflächlich dargestellt, trifft jedoch den Kern des Grundsatzes und ist gut verständlich. Das gewählte Beispiel zur Aufbewahrungsfrist von Rechnungen ist allerdings falsch: Diese dürfen nicht 10 Jahre, sondern lediglich 8 Jahre aufbewahrt werden.¹⁹

Die Inhalte der Beschreibung des Grundsatzes der „Integrität und Vertraulichkeit“ sind zwar nicht falsch, es fehlt jedoch der Hinweis, dass personenbezogene Daten auch vor einer unrechtmäßigen Verarbeitung und vor einer unbeabsichtigten Schädigung zu schützen sind. Es fehlt darüber hinaus der Hinweis, dass dieser Schutz durch geeignete technische und organisatorische Maßnahmen herzustellen ist. Die Hinweise zur praktischen Umsetzung führen zwar (beispielhafte) technische und organisatorische Maßnahmen auf, versäumt wird jedoch explizit zu benennen, dass es sich hierbei um technische und organisatorische Maßnahmen handelt sowie, dass es sich hierbei um Beispiele handelt. Hervorzuheben ist im Zusammenhang mit den Hinweisen zur praktischen Umsetzung außerdem der folgende Hinweis „Melden Sie Sicherheitsvorfälle sofort“. Mangels Konkretisierung dahingehend, an wen Sicherheitsvorfälle zu melden sind (was im Übrigen auch organisationsspezifisch unterschiedlich sein wird), könnte der Hinweis so verstanden werden, dass entsprechende Vorfälle an die offiziellen Aufsichtsbehörden gemeldet werden sollen. Dies dürfte in der Praxis i. d. R. nicht ohne eine vorherige interne Abstimmung gewünscht sein. Verstärkt wird dies durch den Umstand, dass jegliche Erläuterung hinsichtlich des Begriffs „Sicherheitsvorfall“ fehlt, was wiederum dazu führt, dass Mitarbeitende nicht einschätzen können, was ein Sicherheitsvorfall ist und demnach auch nicht einschätzen können, was sie (an wen) melden müssen. Insbesondere fehlt jegliche Verknüpfung – auch begrifflich – zu den in Kapitel 6. behandelten Inhalten.

Es fehlt der Hinweis auf die „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO, Art. 24 DSGVO). Die Schulung verschweigt, dass der Verantwortliche die Einhaltung der DSGVO nachweisen können muss und versäumt in diesem Zusammenhang auf die Dokumentationspflicht hinzuweisen.

4. Betroffenenrechte – Was müssen Sie wissen?

Positiv fällt auf, dass fast alle wesentlichen Betroffenenrechte aufgezählt werden. Gänzlich unerwähnt bleiben jedoch die „Informationspflicht“ (Art. 13, 14 DSGVO), das „Recht auf Widerruf der Einwilligung“ (Art. 7 Abs. 3 DSGVO), die „Mitteilungspflicht“ (Art. 19 DSGVO) sowie das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO).

Die Erklärungen zu den verschiedenen Rechten der betroffenen Person sind zwar grundsätzlich richtig und verständlich, jedoch teilweise stark verkürzt. Das „Auskunftsrecht“ (Art. 15 DSGVO) wird nicht in seiner gesamten Reichweite dargestellt. Es wird allein dargestellt, dass betroffene Personen erfragen können, welche Daten über sie gespeichert wurde. Es fehlt jedoch die Information, dass auch Auskunft über Herkunft, Zweck, Empfänger, Speicherdauer, Betroffenenrechte, das Bestehen einer automatisierten Entscheidungsfindung und etwaige Drittlandübermittlungen zu erteilen ist. Auch die Beschreibung des Vorgehens bei Auskunftsanfragen dürfte nicht für jede Organisation passend sein. Zwar wird die Weiterleitung von Auskunftsanfragen an den

¹⁸ Vgl. Art. 18 Abs. 1 lit. a DSGVO (Einschränkung der Verarbeitung bei bestrittener Richtigkeit); Art. 17 Abs. 3 DSGVO (Ausnahmen vom Löschungsrecht).

¹⁹ Brandl, in: Bunjes, UStG § 26a Rdnr. 17.

Datenschutzbeauftragten in vielen Organisationen so gelebt, es gibt jedoch auch Organisationen, die gar keinen Datenschutzbeauftragten haben oder in denen die Aufgaben anders verteilt sind. Zudem könnte die Erwähnung der einmonatigen Antwortfrist (Art. 12 Abs. 3 DSGVO) zu Missverständnissen führen. Zwar ist es grundsätzlich richtig, dass Betroffenenrechte i. d. R. innerhalb eines Monats umgesetzt und beantwortet werden müssen, gleichzeitig weist die Schulung jedoch darauf hin, dass die Mitarbeitenden die Anfragen lediglich an den Datenschutzbeauftragten weiterleiten sollen und im Übrigen gerade nicht selbst tätig werden sollen.

Beim „Recht auf Berichtigung“ (Art. 16 DSGVO) wäre eine Ergänzung dahingehend hilfreich, wann Daten unrichtig sind – etwa, wenn sie objektiv falsch oder veraltet sind oder im falschen Kontext stehen. Werturteile, wie Meinungen, können hingegen nicht „unrichtig“ sein. Im Zusammenhang mit dem „Recht auf Löschung“ (Art. 17 DSGVO) wird zwar dessen Grundsatz genannt, nicht jedoch dessen Abhängigkeit von den Voraussetzungen des Art. 17 Abs. 1 DSGVO. Ebenso wenig wird auf die Ausnahmen des Art. 17 Abs. 3 DSGVO hingewiesen. Das „Recht auf Vergessenwerden“ wird nur im Zusammenhang mit dem Recht auf Löschung genannt und nicht separat erklärt. Es fehlt der Hinweis auf Art. 17 Abs. 2 DSGVO, wonach ein Verantwortlicher, der Daten öffentlich gemacht hat, auch Dritte zur Löschung auffordern muss.

Einige weitere Rechte der betroffenen Person – „Einschränkung“ (Art. 18 DSGVO), „Datenübertragbarkeit“ (Art. 20 DSGVO), „Widerspruch“ (Art. 21 DSGVO) – werden lediglich stichwortartig ohne jegliche Erläuterung erwähnt. Eine grundlegende Erklärung, etwa zur Datenübertragbarkeit im Sinne eines maschinenlesbaren Formats oder etwa zum Widerspruch, wäre selbst bei knapper Darstellung sinnvoll gewesen. Einen erheblichen Mangel stellt zudem das Fehlen der „Informationspflichten“ (Art. 13, 14 DSGVO) dar. Ohne entsprechenden Hinweis können Mitarbeitende nicht wissen, dass bei Aufnahme einer neuen Verarbeitungstätigkeit eine Datenschutzinformation gegenüber der betroffenen Person bereitzustellen ist.

5. Technische und organisatorische Maßnahmen

Die Darstellung der technischen und organisatorischen Maßnahmen ist insgesamt gelungen und anschaulich, wenn auch nicht für jede Organisation 1:1 anwendbar. Die Begriffe werden mit einigen konkreten Beispielen hinterlegt und auf den Arbeitsalltag übertragen. Jedoch fehlt der Hinweis, dass die Auswahl der Maßnahmen risikobasiert erfolgen muss (Art. 24, 25 und 32 DSGVO). Auffällig ist des Weiteren, dass die aufgeführten technischen und organisatorischen Maßnahmen vor allem die Sicherheit der Verarbeitung personenbezogener Daten i. S. v. Art. 32 DSGVO betreffen. Technische und organisatorische Maßnahmen zur Sicherstellung und zum Nachweis, dass die gesamte Verarbeitung gemäß der DSGVO erfolgt und dass insbesondere die Grundsätze der Verarbeitung nach Art. 5 Abs. 1 DSGVO umgesetzt werden (Art. 24 und 25 DSGVO), werden dagegen nicht erwähnt. In diesem Zusammenhang fehlen insbesondere Hinweise auf „Privacy by Design“ und „Privacy by Default“.

6. Datenschutzverletzungen erkennen und melden

Der Abschnitt zu Datenschutzverletzungen gibt die Definition der DSGVO im Wesentlichen zutreffend wieder. Positiv hervorzuheben sind die gewählten Beispiele, die Hinweise auf die Dokumentationspflicht und die Aufforderung zum Stoppen der Verletzungshandlung. Eine Vertiefung der Begriffe „Vernichtung, Verlust, Veränderung und Offenlegung“ – etwa durch kurze Beispiele – hätte helfen können, das Verständnis zu schärfen.

Die Darstellung der Meldepflichten im Falle einer Datenschutzverletzung bleibt zu pauschal. Es fehlen Hinweise auf das Erfordernis einer Risikobewertung, auf die Meldepflicht gegenüber der Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO) und die

3. KI-generierte Schulungen

Unterrichtungspflicht gegenüber den betroffenen Personen (Art. 34 DSGVO). Ebenso fehlt die Klarstellung, dass Datenschutzverletzungen nur dann zu melden sind, wenn sie mindestens mit einem Risiko verbunden sind, nicht jedoch bei einem geringen Risiko. Auch fehlt der Hinweis, dass die Einschätzung idealerweise gemeinsam mit einer für den Datenschutz zuständigen Person innerhalb der Organisation erfolgen sollte (je nach Organisation z. B. der Datenschutzkoordination, dem Datenschutzbeauftragten, der Geschäftsführung oder einer benannten Person) und keine unabgesprochene Meldung und Benachrichtigung nach den Art. 33, 34 DSGVO erfolgen soll. Die interne Kommunikation an Vorgesetzte, Datenschutzbeauftragte und IT-Abteilung wird zwar genannt, bleibt aber oberflächlich. Zudem ist davon auszugehen, dass nicht jede Organisation über einen Datenschutzbeauftragten oder eine IT-Abteilung verfügt. Hier wären also unternehmensspezifische Anpassungen erforderlich – sowohl hinsichtlich zuständiger Personen als auch hinsichtlich unternehmensinterner Vorfallprozesse oder Vorlagen (z. B. Meldeformulare). Platzhalter hätten eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

7. Praktische Tipps für den Arbeitsalltag

Die praktischen Tipps für den Arbeitsalltag sind gelungen. Sie sind klar strukturiert und auf typische Alltagssituationen im Arbeitsumfeld zugeschnitten, wenn auch nicht 1:1 auf jede Organisation anwendbar. Die Unterteilung in Themenbereiche wie E-Mail-Verkehr, Arbeitsplatzsicherheit und mobile Geräte erleichtert die Orientierung und trägt zur leichten Zugänglichkeit und Umsetzbarkeit der Inhalte bei. Die Formulierung als „Do's“ und „Don'ts“ ist praxisnah und handlungsorientiert. Sie zeigt nicht nur, was zu tun ist, sondern auch, was vermieden werden sollte. Die Beispiele sind konkret und realistisch und können Mitarbeitenden helfen, sich in ihrem Arbeitsalltag datenschutzkonform zu verhalten.

8. Häufige Fragen und Antworten

Die häufigen Fragen und Antworten sind grundsätzlich praxisnah formuliert und greifen typische Unsicherheiten aus dem Arbeitsalltag auf. Die Antworten sind klar, verständlich und geben konkrete Handlungsanweisungen, ohne juristisch überfrachtet zu wirken. Besonders hilfreich ist der Hinweis, bei Unsicherheiten lieber Rücksprache zu halten, denn das kann ein verantwortungsbewusstes Verhalten im Umgang mit personenbezogenen Daten fördern. Die Antworten stärken das Bewusstsein für den Datenschutz und zeigen, wie Mitarbeiter sich in arbeitstypischen Situationen – etwa beim Umgang mit Kundendaten, E-Mails oder telefonischen Anfragen – richtig verhalten können.

9. Wichtige Kontakte

Die Übersicht zu den wichtigen Kontakten bietet Mitarbeitenden eine schnelle Orientierung. Die strukturierte Darstellung mit Platzhaltern für Name, E-Mail und Telefonnummer ermöglicht eine einfache Anpassung an die jeweilige Organisation. Aus didaktischer Sicht wäre es sinnvoll, diesen Abschnitt am Ende der Schulung zu platzieren. So wird der Informationsfluss nicht unterbrochen und die Kontaktinformationen stehen dort zur Verfügung, wo sie im Bedarfsfall am schnellsten auffindbar sind.

10. Selbsttest: Haben Sie alles verstanden?

Der Selbsttest mit drei realitätsnahen Szenarien ist gelungen und motivierend. Die gewählten Situationen spiegeln häufige Probleme im Arbeitsalltag wider, und die jeweiligen Lösungen sind nachvollziehbar. Ergänzt werden könnte ein Hinweis darauf, an wen konkrete Vorfälle (intern) zu melden sind. Es ist davon auszugehen, dass es regelmäßig nicht im Interesse einer Organisation liegt, dass datenschutzrelevante Vorfälle unreflektiert und unabgesprochen an die zuständige Aufsichtsbehörde gemeldet werden.

11. Abschluss und Verpflichtung

Der Abschnitt ist ebenfalls gelungen. Besonders positiv fällt auf, dass er nicht nur zusammenfasst, sondern den Mitarbeitende auch zur persönlichen Verantwortung motiviert. Die Kombination aus Selbstverpflichtung einerseits und die Erinnerung an die Bedeutung des Datenschutzes andererseits, schafft eine gute Balance zwischen Pflicht und eigenem Nutzen und stärkt so eine verantwortungsbewusste Haltung. Die Selbstverpflichtungspunkte sind praxisnah und stärken das Bewusstsein für die eigene Rolle im Datenschutz. Gleichzeitig vermitteln die abschließenden Hinweise („Im Zweifelsfall: Fragen Sie nach!“) eine unterstützende Haltung, die Unsicherheiten nicht sanktioniert, sondern zur aktiven Klärung ermutigt. Das ist didaktisch wertvoll und fördert eine offene, verantwortungsbewusste Unternehmenskultur.

Zusammenfassend bietet die Schulung eine in ihrer Darstellung verständliche und adressatengerechte Einführung in das Datenschutzrecht. Der Aufbau ist logisch und orientiert sich sinnvoll an der Struktur der DSGVO. Icons und klare Lernziele fördern die Lesbarkeit und Motivation. Besonders positiv hervorzuheben sind die praxisnahen Beispiele (z. B. E-Mail-Versand, Clean-Desk, Zugriffskontrolle), die den konkreten Nutzen für Mitarbeitende erhöhen. Die Inhalte sind größtenteils richtig und praxisnah aufbereitet, weisen jedoch an vielen Stellen rechtliche Verkürzungen und fehlende Definitionen auf. So wird bspw. die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) nicht erwähnt bzw. erläutert, obwohl sie bei hohem Risiko verpflichtend ist. Ebenso wenig erfolgt kein Hinweis, dass Verantwortliche und Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten führen müssen (Art. 30 DSGVO). Zudem werden keine konkreten Normen genannt, sodass neue Mitarbeitende nicht wissen, wo sie weiterführende Informationen finden können. Abweichende Rahmenbedingungen, insbesondere kleinerer Organisationen bleiben unberücksichtigt – etwa der Umstand, dass manche Organisationen über keinen Datenschutzbeauftragten verfügen, lediglich flache Hierarchien pflegen und über keine IT-Abteilung verfügen. Ebenso bleiben naturgemäß spezifische Anforderungen von (größeren) Organisationen unberücksichtigt – etwa interne Abläufe, Zuständigkeiten oder Organisationsanweisungen. Die Einheit ist als Einstiegsmaterial geeignet, ist jedoch als vollständige DSGVO-Schulung unzureichend.

3.2 Command-a-03-2025 (Cohere, Anwendung: Cohere Playground)

3.2.1 KI-generierter Inhalt²⁰

Selbstlerneinheit: Grundlagen des Datenschutzrechts gemäß DSGVO

Für neue Mitarbeiter:innen in Organisationen, die unter die Datenschutz-Grundverordnung (DSGVO) fallen

Einführung

Willkommen in unserer Organisation! Als neue:r Mitarbeiter:in ist es wichtig, dass Sie die Grundlagen des Datenschutzrechts verstehen und wissen, wie Sie diese in der Praxis umsetzen können. Diese Selbstlerneinheit vermittelt Ihnen das notwendige Wissen zur Datenschutz-Grundverordnung (DSGVO), die in unserer Organisation Anwendung findet.

1. Was ist die DSGVO?

Die **Datenschutz-Grundverordnung (DSGVO)** ist eine europaweit geltende Verordnung, die den Schutz personenbezogener Daten sicherstellt. Sie trat am **25. Mai**

²⁰ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell Command-a-03-2025 über Cohere Playground generiert.

3. KI-generierte Schulungen

2018 in Kraft und gilt für alle Organisationen, die personenbezogene Daten von Personen in der EU verarbeiten, unabhängig vom Sitz der Organisation.

Ziel der DSGVO:

- Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere des Rechts auf Schutz personenbezogener Daten.
- Sicherstellung des freien Verkehrs personenbezogener Daten innerhalb der EU.

2. Wichtige Begriffe der DSGVO

Bevor wir tiefer einsteigen, sollten Sie folgende Begriffe kennen:

- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z. B. Name, Adresse, E-Mail, IP-Adresse).
- **Verarbeitung:** Jeder Vorgang im Zusammenhang mit personenbezogenen Daten (z. B. Erheben, Speichern, Verändern, Übermitteln, Löschen).
- **Betroffene Person:** Die natürliche Person, deren Daten verarbeitet werden.
- **Verantwortlicher:** Die Organisation, die allein oder gemeinsam die Zwecke und Mittel der Datenverarbeitung festlegt (in unserem Fall: unsere Organisation).
- **Auftragsverarbeiter:** Ein externer Dienstleister, der Daten im Auftrag des Verantwortlichen verarbeitet.

3. Grundsätze der Datenverarbeitung

Die DSGVO legt sieben Grundsätze fest, die bei der Verarbeitung personenbezogener Daten beachtet werden müssen:

1. **Rechtmäßigkeit, Zweckbindung und Transparenz:** Daten dürfen nur rechtmäßig, für einen bestimmten Zweck und transparent verarbeitet werden.
2. **Datenminimierung:** Es dürfen nur die Daten erhoben werden, die für den Zweck erforderlich sind.
3. **Richtigkeit:** Daten müssen richtig und bei Bedarf aktualisiert werden.
4. **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.
5. **Integrität und Vertraulichkeit:** Daten müssen durch geeignete Maßnahmen geschützt werden.
6. **Rechenschaftspflicht:** Der Verantwortliche muss nachweisen, dass die DSGVO-Anforderungen eingehalten werden.

4. Rechtmäßigkeit der Datenverarbeitung

Daten dürfen nur verarbeitet werden, wenn eine der folgenden Rechtsgrundlagen vorliegt:

1. **Einwilligung:** Die betroffene Person hat freiwillig und informiert zugestimmt.
2. **Vertragserfüllung:** Die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich.
3. **Rechtliche Verpflichtung:** Die Verarbeitung ist gesetzlich vorgeschrieben.
4. **Schutz lebenswichtiger Interessen:** Die Verarbeitung ist notwendig, um lebenswichtige Interessen der betroffenen Person zu schützen.
5. **Öffentliches Interesse:** Die Verarbeitung ist für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich.
6. **Berechtigte Interessen:** Die Verarbeitung ist zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte der betroffenen Person überwiegen.

5. Rechte der betroffenen Personen

Die DSGVO gewährt betroffenen Personen folgende Rechte:

1. **Auskunftsrecht:** Betroffene können Auskunft über ihre gespeicherten Daten verlangen.

2. **Recht auf Berichtigung:** Falsche Daten müssen korrigiert werden.
3. **Recht auf Löschung ("Recht auf Vergessenwerden"):** Betroffene können die Löschung ihrer Daten verlangen, wenn bestimmte Voraussetzungen erfüllt sind.
4. **Recht auf Einschränkung der Verarbeitung:** Betroffene können verlangen, dass die Verarbeitung ihrer Daten eingeschränkt wird.
5. **Recht auf Datenübertragbarkeit:** Betroffene können verlangen, dass ihre Daten in einem gängigen Format übermittelt werden.
6. **Widerspruchsrecht:** Betroffene können der Verarbeitung ihrer Daten widersprechen, sofern diese auf berechtigten Interessen basiert.
7. **Recht auf Widerruf der Einwilligung:** Betroffene können ihre Einwilligung zur Datenverarbeitung widerrufen.

6. Praktische Relevanz und Tipps zur Umsetzung

Hier sind einige praktische Tipps, wie Sie die DSGVO-Anforderungen in Ihrem Arbeitsalltag umsetzen können:

- **Datenminimierung:** Erheben Sie nur die Daten, die für Ihre Aufgabe wirklich notwendig sind.
- **Transparenz:** Informieren Sie betroffene Personen klar und verständlich über die Verarbeitung ihrer Daten (z. B. über Datenschutzerklärungen).
- **Sicherheit:** Achten Sie auf die Sicherheit der Daten, z. B. durch Verschlüsselung, Zugriffsbeschränkungen und regelmäßige Backups.
- **Dokumentation:** Halten Sie fest, welche Daten Sie verarbeiten, zu welchem Zweck und auf welcher Rechtsgrundlage.
- **Schulungen:** Nehmen Sie regelmäßig an Datenschutzschulungen teil, um auf dem neuesten Stand zu bleiben.
- **Datenschutzbeauftragter:** Wenden Sie sich bei Unsicherheiten an den Datenschutzbeauftragten unserer Organisation.

7. Folgen bei Verstößen gegen die DSGVO

Verstöße gegen die DSGVO können zu hohen Geldbußen führen – bis zu **20 Millionen Euro** oder **4 % des weltweiten Jahresumsatzes**, je nachdem, welcher Betrag höher ist. Zudem können Verstöße das Vertrauen der Kunden und Partner in unsere Organisation beschädigen.

8. Zusammenfassung

Die DSGVO ist ein zentrales Instrument zum Schutz personenbezogener Daten. Als Mitarbeiter:in unserer Organisation ist es Ihre Aufgabe, die Grundsätze der DSGVO zu beachten und in der Praxis umzusetzen. Durch datenschutzgerechtes Handeln tragen Sie dazu bei, die Rechte der betroffenen Personen zu wahren und das Vertrauen in unsere Organisation zu stärken.

9. Selbsttest

Testen Sie Ihr Wissen mit den folgenden Fragen:

1. Was versteht man unter personenbezogenen Daten?
2. Nennen Sie drei Rechtsgrundlagen für die Datenverarbeitung.
3. Welche Rechte hat eine betroffene Person gemäß DSGVO?
4. Was können Sie tun, um die Datensicherheit zu gewährleisten?

10. Weiterführende Informationen

- **DSGVO-Text:** [Verordnung \(EU\) 2016/679](#)
- **Datenschutzbeauftragter unserer Organisation:** Kontaktieren Sie [Name/E-Mail] bei Fragen oder Unsicherheiten.

Vielen Dank für Ihre Aufmerksamkeit und viel Erfolg bei der Umsetzung des Datenschutzes in Ihrem Arbeitsalltag!

3.2.2 Bewertung

Die von Command-a-03-2025 erstellte Schulung zu den Grundlagen des Datenschutzes überzeugt durch einen klar strukturierten Aufbau – von der Einführung über Grundlagen, Begriffe, Grundsätze, Rechtsgrundlagen, Betroffenenrechte, Praxis, Sanktionen, Zusammenfassung, bis hin zu einem Selbsttest – sowie durch eine einsteigerfreundliche Sprache mit kurzen Sätzen und anschaulichen Beispielen. Die inhaltliche Tiefe der Kapitel ist jedoch zu gering, um ein solides Rechtsverständnis zu vermitteln: So werden bspw. die Rechtsgrundlagen lediglich stichpunktartig aufgeführt, ohne die jeweiligen Voraussetzungen zu erläutern, und verschiedene datenschutzrechtliche Grundsätze werden (teilweise falsch) zusammengefasst, ohne sie jeweils im Einzelnen zu erläutern. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einführung

Mit der Begrüßung „Willkommen in unserer Organisation!“ wird ein positiver und motivierender Einstieg gewählt. Die Zielgruppe („neue Mitarbeiter“) wird klar benannt. Die direkte Ansprache („Sie“) und der Hinweis, dass Mitarbeitenden des Unternehmens die Grundlagen des Datenschutzrechts kennen und umsetzen können müssen, stärken das Pflicht- und Verantwortungsbewusstsein. Die Erwähnung der Zielsetzung der Schulung („das notwendige Wissen zur DSGVO“) ist zwar vorhanden, allerdings fehlen konkrete Lernziele und eine Übersicht über die Inhalte, welche die Struktur und Orientierung innerhalb der Schulung erleichtern würden.

1. „Was ist die DSGVO?“

Die zeitliche Einordnung der DSGVO zum 25. Mai 2018 sowie ihr Geltungsbereich – die Verarbeitung personenbezogener Daten von Personen in der EU, unabhängig vom Sitz des Unternehmens – sind richtig dargestellt. Dabei wird jedoch versäumt klarzustellen, dass die DSGVO auch dann gilt, wenn eine Organisation ihren Sitz in der EU hat und personenbezogene Daten von Personen außerhalb der EU verarbeitet. Die Zielsetzung der DSGVO wird grundsätzlich richtig dargestellt. Der Begriff „freier Datenverkehr“ wird zwar erwähnt, jedoch nicht erklärt. Ohne diese Erklärung könnte er missverstanden werden, etwa als „Daten dürfen frei herumgereicht werden“. Zudem bleibt der Text sehr theoretisch. Es fehlt der konkrete Bezug für die Mitarbeitenden. Eine direkte Ansprache wie „Für Sie bedeutet das...“ hätte diesen Praxisbezug hergestellt und die Relevanz für den Arbeitsalltag deutlich gemacht.

2. Wichtige Begriffe der DSGVO

Es ist positiv hervorzuheben, dass wesentliche Grundbegriffe wie „personenbezogene Daten“ (Art. 4 Nr. 1 DSGVO), „Verarbeitung“ (Art. 4 Nr. 2 DSGVO), „betroffene Person“, „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO) und „Auftragsverarbeiter“ (Art. 4 Nr. 8 DSGVO) genannt werden. Ebenso erleichtern die für jeden Begriff gewählten Beispiele, wie die IP-Adresse, das Verständnis für die Mitarbeitenden. Allerdings ist die Definition des personenbezogenen Datums verkürzt. Es fehlt eine Erläuterung des Unterschieds zwischen den Begriffen identifiziert und identifizierbar. Da es für die Fähigkeit Informationen als personenbezogene Daten einzuführen, zentral ist zu verstehen, wann eine natürliche Person identifizierbar ist, könnte die fehlende Erläuterung zu einem mangelnden Verständnis und einer mangelnden Umsetzung in der Praxis führen. Ebenso fehlt die Unterscheidung zwischen direkt und indirekt identifizierenden Daten. Auch die Unterscheidung zwischen personenbezogenen, anonymen und pseudonymen Daten fehlt. Zu einem mangelnden Verständnis kann zudem der Umstand führen, dass der Begriff der „natürlichen Personen“ nicht erläutert wird. Insbesondere bei Mitarbeitenden

mit wenig juristischen Vorkenntnissen kann nicht vorausgesetzt werden, dass sie den Begriff der natürlichen Person kennen. Es wäre dem Verständnis weiterhin zuträglich gewesen, Beispiele für personenbezogene Daten aufzulisten, die in den verschiedenen Unternehmensbereichen typischerweise vorkommen.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) und deren erhöhte Schutzanforderungen werden nicht behandelt. Die Definition der „betroffenen Person“ entspricht zwar nicht dem Wortlaut des Art. 4 Nr. 1 DSGVO („identifizierte oder identifizierbare natürliche Person“), ist für Mitarbeitende jedoch verständlich. Sinnvoll wäre hier jedoch gewesen, einen Bezug zu der Begriffsbestimmung hinter „identifizierte oder identifizierbare natürliche Person“ der Zusatz „(sog. betroffene Person)“ ergänzt worden wäre. Bei der Definition des Verantwortlichen ist positiv zu vermerken, dass „Zwecke und Mittel“ erwähnt werden und dass auch darauf hingewiesen wird, dass gemeinsam (mit jemand anderem) über die Zwecke und Mittel entschieden werden kann. Die Beschreibung des Auftragsverarbeiters hätte um Hinweise zu dessen Weisungsgebundenheit ergänzt werden können. Negativ anzumerken ist die in der Schulung verwendete verkürzte Formulierung „Daten“ statt „personenbezogene Daten“. Dies ist problematisch, da so der Eindruck erweckt wird, auch nicht personenbezogene Daten könnten dem Anwendungsbereich der DSGVO unterliegen.

3. Grundsätze der Datenverarbeitung

Positiv ist, dass alle wesentlichen Grundsätze der DSGVO (Art. 5 DSGVO) angesprochen werden – einschließlich der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) – und dass die Kurzbeschreibungen gut verständlich sind. Ebenfalls fällt positiv ins Gewicht, dass der Wortlaut der DSGVO „Grundsätze“ genutzt wird. Negativ fällt jedoch auf, dass Rechtmäßigkeit, Zweckbindung und Transparenz falsch zusammengefasst werden, denn der Grundsatz der „Zweckbindung“ ist ein eigenständiger Grundsatz. Bei dem Grundsatz der „Rechtmäßigkeit“ fehlt zudem der Hinweis auf die notwendige Rechtsgrundlage (Art. 6 Abs. 1 DSGVO). Auch die Wortlautverkürzungen der einzelnen Grundsätze sind problematisch: Bei dem Grundsatz der „Zweckbindung“ fehlt der Hinweis, dass eine Weiterverarbeitung zu anderen Zwecken als dem Erhebungszweck zulässig sein kann, wenn sie mit dem ursprünglichen Zweck vereinbar ist (Art. 6 Abs. 4 DSGVO). Bei dem Grundsatz der „Datenminimierung“ wird nicht hinreichend deutlich, dass die Daten nach Art. 5 Abs. 1 lit. c DSGVO „dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt“ sein müssen. Dies hätte etwa durch Formulierungen wie „unbedingt erforderlich“ oder „tatsächlich notwendig“ verdeutlicht werden können. Im Zusammenhang mit dem Grundsatz der „Richtigkeit“ wird nicht hinreichend deutlich, dass es um die sachliche Richtigkeit von Daten geht. Positiv hervorzuheben ist jedoch, dass durch die Formulierung „bei Bedarf aktualisiert“ zumindest implizit deutlich wird, dass personenbezogene Daten nur „erforderlichenfalls auf dem neuesten Stand“ sein müssen, ohne dass eine generelle Aktualisierungspflicht besteht. Der Grundsatz der „Speicherbegrenzung“ wird zwar nur kurz und knapp dargestellt, trifft jedoch den Kern des Grundsatzes und ist gut verständlich. Bei dem Grundsatz „Integrität und Vertraulichkeit“ fehlen Hinweise darauf, dass es um die Sicherheit der Daten geht und wovor die Daten konkret zu schützen sind. Zudem fehlen ein Bezug zu den technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) sowie Praxisbeispiele und konkrete Umsetzungstipps.

4. Rechtmäßigkeit der Datenverarbeitung

Positiv hervorzuheben ist, dass alle sechs Rechtsgrundlagen aus Art. 6 Abs. 1 DSGVO genannt werden und jeweils kurze, verständliche Erläuterungen gegeben sind. Es hätte jedoch ein stärkerer Bezug zum zugrundeliegenden (Teil-)Grundsatz der Rechtmäßigkeit Bezug genommen werden können, um einen stärkeren Bezug zwischen Theorie und praktischer Bedeutung herzustellen. Auch wird das grundlegende Prinzip des „Verbots

mit Erlaubnisvorbehalt“ nicht genannt. Positiv ist jedoch, dass es aus der Formulierung „Daten dürfen nur verarbeitet werden, wenn eine der folgenden Rechtsgrundlagen vorliegt“ indirekt hervorgeht.

Notwendig wäre gewesen, auf die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) einzugehen und diesbezüglich klarzustellen, dass besondere Voraussetzungen gelten, die sich aus Art. 9 DSGVO ergeben. Ebenso hätten praxisnahe Beispiele für die einzelnen Rechtsgrundlagen geholfen, um den Transfer in die Praxis zu ermöglichen und das Verständnis zu erhöhen.

5. Rechte der betroffenen Personen

Positiv fällt auf, dass fast alle Betroffenenrechte aufgezählt werden. Jedoch bleibt die Mitteilungspflicht (Art. 19 DSGVO) sowie das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO), gänzlich unerwähnt. Auch die Informationspflichten nach Art. 13 und 14 DSGVO werden vollständig ausgelassen. Dies ist in Anbetracht deren zentraler Relevanz eine erhebliche Lücke.

Die Erklärungen zu den verschiedenen Rechten der betroffenen Person sind zwar grundsätzlich richtig und verständlich, jedoch teilweise stark verkürzt. So wird lediglich im Zusammenhang mit dem Löschrecht (Art. 17 DSGVO) und dem Recht auf Datenübertragbarkeit (Art. 20 DSGVO) (hier jedoch unvollständig) auf bestehende Voraussetzungen hingewiesen, ohne Konkretisierung der einschlägigen Voraussetzungen. Besonders beim Löschrecht fehlt ein Hinweis auf dessen Abhängigkeit von den Voraussetzungen des Art. 17 Abs. 1 DSGVO und die Ausnahmen des Art. 17 Abs. 3 DSGVO sowie ein Hinweis auf Abs. 2, wonach ein Verantwortlicher, der Daten öffentlich gemacht hat, auch Dritte zur Löschung auffordern muss. Im Übrigen entsteht durch die absolute Formulierung der Betroffenenrechte der Eindruck, dass diese grundsätzlich gelten. So wird etwa im Zusammenhang mit dem Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) erläutert, dass Betroffene verlangen können, dass die Verarbeitung ihrer Daten eingeschränkt wird. Dies könnte insbesondere in Kombination mit fehlenden Hinweisen zu Fristen (Art. 12 Abs. 3 DSGVO) und internen Zuständigkeiten und Abläufen dazu führen, dass bei entsprechenden Betroffenenanträgen unreflektiert die Verarbeitung eingeschränkt wird. Zudem enthalten die Erläuterungen einige punktuelle Ungenauigkeiten: Das „Auskunftsrecht“ (Art. 15 DSGVO) wird unvollständig dargestellt, da nicht erwähnt wird, dass auch Auskünfte über bestimmte Informationen (z. B. über Verarbeitungszwecke, Datenherkunft, Datenempfänger und Speicherdauer, Betroffenenrechte, das Bestehen einer automatisierten Entscheidungsfindung und etwaige Drittlandübermittlungen) erteilt werden müssen. Bei dem „Recht auf Berichtigung“ (Art. 16 DSGVO) fehlt eine Definition, wann Daten „falsch“ sind. Beim Recht auf „Lösung“ fehlt die Abgrenzung zum sogenannten „Recht auf Vergessenwerden“. Insgesamt fehlen Praxisbeispiele und Praxistipps.

6. Praktische Relevanz und Tipps zur Umsetzung

Positiv zu vermerken sind die praxisnahen Hinweise zu Datenminimierung, Transparenz, Sicherheit, Dokumentation, Schulung und dem Kontakt zum Datenschutzbeauftragten, die alltagsrelevant und verständlich aufbereitet sind. Letzteres setzt jedoch voraus, dass die Organisation über einen Datenschutzbeauftragten verfügt und dass der Verweis auch zur internen Zuständigkeit und Aufgabenverteilung passt. Einige Formulierungen sind knapp oder unklar, etwa „Halten Sie fest, welche Daten Sie verarbeiten...“, ohne zu erläutern, was genau, wie, wo und von wem festgehalten werden soll. Hier hätte z. B. auch auf die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, hingewiesen werden können. Zudem wäre hier ein geeigneter Platz, um Hinweise zu internen Zuständigkeiten, Dokumenten, Verfahren und Richtlinien zu ergänzen.

7. Folgen bei Verstößen

Positiv fällt auf ist, dass der Bußgeldrahmen richtig nach Art. 83 DSGVO dargestellt wird, dass Vertrauensverlust als immaterieller Schaden sinnvoll benannt wird. Negativ fällt jedoch auf, dass keine Erklärung oder Definition gegeben wird, wann ein Verstoß gegen die DSGVO vorliegt.

8. Zusammenfassung

Abschließend wird kurz und knapp zusammengefasst, warum die DSGVO wichtig ist. In diesem Zusammenhang wird ausdrücklich auch auf die Aufgabe der Mitarbeitenden verwiesen, den Datenschutz (mit) umzusetzen – dies fördert das Verantwortungsbewusstsein.

9. Selbsttest

Positiv ist, dass die Schulung einen Selbsttest enthält, denn ein solcher dient grundsätzlich der Selbstreflektion und der Vertiefung des Wissens. Die Fragen decken dabei zentrale Aspekte der DSGVO ab. Sie könnten jedoch etwas präziser formuliert werden und durch Hinweise oder Antwortvorschläge ergänzt werden, um den Lerneffekt zu steigern. Ebenso hätten die Lösungen mitgeliefert werden können.

10. Weiterführende Informationen

Positiv ist, dass der DSGVO-Text verlinkt ist und ein Kontakt zum Datenschutzbeauftragten genannt wird. Allerdings verfügt nicht jede Organisation über einen Datenschutzbeauftragten, sodass Platzhalter hier eine einfache und flexible Anpassung ermöglicht hätten.

Zusammenfassend bietet die Schulung eine klare Gliederung und einsteigerfreundliche Darstellung, die die wichtigsten Themen von den Grundlagen bis zu Sanktionen grundsätzlich abdeckt. Besonders positiv hervorzuheben ist der Selbsttest, der einen didaktischen Mehrwert darstellt und das Verständnis der Inhalte fördert. Allerdings ist die Schulung stellenweise juristisch nicht präzise genug und behandelt mehrere wichtige Themen nur oberflächlich oder gar nicht. So werden keine konkreten Normen genannt, sodass neue Mitarbeitende nicht wissen, wo sie weiterführende Informationen finden können. Wichtige Themen wie die Erläuterung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO), Voraussetzungen, Ausnahmen und Fristen bei den Betroffenenrechten sowie Datenschutzverletzungen und deren Meldepflichten (Art. 33 und 34 DSGVO) sowie Informationspflichten (Art. 13, 14 DSGVO) werden nicht behandelt. Ebenso fehlt die Vermittlung der Grundlogik der DSGVO des „Verbots mit Erlaubnisvorbehalt“. Auch werden das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) nicht behandelt. Technische und organisatorische Maßnahmen (Art. 32 DSGVO) werden nicht explizit erläutert. Praxisnahe Beispiele für Verstöße sowie deren Folgen fehlen ebenfalls. Zudem fehlen spezifische Handlungsanweisungen für den Arbeitsalltag. Die Schulung ist folglich gut und verständlich strukturiert, reicht jedoch inhaltlich nicht für eine vollständige DSGVO-Grundlagenschulung aus.

3.3 DeepSeek V3 (DeepSeek AI, Anwendung: DeepSeek Chat)

3.3.1 KI-generierter Inhalt²¹

Selbstlerneinheit: Grundlagen des Datenschutzrechts nach der DSGVO

²¹ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell DeepSeek V3 über DeepSeek Chat generiert.

Einleitung

Herzlich willkommen in unserer Organisation! Als neuer Mitarbeiter spielen Sie eine wichtige Rolle beim Schutz personenbezogener Daten. Die **Datenschutz-Grundverordnung (DSGVO)** ist die zentrale Rechtsvorschrift in der EU, die den Umgang mit personenbezogenen Daten regelt. Diese Selbstlernheit vermittelt Ihnen die Grundlagen der DSGVO, ihre Bedeutung für unsere Organisation und praktische Tipps für Ihren Arbeitsalltag.

1. Warum ist Datenschutz wichtig?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z. B. Name, E-Mail, Kundennummer, Standortdaten).

Relevanz für unsere Organisation:

- **Rechtliche Pflicht:** Die DSGVO ist verbindlich – Verstöße können hohe Bußgelder nach sich ziehen.
- **Vertrauensschutz:** Kunden, Mitarbeiter und Partner vertrauen uns ihre Daten an.
- **Reputationsrisiko:** Datenschutzverletzungen schaden unserem Image.

Praxis-Tipp: Gehen Sie immer sorgfältig mit Daten um – selbst vermeintlich harmlose Informationen können sensibel sein.

2. Grundprinzipien der DSGVO

Die DSGVO basiert auf sechs zentralen Prinzipien:

Prinzip	Kurzbeschreibung	Beispiel aus der Praxis
Rechtmäßigkeit	Daten müssen legal verarbeitet werden (z. B. mit Einwilligung oder Vertragserfüllung).	Ein Kunde bestellt online – wir speichern seine Adresse nur für die Lieferung.
Transparenz	Personen müssen wissen, wie ihre Daten genutzt werden (z. B. durch Datenschutzhinweise).	Wir informieren Kunden in unserer Privacy Policy.
Zweckbindung	Daten dürfen nur für den vorher definierten Zweck genutzt werden.	Eine Bewerber-E-Mail darf nicht für Werbung verwendet werden.
Datenminimierung	Es dürfen nur die wirklich notwendigen Daten erhoben werden.	Ein Formular fragt nur ab, was wirklich benötigt wird.
Richtigkeit	Daten müssen aktuell und richtig sein.	Kundendaten werden regelmäßig aktualisiert.
Speicherbegrenzung	Daten werden nur so lange gespeichert wie nötig.	Bewerbungsunterlagen werden nach Absage gelöscht.

Prinzip	Kurzbeschreibung	Beispiel aus der Praxis
Integrität & Vertraulichkeit	Daten müssen sicher sein (z. B. durch Passwörter oder Verschlüsselung).	Vertrauliche Dokumente werden nicht offen herumliegen gelassen.

Praxis-Tipp: Fragen Sie sich bei jeder Datenverarbeitung: „*Ist das notwendig? Habe ich eine rechtliche Grundlage? Bin ich transparent?*“

3. Wichtige Begriffe und Pflichten

a) Rollen nach der DSGVO

- **Verantwortlicher** (wir als Organisation) – entscheidet über die Datenverarbeitung.
- **Auftragsverarbeiter** (externe Dienstleister) – verarbeitet Daten in unserem Auftrag (z. B. Cloud-Anbieter).

b) Betroffenenrechte

Jede Person hat unter der DSGVO Rechte, auf die wir reagieren müssen:

- **Auskunft** („Welche Daten speichern Sie über mich?“)
- **Berichtigung** („Korrigieren Sie meine falsche Adresse.“)
- **Löschen** („Löschen Sie alle meine Daten.“) – Achtung: Nicht immer möglich!
- **Datenübertragbarkeit** („Geben Sie mir meine Daten in einem gängigen Format.“)

Praxis-Tipp: Bei Anfragen von Betroffenen immer schnell und richtig reagieren – wenden Sie sich an unsere/n Datenschutzbeauftragte/n!

4. Praktische Umsetzung im Arbeitsalltag

a) Sichere Datenverarbeitung

- **Passwörter:** Nutzen Sie starke Passwörter und keine einfachen Kombinationen wie „123456“.
- **E-Mails:** Versenden Sie sensible Daten nur verschlüsselt oder über sichere Portale.
- **Papierdokumente:** Vernichten Sie vertrauliche Unterlagen (kein Papierkorb!).

b) Datenpannen melden

- Wenn Sie einen Verlust oder unrechtmäßigen Zugriff auf Daten bemerken: **sofort melden!** (z. B. an Vorgesetzte oder Datenschutzbeauftragte).

c) Homeoffice & mobile Arbeit

- Auch unterwegs: Keine sensiblen Daten in Cafés oder öffentlichen WLANs ungeschützt bearbeiten.
- Laptops/Handys immer sperren, wenn sie unbeaufsichtigt sind.

5. Zusammenfassung & nächste Schritte

- ✓ Die DSGVO schützt personenbezogene Daten und ist für uns verpflichtend.
- ✓ Grundprinzipien wie Datenminimierung und Transparenz leiten unser Handeln.
- ✓ Betroffene haben Rechte – wir müssen angemessen reagieren.
- ✓ Sichere Datenverarbeitung ist tägliche Pflicht (Passwörter, Dokumente, Meldepflicht).

Ihre Aufgabe:

- Lesen Sie unsere interne Datenschutzrichtlinie (verlinkt im Mitarbeiterportal).
- Bei Fragen: Wenden Sie sich an unsere/n Datenschutzbeauftragte/n: **[Kontakt einfügen]**.

Vielen Dank, dass Sie zum Datenschutz in unserer Organisation beitragen!

© [Organisationsname] – Version 1.0

(Diese Schulung wird regelmäßig aktualisiert. Letzte Prüfung: [Datum einfügen].)

Anpassungshinweis für die Organisation:

- Ersetzen Sie **[Organisationsname]** und **[Kontakt einfügen]** mit Ihren internen Daten.
- Optional: Fügen Sie ein Quiz oder Fallbeispiele hinzu, um den Lernerfolg zu überprüfen.
- Bei spezifischen Branchenanforderungen (z. B. Gesundheitswesen) können zusätzliche Module ergänzt werden.

Diese Einheit ist bewusst allgemein gehalten, um für alle neuen Mitarbeiter verständlich zu sein.

3.3.2 Bewertung

Die von DeepSeek V3 generierte Schulung zu den Grundlagen des Datenschutzes ist logisch aufgebaut, von Einleitung über Relevanz, Grundprinzipien sowie Begriffe und Pflichten bis hin zur praktischen Umsetzung und einer abschließenden Zusammenfassung. Die klare Gliederung der Schulung erleichtert das Lesen. Die Tabellenform bei den Grundprinzipien der DSGVO sorgt für Übersichtlichkeit. Die Sprache ist grundsätzlich einfach und verständlich und damit gut für Einsteiger ohne juristische Vorkenntnisse geeignet. Mehrere in der Schulung enthaltene Praxis-Tipps fördern den Transfer in den Arbeitsalltag. Gleichzeitig reicht die inhaltliche Tiefe nicht aus, um ein nachhaltiges Verständnis zu sichern: Inhalte werden häufig nur oberflächlich angerissen, ohne Verweis auf die einschlägigen Artikel in der DSGVO, und die Zusammenhänge zwischen Theorie und Praxis werden nicht durchgängig hergestellt. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einleitung

Mit der Begrüßung „Herzlich willkommen in unserer Organisation!“ wird ein positiver und motivierender Einstieg gewählt. Die Zielgruppe („neuer Mitarbeiter“) wird klar benannt. Die direkte Ansprache („Sie“) und der Hinweis, dass Mitarbeiter „eine wichtige Rolle“ spielen, stärken das Pflicht- und Verantwortungsbewusstsein. Die genannten Ziele der Schulung – Grundlagen, Bedeutung für die Organisation und praktische Tipps – sind verständlich formuliert. Richtig ist die Einordnung der DSGVO als zentrale EU-Rechtsvorschrift und die Betonung ihrer Bedeutung. Der sachliche Anwendungsbereich der DSGVO wird – wenn auch nur oberflächlich – erwähnt.

1. Warum ist Datenschutz wichtig?

Im Kern richtig ist die Definition der „personenbezogener Daten“ (Art. 4 Nr. 1 DSGVO). Beispiele für personenbezogene Daten sind zwar knapp, aber vorhanden. Es fehlt jedoch eine Erläuterung des Unterschieds zwischen den Begriffen „identifiziert“ und „identifizierbar“. Da es für die Fähigkeit Informationen als personenbezogene Daten einzurichten zentral ist zu verstehen, wann eine natürliche Person identifizierbar ist, könnte die fehlende Erläuterung zu einem mangelnden Verständnis und einer mangelnden Umsetzung in der Praxis führen. Ebenso fehlt die Unterscheidung zwischen direkt und indirekt identifizierenden Daten. Auch die Unterscheidung zwischen personenbezogenen, anonymen und pseudonymen Daten fehlt. Zu einem mangelnden Verständnis kann zudem der Umstand führen, dass der Begriff der „natürlichen Personen“ nicht erläutert wird. Insbesondere bei Mitarbeitenden mit wenig juristischen Vorkenntnissen kann nicht vorausgesetzt werden, dass sie den Begriff der natürlichen Person kennen. Es wäre dem Verständnis weiterhin zuträglich gewesen, Beispiele für personenbezogene Daten aufzuzählen, die in den verschiedenen Unternehmensbereichen typischerweise vorkommen. Die Definition und Einordnung der besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) fehlen gänzlich. Die drei zentralen Gründe für Datenschutz – rechtliche Pflicht, Vertrauen und Reputation – werden klar und praxisnah dargestellt. Der Bezug zur Organisation („Relevanz für unsere Organisation“) verdeutlicht

neuen Mitarbeitenden den praktischen Nutzen der Inhalte im konkreten Arbeitsumfeld. Der Praxis-Tipp ist sensibilisierend.

2. Grundprinzipien der DSGVO

Positiv ist, dass die wichtigsten Grundsätze der DSGVO (Art. 5 DSGVO) nahezu vollständig aufgeführt und in einer Tabelle mit Kurzbeschreibung und Praxisbeispiel didaktisch gut aufbereitet sind. Zudem ist der abschließende Praxis-Tipp, bei jeder Datenverarbeitung über bestimmte Fragen nachzudenken, hilfreich für die praktische Arbeit. Fachlich sollte jedoch der Begriff „Prinzipien“ durch „Grundsätze“ ersetzt werden (Art. 5 DSGVO).

Die Kurzbeschreibung und Praxisbeispiele zu den jeweiligen Grundsätzen sind kurz und prägnant sowie weitgehend richtig. Stellenweise sind die Erläuterungen jedoch fehlerhaft oder bedürfen detaillierteren Ausführungen. So ist die im Zusammenhang mit dem Grundsatz „Rechtmäßigkeit“ vorgenommene Kurzbeschreibung „Daten müssen legal verarbeitet werden“ zu unpräzise. Zutreffend wäre: Jede Verarbeitung bedarf einer Rechtsgrundlage. Das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ wird damit nicht explizit erläutert, was das Verständnis der DSGVO-Struktur erschwert. Hier hätte auch eine Aufführung und Erklärung der wichtigen Rechtsgrundlagen zur Präzisierung ergänzt werden können. Das gewählte Beispiel „Ein Kunde bestellt online – wir speichern seine Adresse nur für die Lieferung“ ist unpassend für den Grundsatz der Rechtmäßigkeit gewählt, da keine Rechtsgrundlage genannt wird. Der Grundsatz der „Zweckbindung“ (Art. 5 Abs. 1 lit. b DSGVO) ist verkürzt – er bezieht sich lediglich auf die Datenverarbeitung für einen vorher definierten Zweck, ohne auf die Möglichkeit einer Weiterverarbeitung bei Zweckvereinbarkeit einzugehen. Auch der Grundsatz der „Richtigkeit“ (Art. 5 Abs. 1 lit. d DSGVO) wird sowohl in der Kurzbeschreibung als auch im Praxisbeispiel zu absolut dargestellt; es fehlt die Klarstellung, dass Daten lediglich „sachlich richtig und erforderlichenfalls auf dem neuesten Stand“ sein müssen. Bei dem Grundsatz der „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f DSGVO) könnte der Schutzgegenstand verdeutlicht werden, um das Verständnis zu erhöhen (vor welchen Risiken müssen Daten sicher sein). Zudem fehlt die Klarstellung, dass die Sicherheit durch „geeignete technische und organisatorische Maßnahmen“ (Art. 32 DSGVO) gewährleistet sein muss. Außerdem ist die Formulierung des Praxisbeispiels „Vertrauliche Dokumente werden nicht offen herumliegen gelassen“ stilistisch und grammatisch falsch. Schließlich fehlt der (Teil-)Grundsatz von „Treu und Glauben“ (Art. 5 Abs. 1 lit. a DSGVO) und die „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO). Letzteres ist eine zentrale Anforderung der DSGVO und sollte daher in einer Grundlagenschulung Erwähnung finden.

3. Wichtige Begriffe und Pflichten

Im Grundsatz verständlich sind die Beschreibungen von „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO) und „Auftragsverarbeiter“ (Art. 4 Nr. 8 DSGVO). Es fehlt jedoch eine Erläuterung der Rolle der betroffenen Person. Zudem mangelt es diesem Abschnitt an juristischer Präzision. Der Kern aus Art. 4 Nr. 7 DSGVO („entscheidet über Zwecke und Mittel der Verarbeitung“) wird in der Beschreibung des Verantwortlichen nicht hinreichend deutlich. Ebenso wenig wird im Zusammenhang mit dem Auftragsverarbeiter klargestellt, dass dieser weisungsgebunden agiert. Das Cloud-Beispiel ist gleichwohl gut und verständlich gewählt. Negativ fällt außerdem auf, dass die Schulung pauschal feststellt „wir als Organisation“ sind Verantwortlicher und „externe Dienstleister“ sind Auftragsverarbeiter. Hierdurch könnte der Eindruck entstehen, dass die Beteiligung einer weiteren Partei immer mit einem Auftragsverhältnis einhergeht, obwohl insbesondere auch eine gemeinsame Verantwortlichkeit (Art. 26 DSGVO) möglich ist.

Die Auflistung der Betroffenenrechte benennt zwar wichtige Betroffenenrechte, bleibt jedoch unvollständig (ohne darauf durch einen Zusatz „z. B.“ hinzuweisen). Besonders ungünstig ist dies im Zusammenhang mit den Informationspflichten (Art. 13, 14 DSGVO)

3. KI-generierte Schulungen

– eine zentrale Pflicht der DSGVO. Diese Pflicht ergibt sich zwar bereits aus der Erläuterung des (Teil-)Grundsatzes der „Transparenz“, es wird jedoch versäumt im Zusammenhang mit den Betroffenenrechten die Informationspflichten nach Art. 13 und 14 DSGVO noch mal explizit zu erwähnen und hierdurch auch eine Verbindung zwischen den verschiedenen rechtlichen Vorgaben herzustellen. Im Übrigen sind die Ausführungen sachlich richtig, bleiben jedoch zu oberflächlich. Falsch ist die Formulierung „jede Person“ sei betroffene Person, da sie den Eindruck erwecken kann, dass auch Personen ohne Verarbeitung ihrer personenbezogenen Daten als betroffene Personen gelten würden. Fristen (Art. 12 Abs. 3 DSGVO) zur Umsetzung der Betroffenenrechte fehlen ebenso wie Hinweise auf Voraussetzungen und Ausnahmen. Lediglich im Zusammenhang mit dem Löschrecht wird darauf hingewiesen, dass eine Löschung nicht immer möglich ist. Positiv hervorzuheben ist jedoch der ausdrückliche Hinweis, dass Betroffenenanfragen schnell und richtig bearbeitet werden müssen und dass sich die Mitarbeiter daher an den Datenschutzbeauftragten wenden sollten. Letzteres setzt jedoch voraus, dass die Organisation, die die Schulung einzusetzen bezweckt auch über einen Datenschutzbeauftragten verfügt. Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

4. Praktische Umsetzung im Arbeitsalltag

Sinnvoll sind die Grundregeln zur sicheren Datenverarbeitung – konkret zum Passwortschutz, E-Mail-Versand und zur Dokumentvernichtung – sowie zur mobilen Arbeit. Die diesbezüglichen Empfehlungen sind relevant, verständlich und leicht umsetzbar. Die Empfehlung „Versenden Sie sensible Daten nur verschlüsselt oder über sichere Portale“ bleibt ohne Beispiel, was als „sicheres Portal“ gilt, unkonkret. Zudem ist dieser Hinweis nicht für jede Organisation unmittelbar anwendbar. So ist davon auszugehen, dass nicht jede Organisation über Verschlüsselungsmöglichkeiten verfügt. Insoweit bedarf es hier organisationsspezifischen Konkretisierungen.

Grundsätzlich sinnvoll sind auch die Hinweise zu „Datenpannen melden“. Insgesamt bleiben sie jedoch zu oberflächlich und unkonkret. So wird der Begriff der Datenpanne lediglich durch den „Verlust oder unrechtmäßigen Zugriff auf Daten“ konkretisiert. Diese zwei Alternativen sind jedoch nicht die einzigen Szenarien, die eine Datenpanne darstellen. Vielmehr umfassen Datenpannen nach Art. 4 Nr. 12 DSGVO auch unbeabsichtigte oder unrechtmäßige Vernichtungen, Verluste und Veränderungen sowie unbefugte Offenlegungen oder unbefugte Zugänge. Diese Verkürzung kann zu Missverständnissen in der Praxis führen. Auch fehlt eine Klarstellung, dass Datenpannen von der datenschutzverantwortlichen Stelle der Organisation innerhalb von 72 Stunden an die Aufsichtsbehörde (Art. 33 DSGVO) gemeldet werden müssen, wenn sie mit einem Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind, nicht jedoch bei lediglich geringem Risiko. Auch fehlt der Hinweis, dass die Einschätzung idealerweise gemeinsam mit einer für den Datenschutz zuständigen Person innerhalb der Organisation erfolgen sollte (je nach Organisation z. B. der Datenschutzkoordination, dem Datenschutzbeauftragten, der Geschäftsführung oder einer benannten Person) und keine unabgesprochene, eigenständige Meldung und Benachrichtigung nach den Art. 33, 34 DSGVO durch den Mitarbeitenden erfolgen soll. Die interne Kommunikation an Vorgesetzte oder Datenschutzbeauftragte wird zwar genannt, bleibt aber oberflächlich. Zudem ist davon auszugehen, dass nicht jede Organisation über einen Datenschutzbeauftragten verfügt. Hier wären also unternehmensspezifische Anpassungen erforderlich – sowohl hinsichtlich zuständiger Personen als auch hinsichtlich unternehmensinterner Vorfallprozesse oder Vorlagen (z. B. Meldeformulare).

5. Zusammenfassung & nächste Schritte

Die Kernaussagen werden klar und knapp wiederholt. Positiv hervorzuheben ist der Platzhalter für interne Richtlinien und Kontakte. Auch hier gilt jedoch, dass nicht jede Organisation über eine Datenschutzrichtlinie, ein Mitarbeiterportal oder einen

Datenschutzbeauftragten verfügt. Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

Zusammenfassend ist die Schulung in verständlicher und zugänglicher Sprache gehalten. Die Grundstruktur ist logisch und folgt einem sinnvollen Ablauf. Besonders positiv hervorzuheben ist, dass sich teils praxisnahe Tipps und direkte Handlungsanweisungen finden. Allerdings ist die Darstellung in weiten Teilen juristisch unpräzise und unvollständig. Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. Insgesamt fehlen die vollständigen Definitionen der zentralen Grundbegriffe – insbesondere personenbezogene Daten, besondere Kategorien, Verarbeitung, Verantwortlicher, Auftragsverarbeiter, betroffene Person – jeweils mit Artikel-Fundstellen und Beispielen aus dem Unternehmensalltag. Ebenso fehlt die Erläuterung sämtlicher Rechtsgrundlagen und dazu gehörige Praxisbeispiele. Die Grundlogik der DSGVO, das „Verbot mit Erlaubnisvorbehalt“, wird nicht benannt. Die Betroffenenrechte werden unpräzise dargestellt, praxisnahe Beispiele sowie Ausnahmen, Fristen und internen Meldewegen fehlen. Die Datenschutzgrundsätze werden nicht mit der erforderlichen juristischen Präzision erklärt, und die Rechenschaftspflicht wird nicht näher erläutert; konkrete Anweisungen zur Umsetzung im Arbeitsalltag fehlen. Technische und organisatorische Maßnahmen werden nicht definiert. Interne Bezüge wie zuständige Personen, Meldeketten oder relevante Richtlinien sind nicht klar erkennbar. Die Datenschutz-Folgenabschätzung und das Verzeichnis von Verarbeitungstätigkeiten werden nicht behandelt. Interaktive Elemente (Quiz, Fallstudien) und Visualisierungen (z. B. Icons), die das Verständnis und die Erinnerung fördern könnten, werden nicht eingesetzt. Die Selbstlernerheit damit nicht den Anforderungen an eine vollständige DSGVO-Grundlagenschulung, da sie die rechtlichen Inhalte der DSGVO nur oberflächlich wiedergibt und Mitarbeitende nicht ausreichend befähigt, die Vorgaben im Arbeitsalltag sicher und richtig umzusetzen.

3.4 Gemma 3n E2B (Google AI, Anwendung: Google AI Studio)

3.4.1 KI-generierter Inhalt²²

Selbstlernkurs: Datenschutz-Grundverordnung (DSGVO) – Ein Leitfaden für neue Mitarbeiter

Willkommen! Dieser Kurs wurde speziell für neue Mitarbeiter entwickelt, die in unsere Organisation eintreten. Er soll Ihnen die wichtigsten Grundlagen der Datenschutz-Grundverordnung (DSGVO) vermitteln, damit Sie datenschutzkonform handeln und einen wertvollen Beitrag zum Schutz unserer Daten leisten können.

Ziel: Sie verstehen die grundlegenden Prinzipien der DSGVO, erkennen relevante Risiken im Arbeitsalltag und wissen, wie Sie datenschutzkonform handeln.

Dauer: Ungefähr 60-90 Minuten.

Lernziele: Nach Abschluss dieses Kurses können Sie:

- Die DSGVO verstehen und ihre wichtigsten Bestimmungen erklären.
- Die Bedeutung von Datenschutz für unsere Organisation und unsere Kunden einschätzen.
- Risiken im Arbeitsalltag identifizieren, die Datenschutz verletzen können.
- Grundlegende Maßnahmen zur Einhaltung der DSGVO ergreifen.
- Verantwortlichkeiten im Bereich Datenschutz kennen.

²² Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell Gemma 3n E2B über Google AI Studio generiert.

- Fragen zum Datenschutz stellen.

Modul 1: Einführung in die DSGVO – Was ist das überhaupt?

- **Was ist die DSGVO?**
 - Die DSGVO ist eine EU-Verordnung, die die Verarbeitung personenbezogener Daten regelt. Sie gilt für alle Unternehmen, die Daten von EU-Bürgern verarbeiten, unabhängig davon, wo sich das Unternehmen befindet.
 - **Zweck:** Die DSGVO soll den Schutz der Rechte natürlicher Personen (wie z. B. das Recht auf Auskunft, Berichtigung und Löschung) verbessern und die Verhältnismäßigkeit der Verarbeitung personenbezogener Daten gewährleisten.
- **Die wichtigsten Grundsätze der DSGVO:**
 - **Rechtmäßigkeit, Angemessenheit und Zweckbindung:** Die Verarbeitung darf nur rechtmäßig, angemessen und für einen bestimmten, klaren und legitimen Zweck erfolgen.
 - **Transparenz:** Personen müssen klar und verständlich darüber informiert werden, welche Daten verarbeitet werden und wie.
 - **Datenminimierung:** Nur die Daten, die für den jeweiligen Zweck unbedingt erforderlich sind, dürfen verarbeitet werden.
 - **Richtigkeit:** Die Daten müssen richtig und auf dem neuesten Stand gehalten werden.
 - **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.
 - **Integrität und Vertraulichkeit:** Die Daten müssen vor unbefugtem Zugriff und Verlust geschützt werden.
 - **Rechenschaftspflicht:** Unternehmen müssen nachweisen können, dass sie die DSGVO einhalten.
- **Die Rechtsgrundlagen der DSGVO:**
 - **Art. 6 DSGVO:** Rechtsgrundlagen für die Verarbeitung (z.B. Einwilligung, Vertragserfüllung, berechtigtes Interesse).
 - **Art. 9 DSGVO:** Verarbeitung sensibler Daten (z.B. Gesundheitsdaten, religiöse Überzeugungen).

Übung: Denken Sie über Ihre täglichen Aufgaben nach. In welchen Bereichen werden personenbezogene Daten verarbeitet? (Hinweis: Beispiele sind Kundendaten, Mitarbeiterdaten, Daten von Lieferanten, etc.)

Modul 2: Personenbezogene Daten – Was sind das?

- **Was sind personenbezogene Daten?**
 - Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
 - **Beispiele:**
 - Name
 - Adresse
 - E-Mail-Adresse
 - Telefonnummer
 - Geburtsdatum
 - Sozialversicherungsnummer
 - IP-Adresse
 - Cookies
 - Biometrische Daten
- **Identifizierbare natürliche Person:**
 - Eine identifizierbare natürliche Person ist eine Person, die anhand von Informationen identifiziert werden kann, die nicht öffentlich zugänglich sind.

- **Verarbeitung von sensiblen Daten:**

- Sensible Daten sind Daten, die besonderen Schutz benötigen, da sie die Würde, die Rechte und Freiheiten einer Person beeinträchtigen können.
- **Beispiele:**
 - Gesundheitsdaten
 - Politische Überzeugungen
 - Religionszugehörigkeit
 - Gewerkschaftsmitgliedschaft
 - Vorurteile
 - Ethnische Zugehörigkeit
 - Rasse
 - sexuelle Orientierung
 - genetische oder biometrische Daten

Frage zur Reflexion: Können Sie Beispiele für personenbezogene Daten nennen, die in Ihrer Arbeit verarbeitet werden?

Modul 3: Datenschutz im Arbeitsalltag – Risiken und Maßnahmen

- **Risiken im Arbeitsalltag:**

- **Unzureichende Datensicherheit:** Fehlende oder unzureichende Sicherheitsmaßnahmen können zu Datenverlust oder -missbrauch führen.
- **Mitarbeitereschulungen:** Mitarbeiter, die nicht über ausreichende Kenntnisse im Datenschutz verfügen, können Datenschutzverletzungen verursachen.
- **Verarbeitung von sensiblen Daten ohne Einwilligung:** Die Verarbeitung sensibler Daten ohne die ausdrückliche Einwilligung der betroffenen Person ist unzulässig.
- **Fehlende Datenschutzrichtlinien:** Das Fehlen klarer Datenschutzrichtlinien erschwert die Einhaltung der DSGVO.
- **Unzureichende Dokumentation:** Eine fehlende oder unvollständige Dokumentation der Datenverarbeitung erschwert die Nachweisführung bei Datenschutzverletzungen.

- **Maßnahmen zur Vermeidung von Datenschutzverletzungen:**

- **Datenschutzrichtlinien:** Entwicklung und Umsetzung klarer Datenschutzrichtlinien.
- **Datenschutz-Folgeabschätzung:** Durchführung von Datenschutz-Folgeabschätzungen bei neuen Verarbeitungsvorgängen.
- **Technische und organisatorische Maßnahmen:** Implementierung geeigneter Sicherheitsmaßnahmen zum Schutz der Daten (z.B. Verschlüsselung, Zugriffskontrollen, Passwortrichtlinien).
- **Mitarbeitereschulungen:** Regelmäßige Schulungen zum Datenschutz.
- **Dokumentation der Datenverarbeitung:** Führen einer detaillierten Dokumentation der Datenverarbeitung.
- **Einwilligung:** Einholung einer eindeutigen Einwilligung bei der Verarbeitung sensibler Daten.
- **Datenminimierung:** Verarbeitung nur der notwendigen Daten.

Praktischer Tipp: Beachten Sie bei der Bearbeitung von Kundenanfragen oder der Erstellung von Berichten, ob personenbezogene Daten verarbeitet werden und welche Maßnahmen erforderlich sind, um die Datenschutzbestimmungen einzuhalten.

Modul 4: Ihre Rechte und Verantwortlichkeiten

- **Ihre Rechte als Mitarbeiter:**

- **Recht auf Auskunft:** Sie haben das Recht, Informationen über die Verarbeitung Ihrer personenbezogenen Daten zu erhalten.

- **Recht auf Berichtigung:** Sie haben das Recht, fehlerhafte Daten zu korrigieren.
- **Recht auf Löschung:** Sie haben das Recht, Daten zu löschen, wenn sie nicht mehr benötigt werden.
- **Recht auf Einschränkung der Verarbeitung:** Sie haben das Recht, die Verarbeitung Ihrer Daten einzuschränken.
- **Recht auf Datenübertragbarkeit:** Sie haben das Recht, Ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
- **Recht auf Widerspruch:** Sie haben das Recht, der Verarbeitung Ihrer Daten zu widersprechen.
- **Ihre Verantwortlichkeiten:**
 - **Datenschutzrichtlinien beachten:** Sie müssen die Datenschutzrichtlinien unserer Organisation kennen und einhalten.
 - **Datenschutzregeln einhalten:** Sie müssen sich an die Datenschutzregeln unserer Organisation halten.
 - **Datenschutzverletzungen melden:** Sie müssen Datenschutzverletzungen unverzüglich melden.
 - **Vertraulichkeit wahren:** Sie müssen die Vertraulichkeit personenbezogener Daten wahren.
 - **Recht auf Information:** Sie sind verpflichtet, Informationen über die Verarbeitung von Daten bereitzustellen, wenn dies erforderlich ist.

Wichtig: Bei Fragen zum Datenschutz wenden Sie sich an den Datenschutzbeauftragten (Name und Kontaktdataen).

Modul 5: Häufig gestellte Fragen (FAQ)

- **Wo finde ich die Datenschutzrichtlinien unserer Organisation?** (Link zur Webseite)
- **Was tun, wenn ich vermute, dass meine Daten missbraucht werden?** (Link zum Meldeformular)
- **Kann ich meine Daten jederzeit ändern lassen?** (Ja, gemäß Art. 16 DSGVO)
- **Wer ist der Verantwortliche für die Datenverarbeitung in unserer Organisation?** (Name und Kontaktdataen des Verantwortlichen)
- **Was ist bei der Verarbeitung von Daten von Kindern zu beachten?** (Besondere Vorsicht geboten - Einwilligung der Eltern erforderlich)

Abschluss:

Herzlichen Glückwunsch! Sie haben erfolgreich diesen Selbstlernkurs abgeschlossen. Wir hoffen, dass Sie die gewonnenen Kenntnisse nutzen, um datenschutzkonform zu handeln und unseren Ruf als datenschutzorientierte Organisation zu stärken.

Wir wünschen Ihnen viel Erfolg bei Ihrem neuen Job!

Hinweis: Dieser Kurs ist eine Einführung in die DSGVO. Für detailliertere Informationen und spezifische Fragen wenden Sie sich bitte an unseren Datenschutzbeauftragten.

3.4.1 Bewertung

Die von Gemma 3n E2B generierte Schulung zu den Grundlagen des Datenschutzes ist logisch aufgebaut, beginnend mit einer Einführung und den Lernzielen, gefolgt von einer Einführung in die DSGVO, einer Erläuterung personenbezogener Daten, einem Abschnitt zu Risiken und Maßnahmen, der Darstellung von Rechten und Verantwortlichkeiten der Mitarbeitenden hin zu einem FAQ-Bereich. Die Sprache ist grundsätzlich einfach und verständlich und damit gut für Einsteiger ohne juristische Vorkenntnisse geeignet.

Mehrere in der Schulung enthaltene praxisnahe Beispiele fördern den Transfer in den Arbeitsalltag. Gleichzeitig reicht die inhaltliche Tiefe nicht aus, um ein nachhaltiges Verständnis zu sichern: Viele Themen sind zu oberflächlich ausgeführt, insbesondere die

Betroffenenrechte und die Rechtsgrundlagen. Zudem wird die juristische Präzision teils nicht eingehalten, da falsche oder unvollständige Begriffe verwendet werden und Definitionen fehlen oder nicht dem Wortlaut der DSGVO entsprechen. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einführung

Der Einstieg mit „Willkommen!“ wirkt positiv motivierend. Die Zielgruppe („neue Mitarbeiter“) wird klar benannt. Die direkte Ansprache in der „Sie“-Form stärkt Identifikation und das eigene Pflichtbewusstsein, während die präzise Zielbeschreibung („Sie verstehen...“) die Erwartungen der Mitarbeitenden steuert. Die Lernziele sind motivierend und geben einen strukturierten Überblick über den Kursinhalt. Die Zeitangabe von 60–90 Minuten unterstützt die Planbarkeit, scheint jedoch unrealistisch. Es ist davon auszugehen, dass Mitarbeitende nicht mehr als 30–45 Minuten benötigen würden, um die Schulungsinhalte zu lesen und zu verstehen.

Modul 1: Einführung in die DSGVO

Die Überschrift „Was ist das überhaupt?“ wirkt ansprechend und weckt Neugier. Grundsätzlich positiv ist zu vermerken, dass das Marktortprinzip indirekt angesprochen wird („alle Unternehmen, die Daten von EU-Bürgern verarbeiten, unabhängig davon, wo sich das Unternehmen befindet“). Dabei wird jedoch versäumt klarzustellen, dass die DSGVO auch dann gilt, wenn eine Organisation ihren Sitz in der EU hat und personenbezogene Daten von Personen außerhalb der EU verarbeitet (Niederlassungsprinzip). Der angegebene Zweck der DSGVO ist zwar im Kern richtig, aber juristisch unpräzise: Richtig ist, dass die DSGVO die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren in Art. 8 Abs. 1 GRC garantiertes Recht auf Schutz der sie betreffenden personenbezogenen Daten, schützt (Art. 1 Abs. 2 DSGVO) und die Verhältnismäßigkeit bei der Verarbeitung personenbezogener Daten sicherstellt.²³

Die sieben Grundsätze der DSGVO (Art. 5 DSGVO) werden zwar genannt, die Inhalte sind jedoch stellenweise fehlerhaft, ungenau oder zu abstrakt. Kritisch ist insbesondere, dass der Grundsatz der „Rechtmäßigkeit, Transparenz und Treu und Glauben“ i. S. v. Art. 5 Abs. 1 lit. a DSGVO teilweise aufgeteilt wird und teilweise mit anderen Grundsätzen vermischt wird. So nennt die Schulung einerseits „Rechtmäßigkeit, Angemessenheit und Zweckbindung“ und andererseits „Transparenz“. Durch „Rechtmäßigkeit, Angemessenheit und Zweckbindung“ werden nicht nur der (Teil-)Grundsatz der Rechtmäßigkeit und der Grundsatz der Zweckbindung vermischt, vielmehr ist auch der Zusatz der Angemessenheit eine Abweichung vom Normtext und somit unzutreffend. Im Übrigen ist die Beschreibung der (Teil-)Grundätze der Rechtmäßigkeit, Transparenz und Zweckbindung im Kern richtig. Im Zusammenhang mit dem Grundsatz der „Zweckbindung“ wird nicht darauf hingewiesen, dass eine Weiterverarbeitung zu anderen Zwecken möglich ist, sofern diese Zwecke mit dem ursprünglichen Verarbeitungszweck kompatibel ist (Art. 6 Abs. 4 DSGVO). Der Grundsatz der „Datenminimierung“ wird zwar leicht verkürzt, aber dennoch fehlerfrei und verständlich beschrieben. Im Zusammenhang mit dem Grundsatz der „Richtigkeit“ fehlt der Hinweis, dass Daten sachlich richtig und erforderlichenfalls aktuell sein müssen, inklusive kurzer Erläuterung, wann Daten „falsch“ sind. Die Darstellung des Grundsatzes der „Integrität und Vertraulichkeit“ beschränkt sich inhaltlich auf den Schutz vor unbefugtem Zugriff und Verlust. Es wird versäumt generell auf die Gewährleistung der Sicherheit der Daten abzustellen und weitere in Art. 5 Abs. 1 lit. f DSGVO explizit benannte Gefahren (unbefugte oder unrechtmäßige Verarbeitung, unbeabsichtigter Verlust, Zerstörung oder Schädigung) hinzuweisen. Zudem wird es versäumt, darauf Bezug zu nehmen, dass die

²³ Heberlein, EuR 2021, 672 (672).

3. KI-generierte Schulungen

Sicherheit durch technische und organisatorische Maßnahmen (Art. 32 DSGVO) sichergestellt werden muss.

Grundsätzlich positiv hervorzuheben ist, dass die Schulung auf die Rechtsgrundlagen nach Art. 6 und Art. 9 DSGVO eingeht. Die Rechtsgrundlagen werden dabei jedoch ohne Bezugnahme zum (Teil-)Grundsatz der Rechtmäßigkeit dargestellt und ein klarer Verweis auf das „Verbot mit Erlaubnisvorbehalt“ als Grundlogik fehlt. Es fehlt eine Erklärung, dass jede Verarbeitung einer Rechtsgrundlage bedarf und welche Voraussetzungen für die beispielhaft aufgeführten Rechtsgrundlagen nach Art. 6 DSGVO vorliegen müssen. Insbesondere im Zusammenhang mit der Einwilligung wäre dies sinnvoll. Im Zusammenhang mit Art. 9 DSGVO wird unpräzise von der „Verarbeitung sensibler Daten“ gesprochen, nicht von „besonderen Kategorien personenbezogener Daten“. Trotz der angeführten Beispiele für entsprechende personenbezogene Daten, könnte diese unpräzise Formulierung zu Verwirrungen und Verständnisproblemen bei juristischen Laien führen, da sie möglicherweise nicht erkennen können, ob es sich um denselben Begriff handelt oder um zwei unterschiedliche Datenarten.

Zentrale Begriffe wie „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO), „gemeinsamer Verantwortlicher“ (Art. 26 DSGVO), „Auftragsverarbeiter“ (Art. 4 Nr. 8 DSGVO) oder „betroffene Person“ werden weder definiert, noch erläutert.

Positiv hervorzuheben ist die Reflexionsübung, mit der die Mitarbeitenden angehalten werden über die Verarbeitung personenbezogener Daten in ihrem eigenen Arbeitsalltag nachzudenken. Sinnvoll wäre hier jedoch eine Auflösung der Reflexionsfrage durch praktische Verarbeitungsbeispiele und deren Rechtsgrundlage in verschiedenen Arbeitsbereichen gewesen – diese hätte die Verständlichkeit deutlich erhöht.

Modul 2: Personenbezogene Daten

Die Begriffsbestimmung von personenbezogenen Daten (Art. 4 Nr. 1 DSGVO) ist inhaltlich richtig und vollständig. Untermauert wird dies durch praxisnahe Beispiele für personenbezogene Daten, einschließlich technischer Daten wie IP-Adresse und Cookies. Negativ fällt jedoch die Definition der „identifizierbaren natürlichen Person“ auf, diese ist insoweit fehlerhaft als für die „Identifizierbarkeit“ unerheblich ist, ob Daten öffentlich zugänglich sind oder nicht. Maßgeblich ist vielmehr, dass die Identität nicht unmittelbar aus den vorliegenden Informationen folgt, sondern einer vorherigen Verknüpfung mit weiteren Informationen bedarf. Hierdurch gelingt es der Schulung auch nicht die Begriffe „identifiziert“ und „identifizierbar“ voneinander abzugrenzen. Ebenso wenig werden personenbezogenen Daten von pseudonymen und anonymen Daten abgegrenzt. Auch wird der Begriff der „natürlichen Person“ nicht definiert, was für juristische Laien zu Verständnisproblemen führen kann.

Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) wird separat behandelt, inklusive Beispielen und dem Hinweis auf den besonderen Schutz. An dieser Stelle wird jedoch erneut unpräzise von „sensiblen Daten“ gesprochen. Positiv hervorzuheben ist jedoch die Begriffserläuterung, welche den besonderen Schutzbedarf entsprechender Daten herausstellt, sowie die (weitgehend richtige) Liste der „sensibler Daten“. Fälschlicherweise werden hier jedoch auch „Vorurteile“ aufgelistet. Ebenso ist der Begriff der „Rasse“ unglücklich gewählt; zutreffender wäre hier die Formulierung „ethische Herkunft“.

Abschließend enthält auch dieses Modul eine Reflexionsfrage, welche Mitarbeitende anregt, über die Verarbeitung von konkreten personenbezogenen Daten in Ihrem Arbeitsalltag nachzudenken. Dies kann die Awareness für die Relevanz des Datenschutzrechts in der eigenen praktischen Tätigkeit erhöhen. Ergänzt werden hätte

jedoch eine Auflösung der Reflexionsfrage durch konkrete Beispiele in verschiedenen Abteilungen bzw. Arbeitsbereichen – diese hätte die Verständlichkeit deutlich erhöht.

Modul 3: Datenschutz im Arbeitsalltag

Die Darstellung der Risiken und Maßnahmen ist grundsätzlich klar strukturiert, und zentrale Risiken wie fehlende technische und organisatorische Maßnahmen, unklare Richtlinien oder ungeschulte Mitarbeiter werden benannt. Die Maßnahmenliste umfasst Verschlüsselung, Schulungen und Dokumentation, sensibilisiert für besondere Kategorien personenbezogener Daten und deckt zentrale DSGVO-Anforderungen wie die Datenschutz-Folgenabschätzung und Datenminimierung ab. Ein praktischer Tipp am Ende unterstützt zudem die Umsetzung im Arbeitsalltag.

Allerdings weist das Modul auch erhebliche Lücken auf: Grundsätzlich bleibt die Darstellung zu abstrakt und verzichtet auf notwendige Kontextualisierung. Kritisch ist die Darstellung der Einwilligung als alleinige Rechtsgrundlage bei besonderen Kategorien personenbezogener Daten. Dies ist unzutreffend, da Art. 9 Abs. 2 DSGVO weitere Erlaubnistatbestände vorsieht. Die Datenminimierung bleibt abstrakt; konkrete Beispiele werden nicht genannt. Auch die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) wird lediglich erwähnt, ohne die Voraussetzungen nach Art. 35 DSGVO oder das Instrument als solches zu erklären. Technische und organisatorische Maßnahmen (Art. 32 DSGVO) werden nur beispielhaft genannt, ohne sie zu erklären oder zwischen beiden Kategorien zu unterscheiden. Ebenso wird es versäumt, auf „Privacy by Design“ und „Privacy by Default“ (Art. 25 DSGVO) hinzuweisen. Die Dokumentationspflicht wird angesprochen, aber ohne Bezug auf konkrete Anforderungen wie das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Insgesamt mangelt es dem Modul an Kontextualisierung und näherer Erläuterung; Begriffe werden aufgelistet, aber kaum erklärt, veranschaulicht oder in den DSGVO-Kontext eingeordnet.

Modul 4: Rechte und Verantwortlichkeiten

Die Rechte der Mitarbeitenden sind verständlich und richtig benannt. Positiv ist die Trennung zwischen Rechten als betroffene Personen und Pflichten als Beschäftigte; dieser Dualismus hätte aber klarer durch Gegenüberstellungen oder praxisnahe Beispiele herausgestellt werden können.

Im Zusammenhang mit den Rechten der betroffenen Person wird versäumt klarzustellen, dass diese Rechte nicht nur für die Mitarbeiter gelten, sondern auch für andere betroffene Person (etwa Kunden und Kundinnen). Dies führt dazu, dass nicht deutlich wird, dass die Rechte der Mitarbeiter auch zu (Umsetzungs- bzw. Mitwirkungs-)Pflichten der Mitarbeiter führen können. Es fehlt daher auch an einer Kontextualisierung, wie Mitarbeiter damit umgehen müssen, wenn eine betroffene Personen von einem entsprechenden Recht Gebrauch macht.

Im Übrigen werden zwar wesentliche Rechte genannt, die Darstellung ist jedoch ungenau und unvollständig. Das Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO), die Mitteilungspflicht (Art. 19 DSGVO) sowie das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO) fehlen. Insbesondere aber fehlt die zentrale Pflicht zur Information (Art. 13, 14 DSGVO) gänzlich; Voraussetzungen und Ausnahmen einzelner Rechte werden weder erklärt noch wird auf deren Existenz hingewiesen. Das „Auskunftsrecht“ (Art. 15 DSGVO) ist zu knapp beschrieben. Es fehlt der Hinweis, dass das Auskunftsrecht die konkreten personenbezogenen Daten betrifft und auch ein Recht auf Kopie der Daten enthält. „Das Berichtigungsrecht“ (Art. 16 DSGVO) wird ohne den Hinweis auf „unverzügliche“ Umsetzung genannt. Zudem impliziert die allgemeine Formulierung „Sie haben das Recht, fehlerhafte Daten zu korrigieren“, dass die Berichtigung unmittelbar durch den Mitarbeiter durchgeführt werden darf und im Zweifel auch die Daten anderer natürlicher

3. KI-generierte Schulungen

Personen betreffen darf. Das „Löscrecht“ (Art. 17 DSGVO) bleibt allgemein, ohne Voraussetzungen und Ausnahmen sowie ohne Abgrenzung zum „Recht auf Vergessenwerden“ (Abs. 2). Zudem impliziert die allgemeine Formulierung „Sie haben das Recht, Daten zu löschen“, dass die Löschung unmittelbar durch den Mitarbeiter durchgeführt werden darf und im Zweifel auch die Daten anderer natürlicher Personen betreffen darf. Das Recht der „Einschränkung der Verarbeitung“ (Art. 18 DSGVO) erscheint ohne typische Anwendungsfälle (z. B. strittige Richtigkeit, ausstehende Prüfung eines Widerspruchs). Auch hier impliziert die aktive Formulierung, dass der Mitarbeiter eigenmächtig über die Einschränkung seiner Daten entscheiden kann. Das Recht der „Datenübertragbarkeit“ (Art. 20 DSGVO) ist ebenso nur oberflächlich beschrieben. Voraussetzungen wie Einwilligung bzw. Vertrag und automatisierte Verarbeitung fehlen. Auch das „Widerspruchsrecht“ (Art. 21 DSGVO) ist zu knapp erläutert, ohne Einschränkung auf Verarbeitungen, die auf dem öffentlichen oder berechtigten Interesse basieren sowie ohne Differenzierung zwischen Art. 21 Abs. 1 und Abs. 2 DSGVO (zwingende schutzwürdige Gründe). Solche Verkürzungen können zu Missverständnissen führen.

Die Verantwortlichkeiten sind praxisnah formuliert und fördern bewusstes Verhalten. Die Hinweise „Datenschutzregeln einhalten“ und „Datenschutzrichtlinien beachten“ sind jedoch redundant und sollten präzisiert werden, etwa in Form von organisationspezifischen Ergänzungen bzw. Verlinkungen auf entsprechende Inhalte.

Der allgemeine Hinweis, dass Datenschutzverletzungen gemeldet werden müssen, führt ohne Hinweis bezüglich des Meldeempfängers ins Leere. Mangels Klarstellung, was Datenschutzverletzungen sind, könnte der Hinweis zudem zu einer unerwünschten Umsetzung führen: Mangels Klarstellung, was meldepflichtige Datenschutzverletzungen sind, könnte der Eindruck entstehen, jeder geringfügige Verstoß gegen datenschutzrechtliche Vorgaben – etwa eine zwei Tage verspätete Löschung personenbezogener Daten –, der lediglich mit einem geringen Risiko verbunden ist, müsse an die Aufsichtsbehörde gemeldet werden. Nicht erwähnt wird die 72-Stunden-Frist nach Art. 33 DSGVO. Auch fehlt die Klarstellung, dass nicht der Mitarbeitende selbst an die Aufsichtsbehörde melden soll, sondern intern an die datenschutzverantwortliche Stelle der Organisation (Datenschutzbeauftragter, Geschäftsführung oder andere zuständige Stelle), die dann gegebenenfalls die externe Meldung vornimmt. Ohne diese Präzisierungen besteht die Gefahr von Fehlmeldungen oder verspäteten Meldungen.

Das „Recht auf Information“ wird zwar genannt, ist jedoch nicht nur systematisch fehlplatziert, sondern auch zu knapp behandelt. Es fehlen insbesondere Beispiele, welche Informationen über Datenverarbeitungen bereitgestellt werden müssen. Außerdem fehlen Platzhalter für Hinweise zum internen Umgang mit dieser Pflicht.

Der abschließende Hinweis, sich bei Fragen an den Datenschutzbeauftragten zu wenden ist wichtig und gut platziert, setzt jedoch voraus, dass die Organisation, die die Schulung einzusetzen bezieht, über einen Datenschutzbeauftragten verfügt. Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

Modul 5: FAQ

Das FAQ-Format ist benutzerfreundlich und fördert die Wiederholung zentraler Inhalte. Die Fragen sind alltagsrelevant (z. B. Änderung eigener Daten, Daten von Kindern) und es gibt Anpassungsmöglichkeiten durch Verlinkungen zu internen Richtlinien und Meldeformularen. Die Frage zu Handlungsmöglichkeiten bei einem vermuteten Datenmissbrauch scheint für eine Datenschutzschulung für Mitarbeiter jedoch nicht optimal zu sein, da sie den Eindruck wecken könnte, der Mitarbeiter müsse Sorge um den Umgang mit seinen Daten haben. Die Frage zu Daten von Kindern bleibt jedoch oberflächlich, insbesondere in Anbetracht dessen, dass die Verarbeitung von Daten von

Kindern zuvor kein Gegenstand der Schulung war. Ebenso greift die Antwort auf die Frage, ob Daten jederzeit geändert werden können zu kurz: Nur bei unrichtigen Daten kann eine Berichtigung verlangt werden.

Abschluss

Die Abschlussbotschaft ist motivierend und wertschätzend; der Hinweis auf den Datenschutzbeauftragten als zentrale Anlaufstelle ist hilfreich, könnte für manche Organisationen jedoch anpassungsbedürftig sein.

Zusammenfassend bietet die Schulung einen positiven, motivierenden Einstieg mit direkter Ansprache und vermittelt zu Beginn klar formulierte, anwendungsbezogene Lernziele. Die Module sind strukturiert und übersichtlich aufgebaut, was die Vermittlung der Grundlagen der DSGVO in verständlicher Sprache unterstützt. Allerdings ist die Schulung inhaltlich unvollständig und weist zahlreiche Ungenauigkeiten, Verkürzungen und Fehler auf. Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. So fehlen u.a. eine Erläuterung des Begriffs der Verarbeitung, eine Darstellung der Informationspflichten (Art. 13, 14 DSGVO), die Erläuterung der besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO). Die Schulung weist Ungenauigkeiten und Verkürzungen („Ihre Rechte als Mitarbeiter“) sowie Fehler auf – beispielsweise wird die „identifizierbare natürliche Person“ mit einer unzutreffenden Einschränkung beschrieben. Ebenso werden manche Grundsätze falsch erläutert. Es fehlt insbesondere eine klare Erläuterung, was Datenschutzverletzungen sind und welche Meldewege und Fristen hierbei bestehen. Zudem fehlt eine verständliche und umfassende Erläuterung von technischen und organisatorischen Maßnahmen, dem Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Die Vermischung juristischer Terminologie mit vereinfachter Sprache kann zudem Missverständnisse hervorrufen. Die Schulung eignet sich daher nicht als Grundlagenschulung für das Datenschutzrecht, da sie wesentliche Lücken, Verkürzungen und Fehler aufweist, die zu Unsicherheiten, Missverständnissen und Fehlern in der Umsetzung führen können. Die rechtlichen Inhalte der DSGVO werden nur oberflächlich wiedergegeben, sodass Mitarbeiter nicht ausreichend befähigt werden, die Vorgaben im Arbeitsalltag sicher und richtig umzusetzen.

3.5 GPT-4.1 (OpenAI, Anwendung: ChatGPT)

3.5.1 KI-generierter Inhalt²⁴

Selbstlerneinheit: Datenschutz-Grundlagen für neue Mitarbeiter

Dauer: ca. 45–60 Minuten

Zielgruppe: Alle neuen Mitarbeitern

Ziel: Verständnis der Grundlagen der Datenschutz-Grundverordnung (DSGVO) und sichere Umsetzung im Arbeitsalltag

1. Einführung: Warum ist Datenschutz wichtig?

Datenschutz betrifft uns alle – im privaten wie im beruflichen Umfeld.

Die DSGVO schützt die **Grundrechte und Freiheiten natürlicher Personen**, insbesondere ihr Recht auf den Schutz personenbezogener Daten.

Für Unternehmen bedeutet das:

- Daten dürfen nur rechtmäßig und zweckgebunden verarbeitet werden.
- Ein Verstoß kann zu **hohen Bußgeldern** und **Vertrauensverlust** führen.
- Datenschutz ist Teil einer **professionellen Arbeitsweise**.

²⁴ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell GPT-4.1 über ChatGPT generiert.

Praxisbeispiel:

Wenn Sie eine E-Mail mit Kundendaten versehentlich an die falsche Adresse senden, kann das rechtliche Folgen haben und dem Ruf der Organisation schaden.

2. Grundbegriffe der DSGVO

Damit Sie sicher arbeiten, müssen einige Schlüsselbegriffe klar sein:

1. Personenbezogene Daten

→ Alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen

Beispiele: Name, Adresse, E-Mail, Telefonnummer, Personalnummer, Fotos, Standortdaten

2. Verarbeitung

→ Jeder Vorgang im Umgang mit Daten, z. B.:

Erfassen, Speichern, Übermitteln, Löschen

3. Verantwortlicher

→ Unsere Organisation, die entscheidet, **warum und wie** Daten verarbeitet werden

4. Betroffene Person

→ Die Person, deren Daten verarbeitet werden (z. B. Kundin, Mitarbeiter, Bewerber)

5. Auftragsverarbeitung

→ Wenn ein externer Dienstleister in unserem Auftrag Daten verarbeitet

Beispiel: Externe Lohnabrechnung oder Cloud-Dienst

3. Grundprinzipien der DSGVO

Die DSGVO nennt in **Art. 5** die zentralen Prinzipien, die für alle gelten:

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

- Daten nur mit einer Rechtsgrundlage (z. B. Vertrag, Einwilligung) verarbeiten
- Betroffene sollen wissen, was mit ihren Daten geschieht

2. Zweckbindung

- Daten nur für den **klar definierten Zweck** nutzen, für den sie erhoben wurden

3. Datenminimierung

- So viele Daten wie nötig, aber so wenige wie möglich verarbeiten

4. Richtigkeit

- Daten müssen richtig und aktuell sein

5. Speicherbegrenzung

- Daten nicht länger aufbewahren, als es notwendig ist

6. Integrität und Vertraulichkeit (Sicherheit)

- Schutz vor unbefugtem Zugriff, Verlust oder Zerstörung

4. Rechte der Betroffenen

Jede Person hat nach der DSGVO bestimmte Rechte. Dazu gehören:

• Auskunftsrecht

→ „Welche Daten haben Sie über mich gespeichert?“

• Recht auf Berichtigung und Löschung

→ Falsche oder nicht mehr notwendige Daten müssen korrigiert oder gelöscht werden

• Recht auf Datenübertragbarkeit

→ Daten in einem gängigen Format erhalten

• Recht auf Beschwerde bei einer Aufsichtsbehörde

Praxisbeispiel:

Ein Kunde fordert die Löschung seiner Kontaktdaten. Sie leiten die Anfrage an die zuständige Datenschutzstelle in Ihrer Organisation weiter, statt selbst zu löschen.

5. Praktische Relevanz für Ihren Arbeitsalltag

Do's (empfohlenes Verhalten):

- Verwenden Sie **starke Passwörter** und sperren Sie Ihren Rechner, wenn Sie den Arbeitsplatz verlassen.
- Nutzen Sie **nur dienstliche Systeme** für dienstliche Daten.
- Prüfen Sie vor dem Versand von E-Mails, ob alle Empfänger berechtigt sind.
- Halten Sie sich an **interne Richtlinien**, z. B. Clean-Desk-Policy.

Don'ts (zu vermeiden):

- Keine personenbezogenen Daten auf privaten Geräten speichern
- Keine Unterlagen mit personenbezogenen Daten offen liegen lassen
- Keine unverschlüsselten USB-Sticks oder Cloud-Dienste nutzen

6. Tipps zur Umsetzung im Alltag

- **Im Zweifel fragen:** Bei Unsicherheiten wenden Sie sich an den Datenschutzbeauftragten.
- **Melden statt vertuschen:** Datenschutzvorfälle (z. B. Verlust eines Laptops) müssen sofort gemeldet werden.
- **Sensibilisierung:** Behandeln Sie alle personenbezogenen Daten so, als wären es Ihre eigenen.

7. Wissenstest zur Selbstkontrolle

1. Was sind personenbezogene Daten?
2. Nennen Sie drei Grundprinzipien der DSGVO.
3. Was tun Sie, wenn Sie eine E-Mail versehentlich an die falsche Person senden?
4. Dürfen Sie private Cloud-Dienste zur Speicherung dienstlicher Daten nutzen?

(Lösungshinweise am Ende des Dokuments)

8. Zusammenfassung

- Datenschutz ist **rechtlich verpflichtend** und **praktisch wichtig**.
- Die DSGVO schützt personenbezogene Daten – und wir sind verpflichtet, diese sicher zu verarbeiten.
- Jeder Mitarbeiter trägt zum Datenschutz bei.

Lösungshinweise zum Wissenstest:

1. Informationen über eine identifizierte oder identifizierbare Person
2. Rechtmäßigkeit, Zweckbindung, Datenminimierung (weitere möglich)
3. Sofort melden und die zuständige Stelle informieren
4. Nein, nur freigegebene dienstliche Systeme verwenden

3.5.2 Bewertung

Die von GPT-4.1 generierte Schulung zu den Grundlagen des Datenschutzes ist strukturell gut angelegt: Die Zeitangabe zu Beginn („ca. 45–60 Minuten“) erleichtert die Lernplanung, und die Beschreibung des Lernziels schafft Klarheit darüber, was genau gelernt werden soll und stärkt eine zielgerichtete Motivation. Die Zeitangabe ist dabei jedoch sehr unrealistisch. Aufgrund der Knappheit der Schulung ist davon auszugehen, dass Mitarbeitende nicht mehr als 15-20 Minuten benötigen, um sie zu lesen und zu verstehen. Der Aufbau der Schulung ist klar und logisch – von Einführung über Grundbegriffe, Grundprinzipien/-sätze, Rechte der Betroffenen und praktische Relevanz bis zu Tipps, Wissenstest und Zusammenfassung – und die persönliche Ansprache („Sie...“, „Ihr Arbeitsalltag...“) bindet Mitarbeitende an mehreren Stellen direkt ein. Inhaltlich wirkt die Schulung jedoch überblicksartig, ohne ausreichende Vertiefungen. Viele Aspekte bleiben stichwortartig und erklären zentrale Begriffe nicht – für datenschutzrechtliche Laien ist das unzureichend. Übergeordnet ist festzustellen, dass die

3. KI-generierte Schulungen

Schulung die Begriffe „personenbezogene Daten“ und „Daten“ synonym zu verwenden scheint, was zu Missverständnissen führen könnte. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

1. Einführung: Warum ist Datenschutz wichtig?

Positiv ist der verständliche Einstieg, der verdeutlicht, dass Datenschutz alle betrifft, wodurch Verantwortungs- und Pflichtbewusstsein gefördert und Mitarbeitende direkt adressiert werden. Die Formulierung, dass die DSGVO die Grundrechte und Freiheiten natürlicher Personen schützt, entspricht Art. 1 DSGVO und vermeidet die verkürzte Aussage, sie „schütze Daten“. Die Erläuterung der Bedeutung für Unternehmen bietet einen kompakten Überblick über zentrale Grundsätze sowie die Folgen von Verstößen; insbesondere die Hinweise auf mögliche Bußgelder und den Verlust von Vertrauen unterstreichen die Tragweite des Themas. Das praxisnahe Beispiel einer falsch adressierten E-Mail veranschaulicht anschaulich, wie schnell ein Datenschutzverstoß eintreten kann.

2. Grundbegriffe der DSGVO

Positiv fällt die übersichtliche Darstellung zentraler DSGVO-Begriffe mit verständlichen Erklärungen und praxisrelevanten Beispielen auf. Die Erklärungen bleiben jedoch teilweise zu oberflächlich oder ungenau. So fehlen im Zusammenhang mit „personenbezogenen Daten“ (Art. 4 Nr. 1 DSGVO) die Unterscheidungen zwischen den Begriffen der identifizierten und identifizierbaren Person sowie der direkten und indirekten Identifizierung – diese Unterscheidungen werden auch durch die (an sich richtig) aufgeführten Beispiele nicht hinreichend deutlich. Zudem fehlt der klare Hinweis, dass sich personenbezogene Daten auf eine „natürliche Person“ beziehen müssen. Ebenso fehlt eine Abgrenzung zu pseudonymen und anonymen Daten sowie eine Erläuterung der besonders schutzbedürftigen besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO. Im Zusammenhang mit dem Begriff der „Verarbeitung“ (Art. 4 Nr. 2 DSGVO) wird allgemein auf den „Umgang mit Daten“ abgestellt. Nach der Legaldefinition in Art. 4 Nr. 2 DSGVO bezieht sich der Begriff der „Verarbeitung“ jedoch ausschließlich auf Vorgänge im Zusammenhang mit personenbezogenen Daten. Problematisch ist dies insbesondere, da die Definition in der Schulung den Eindruck erweckt, auch nicht personenbezogene Daten könnten unter die Verarbeitung im Sinne der DSGVO fallen. Die Erläuterungen im Zusammenhang mit den Begriffen „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO) und „Auftragsverarbeitung“ (Art. 28 DSGVO) sind zwar grundsätzlich richtig, weisen jedoch allesamt inhaltliche Lücken auf. So kann eine Organisation für bestimmte Verarbeitungen Verantwortlicher sein, während sie für andere Verarbeitungen Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) ist (so z. B. bei Webhosting-Unternehmen)²⁵. Die pauschale Feststellung, dass „unsere Organisation“ Verantwortlicher ist, da sie „entscheidet, warum und wie Daten verarbeitet werden“ ist daher zu absolut und könnte in der Praxis zu Missverständnissen und Fehlern bei der praktischen Umsetzung führen. Gleichermaßen gilt für die Erläuterung der Auftragsverarbeitung, wonach eine solche nur dann vorliegt, „wenn ein externer Dienstleister in unserem Auftrag Daten verarbeiten“. In diesem Zusammenhang fehlen außerdem Hinweise zur Weisungsgebundenheit sowie zum Umstand, dass der Auftraggeber Verantwortlicher bleibt.

3. Grundprinzipien der DSGVO

Die Grundsätze der DSGVO (Art. 5 DSGVO) werden vorliegend als „Grundprinzipien“ bezeichnet, was zwar nicht falsch ist, aber nicht dem genauen Wortlaut der Norm entspricht. Dadurch kann der Eindruck entstehen, dass es sich um eine eigenständige normative Bezeichnung handelt.

²⁵ DSK, Kurzpapier Nr. 13, S. 4.

Die Darstellung der Datenschutzgrundsätze ist klar und übersichtlich aufgebaut. Fast alle Grundsätze aus Art. 5 DSGVO werden genannt, was grundsätzlich einen guten Überblick vermittelt. Bei dem Grundsatz „Rechtmäßigkeit, Treu und Glauben sowie Transparenz“ wird zutreffend auf die Erforderlichkeit einer Rechtsgrundlage hingewiesen, ergänzt durch kurze Beispiele wie Vertrag oder Einwilligung. Es fehlt die Erläuterung des Prinzips „Verbot mit Erlaubnisvorbehalt“, wobei positiv zu vermerken ist, dass dessen Essenz aus der Formulierung „Daten nur mit einer Rechtsgrundlage verarbeiten“ zumindest indirekt deutlich wird. Zudem fehlt es aus Ausführungen zu den wichtigsten Rechtsgrundlagen. Positiv hervorzuheben ist, dass auch der (Teil-)Grundsatz der Transparenz erläutert wird; versäumt wird hierbei jedoch, auf die Informationspflichten (Art. 13, 14 DSGVO) hinzuweisen. Die Darstellung der „Zweckbindung“ ist zu eng gefasst („nur für den klar definierten Zweck“). Art. 5 Abs. 1 lit. b DSGVO ermöglicht zudem eine Weiterverarbeitung, wenn diese mit den ursprünglichen Zwecken vereinbar ist. Der Grundsatz der „Datenminimierung“ ist mangels Bezugs auf die Erforderlichkeit für die Verarbeitungszwecke ebenfalls zu knapp dargestellt. Auch der Grundsatz der „Richtigkeit“ ist zu oberflächlich beschrieben. Es fehlt die Klarstellung, dass die Daten nur erforderlichenfalls aktuell sein müssen. Zudem fehlt eine Erläuterung, wann Daten „unrichtig“ im Sinne der Norm sind. Der Grundsatz der „Integrität und Vertraulichkeit“ wird ebenfalls zu kurz erläutert. Es fehlt die Klarstellung, dass allgemein die Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO) gewährleistet werden soll und dass es unerheblich ist, ob die Sicherheit unbefugt oder unbeabsichtigt beeinträchtigt wird. Der Verweis auf den Schutz vor unbefugtem Zugriff, Verlust oder Zerstörung greift damit zu kurz. Der Grundsatz der „Speicherbegrenzung“ wird zwar etwas verkürzt dargestellt, vermittelt den Kern des Grundsatzes aber dennoch verständlich und präzise. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO fehlt schließlich vollständig.

4. Rechte der Betroffenen

Die Darstellung der Betroffenenrechte ist zwar grundsätzlich vorhanden, bleibt jedoch inhaltlich zu oberflächlich und unvollständig. Zwar werden einzelne Rechte im Groben genannt, doch zentrale Ansprüche aus Art. 15–22 DSGVO fehlen gänzlich, darunter das Recht auf „Einschränkung der Verarbeitung“ (Art. 18 DSGVO), das „Widerspruchsrecht“ (Art. 21 DSGVO), das Recht auf „Widerruf der Einwilligung“ (Art. 7 Abs. 3 DSGVO), die Mitteilungspflicht (Art. 19 DSGVO) sowie das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DSGVO). Ebenso werden die Informationspflichten nach Art. 13 und 14 DSGVO vollständig ausgelassen. Statt verständlicher Erläuterungen werden die Rechte lediglich in Form von Stichpunkten aufgezählt; notwendige Angaben zu Voraussetzungen, Umfang und möglichen Ausnahmen fehlen. Falsch ist die Formulierung „jede Person“ sei betroffene Person, da sie den Eindruck erwecken kann, dass auch Personen ohne Verarbeitung ihrer personenbezogenen Daten als betroffene Personen gelten würden. Die Verständlichkeit wird jedoch durch die Überschrift „Betroffenenrechte“ und die vorhandene Definition der betroffenen Person nicht kritisch beeinflusst.

Im Hinblick auf das „Auskunftsrecht“ (Art. 15 DSGVO) wird nicht dargestellt, dass auch Informationen zur Verarbeitung der personenbezogenen Daten beauskunftet werden müssen, z. B. zu den Zwecken der Verarbeitung, zur Herkunft der Daten oder zur (geplanten) Speicherdauer. Das „Recht auf Berichtigung“ (Art. 16 DSGVO) und das „Recht auf Löschung“ (Art. 17 DSGVO) werden zusammen und weitestgehend alternativ zueinander dargestellt. Das kann insoweit zu Missverständnissen führen als der Eindruck entsteht, dass falsche Daten entweder korrigiert oder gelöscht werden müssen bzw. nicht mehr notwendige Daten entweder korrigiert oder gelöscht werden müssen. Im Zusammenhang mit dem Berichtigungsrecht wird nicht darauf hingewiesen, was „falsche“ Daten im Sinne der Norm sind. Im Zusammenhang mit dem Löschrecht fehlt eine Klarstellung, dass eine Löschung nur unter bestimmten Voraussetzungen erfolgen

3. KI-generierte Schulungen

muss. Auch beim „Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO) fehlt der Hinweis, dass das Recht nur unter bestimmten Bedingungen besteht (etwa, dass die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und automatisiert erfolgt). Wichtige Aspekte wie Fristen (Art. 12 Abs. 3 DSGVO) werden nicht erwähnt. Ebenso wenig wird allgemein darauf hingewiesen, dass Betroffenenanfragen nicht durch einzelne Mitarbeiter behandelt werden, sondern an die für den Datenschutz zuständige Person in der Organisation weitergeleitet werden sollten – dies erfolgt lediglich in Form von einem Praxisbeispiel.

Das vorhandene Praxisbeispiel ist zwar richtig, beschränkt sich jedoch auf das Löschrecht und verweist pauschal auf den Datenschutzbeauftragten. Weshalb die Schulung ohne vorherige Prüfung und ggf. Anpassung nicht für jede Organisation anwendbar ist. Weitere Praxisbeispiele sowie allgemeine Hinweise zu internen Prozessen (z. B. Einbindung der für den Datenschutz zuständigen Person) würden den Praxisbezug und die richtige praktische Umsetzung erheblich stärken, insbesondere in Anbetracht der Knappheit der Informationen.

5. Praktische Relevanz für Ihren Arbeitsalltag

Positiv hervorzuheben ist die klare Do's/Don'ts-Struktur des Abschnitts, die eine schnelle Erfassung der wichtigsten Verhaltensregeln ermöglicht. Die Inhalte sind praxisnah gestaltet, bspw. durch Hinweise zu Passwörtern, E-Mail-Versand und Arbeitsplatzsicherung, und betonen zentrale Sicherheitsaspekte wie starke Passwörter, Gerätesperre, Berechtigungsprüfung und Verschlüsselung. Dabei werden sowohl organisatorische als auch technische Maßnahmen genannt. Die einfachen, klaren Formulierungen machen die Inhalte unmittelbar handlungsleitend.

Kritisch bleibt, dass die Begründungen für die einzelnen Regeln fehlen; es wird nicht erläutert, warum diese Maßnahmen wichtig sind, etwa im Hinblick auf das Risiko von Datenverlust, unbefugtem Zugriff oder Verstöße gegen Art. 32 DSGVO. Auch der rechtliche Kontext fehlt: Das rechtliche und theoretisch Fundament für die genannten Do's/Don'ts wurde im theoretischen Teil Schulung nicht gebildet – so fehlen etwa Erläuterungen zu technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und zum Umgang mit Datenschutzverletzungen nach Art. 33, 34 DSGVO. Die genannten Do's/Don'ts könnten außerdem teilweise ergänzt werden: So stellt sich etwa im Zusammenhang mit dem Hinweis, dass starke Passwörter verwendet werden sollen, die Frage, was starke Passwörter sind. Anzumerken ist schließlich, dass die genannten Dos and Don'ts zum Teil bestimmte Organisationspezifika voraussetzen, so etwa im Zusammenhang mit bestehenden internen Richtlinien sowie im Zusammenhang mit zugelassenen, verschlüsselten Cloud-Diensten.

6. Tipps zur Umsetzung im Alltag

Positiv hervorzuheben sind die adressatengerechte, knappe Sprache, der präventive Ansatz („Im Zweifel fragen“) und der Hinweis „Melden statt vertuschen“, was Fehlerkultur und Meldepflicht-Compliance stärkt. Die Bewusstseinsbildung („Behandeln Sie alle personenbezogenen Daten, als wären es Ihre eigenen“) ist einprägsam und appelliert an das eigene Verantwortungsbewusstsein. Der Verweis auf den Datenschutzbeauftragten bei Fragen könnte so jedoch nicht auf jede Organisation übertragbar sein, insbesondere, wenn eine Organisation über keinen Datenschutzbeauftragten verfügt oder intern über eine andere Arbeitsaufteilung verfügt. Der Hinweis auf die Meldung von Datenschutzvorfällen fällt nicht nur zu knapp aus, da nicht klar wird, an wen Vorfälle gemeldet werden sollen, vielmehr fehlt es auch an einem rechtlichen Rahmen, v.a. hinsichtlich der Definition eines Datenschutzvorfalls und den bestehenden Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO). Der Sensibilisierungs-Hinweis bleibt zu allgemein.

7. Wissenstest zur Selbstkontrolle

Der abschließende Wissenstest ist didaktisch gut konzipiert und praxisnah gestaltet, beispielsweise durch Fragen zu E-Mail-Fehlversand oder der Nutzung privater Cloud-Dienste. Positiv hervorzuheben ist, dass die Antworten zu den Fragen im Anhang der Schulung bereitgestellt werden, was die Selbstkontrolle der Mitarbeitenden unterstützt. Die Kürze des Tests trägt zusätzlich dazu bei, die Hürde zur Teilnahme niedrig zu halten und damit die Motivation zu fördern.

Kritisch zu betrachten ist jedoch die geringe inhaltliche Tiefe: Die Fragen prüfen weitgehend Basiswissen und reflektieren nicht die Anwendung der Datenschutzgrundsätze in komplexeren Alltagssituationen. Kritisch ist des Weiteren die Antwort auf die dritte Frage, was zu tun ist, wenn eine E-Mail versehentlich an die falsche Person gesendet wird. Die Antwort hierauf lautet „Sofort melden und die zuständige Stelle informieren“. Mangels rechtlicher Erläuterung oder Konkretisierung, dass hier die intern zuständige Stelle gemeint ist, könnte dies dazu führen, dass Datenschutzvorfälle unreflektiert und unabgesprochen an die zuständige Datenschutz-Aufsichtsbehörde gemeldet werden. Dies dürfte durch die Organisationen in der Regel nicht erwünscht sein.

8. Zusammenfassung

Positiv hervorzuheben ist der klare Abschluss der Schulung: Drei Kernaussagen verdichten den Gesamteinheit, der motivierende Ton („jeder Mitarbeiter trägt zum Datenschutz bei“) stärkt die Eigenverantwortung, und die knappe Wiederholung dient der Festigung der Hauptbotschaften. Der Abschnitt bleibt zwar insgesamt allgemein, da der Bezug zu den im Kurs behandelten Inhalten wie Betroffenenrechte, Pflichten der Mitarbeiter oder technische und organisatorische Maßnahmen fehlt, er fasst aber dennoch prägnant zusammen, warum die DSGVO umgesetzt werden muss, und dass dabei jeder Mitarbeiter seinen Teil beitragen muss. Sinnvoll wäre die Einbindung von Kontaktdata zu Ansprechpersonen (z. B. Datenschutzbeauftragter mit Name/E-Mail). Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

Zusammenfassend bietet die Schulung einen übersichtlichen Aufbau in logischer Reihenfolge mit klaren Lernzielen, Zeitangabe, praktischen Tipps im Do's-&-Don'ts-Format sowie einem Wissenstest mit Lösungshinweisen. Allerdings bleibt die Schulung inhaltlich deutlich zu oberflächlich und weist Lücken sowie punktuelle Ungenauigkeiten auf. Es handelt sich um einen sehr abstrakten Überblick über ausgewählte Pflichten der DSGVO. Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. So fehlen Beispiele aus dem Unternehmensalltag; eine Darstellung aller Rechtsgrundlagen (Art. 6, 9 DSGVO) mit kurzer Erläuterung, wann welche greift; ein klarer Verweis auf das „Verbot mit Erlaubnisvorbehalt“ als Grundlogik; die Erklärung der besonderen Kategorien inkl. besonderer Verarbeitungsvoraussetzungen (Art. 9 DSGVO); eine vollständige, praxisnahe Erläuterung aller Betroffenenrechte (Art. 15–22 DSGVO) inkl. Einschränkungen und Fristen; konkrete Anweisungen und Beispiele zur Umsetzung der Grundsätze (Art. 5 DSGVO) und Betroffenenrechte im Arbeitsalltag; Erläuterungen zur Meldung von Vorfällen (Art. 33, 34 DSGVO: Fristen, Zuständigkeiten, Risikobewertung); ein Hinweis auf die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO), das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und die Erforderlichkeit, technische und organisatorische Maßnahmen zu ergreifen (Art. 32 DSGVO) sowie ein Hinweis auf die ggf. erforderliche Durchführung einer Datenschutz-Folgenabschätzung bei hohem Risiko (Art. 35 DSGVO). Die juristische Präzision der Schulungsinhalte ist unzureichend, Begriffe und Grundsätze sind oft unvollständig oder verkürzt dargestellt, und der Kontext, wie Mitarbeitende das Gelernte konkret umsetzen sollen, fehlt weitestgehend. Die Schulung eignet sich daher eher als grober Überblick oder Einstieg, nicht jedoch als fundierte Grundlage, um im Anschluss rechtssicher und DSGVO-konform arbeiten zu können.

3.6 Grok 3 (xAI, Anwendung: Grok Web-App)

3.6.1 KI-generierter Inhalt²⁶

Selbstlerneinheit: Grundlagen des Datenschutzrechts nach DSGVO

Einführung

Willkommen in unserer Organisation! Diese Selbstlerneinheit vermittelt Ihnen die Grundlagen des Datenschutzrechts gemäß der **Datenschutz-Grundverordnung (DSGVO)**, die in unserer Organisation Anwendung findet. Ziel ist es, Ihnen ein Verständnis für die theoretischen Grundlagen sowie die praktische Umsetzung von Datenschutzvorgaben zu vermitteln. Diese Schulung ist für alle neuen Mitarbeitern konzipiert, unabhängig von Ihrer Rolle oder Ihrem Hintergrund. Sie benötigen keine Vorkenntnisse.

1. Theoretische Grundlagen der DSGVO

1.1 Was ist die DSGVO?

Die **Datenschutz-Grundverordnung (DSGVO)** ist eine EU-Verordnung, die seit dem 25. Mai 2018 den Schutz personenbezogener Daten in der gesamten Europäischen Union regelt. Sie gilt für alle Organisationen, die personenbezogene Daten von Personen innerhalb der EU verarbeiten.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z. B.:

- Name, Adresse, E-Mail-Adresse, Telefonnummer
- Geburtsdatum, Kontodaten
- IP-Adressen, Standortdaten

Ziel der DSGVO: Schutz der Privatsphäre von Einzelpersonen und einheitliche Regeln für den Umgang mit personenbezogenen Daten.

1.2 Grundprinzipien der DSGVO

Die DSGVO legt sieben zentrale Prinzipien fest, die bei der Verarbeitung personenbezogener Daten eingehalten werden müssen:

1. **Rechtmäßigkeit, Fairness und Transparenz:** Daten dürfen nur auf rechtlicher Grundlage und transparent verarbeitet werden.
2. **Zweckbindung:** Daten dürfen nur für festgelegte, legitime Zwecke verarbeitet werden.
3. **Datenminimierung:** Es dürfen nur die Daten verarbeitet werden, die für den Zweck notwendig sind.
4. **Richtigkeit:** Daten müssen richtig und aktuell gehalten werden.
5. **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.
6. **Integrität und Vertraulichkeit:** Daten müssen sicher vor unbefugtem Zugriff geschützt werden.
7. **Rechenschaftspflicht:** Die Organisation muss nachweisen können, dass sie die DSGVO einhält.

1.3 Rechte der Betroffenen

Personen, deren Daten verarbeitet werden, haben nach der DSGVO folgende Rechte:

- **Recht auf Auskunft:** Betroffene können erfahren, welche Daten über sie gespeichert sind.
- **Recht auf Berichtigung:** Falsche Daten müssen korrigiert werden.
- **Recht auf Löschung** („Recht auf Vergessenwerden“): Daten müssen unter bestimmten Bedingungen gelöscht werden.

²⁶ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell Grok 3 über Grok generiert.

- **Recht auf Einschränkung der Verarbeitung:** Die Verarbeitung kann in bestimmten Fällen eingeschränkt werden.
- **Recht auf Datenübertragbarkeit:** Betroffene können ihre Daten in einem maschinenlesbaren Format erhalten.
- **Widerspruchsrecht:** Betroffene können der Verarbeitung ihrer Daten widersprechen, z. B. zu Werbezwecken.
- **Recht auf Nicht-Diskriminierung:** Niemand darf benachteiligt werden, wenn er seine Rechte ausübt.

1.4 Rechtliche Grundlagen für die Datenverarbeitung

Daten dürfen nur verarbeitet werden, wenn mindestens eine der folgenden Rechtsgrundlagen gemäß Art. 6 DSGVO vorliegt:

- **Einwilligung** der betroffenen Person
- **Vertragserfüllung** (z. B. Arbeitsvertrag, Kundendaten für Lieferungen)
- **Rechtliche Verpflichtung** (z. B. Steuerdaten)
- **Schutz lebenswichtiger Interessen**
- **Öffentliches Interesse** oder **berechtigtes Interesse** der Organisation (sofern die Rechte der Betroffenen nicht überwiegen)

2. Praktische Relevanz der DSGVO in unserer Organisation

2.1 Datenverarbeitung in der Praxis

In unserer Organisation verarbeiten wir personenbezogene Daten in verschiedenen Bereichen, z. B.:

- **Personalwesen:** Mitarbeiterdaten (z. B. Gehaltsabrechnungen, Krankmeldungen)
- **Kundenmanagement:** Kundendaten für Verträge, Rechnungen oder Support
- **Marketing:** E-Mail-Adressen für Newsletter (nur mit Einwilligung)
- **IT-Systeme:** Zugriffsprotokolle, IP-Adressen

Beispiel: Wenn Sie im Kundensupport arbeiten, könnten Sie Zugriff auf Namen, Adressen oder Telefonnummern haben. Diese Daten dürfen nur für den vorgesehenen Zweck (z. B. Beantwortung einer Anfrage) verwendet werden.

2.2 Häufige Risiken

- **Unbefugter Zugriff:** Daten, die auf ungesicherten Geräten oder Servern gespeichert sind.
- **Datenlecks:** Versehentliches Weiterleiten von E-Mails mit sensiblen Daten.
- **Missbrauch von Daten:** Nutzung von Kundendaten für nicht genehmigte Zwecke.
- **Fehlende Dokumentation:** Nicht nachweisbare Einhaltung der DSGVO-Vorgaben.

Folgen von Verstößen: Hohe Geldstrafen (bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes), Reputationsverlust, rechtliche Konsequenzen.

3. Tipps zur praktischen Umsetzung der DSGVO

3.1 Verhalten im Arbeitsalltag

- **Vertraulichkeit wahren:** Geben Sie personenbezogene Daten nicht an Unbefugte weiter, auch nicht innerhalb der Organisation, wenn es nicht erforderlich ist.
- **Sichere Passwörter:** Verwenden Sie starke Passwörter und ändern Sie diese regelmäßig.
- **Geräte sichern:** Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz verlassen.
- **E-Mails prüfen:** Überprüfen Sie Empfängerlisten, bevor Sie sensible Daten versenden. Nutzen Sie BCC für Massen-E-Mails.

- **Einwilligungen einholen:** Wenn Sie Daten (z. B. für Marketing) erheben, holen Sie eine ausdrückliche Einwilligung ein.

3.2 Umgang mit Anfragen von Betroffenen

- Leiten Sie Anfragen zu Auskunft, Löschung oder Berichtigung unverzüglich an die zuständige Abteilung (z. B. Datenschutzbeauftragte/r) weiter.
- Antworten Sie nicht direkt auf solche Anfragen, sondern folgen Sie den internen Prozessen.

3.3 Meldepflicht bei Datenpannen

- Wenn Sie einen möglichen Datenschutzvorfall bemerken (z. B. Verlust eines Laptops, fehlerhafte E-Mail), informieren Sie **umgehend** den Datenschutzbeauftragten.
- Dokumentieren Sie den Vorfall (z. B. Datum, Art der Daten, betroffene Personen).

3.4 Schulungen und Sensibilisierung

- Nehmen Sie an regelmäßigen Datenschutzschulungen teil.
- Seien Sie wachsam für Phishing-E-Mails oder andere Angriffe, die Daten gefährden könnten.

4. Zusammenfassung und Checkliste

Wichtige Punkte:

- Personenbezogene Daten nur auf rechtlicher Grundlage und zweckgebunden verarbeiten.
- Rechte der Betroffenen respektieren und Anfragen richtig weiterleiten.
- Daten sicher speichern und vertraulich behandeln.
- Bei Datenpannen sofort handeln und melden.

Checkliste für den Arbeitsalltag:

- Habe ich Zugriff auf personenbezogene Daten? Wenn ja, kenne ich den Zweck der Verarbeitung?
- Sind meine Arbeitsgeräte (PC, Smartphone) gesichert?
- Habe ich sensible Daten richtig gespeichert (z. B. nicht auf dem Desktop)?
- Kenne ich den Ansprechpartner für Datenschutzfragen in der Organisation?
- Bin ich mir der Meldepflicht bei Datenpannen bewusst?

5. Abschluss

Der Schutz personenbezogener Daten ist eine gemeinsame Verantwortung. Durch die Einhaltung der DSGVO tragen Sie dazu bei, das Vertrauen unserer Kunden, Partner und Kollegen zu bewahren. Bei Fragen wenden Sie sich an den Datenschutzbeauftragten unserer Organisation.

Kontakt: [Hier internen Ansprechpartner einfügen, z. B. E-Mail-Adresse oder Telefonnummer]

Vielen Dank für Ihre Aufmerksamkeit und Ihr Engagement für den Datenschutz!

3.6.2 Bewertung

Die von Grok 3 generierte Selbstlerneinheit zu den Grundlagen der DSGVO überzeugt in weiten Teilen durch einen klar strukturierten Aufbau, der sich an der Systematik der DSGVO orientiert. Die vier Kapitel bauen logisch aufeinander auf, sind sprachlich an Einsteiger ohne juristische Vorkenntnisse angepasst und durchgängig gut verständlich formuliert. Die direkte Ansprache neuer Mitarbeiter („Willkommen in unserer Organisation“) schafft eine positive Lernatmosphäre, die durch praxisnahe und passende Beispiele zusätzlich unterstützt wird. Gleichwohl weist die Schulung Schwächen auf, die sich nachteilig auf die Qualität auswirken. Zentrale Begriffe der DSGVO sind teilweise

ungenau oder gar nicht definiert. Wichtige datenschutzrechtliche Konzepte und Instrumente fehlen oder werden nicht systematisch eingeführt. Zudem werden die Begriffe „Daten“ und „personenbezogene Daten“ synonym zueinander genutzt, was zu Missverständnissen führen kann. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einführung

Die Einleitung ist insgesamt sehr gelungen, denn Sie schafft eine gute Balance zwischen Information, Motivation und Zugänglichkeit. Sie beschreibt das Ziel der Schulung klar und weist darauf hin, dass die DSGVO in der Organisation Anwendung findet. Positiv ist auch der Hinweis, dass keine Vorkenntnisse erforderlich sind. Dies senkt die Einstiegshürde und macht deutlich, dass die Schulung inklusiv gedacht ist.

1. Theoretische Grundlagen der DSGVO

1.1 Was ist die DSGVO?

Im Abschnitt „Was ist die DSGVO?“ wird zunächst erklärt, dass die DSGVO den Schutz personenbezogener Daten regelt. Diese Erklärung ist nicht ganz treffend: Die DSGVO regelt vielmehr die Verarbeitung personenbezogener Daten mit dem Ziel, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen und gleichzeitig den freien Verkehr solcher Daten zu ermöglichen (Art. 1 Abs. 1, 2 DSGVO). Das Ziel der DSGVO als „Schutz der Privatsphäre“ zu beschreiben, greift zu kurz – die Privatsphäre ist nur ein Teilaspekt des umfassenderen Grundrechtsschutzes.

Grundsätzlich positiv ist zu vermerken, dass das Marktortprinzip indirekt angesprochen wird („alle Organisationen, die personenbezogene Daten von Personen innerhalb der EU verarbeiten“). Dabei wird jedoch versäumt klarzustellen, dass die DSGVO auch dann gilt, wenn eine Organisation ihren Sitz in der EU hat und personenbezogene Daten von Personen außerhalb der EU verarbeitet.

Die Definition des Begriffs „personenbezogene Daten“ entspricht dem Wortlaut des Art. 4 Nr. 1 DSGVO, ist jedoch unvollständig. So fehlt eine Erläuterung der Begriffe „identifiziert“ und „identifizierbar“ – nur ein Verständnis von diesen Begriffen ermöglicht es in der Praxis entscheiden zu können, ob eine natürliche Person identifiziert oder identifizierbar ist. Zudem wird versäumt darauf hinzuweisen, dass eine Identifizierung direkt und indirekt erfolgen kann. Die gewählten Beispiele für personenbezogene Daten sind zutreffend und praxisnah. Zudem fehlt eine Abgrenzung von personenbezogenen Daten zu pseudonymen und anonymen Daten. Der Begriff „natürliche Person“ wird nicht definiert, ebenso wenig wird auf besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) eingegangen; es fehlt damit auch die Erläuterung ihres besonderen Schutzbedarfs.

Weitere Begriffe werden nicht eingeführt: Es fehlt die Definition von „Verarbeitung“. Die Rollen „Verantwortlicher“, „gemeinsamer Verantwortlicher“ und „Auftragsverarbeiter“ werden nicht erläutert, ebenso wenig deren Abgrenzung.

1.2 Grundprinzipien der DSGVO

Die Grundsätze der Verarbeitung (Art. 5 DSGVO) werden vorliegend als „Grundprinzipien“ bezeichnet, was zwar nicht falsch ist, aber nicht dem genauen Wortlaut der Norm entspricht. Dadurch kann der Eindruck entstehen, dass es sich um eine eigenständige normative Bezeichnung handelt.

Positiv fällt auf, dass alle sieben Grundsätze aus Art. 5 DSGVO genannt werden. Die jeweiligen Ausführungen sind jedoch stark verkürzt und teilweise ungenau. Zudem werden keinerlei Hinweise zu deren praktischen Relevanz und praktischen Umsetzung

gegeben. Ebenso wenig werden grundlegende und praxisnahe Beispiele gegeben. Insgesamt werden damit zwar die Grundsätze der DSGVO vollständig benannt, jedoch inhaltlich unzureichend ausgeführt, um Verständnis bzw. Anwendungswissen zu vermitteln.

Der Grundsatz der „Rechtmäßigkeit, Fairness und Transparenz“ wird in einem Satz zusammengefasst, ohne die einzelnen Elemente zu erklären oder durch Beispiele zu veranschaulichen. Überdies lautet das Gebot nach dem Wortlaut des Gesetzes „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, sodass der Begriff „Fairness“ hier eher umgangssprachlich wirkt. Lobenswert ist, dass der Hinweis erfolgt, dass Daten – richtig wäre hier und bei allen anderen Grundsätzen „personenbezogene Daten“ – nur auf rechtlicher Grundlage verarbeitet werden dürfen. Im Rahmen der Transparenz hätte bereits auf die Informationspflichten (Art. 13, 14 DSGVO) des Verantwortlichen hingewiesen werden können. Der Grundsatz der „Zweckbindung“ wird zu eng gefasst und entspricht nicht dem Wortlaut des Art. 5 Abs. 1 lit. b DSGVO. Es fehlt insbesondere der Hinweis, dass eine Weiterverarbeitung von personenbezogenen Daten zulässig sein kann, wenn sie mit dem ursprünglichen Zweck vereinbar ist (Art. 6 Abs. 4 DSGVO). Der Grundsatz der „Datenminimierung“ ist zwar grundsätzlich fehlerfrei, er wird jedoch unvollständig beschrieben, da die Kriterien „angemessen“ und „erheblich“ weder explizit erwähnt noch implizit enthalten sind. Der Grundsatz der „Richtigkeit“ wird ohne den Zusatz erläutert, dass eine Pflicht zur Aktualisierung nur „erforderlichenfalls“ besteht. Der Grundsatz der „Speicherbegrenzung“ wird grundsätzlich zutreffend erklärt, jedoch ohne den Zusatz, dass die „Identifizierung nur so lange möglich sein darf, wie es für den Zweck erforderlich ist“. Der Grundsatz der „Integrität und Vertraulichkeit“ wird unvollständig dargestellt. Es wird einzig Bezug auf den Schutz vor unbefugtem Zugriff genommen, nicht jedoch allgemeiner auf den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Zudem wird versäumt auch den Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu erwähnen. Es fehlt des Weiteren der Hinweis, dass hierfür technische und organisatorische Maßnahmen zu treffen sind. Die „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO) wird richtig, aber zu oberflächlich erläutert.

1.3 Rechte der Betroffenen

Die Aufzählung umfasst die wesentlichen Betroffenenrechte, allerdings mit teils ungenauer oder unvollständiger Beschreibung. Beim „Auskunftsrecht“ (Art. 15 DSGVO) fehlt, dass auch Zweck, Rechtsgrundlage, Empfänger, Speicherdauer, Herkunft, Drittlandübermittlungen und automatisierte Entscheidungen anzugeben sind. Das „Berichtigungsrecht“ (Art. 16 DSGVO) wird grundsätzlich richtig genannt, jedoch ohne Hinweis auf die Unverzüglichkeit. Das „Löscrecht“ (Art. 17 DSGVO) wird nur allgemein erwähnt; die Voraussetzungen, Ausnahmen und Unterschiede zum Recht auf Vergessenwerden fehlen. Die „Einschränkung der Verarbeitung“ (Art. 18 DSGVO) wird ohne die jeweiligen Voraussetzungen und ohne Beispiele genannt. Die „Datenübertragbarkeit“ (Art. 20 DSGVO) wird oberflächlich beschrieben, ohne die Voraussetzungen einer Einwilligung oder eines Vertrags und die Anforderung automatisierter Verarbeitung. Das „Widerspruchsrecht“ (Art. 21 DSGVO) wird ebenfalls zu knapp dargestellt, ohne die Unterscheidung zwischen Fällen mit und ohne zwingende schutzwürdige Gründe (Abs. 1 und Abs. 2). Die Nennung eines „Rechts auf Nicht-Diskriminierung“ ist rechtlich unzutreffend, denn ein solches Recht wird in der DSGVO nicht ausdrücklich genannt.

Negativ fällt auf, dass praxisrelevante Hinweise zu Umsetzung, Fristen (Art. 12 Abs. 3 DSGVO), typischen internen Prozessen und Meldewegen fehlen. Ebenso wird nicht erläutert, wie mit Anfragen betroffener Personen umzugehen ist und dass in jedem Fall zunächst Rücksprache mit einer intern zuständigen Person zu halten ist.

1.4 Rechtliche Grundlagen für die Datenverarbeitung

Das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ (Art. 6 Abs. 1 DSGVO) wird nicht erläutert, wodurch das Verständnis der DSGVO-Struktur erschwert wird. Positiv ist jedoch zu vermerken, dass die Essenz des Grundsatzes aus Formulierungen wie „Daten dürfen nur auf rechtlicher Grundlage verarbeitet werden“ bzw. „Daten dürfen nur verarbeitet werden, wenn mindestens eine der folgenden Rechtsgrundlagen vorliegt“ indirekt hervorgeht. Die sechs Rechtsgrundlagen aus Art. 6 Abs. 1 DSGVO werden genannt, aber teils ungenau beschrieben. „Öffentliches Interesse“ (Art. 6 Abs. 1 lit. e DSGVO) und „berechtigtes Interesse“ (Art. 6 Abs. 1 lit. f DSGVO) werden vermischt. Die Voraussetzungen der Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO) werden nicht erläutert. Eine klare Erklärung der „rechtlichen Verpflichtung“ (Art. 6 Abs. 1 lit. c DSGVO) fehlt. Beim „berechtigten Interesse“ (Art. 6 Abs. 1 lit. f DSGVO) fehlen Hinweise zur erforderlichen Interessenabwägung. Insgesamt sind die Ausführungen zur rechtlichen Grundlage zu knapp gefasst. Es fehlt eine konkrete Erläuterung, wann jede Rechtsgrundlage greift, sodass unklar bleibt, welche Grundlage in der Praxis anzuwenden ist. Ebenso fehlen praxisnahe Beispiele, etwa wann das berechtigte Interesse oder die Einwilligung relevant sein könnte. Insgesamt bietet die Auflistung nur einen theoretischen Überblick, ohne Mitarbeitende handlungsfähig zu machen.

2. Praktische Relevanz in der Organisation

Der Abschnitt zur praktischen Relevanz der DSGVO in der Organisation ist grundsätzlich positiv zu bewerten, da er den Mitarbeitenden die theoretischen Datenschutzgrundlagen praxisnah vermittelt und somit die Umsetzung im Arbeitsalltag erleichtert. Die Beispiele für typische Verarbeitungen in Personalwesen, Kundenmanagement, Marketing und IT sind gelungen und praxisnah. Die Beispiele für Risiken („Unbefugter Zugriff“, „Datenlecks“, „Missbrauch von Daten“, „Fehlende Dokumentation“) sind praxisnah und für Mitarbeitende gut nachvollziehbar. Auch die dargestellten Folgen von Verstößen verdeutlichen die Relevanz der DSGVO in der Organisation. Negativ fällt jedoch auf, dass die beschriebenen Risiken weitgehend Datenschutzverletzungen beschreiben, ohne entsprechend eingeordnet zu werden. In der Folge fehlt es hier auch an Hinweisen zum Umgang mit entsprechenden Datenschutzverletzungen, insbesondere im Zusammenhang mit ggf. bestehenden Melde- und Benachrichtigungspflichten. Negativ fällt des Weiteren auf, dass der Abschnitt zur praktischen Relevanz sehr kurz ausfällt und die praktische Relevanz daher auch nur fragmentarisch darstellt.

3. Tipps zur praktischen Umsetzung

Die Hinweise sind praxisnah, bleiben jedoch zu allgemein. Bei „sicheren Passwörtern“ fehlen konkrete Anforderungen wie Mindestlänge, Komplexität und der Einsatz von Passwortmanagern. Der Punkt „Einwilligungen einholen“ könnte fälschlicherweise den Eindruck erwecken, dass Einwilligung die Standardrechtsgrundlage ist, obwohl sie nur eine von mehreren Rechtsgrundlagen darstellt. Beim Umgang mit Betroffenenanfragen fehlen gesetzliche Fristen (grundsätzlich ein Monat), Hinweise zum Umfang der Auskunft sowie zur Dokumentationspflicht. Zudem wird lediglich Bezug auf Auskunfts-, Lösch- und Berichtigungsanfragen genommen, was zu Missverständnissen führen kann.

Die Meldepflicht bei Datenpannen wird zwar angesprochen („informieren Sie umgehend den Datenschutzbeauftragten“), jedoch ohne Definition, was als meldepflichtige Datenpanne gilt. Mängels Klarstellung, ab welcher Risikoschwelle eine Meldepflicht besteht, könnte der Eindruck entstehen, jeder Vorfall müsse gemeldet werden – auch solche, die lediglich mit einem geringen Risiko verbunden sind. Nicht erwähnt wird die 72-Stunden-Frist nach Art. 33 DSGVO. Positiv ist der Verweis auf die interne Meldung an den Datenschutzbeauftragten, allerdings fehlt die Klarstellung, dass dieser bzw. die Organisation dann die Risikobewertung vornimmt und gegebenenfalls die externe Meldung durchführt. Ohne diese Präzisierungen besteht die Gefahr von Fehlmeldungen oder verspäteten Meldungen. Auffällig ist des Weiteren, dass die Mitarbeiter unter

3. KI-generierte Schulungen

„Umgang mit Anfragen von Betroffenen“ angehalten werden, Anfragen „an die zuständige Abteilung (z. B. Datenschutzbeauftragten)“ weiterzuleiten, während sie unter „Meldepflicht bei Datenpannen“ angehalten werden, den Datenschutzbeauftragten zu informieren. Hierdurch könnten nicht nur Fragen im Zusammenhang mit der internen Zuständigkeit für verschiedene Aufgaben entstehen, es wird außerdem nicht dem Umstand Rechnung getragen, dass nicht jede Einrichtung über einen Datenschutzbeauftragten verfügt. Sinnvoller wäre hier Platz für eine organisationsspezifische Präzisierung zu lassen.

4. Zusammenfassung und Checkliste

Die Zusammenfassung ist richtig, aber zu allgemein. Es fehlen Wiederholungen der wichtigsten Rechtsgrundlagen, Grundprinzipien und Pflichten, um das Gelernte nachhaltig zu verankern. Die Checkliste ist sinnvoll, jedoch unvollständig. Dadurch besteht das Risiko, dass Mitarbeitende falsche Annahmen treffen oder ihre Pflichten nur teilweise kennen.

5. Abschluss

Positiv fällt auf, dass nochmals an die (Mit-)Verantwortung der Mitarbeitenden appelliert wird. Der Satz „Durch die Einhaltung der DSGVO tragen Sie dazu bei, das Vertrauen unserer Kunden, Partner und Kollegen zu bewahren“ spricht das Pflicht- und Verantwortungsbewusstsein der Mitarbeitenden direkt an. Die Erwähnung interner Ansprechpartner am Ende der Schulung ist sinnvoll.

Zusammenfassend ist die Schulung in Sprache, Struktur und Praxisbezug gut als Einstieg geeignet und vermittelt zentrale Grundgedanken der DSGVO in zugänglicher Form. Allerdings fehlen der Schulung mehrere wichtige Punkte: Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. Zentrale Begriffe werden nicht oder nur unzureichend definiert, wodurch Mitarbeiter Schwierigkeiten haben könnten, die Inhalte richtig einzuordnen. Das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ wird nicht erläutert, wodurch das Verständnis der DSGVO-Struktur erschwert wird. Technische und organisatorische Maßnahmen (Art. 32 DSGVO) werden nur indirekt angesprochen, jedoch nicht systematisch erläutert, sodass der praktische Nutzen begrenzt bleibt. Zudem fehlt ein Hinweis auf die Datenschutz-Folgenabschätzung (Art. 35 DSGVO), die bei Verarbeitungsvorgängen mit hohem Risiko verpflichtend ist. Auch das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) wird nicht erwähnt. Schließlich wird der Umgang mit Datenschutzverletzungen (Art. 33, 34 DSGVO) nicht erläutert, einschließlich der internen Meldewege und Fristen. Die Schulung erfüllt daher nicht die Anforderungen einer rechtlich fundierten Schulung, da wesentliche juristische Inhalte, präzise Definitionen, eine systematische Darstellung der DSGVO-Struktur und die Behandlung zentraler Pflichten fehlen. Die Einheit ist als Einstiegsmaterial geeignet, aber als vollständige DSGVO-Schulung unzureichend

3.7 LLaMA 4 (Meta AI, Anwendung: LLaMA Chat)

3.7.1 KI-generierter Inhalt²⁷

Selbstlerneinheit: Datenschutz-Grundlagen nach DSGVO

Einleitung

Herzlich willkommen bei unserer Selbstlerneinheit zum Thema Datenschutz! Als neuer Mitarbeiter unserer Organisation ist es wichtig, dass du die Grundlagen des Datenschutzrechts verstehst und weißt, wie du diese in deiner täglichen Arbeit umsetzen

²⁷ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell LLaMA 4 über LLaMA Chat generiert.

kannst. Diese Schulung soll dir dabei helfen, die Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu verstehen und praktisch anzuwenden.

Theoretische Grundlagen

1. Was ist Datenschutz?

Datenschutz bedeutet den Schutz personenbezogener Daten vor Missbrauch, Verlust oder unbefugtem Zugriff. Die DSGVO ist eine EU-Verordnung, die den Schutz personenbezogener Daten in der Europäischen Union regelt.

2. Grundprinzipien der DSGVO

- **Transparenz:** Datenverarbeitung muss transparent und nachvollziehbar sein.
- **Zweckbindung:** Daten dürfen nur für einen bestimmten Zweck verarbeitet werden.
- **Datenminimierung:** Es dürfen nur die Daten verarbeitet werden, die unbedingt notwendig sind.
- **Speicherbegrenzung:** Daten dürfen nur solange gespeichert werden, wie es notwendig ist.
- **Integrität und Vertraulichkeit:** Daten müssen sicher und vertraulich verarbeitet werden.

3. Rollen und Verantwortlichkeiten

- **Datenschutzbeauftragter (DSB):** Der DSB ist für die Überwachung der Einhaltung der DSGVO-Anforderungen verantwortlich.
- **Verantwortlicher:** Der Verantwortliche ist die Organisation oder Person, die die Datenverarbeitung durchführt.
- **Auftragsverarbeiter:** Der Auftragsverarbeiter ist ein Dienstleister, der Daten im Auftrag des Verantwortlichen verarbeitet.

Praktische Relevanz und Tipps zur Umsetzung

1. Datenvermeidung

- **Tipps:**
 - Überlege dir vor der Datenerhebung, ob die Daten wirklich notwendig sind.
 - Verwende anonymisierte oder pseudonymisierte Daten, wenn möglich.

2. Datensicherheit

- **Tipps:**
 - Verwende starke Passwörter und sichere Authentifizierungsmethoden.
 - Aktualisiere regelmäßig deine Software und Systeme.
 - Sichere deine Daten durch regelmäßige Backups.

3. Transparenz und Informationspflichten

- **Tipps:**
 - Informiere betroffene Personen über die Datenverarbeitung und ihre Rechte.
 - Stelle sicher, dass deine Datenschutzhinweise klar und verständlich sind.

4. Rechte der betroffenen Personen

- **Tipps:**
 - Stelle sicher, dass du Anfragen von betroffenen Personen zeitnah und richtig bearbeitest.
 - Informiere betroffene Personen über die Möglichkeiten, ihre Rechte auszuüben.

Fazit und nächste Schritte

Du hast jetzt die Grundlagen des Datenschutzrechts nach DSGVO kennengelernt und Tipps zur praktischen Umsetzung erhalten. Es ist wichtig, dass du diese Kenntnisse in deiner täglichen Arbeit anwendest und regelmäßig auffrischst. Wenn du Fragen hast oder weitere Informationen benötigst, stehe ich gerne zur Verfügung.

Überprüfung deiner Kenntnisse

Um sicherzustellen, dass du die Inhalte dieser Selbstlerneinheit verstanden hast, empfehlen wir dir, einen kurzen Test durchzuführen. Bitte wende dich an deinen Vorgesetzten oder den Datenschutzbeauftragten, um den Test zu erhalten.

3. KI-generierte Schulungen

Ich hoffe, diese Selbstlerneinheit hat dir geholfen, die Grundlagen des Datenschutzrechts nach DSGVO zu verstehen und praktisch anzuwenden. Wenn du weitere Fragen hast, stehe ich gerne zur Verfügung.

3.7.2 Bewertung

Die von LLaMA 4 generierte Selbstlerneinheit ist für eine Grundlagenschulung zur DSGVO insgesamt deutlich zu kurz und oberflächlich gehalten. Sie weist erhebliche inhaltliche Mängel auf. Zentrale datenschutzrechtliche Begriffe sowie grundlegende Instrumente und Pflichten des Datenschutzes werden entweder gar nicht thematisiert, nur oberflächlich angerissen oder inhaltlich unzutreffend dargestellt. Darüber hinaus mangelt es der Schulung an praktischen Beispielen und konkreten Anwendungstipps. Die Inhalte sind fragmentarisch, teilweise fehlerhaft und lassen jegliche inhaltliche Tiefe vermissen. Eine Vermittlung von Grundlagenwissen findet nicht statt.

Insgesamt positiv hervorzuheben ist die Ansprache der Schulung: Die Einleitung erklärt Zweck und Nutzen der Schulung verständlich und motivierend, indem sie die Mitarbeitenden direkt adressiert („Diese Schulung soll *dir* dabei helfen...“). Damit ist ein positiver Einstieg gelungen. Allerdings fehlt ein orientierender Überblick über die behandelten Themen und es werden keine konkreten DSGVO-Artikel genannt. Die Gliederung in „Theoretische Grundlagen“ und „Praktische Relevanz“ ist zwar nachvollziehbar, didaktisch aber nicht optimal umgesetzt, denn Theorie und Anwendung stehen somit nebeneinander, ohne Zusammenhänge deutlich zu machen und systematisch aufeinander aufzubauen. Hinzu kommen inkonsistente Begrifflichkeiten zwischen den Kapiteln sowie ein angekündigter, aber nicht bereitgestellter Test.

Einleitung

Die Einleitung ist insgesamt sehr gelungen, denn sie spricht den Mitarbeitenden direkt an und macht klar, warum diese Selbstlerneinheit relevant ist. Das „Herzlich willkommen“ schafft einen freundlichen Einstieg, und der Hinweis auf die praktische Anwendung in der täglichen Arbeit zeigt dem Mitarbeitenden unmittelbar, welchen Nutzen die Schulung für ihn hat.

Theoretische Grundlagen

1. Was ist Datenschutz?

Die Kerndefinition ist fehlerhaft, denn die DSGVO bzw. der Datenschutz schützt nicht die personenbezogenen Daten selbst, sondern die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten (Art. 1 Abs. 2 DSGVO). Zentrale datenschutzrechtliche Begriffe werden nicht eingeführt; insbesondere fehlen Definitionen der Begriffe „personenbezogene Daten“ (Art. 4 Nr. 1 DSGVO) und „Verarbeitung“ (Art. 4 Nr. 2 DSGVO). Ohne dieses begriffliche Fundament bleibt die weitere Darstellung für juristische Laien weitgehend unverständlich. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden weder definiert noch in ihrer erhöhten Sensibilität erklärt. Die Schulung lässt ebenso offen, warum die DSGVO in der Organisation Anwendung findet. Sie erläutert den Geltungsbereich der Verordnung nicht

2. Grundprinzipien der DSGVO

Die Grundsätze der Verarbeitung (Art. 5 DSGVO) werden vorliegend als „Grundprinzipien“ bezeichnet. Das ist zwar nicht falsch, entspricht jedoch nicht dem Wortlaut der Norm. Das kann wiederum den Eindruck erwecken, dass es sich um eine eigene Norm handelt.

Die Aufzählung der Grundsätze der Verarbeitung lehnt sich im Kern an Art. 5 Abs. 1 DSGVO an, bleibt aber in den Erläuterungen zu knapp und unvollständig. Der (Teil-)Grundsatz der „Rechtmäßigkeit“ wird nicht herausgearbeitet. Damit fehlt auch der

Hinweis auf das tragende Strukturprinzip der DSGVO – das „Verbot mit Erlaubnisvorbehalt“ – sowie die Erläuterung, dass jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage bedarf. Der (Teil-)Grundsatz der „Transparenz“ ist auch kein eigenständiger Grundsatz, sondern lautet („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Nicht erwähnt und erläutert werden außerdem der „Grundsatz der Richtigkeit“ (Art. 5 Abs. 1 lit. d DSGVO) und die „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO).

3. Rollen und Verantwortlichkeiten

Die Rolle des Datenschutzbeauftragten wird knapp dargestellt. Die Definition des „Verantwortlichen“ ist unpräzise. Maßgeblich ist nicht, wer die Datenverarbeitung durchführt, sondern wer über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). Die praktische Durchführung obliegt regelmäßig Mitarbeitern, die selbst nicht Verantwortliche im Sinne der DSGVO sind. Die Beschreibung des Auftragsverarbeiters (Art. 28 DSGVO) bleibt oberflächlich. Es fehlt der Hinweis, dass er ausschließlich auf Weisung des Auftraggebers handelt und dass bei Auftragsverarbeitung der Auftraggeber Verantwortlicher im Sinne der DSGVO bleibt. Die gemeinsame Verantwortlichkeit (Art. 26 DSGVO) bleibt gänzlich unerwähnt, was in der Praxis insoweit zu Missverständnissen führen könnte, als die bloße Erwähnung des (alleinigen) Verantwortlichen und des Auftragsverarbeiters nahelegt, dass die Involvierung mehrerer Parteien immer mit einer Auftragsverarbeitung einhergeht. Eine Definition, wer „betroffenen Person“ ist, fehlt.

Praktische Relevanz und Tipps zur Umsetzung

Die Hinweise zur praktischen Relevanz und zu den Tipps zur Umsetzung enthalten zwar grundsätzlich richtige Informationen, die als „Tipps“ formulierten Hinweise sind jedoch irreführend, da es sich hierbei um rechtliche Pflichten der DSGVO handelt und nicht um Empfehlungen.

Zudem mangelt es an einem theoretischen Fundament für die Umsetzungshinweise. Einzig zur „Datenvermeidung“ und „Transparenz“ wurde im theoretischen Teil bereits ein Fundament geschaffen. Durch die hier gewählte Terminologie im Zusammenhang mit der „Datenvermeidung“, welche nicht nur aus dem alten BDSG stammt und damit überholt ist, sondern auch anders lautet als im theoretischen Teil, in welchem (wie auch die DSGVO) von der „Datenminimierung“ gesprochen wird, ist jedoch davon auszugehen, dass Mitarbeitende diesen Zusammenhang nicht herstellen können. Zudem könnten die unterschiedlichen Begriffe für Missverständnisse sorgen, da sie nahelegen, dass es sich um unterschiedliche Pflichten handelt. Für die Begriffe „Datensicherheit“, „Informationspflichten“ und „Rechte der betroffenen Personen“ mangelt es dagegen an einem konkreten theoretischen Fundament. Zwar basieren die „Datensicherheit“ auf dem Grundsatz der Integrität und Vertraulichkeit und die „Informationspflichten“ und die „Rechte der betroffenen Personen“ auf dem Grundsatz der Transparenz, es ist jedoch davon auszugehen, dass es für datenschutzrechtliche Laien nicht möglich ist, diesen Zusammenhang herzustellen. Zudem wird versäumt auf die weiteren rechtlichen Grundlagen in diesem Zusammenhang hinzuweisen.

So beschreibt die „Datensicherheit“ technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Diese werden nicht als solche benannt, bleiben abstrakt und ohne greifbare Beispiele. Auch wird mangels theoretischer Einordnung deren übergeordneter Zweck nicht deutlich. Für den Mitarbeitenden wird hierdurch nicht einmal indirekt deutlich, dass auch andere Maßnahmen, wie z. B. Zugriffs- und Berechtigungskonzepte, Verschlüsselung, Lösch- und Aufbewahrungskonzepte oder Backup- und Notfallmanagementkonzepte erforderlich sind. Im Zusammenhang mit „Transparenz und Informationspflichten“ werden zwar grundsätzlich wichtige Hinweise gegeben, die zugrundeliegenden Normen (Art. 12–14 DSGVO) werden jedoch nicht genannt.

Hierdurch bleibt unklar, zu welchem Zeitpunkt, in welcher Form und mit welchen Inhalten betroffene Personen informiert werden müssen. Ebenso bleibt der Abschnitt „Rechte der betroffenen Personen“ zu allgemein. Es wird weder Bezug auf die konkreten zugrundeliegenden Normen und Betroffenenrechte genommen noch werden Bearbeitungsfristen und Vorbedingungen für eine Bearbeitung von Betroffenenanfragen, etwa vorherige Einbindung einer in der Organisation zuständigen Person, erwähnt. Ohne klare Handlungsanweisungen oder Verweise auf interne Regelungen entsteht im Betriebsalltag Rechts- und Umsetzungsunsicherheit. Zudem könnte dies zu einer unreflektierten und unabgesprochenen Bearbeitung von Betroffenenanfragen durch Mitarbeitende führen, was erhebliche Konsequenzen für die Organisation haben könnte.

Fazit und nächste Schritte

Die Behauptung, die „Grundlagen“ des Datenschutzrechts seien vermittelt, trifft in der vorliegenden Form nicht zu.

Überprüfung deiner Kenntnisse

Die abschließende Bezugnahme auf einen Test, der vom Vorgesetzten oder Datenschutzbeauftragten zur Verfügung gestellt werden soll, verfehlt den Zweck der durch den KI-Chatbot generierten Selbstlerneinheit, da er nicht mitgeneriert wurde. Zudem fehlt die Einbindung von Kontaktdaten zu Ansprechpersonen (z. B. Datenschutzbeauftragter mit Name/E-Mail). Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

Zusammenfassend bietet die Schulung eine freundliche, verständliche Sprache, eine motivierende Einleitung und eine grundsätzlich sinnvolle Themenauswahl. Dem stehen jedoch gravierende inhaltliche Defizite gegenüber: Insbesondere fehlende Definitionen, unklare oder fehlerhafte Rollenbeschreibungen, eine unvollständige Darstellung der rechtlichen Pflichten, die Verharmlosung rechtlicher Pflichten als „Tipps“, das Ausbleiben von Normbezügen, ein unzureichender Praxisbezug sowie der nicht bereitgestellte Test. Weder werden zentrale Begriffe richtig eingeführt, noch sind Rechte, Pflichten und Zuständigkeiten vollständig und präzise dargestellt. Neben den Hinweisen zur Rechtsmäßigkeit der Verarbeitung und den damit verbundenen möglichen Rechtsgrundlagen für eine Verarbeitung personenbezogener Daten, fehlt es insbesondere auch an einer Aufzählung und Erläuterung der Betroffenenrechte (Art. 12 ff. DSGVO), einer Erläuterung der technischen und organisatorischen Maßnahmen (Art. 24, 25 und 32 DSGVO), einer Darstellung, welche Pflichten im Falle von Datenschutzverletzungen erfüllt werden müssen (Art. 33, 34 DSGVO) und einer Klarstellung, dass eine Rechenschaftspflicht besteht und hierfür insbesondere auch ein Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) geführt werden muss. Ebenso werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. Die Einheit ist damit als vollständige DSGVO-Schulung unzureichend.

3.8 Mistral Medium 3 (Mistral AI, Anwendung: Le Chat)

3.8.1 KI-generierter Inhalt²⁸

Selbstlerneinheit: Grundlagen des Datenschutzrechts nach der Datenschutz-Grundverordnung (DSGVO)

Einführung

²⁸ Der in diesem Unterkapitel abgedruckte Text wurde vollständig von dem Modell Mistral Medium 3 über Le Chat generiert.

Willkommen zu Ihrer Selbstlernseinheit über die Grundlagen des Datenschutzrechts nach der Datenschutz-Grundverordnung (DSGVO). Diese Schulung ist für alle neuen Mitarbeiter unserer Organisation konzipiert und soll Ihnen ein grundlegendes Verständnis der DSGVO vermitteln, unabhängig von Ihrer Position oder Ihrem Aufgabenbereich.

Lernziele

- Verständnis der Grundprinzipien der DSGVO
- Kenntnis der Rechte von betroffenen Personen
- Praktische Umsetzung der DSGVO im Arbeitsalltag
- Sensibilisierung für den Umgang mit personenbezogenen Daten

Modul 1: Einführung in die DSGVO

1.1 Was ist die DSGVO?

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, die den Umgang mit personenbezogenen Daten regelt. Sie trat am 25. Mai 2018 in Kraft und gilt in allen EU-Mitgliedstaaten.

1.2 Ziele der DSGVO

- Schutz personenbezogener Daten
- Stärkung der Rechte von betroffenen Personen
- Vereinheitlichung des Datenschutzrechts in der EU

1.3 Wichtige Begriffe

- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- **Verarbeitung:** Jeder Vorgang im Zusammenhang mit personenbezogenen Daten, wie das Erheben, Speichern oder Nutzen.
- **Betroffene Person:** Eine natürliche Person, deren personenbezogene Daten verarbeitet werden.

Modul 2: Grundprinzipien der DSGVO

2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

2.2 Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

2.3 Datenminimierung

Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für den Verarbeitungszweck tatsächlich notwendig sind.

2.4 Richtigkeit

Personenbezogene Daten müssen sachlich richtig und, falls notwendig, auf dem neuesten Stand sein.

2.5 Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, notwendig ist.

2.6 Integrität und Vertraulichkeit

Personenbezogene 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 Schäden.

Modul 3: Rechte der betroffenen Personen

3.1 Auskunftsrecht

Betroffene Personen haben das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, und gegebenenfalls weitere Informationen zu erhalten.

3.2 Recht auf Berichtigung

Betroffene Personen haben das Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

3.3 Recht auf Löschung („Recht auf Vergessenwerden“)

Betroffene Personen haben das Recht, die unverzügliche Löschung sie betreffender personenbezogener Daten zu verlangen, sofern bestimmte Gründe vorliegen.

3.4 Recht auf Einschränkung der Verarbeitung

Betroffene Personen haben das Recht, die Einschränkung der Verarbeitung zu verlangen, wenn bestimmte Voraussetzungen erfüllt sind.

3.5 Recht auf Datenübertragbarkeit

Betroffene Personen haben das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

3.6 Widerspruchsrecht

Betroffene Personen haben das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen.

Modul 4: Praktische Umsetzung der DSGVO

4.1 Umgang mit personenbezogenen Daten

- Erheben Sie nur die Daten, die für Ihre Arbeit notwendig sind.
- Speichern Sie Daten sicher und nur so lange wie nötig.
- Geben Sie Daten nur an berechtigte Personen weiter.

4.2 Datenschutz im Arbeitsalltag

- Verwenden Sie sichere Passwörter und ändern Sie diese regelmäßig.
- Verschlüsseln Sie sensible Daten.
- Melden Sie Datenschutzverletzungen unverzüglich an den Datenschutzbeauftragten.

4.3 Sensibilisierung und Schulung

- Nehmen Sie regelmäßig an Datenschutzschulungen teil.
- Informieren Sie sich über aktuelle Entwicklungen im Datenschutzrecht.
- Seien Sie sich der Bedeutung des Datenschutzes bewusst und handeln Sie entsprechend.

Modul 5: Tipps zur Umsetzung der DSGVO

5.1 Datenschutzfreundliche Voreinstellungen

Stellen Sie sicher, dass datenschutzfreundliche Voreinstellungen in allen Systemen und Anwendungen aktiviert sind.

5.2 Datenschutz-Folgenabschätzung

Führen Sie eine Datenschutz-Folgenabschätzung durch, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

5.3 Dokumentation

Dokumentieren Sie alle Verarbeitungstätigkeiten und halten Sie diese Dokumentation stets aktuell.

5.4 Zusammenarbeit mit dem Datenschutzbeauftragten

Arbeiten Sie eng mit dem Datenschutzbeauftragten zusammen und konsultieren Sie ihn bei Fragen oder Unsicherheiten.

Abschluss

Herzlichen Glückwunsch! Sie haben die Selbstlernseinheit über die Grundlagen des Datenschutzrechts nach der DSGVO abgeschlossen. Wir hoffen, dass Sie nun ein besseres Verständnis für die Bedeutung des Datenschutzes haben und in der Lage sind, die Anforderungen der DSGVO in Ihrem Arbeitsalltag umzusetzen.

Bei Fragen oder weiteren Informationen wenden Sie sich bitte an unseren Datenschutzbeauftragten.

Vielen Dank für Ihre Aufmerksamkeit und Ihr Engagement für den Datenschutz!

3.8.2 Bewertung

Die von Mistral Medium 3 generierte Selbstlernseinheit zu den Grundlagen des Datenschutzes folgt einem logisch nachvollziehbaren Aufbau, der von der Einführung über die Grundprinzipien und Rechte der betroffenen Personen bis hin zur praktischen Umsetzung, Tipps und dem Abschluss reicht. Die Sprache ist allgemein verständlich formuliert. Die zu Beginn aufgelisteten Lernziele geben neuen Mitarbeitenden eine klare Orientierung und wirken motivierend. Dennoch bleiben wesentliche didaktische Elemente ungenutzt. Es fehlen durchgehend konkrete Artikelverweise auf die DSGVO. Interaktive Elemente wie Kontrollfragen, Fallbeispiele oder Reflexionsaufgaben sind nicht vorhanden, sodass die Schulung rein informativ bleibt. Ein motivierender Einstieg, etwa über die Frage „Warum betrifft mich das?“, ist nicht vorhanden. Viele Aussagen bleiben allgemein, ohne klare Handlungsanweisungen oder praxisnahe Szenarien. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einführung

Positiv ist der Hinweis, dass sich die Schulung an alle neuen Mitarbeiter richtet, unabhängig von Position oder Aufgabenbereich. Dies senkt die Einstiegshürde, vermeidet Überforderung und kann die Lernmotivation fördern. Die drei Lernziele – Verständnis, Rechte, praktische Umsetzung und Sensibilisierung – sind präzise formuliert und decken zentrale Aspekte der DSGVO ab.

Modul 1: Einführung in die DSGVO

3. KI-generierte Schulungen

Das Datum des Inkrafttretens und der Geltungsbereich in der EU werden richtig genannt. Die Darstellung bleibt jedoch verkürzt. Es fehlt der Hinweis, dass die DSGVO auch dann gilt, wenn eine Organisation ihren Sitz in der EU hat und personenbezogene Daten von Personen außerhalb der EU verarbeitet. Die Aussage, dass die DSGVO den Umgang mit „personenbezogenen Daten“ regelt, ist zwar richtig, zusammen mit den (ebenfalls grundsätzlich richtig) aufgelisteten Zielen der DSGVO wird jedoch nicht deutlich genug, dass es in erster Linie um den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sowie um den freien Verkehr solcher Daten geht (Art. 1 Abs. 1, 2 DSGVO).

Mit den Begriffen „personenbezogene Daten“ (Art. 4 Nr. 1 DSGVO), „Verarbeitung“ (Art. 4 Nr. 2 DSGVO) und „betroffene Person“ werden zwar einige zentrale Begriffe der DSGVO genannt, insbesondere die Definition „personenbezogener Daten“ ist dabei jedoch unvollständig. So enthält die Definition keine Erklärung und Abgrenzungen der Begriffe „identifiziert“ und „identifizierbar“. Sie enthält außerdem weder eine Erläuterung, dass zwischen direkt und indirekt identifizierenden Daten unterschieden wird, noch eine beispielhafte Aufzählung (direkt und indirekt identifizierbarer) personenbezogener Daten. Ebenso wird der Unterschied zu pseudonymen und anonymen Daten nicht erläutert. Die Definition der „betroffenen Person“ entspricht zwar nicht dem Wortlaut des Art. 4 Nr. 1 DSGVO, gibt deren Inhalt jedoch verständlich wieder. Die Definition hätte jedoch um eine kurze Erklärung des Begriffs „natürliche Person“ ergänzt werden können.

Weitere zentrale Begriffe wie „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO), „gemeinsamer Verantwortliche“ (Art. 26 DSGVO) oder „Auftragsverarbeiter“ (Art. 4 Nr. 8 DSGVO) werden teils nicht und teils nur implizit definiert und erläutert. Ebenso fehlt die Definition und Erklärung der „besonderen Kategorien personenbezogener Daten“ (Art. 9 DSGVO). Auch Beispiele und Praxistipps zu typischen Verarbeitungen in einem Unternehmen und zu den personenbezogenen Daten fehlen, um die Theorie greifbarer zu machen.

Modul 2: Grundprinzipien der DSGVO

Die Grundsätze der DSGVO (Art. 5 DSGVO) werden vorliegend als „Grundprinzipien“ bezeichnet, was zwar nicht falsch ist, aber nicht wortlautgetreu ist. Dadurch kann der Eindruck entstehen, dass es sich um etwas anderes als die Grundsätze der Verarbeitung handelt.

Die Grundsätze der DSGVO werden im Kern richtig wiedergegeben. Teilweise sind die Formulierungen jedoch zu unpräzise. So hätte bei dem Grundsatz „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz“ das „Verbot mit Erlaubnisvorbehalt“ sowie die Notwendigkeit einer Rechtsgrundlage (Art. 6 Abs. 1 DSGVO) erwähnt und die einzelnen Rechtsgrundlagen erläutert werden können. Ebenso hätte im Rahmen der Transparenz bereits auf die Informationspflichten (Art. 13, 14 DSGVO) des Verantwortlichen hingewiesen werden können. Die Grundsätze der „Zweckbindung“, „Datenminimierung“ und „Speicherbegrenzung“ sind verständlich und richtig wiedergegeben. Positiv hervorzuheben ist auch, dass bei dem Grundsatz der „Richtigkeit“ darauf hingewiesen wird, dass personenbezogene Daten nur auf dem aktuellen Stand sein müssen, „falls notwendig“. Der Grundsatz der „Integrität und Vertraulichkeit“ wird ebenfalls verständlich und richtig dargestellt. Hier hätte jedoch ergänzt werden können, dass der Grundsatz durch geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO) umzusetzen ist. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO wird nicht erwähnt.

Modul 3: Rechte der betroffenen Personen

Die wesentlichen Betroffenenrechte nach den Art. 15 bis 21 DSGVO werden zwar benannt und grundsätzlich verständlich sowie adressatengerecht erklärt, insgesamt

bleiben die Ausführungen jedoch sehr abstrakt. Insbesondere fehlen Praxisbeispiele sowie Hinweise zur Bearbeitung von Betroffenenanfragen, vor allem der Hinweis, dass derartige Anfragen zunächst an eine intern zuständige Stelle weiterzuleiten sind.

Das „Auskunftsrecht“ (Art. 15 DSGVO) ist zwar sehr knapp und verkürzt, aber dennoch richtig dargestellt. Ergänzt werden könnten hier zumindest beispielhafte Informationen, die im Rahmen der Auskunft herausgegeben werden müssen, sowie die Feststellung, dass auch eine Kopie der personenbezogenen Daten herauszugeben ist. Auch das „Recht auf Berichtigung“ (Art. 16 DSGVO) wird kurz und knapp, aber dennoch richtig dargestellt. Hier könnte jedoch eine Erläuterung ergänzt werden, wann Daten als „unrichtig“ gelten. Beim „Recht auf Löschung“ (Art. 17 DSGVO) wird zwar allgemein Bezug auf die Löschgründe genommen (Abs. 1), es werden jedoch weder Beispiele für entsprechende Gründe genannt noch wird Bezug auf die in Art. 17 Abs. 3 DSGVO normierten Ausnahmen genommen. Ebenso fehlen die Erläuterung und Abgrenzung zum „Recht auf Vergessenwerden“, das zwar mit der Löschung verknüpft ist, aber nicht identisch. Damit bleiben die Ausführungen zum Recht auf Löschung sehr allgemein. Ebenso allgemein bleibt die Darstellung zum „Recht auf Einschränkung der Verarbeitung“ (Art. 18 DSGVO). Es wird weder erläutert, was unter einer Einschränkung der Verarbeitung zu verstehen ist noch werden (beispielhaft) Voraussetzungen hierfür benannt. Auch das „Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO) und das „Widerspruchsrecht“ (Art. 21 DSGVO) werden sehr allgemein und fragmentarisch erklärt, aber dennoch richtig und verständlich.

Völlig unerwähnt bleiben die Informationspflichten nach den Art. 13 und 14 DSGVO sowie die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO). Insbesondere der fehlende Hinweis auf Informationspflichten führt zu einer großen Lücke in den vermittelten Inhalten.

Modul 4: Praktische Umsetzung der DSGVO

Positiv hervorzuheben sind die klaren und leicht verständlichen Grundregeln wie „nur notwendige Daten erheben“ oder „Passwörter sichern“. Diese Hinweise sind praxisnah formuliert und beziehen sich auf typische Alltagssituationen im Büro oder im Homeoffice. Allerdings fehlen hier konkretere Angaben, zum Beispiel, wie ein sicheres Passwort aussehen kann oder was konkret unter „nur notwendigen Daten“ zu verstehen ist. Die Darstellung bleibt insgesamt sehr allgemein, da weder unternehmensspezifische Prozesse noch konkrete Verantwortlichkeiten oder Ansprechpersonen benannt werden. Auch gesetzlich relevante Vorgaben wie die 72-Stunden-Frist (Art. 33 DSGVO) für die Meldung von Datenschutzverletzungen werden nicht erwähnt. Darüber hinaus wird weder beschrieben, wann genau eine Datenschutzverletzung vorliegt, noch wird erläutert, wie eine Risikobewertung in solchen Fällen durchzuführen ist. Erwähnt wird, dass Mitarbeitende dazu angehalten werden, sich über aktuelle Entwicklungen im Datenschutzrecht zu informieren und regelmäßig an Datenschutzschulungen teilzunehmen. Diese Ausführungen sind nicht besonders zielführend, da der Hinweis in der Datenschutzschulung an Datenschutzschulungen teilzunehmen ins Leere läuft und es in organisatorischen Prozessen auch nicht sinnvoll oder praktikabel zu sein scheint, dass jeder Mitarbeiter aktuelle Entwicklungen im Datenschutzrecht beobachtet.

Modul 5: Tipps zur Umsetzung der DSGVO

Positiv hervorzuheben ist, dass im Modul auf zentrale Elemente der DSGVO wie „Privacy by Default“, die Datenschutz-Folgenabschätzung sowie die Dokumentation von Verarbeitungstätigkeiten eingegangen wird. Diese Themen bilden wichtige Grundlagen für eine datenschutzkonforme Arbeitsweise. Die Ausführungen bleiben jedoch sehr allgemein: Es fehlt an rechtlichen Einordnungen, Definitionen bzw. Erläuterungen der verwendeten Begriffe und praxisnahen Beispielen, die das Verständnis erleichtern würden. Zudem werden keine konkreten Abläufe dargestellt, an denen sich die

Mitarbeitenden orientieren könnten. Grundsätzlich positiv hervorzuheben ist die Zusammenarbeit mit dem Datenschutzbeauftragten. In Anbetracht dessen, dass nicht jede Organisation über einen Datenschutzbeauftragten verfügt, bedarf es hier jedoch unter Umständen organisationsspezifischen Anpassungen hinsichtlich des internen Ansprechpartners.

Abschluss

Positiv ist der abschließende Dank an die Mitarbeitenden sowie die Ermutigung zur praktischen Umsetzung der vermittelten Inhalte. Allerdings fehlt eine echte Zusammenfassung oder Wiederholung der wichtigsten Punkte, die das Gelernte noch einmal komprimiert darstellt. Ebenso sind weder ein Selbsttest noch Kontrollfragen vorhanden, mit denen die Mitarbeitenden ihr Verständnis überprüfen könnten. Zudem fehlt die Einbindung von Kontaktdaten zu Ansprechpersonen. Hier hätten Platzhalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten.

Zusammenfassend bietet diese Selbstlerneinheit einen kurzen und gut verständlichen sowie strukturierten Überblick über zentrale Themen der DSGVO. Allerdings werden viele zentrale Begriffe, rechtliche Pflichten und Verfahrenshinweise nicht oder nicht ausreichend erklärt. Es fehlen zentrale Begriffsdefinitionen, etwa von den Begriffen „Verantwortlicher“ oder „Auftragsverarbeiter“. Auch die Rechtsgrundlagen der Verarbeitung nach Art. 6 und Art. 9 DSGVO sowie das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ werden nicht genannt bzw. erläutert. Weitere wichtige Punkte wie die Anforderungen an die Einwilligung nach Art. 7 DSGVO, das Bestehen von Informationspflichten (Art. 13, 14 DSGVO), Erläuterungen im Zusammenhang mit technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) sowie Informationen zur Meldung von Datenschutzverletzungen inklusive Fristen und Risikobewertung nach Art. 33 und 34 DSGVO bleiben unerwähnt. Ebenso fehlt eine Klarstellung, dass eine Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) besteht und hierfür insbesondere auch ein Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) geführt werden muss. Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. Darüber hinaus fehlen praxisnahe Elemente wie Beispiele, Checklisten oder Arbeitsabläufe sowie interaktive Bestandteile wie Fragen, Reflexionen oder Fallbeispiele. Die Schulung ist daher weder juristisch vollständig noch didaktisch ausgereift. Die Formulierungen sind teils zu unpräzise, um verlässliches Wissen für die praktische Umsetzung der DSGVO zu vermitteln. Ohne Beispiele und praxisnahe Handlungsschritte bleibt die Umsetzung im Arbeitsalltag unklar. Die Einheit ist als vollständige DSGVO-Schulung unzureichend.

3.9 Qwen 3-235B-A22B-2507 (Alibaba DAMO Academy, Anwendung: Qwen Chat)

3.9.1 KI-generierter Inhalt²⁹

Selbstlerneinheit: Grundlagen des Datenschutzrechts nach der DSGVO für neue Mitarbeiter

Willkommen!

Herzlich willkommen in Ihrer neuen Arbeitsstelle!

Als neuer Mitarbeiter sind Sie Teil eines Teams, das verantwortungsbewusst mit personenbezogenen Daten umgeht. Um diese Verantwortung zu erfüllen, ist es wichtig,

²⁹ Der in diesem Unterkapitel abgedruckte Text wurde vollständig durch das Modell Qwen 3-235B-A22B-2507 über Qwen-Chat generiert.

die Grundlagen des Datenschutzrechts zu verstehen – insbesondere **der Datenschutz-Grundverordnung (DSGVO)**, die in Ihrer Organisation vollständig gilt.

Diese Selbstlerneinheit bietet Ihnen einen praxisnahen Einstieg in die wichtigsten Regelungen der DSGVO. Sie ist für alle neuen Mitarbeiter gleich aufgebaut – unabhängig von Ihrer Position, Ihrem Alter oder Ihrer Vorbildung. Ziel ist es, dass Sie am Ende wissen:

- Was personenbezogene Daten sind,
- welche Rechte betroffene Personen haben,
- welche Pflichten Sie als Mitarbeiter haben,
- und wie Sie im Alltag datenschutzkonform handeln.

Die Einheit dauert etwa **30–45 Minuten**. Am Ende finden Sie eine kurze Wissensüberprüfung, um Ihr Verständnis zu überprüfen.

1. Was ist die DSGVO?

Die **Datenschutz-Grundverordnung (DSGVO)** ist eine europäische Rechtsvorschrift, die seit dem 25. Mai 2018 in allen EU-Mitgliedstaaten gilt. Sie regelt den Umgang mit personenbezogenen Daten und schützt die Privatsphäre von Menschen.

Die DSGVO gilt für alle Organisationen – unabhängig von Größe oder Branche –, die personenbezogene Daten verarbeiten. Das gilt auch für Ihre neue Arbeitsstelle.

⌚ Merke: Die DSGVO ist kein „Papierkrieg“, sondern ein Schutzrecht für Menschen. Jeder Mitarbeiter trägt mit seinem Handeln dazu bei, dass dieser Schutz gewährleistet bleibt.

2. Was sind personenbezogene Daten?

Personenbezogene Daten sind **jegliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen**.

Das klingt abstrakt – deshalb hier Beispiele:

Sind personenbezogene Daten:

- Name, Vorname
- E-Mail-Adresse (z. B. max.mustermann@firma.de)
- Telefonnummer
- Adresse
- Geburtsdatum
- Mitarbeiter-ID
- IP-Adresse (bei bestimmten Kontexten)
- Fotos mit erkennbarem Gesicht
- Bankverbindung
- Gesundheitsdaten (z. B. Krankenmeldungen)

Sind keine personenbezogenen Daten:

- Aggregierte, anonymisierte Daten (z. B. „Im Jahr 2024 nutzten 3000 Kunden unseren Service“)
- Daten über juristische Personen (z. B. „Firma XYZ hat einen Vertrag abgeschlossen“)
- Komplett anonymisierte Daten, bei denen kein Rückschluss auf eine Person möglich ist

⌚ Praxistipp: Wenn Sie unsicher sind, ob eine Information personenbezogen ist – gehen Sie davon aus, dass sie es ist. Sicherheit geht vor.

3. Wer ist betroffen? – Die wichtigsten Akteure

In der DSGVO gibt es drei zentrale Begriffe:

1. Betroffene Person

Die Person, auf die sich die Daten beziehen.

Beispiel: Ein Kunde, ein Bewerber, ein Mitarbeiter.

2. Verantwortlicher

Die Organisation (oder Person), die entscheidet, **warum** und **wie** personenbezogene Daten verarbeitet werden.

→ In Ihrer Organisation ist das **Ihre Firma**.

3. Auftragsverarbeiter

Ein externer Dienstleister, der Daten im Auftrag des Verantwortlichen verarbeitet.

Beispiel: Ein IT-Dienstleister, der Ihre E-Mails hostet.

❖ Ihre Rolle: Sie sind kein Verantwortlicher, sondern Mitarbeiter im Auftrag des Verantwortlichen. Sie verarbeiten Daten im Rahmen Ihrer Tätigkeit – und müssen dabei stets die DSGVO beachten.

4. Die wichtigsten Prinzipien der DSGVO

Die DSGVO basiert auf sieben zentralen Grundsätzen. Diese gelten immer, wenn personenbezogene Daten verarbeitet werden.

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Daten dürfen nur verarbeitet werden, wenn ein **rechtmäßiger Grund** vorliegt (z. B. Einwilligung, Vertragserfüllung, gesetzliche Pflicht). Die betroffene Person muss wissen, was mit ihren Daten passiert.

❖ Beispiel: Ein Kunde gibt seine Adresse für die Lieferung an – das ist vertraglich notwendig.

2. Zweckbindung

Daten dürfen **nur für den ursprünglich festgelegten Zweck** verwendet werden.

❖ Beispiel: Eine E-Mail-Adresse, die für die Rechnungsstellung genutzt wird, darf nicht ohne Zustimmung für Werbung verwendet werden.

3. Datenminimierung

Es dürfen **nur die Daten erhoben werden, die tatsächlich benötigt werden**.

❖ Beispiel: Für eine Bewerbung brauchen Sie Lebenslauf und Zeugnisse – aber nicht das Lieblingssessen des Bewerbers.

4. Richtigkeit

Daten müssen **richtig und aktuell** sein. Fehler müssen berichtigt werden.

❖ Beispiel: Ein Kunde meldet eine neue Adresse – diese muss in Ihrem System aktualisiert werden.

5. Speicherbegrenzung

Daten dürfen **nicht länger als nötig** gespeichert werden.

❖ Beispiel: Bewerbungsunterlagen dürfen nach 6 Monaten gelöscht werden, wenn keine Einwilligung zur längeren Speicherung vorliegt.

6. Integrität und Vertraulichkeit (Sicherheit)

Daten müssen **sicher** vor Verlust, Missbrauch oder unberechtigtem Zugriff geschützt werden.

❖ Beispiel: Passwörter nicht auf Zetteln am Monitor kleben, Laptops verschlüsseln, E-Mails mit sensiblen Daten verschlüsseln.

7. Nachweisbarkeit (Accountability)

Die Organisation muss **nachweisen können**, dass sie die DSGVO einhält.

❖ Beispiel: Dokumentation von Löschfristen, Schulungen, technischen Maßnahmen.

5. Rechte der betroffenen Personen

Betroffene Personen haben **starke Rechte** – auch gegenüber Ihrer Organisation.

Als Mitarbeiter sollten Sie diese kennen und respektieren:

Auskunftsrecht	Die Person darf verlangen, welche Daten über sie gespeichert sind.
Recht auf Berichtigung	Falsche Daten müssen korrigiert werden.

Recht auf Löschung ("Recht auf Vergessenwerden")	Unter bestimmten Bedingungen können Daten gelöscht werden.
Recht auf Einschränkung der Verarbeitung	Die Person kann verlangen, dass ihre Daten vorübergehend nicht verarbeitet werden.
Recht auf Datenübertragbarkeit	Die Person kann ihre Daten in einem gängigen Format erhalten, um sie zu einem anderen Anbieter zu übertragen.
Widerspruchsrecht	Die Person kann gegen die Verarbeitung ihrer Daten widersprechen (z. B. bei Direktwerbung).
Recht auf Beschwerde	Bei Verstößen kann die Person sich bei einer Aufsichtsbehörde beschweren.

 Praxistipp: Wenn eine betroffene Person eines dieser Rechte geltend macht, leiten Sie die Anfrage sofort an die zuständige Stelle in Ihrer Organisation weiter (z. B. Datenschutzbeauftragten oder HR). Handeln Sie nicht eigenmächtig!

6. Ihre Pflichten als Mitarbeiter

Sie sind kein Datenschutzexperte – aber Sie tragen Mitverantwortung für den datenschutzkonformen Umgang mit Daten.

 **Was Sie tun sollten:**

- **Nur erforderliche Daten erfassen** – nicht „zusätzlich mal eben“.
- **Daten verschlüsselt und sicher speichern** – z. B. auf verschlüsselten Festplatten oder im firmeneigenen Cloud-System.
- **Passwörter sicher verwalten** – kein Teilen, keine Notizen an sichtbaren Stellen.
- **Daten nur an berechtigte Personen weitergeben** – nie an Kollegen, die nichts damit zu tun haben.
- **E-Mails mit sensiblen Daten verschlüsseln** – besonders bei externen Empfängern.
- **Geräte sichern** – Laptop schließen, wenn Sie den Arbeitsplatz verlassen.
- **Verdachtsfälle melden** – z. B. verlorener USB-Stick mit Kundendaten → sofort melden!

 **Was Sie nicht tun sollten:**

- Daten auf privaten Geräten speichern (Handy, Privat-PC).
- Screenshot von Kundendaten machen und per WhatsApp versenden.
- Kundendaten an Freunde oder Familie weitergeben – auch aus „Hilfsbereitschaft“.
- Daten länger speichern als vorgesehen – auch „zur Sicherheit“.

 Leitregel: Wenn Sie unsicher sind – fragen Sie nach! Sprechen Sie mit Ihrem Vorgesetzten oder dem Datenschutzbeauftragten.

7. Typische Praxisbeispiele

Hier einige Situationen aus dem Arbeitsalltag – und wie Sie datenschutzkonform reagieren:

 **Beispiel 1: E-Mail mit Kundendaten**

Sie sollen eine Rechnung an einen Kunden schicken. Die Rechnung enthält Name, Adresse und Rechnungsbetrag.

 **Richtig:** E-Mail verschlüsseln, wenn vorgesehen. Nur an die richtige E-Mail-Adresse senden. Keine CC an Kollegen, die nicht beteiligt sind.

 **Beispiel 2: Laptop im Homeoffice**

3. KI-generierte Schulungen

Sie arbeiten von zu Hause. Auf Ihrem Laptop sind Kundendaten gespeichert.

→ **Richtig:** Laptop verschlüsselt, Passwort geschützt, keine Dritten dürfen Zugriff haben.

Keine Daten auf USB-Sticks kopieren.

→ **Beispiel 3: Kollege bittet um Hilfe**

Ein Kollege fragt: „Kannst du mir mal eben die Adresse von Herrn Müller aus der Kundenliste geben? Ich möchte ihn anrufen.“

→ **Richtig:** Nur wenn der Kollege berechtigt ist, darf er die Daten erhalten. Ansonsten:
„Tut mir leid, ich darf dir das nicht geben. Frag bitte den zuständigen Mitarbeiter.“

8. Was passiert bei Verstößen?

Verstöße gegen die DSGVO können **ernste Folgen** haben:

- **Bußgelder** bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes.
- **Imageverlust** für die Organisation.
- **Persönliche Konsequenzen** für Mitarbeiter, wenn vorsätzlich oder grob fahrlässig gehandelt wurde.

⚠ Wichtig: Auch unbeabsichtigte Verstöße (z. B. versehentliche Weitergabe per E-Mail) können sanktioniert werden. Deshalb: Vorsicht und Sorgfalt sind Pflicht.

9. Zusammenfassung: Die 5 wichtigsten Regeln für Sie

1. **Nur erforderliche Daten erfassen und verarbeiten.**
2. **Daten sicher speichern und schützen.**
3. **Keine Weitergabe an unberechtigte Personen.**
4. **Bei Fragen oder Unsicherheit: Nachfragen – lieber einmal zu oft als einmal zu wenig.**
5. **Verdachtsfälle sofort melden.**

10. Wissensüberprüfung

Beantworten Sie die folgenden Fragen, um Ihr Verständnis zu testen:

1. Welche der folgenden Informationen sind personenbezogene Daten?
 - a) Die Anzahl der Kunden im Jahr 2024
 - b) Die E-Mail-Adresse „sarah.meier@kunde.de“
 - c) Die IP-Adresse eines Website-Besuchers
 - d) Der Name „Max Mustermann“

→ **Lösung:** b, c, d
2. Was bedeutet „Zweckbindung“?
 - a) Daten dürfen für beliebige Zwecke verwendet werden.
 - b) Daten dürfen nur für den ursprünglich festgelegten Zweck verwendet werden.
 - c) Daten müssen immer an Dritte weitergegeben werden.

→ **Lösung:** b
3. Welche Maßnahme schützt personenbezogene Daten am besten?
 - a) Passwort auf einem Zettel am Bildschirm
 - b) Verschlüsselter Laptop mit Login-Schutz
 - c) Speicherung auf einem privaten USB-Stick

→ **Lösung:** b
4. Ein Kunde bittet darum, seine Daten zu löschen. Was tun Sie?
 - a) Löschen Sie die Daten sofort aus Ihrem System.
 - b) Leiten Sie die Anfrage an den Datenschutzbeauftragten weiter.
 - c) Ignorieren Sie die Anfrage, da sie nicht schriftlich ist.

→ **Lösung:** b
5. Warum ist die DSGVO wichtig?
 - a) Weil sie Unternehmen mehr Daten sammeln lässt

- b) Weil sie die Privatsphäre von Menschen schützt
 - c) Weil sie nur für Behörden gilt
- **Lösung:** b

11. Kontakt & Unterstützung

Fragen zum Datenschutz?

Sie sind nicht allein!

In Ihrer Organisation ist folgende Stelle für Datenschutz zuständig:

 **Datenschutzbeauftragter:**

Name: [Name des Datenschutzbeauftragten]

E-Mail: datenschutz@ihrefirma.de

Telefon: [interne Durchwahl]

Sie können sich jederzeit an diese Person wenden – auch bei kleineren Unsicherheiten.

Abschluss

Herzlichen Glückwunsch! Sie haben die Selbstlernseinheit erfolgreich abgeschlossen.

Sie wissen nun, was die DSGVO ist, wie sie im Alltag wirkt und welche Rolle Sie dabei spielen.

Denken Sie daran:

Datenschutz ist Teamarbeit.

Jeder Mitarbeiter trägt dazu bei, dass personenbezogene Daten sicher und rechtmäßig verarbeitet werden.

 **Bestätigen Sie bitte den Abschluss dieser Schulung über das interne System oder an Ihre HR-Abteilung.**

Vielen Dank für Ihre Aufmerksamkeit – und willkommen im Team!

Diese Einheit basiert auf der Datenschutz-Grundverordnung (DSGVO) in der aktuellen Fassung. Stand: April 2025.

3.9.2 Bewertung

Die von Qwen 3 erstellte Grundlagenschulung zum Datenschutz überzeugt durch einen sehr gelungenen Aufbau, der nahezu alle zentralen DSGVO-Themen abdeckt. Die klare Struktur – Einführung, Definitionen, Beispiele, Praxistipps – erleichtert die Navigation. Positiv fällt auch die grobe Zeitangabe von 30–45 Minuten auf, die realistisch ist, Orientierung gibt und die Balance hält, indem sie einerseits nicht zu lang (keine Ermüdung) und andererseits nicht zu kurz ist (ausreichend für die Grundlagenvermittlung). Die adressatengerechte Sprache ist für Einsteiger ohne juristische Vorkenntnisse leicht verständlich und spricht neue Mitarbeitende direkt an, was Verantwortungs- und Pflichtbewusstsein stärkt. Der Praxisbezug ist hoch. Zahlreiche alltagsrelevante Beispiele erleichtern den Transfer ins Arbeitsleben. Auch die visuelle Gestaltung unterstützt das Lernen: Fettschrift für Schlagworte fördert die schnelle Erfassung, eine helle graue Absetzung hebt Beispiele vom Fließtext ab, und Icons erhöhen die Lesefreundlichkeit. Die Tabellenform bei den Betroffenenrechten sorgt für zusätzliche Übersichtlichkeit. Die Schulung enthält jedoch auch einige Ungenauigkeiten. Für ein wirkliches Verständnis der Schulungsinhalte bedarf es einer eigenständigen Nachbearbeitung, ohne dass die Schulung dies klar kommuniziert.

Einleitung

Die freundliche Begrüßung („Herzlich willkommen“) schafft eine positive Lernatmosphäre. Die Einbettung in den Arbeitskontext („Teil eines Teams, das

3. KI-generierte Schulungen

verantwortungsbewusst mit Daten umgeht“) motiviert und zeigt die Relevanz der DSGVO in der Organisation. Positiv zu erwähnen ist der Hinweis, dass die Einheit für alle neuen Mitarbeitern konzipiert ist – unabhängig von Position, Alter oder Vorbildung – was die Einstiegshürde senkt. Die vier Ziele der Schulung sind konkret und verständlich formuliert, sprechen Mitarbeiter direkt an („was Sie wissen“, „welche Pflichten Sie haben“) und machen klar: „Das betrifft mich direkt“. Das steigert die Aufmerksamkeit und Lernbereitschaft der Mitarbeitenden. Die erwähnten Lernziele geben Orientierung und unterstützen die Reflexion des Lernfortschritts. Die angekündigte Wissensüberprüfung motiviert zur aktiven Auseinandersetzung mit den gelernten Themen und fördert die Selbstreflexion der Mitarbeitenden.

1. Was ist die DSGVO?

Die zeitliche Einordnung (seit 25. Mai 2018, Geltung in allen EU-Mitgliedstaaten) und der Hinweis auf die Geltung der DSGVO für alle Organisationen unabhängig von Größe/Branche ist richtig. Es fehlt der Hinweis, dass die DSGVO auch dann gilt, wenn eine Organisation ihren Sitz in der EU hat und personenbezogene Daten von Personen außerhalb der EU verarbeite. Positiv fällt auch die motivierende Einordnung („kein Papierkrieg, sondern Schutzrecht für Menschen“) auf. Kritisch zu sehen ist dagegen die Aussage, die DSGVO „schützt die Privatsphäre“, da dies zu eng gefasst ist. Angelehnt an Art. 1 Abs. 2 DSGVO wäre präziser: „Die DSGVO schützt die Rechte und Freiheiten natürlicher Personen“.

2. Was sind personenbezogene Daten?

Positiv fällt auf, dass die Definition weitgehend Art. 4 Nr. 1 DSGVO entspricht, die Beispiele praxisnah sind und typische Datenarten abdecken. Die Gegenüberstellung personenbezogener vs. nicht-personenbezogener Daten macht die Abgrenzung für die Mitarbeitenden greifbar. Der Praxistipp „Im Zweifel davon ausgehen, dass es personenbezogene Daten sind“ ist hilfreich und fördert vorsichtiges, verantwortungsbewusstes Verhalten.

Kritisch anzumerken ist, dass die Schulung die Definition der „natürlichen Person“ sowie die Unterscheidung zwischen „identifiziert“ und „identifizierbar“ nicht erläutert. Auch die Differenzierung zwischen direkter und indirekter Identifikation wird nicht erklärt, obwohl sie für das Verständnis der Verarbeitung personenbezogener Daten zentral ist. Darüber hinaus fehlt eine Abgrenzung zu pseudonymen und anonymen Daten. Diese Begriffe sind insbesondere nötig, um zu verstehen, warum anonyme Daten – so wie explizit erwähnt – keine personenbezogenen Daten sind. Negativ fällt auch auf, dass Gesundheitsdaten zwar genannt werden, es jedoch an einer Definition und Erläuterung der besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) fehlt, sodass der besondere Schutzzweck für die Mitarbeitenden nicht nachvollziehbar wird.

3. Wer ist betroffen? – Die wichtigsten Akteure

Positiv hervorzuheben ist, dass die Begriffe „betroffene Person“, „Verantwortlicher“ (Art. 4 Nr. 7 DSGVO) und „Auftragsverarbeiter“ (Art. 4 Nr. 8 DSGVO) genannt und kurz mit praxisnahen Beispielen erläutert werden. Der Hinweis auf die eigene Rolle („Sie sind kein Verantwortlicher, sondern Mitarbeiter im Auftrag des Verantwortlichen.“) ist zwar grundsätzlich gut platziert, die Formulierung „im Auftrag des Verantwortlichen“ könnte jedoch aufgrund des gleichen Wortlauts im Zusammenhang mit der Erklärung des Auftragsverarbeiters zu Missverständnissen führen.

Die Definition der „betroffenen Person“ entspricht zwar nicht dem genauen Wortlaut von Art. 4 Nr. 1 DSGVO („identifizierte oder identifizierbare natürliche Person“), ist für juristische Laien jedoch verständlicher und greifbarer. Kritisch ist hierbei jedoch, dass die Definition nicht von „personenbezogenen Daten“, die sich auf die Person beziehen, spricht, sondern lediglich von „Daten“. Dies könnte insoweit zu Missverständnissen

führen als der Eindruck entstehen könnte, dass es sich z. B. auch um betroffene Personen handelt, wenn es um anonymisierte Daten geht. Auch die Definition des „Verantwortlichen“ weicht vom Wortlaut der DSGVO ab, dürfte dadurch aber für datenschutzrechtliche Laien verständlicher sein. Klargestellt werden könnte jedoch, dass auch mehrere gemeinsam verantwortlich (Art. 26 DSGVO) sein können – insbesondere zur Abgrenzung vom Auftragsverarbeiter. Dessen Erläuterung ist grundsätzlich richtig und durch das Praxisbeispiel gut verständlich, könnte aber durch Hinweise auf weitere zentrale Elemente des Auftragsverhältnisses (Art. 28 DSGVO) ergänzt werden, insbesondere die Weisungsgebundenheit des Auftragsverarbeiters.

4. Die wichtigsten Prinzipien der DSGVO

Im Zusammenhang mit den Grundsätzen der Verarbeitung (Art. 5 DSGVO) ist positiv anzumerken, dass die sieben Grundsätze der DSGVO in verständlicher Sprache erläutert und vollständig in der Reihenfolge ihres Auftretens in der Verordnung dargestellt werden. Ergänzt werden sie durch alltagsnahe Beispiele, die den Mitarbeitenden die praktische Umsetzung jedes Grundsatzes greifbar machen. Positiv fällt auch auf, dass bei dem Grundsatz der „Rechtmäßigkeit, Treu und Glauben, Transparenz“ die Erforderlichkeit einer Rechtsgrundlage angesprochen wird und Beispiel-Rechtsgrundlagen genannt werden. Jedoch wird das grundlegende Prinzip des „Verbots mit Erlaubnisvorbehalt“ hier nicht erläutert, wobei positiv zu vermerken ist, dass aus der Formulierung „Daten dürfen nur verarbeitet werden, wenn ein rechtmäßiger Grund vorliegt“ zumindest indirekt deutlich wird, dass es einer Rechtsgrundlage für die Verarbeitung bedarf. Ebenso werden die Rechtsgrundlagen nicht vollständig aufgezählt oder erläutert. Darüber hinaus fehlen praxisnahe Beispiele, etwa wann das berechtigte Interesse oder die Einwilligung relevant sein könnte. Positiv hervorzuheben ist, dass der (Teil-)Grundsatz der Transparenz erläutert wird.

Negativ fällt dagegen auf, dass die Grundsätze insgesamt zu knapp beschrieben sind, die Wortwahl teils unpräzise ist und direkte Gesetzesbezüge fehlen. Der Grundsatz der „Zweckbindung“ wird zu eng formuliert („nur für den ursprünglich festgelegten Zweck“), obwohl eine Weiterverarbeitung unter bestimmten Voraussetzungen möglich sein kann, sofern sie dem ursprünglichen Zweck vereinbar ist (Art. 6 Abs. 4 DSGVO). Die Grundsätze der „Datenminimierung“ und der „Speicherbegrenzung“ werden zwar etwas verkürzt dargestellt, vermitteln den Kern der Grundsätze aber dennoch verständlich und präzise. Das im Zusammenhang mit dem Grundsatz der „Speicherbegrenzung“ genannte Beispiel ist jedoch zu weich formuliert („Bewerbungsunterlagen dürfen nach 6 Monaten gelöscht werden“) und könnte dadurch zu Missverständnissen führen. Besser wäre hier die Formulierung „müssen“ oder „sollten“. Der Grundsatz der „Richtigkeit“ wird leicht verkürzt dargestellt. Es fehlt der Zusatz, dass Daten lediglich „erforderlichenfalls“ aktuell sein müssen. Die Erläuterung des Grundsatzes der „Integrität und Vertraulichkeit“ bleibt zu knapp, insbesondere wird nicht hinreichend klargestellt, dass grundsätzlich die Sicherheit der personenbezogenen Daten gewährleistet werden soll und nicht nur vor „Verlust, Missbrauch oder unberechtigtem Zugriff“, sondern etwa auch vor unbeabsichtigter Zerstörung oder Schädigung geschützt werden soll. Zudem wird hier kein Bezug zu den technischen und organisatorischen Maßnahmen hergestellt. Die „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO) wird zwar genannt, aber fälschlicherweise als „Nachweisbarkeit“ bezeichnet. Um Verwirrung oder Interpretationsspielraum zu vermeiden, wäre es sinnvoller den Wortlaut der DSGVO zu nutzen.

5. Rechte der betroffenen Personen

Positiv hervorzuheben ist, dass die wesentlichen Rechte der betroffenen Personen nach Art. 15–21 DSGVO benannt werden, darunter „Auskunft“ (Art. 15 DSGVO), „Berichtigung“ (Art. 16 DSGVO), „Lösung“ (Art. 17 DSGVO) einschließlich des „Rechts auf Vergessenwerden“, „Einschränkung“ (Art. 18 DSGVO), „Datenübertragbarkeit“ (Art. 20 DSGVO), „Widerspruch“ (Art. 21 DSGVO) und „Beschwerde“. Die Darstellung ist

verständlich und adressatengerecht, und der Hinweis, Anfragen an die zuständige Stelle weiterzuleiten, statt eigenständig zu handeln, ist zielführend und i. d. R. im Sinne der Organisationen.

Kritisch bleibt jedoch das Fehlen der Informationspflichten nach Art. 13 und 14 DSGVO. Insgesamt bleibt die Darstellung zu oberflächlich, was potenziell Praxisfehler begünstigt. So werden zentrale Details nicht behandelt: Beim „Auskunftsrecht“ fehlt eine Klarstellung, dass die betroffene Person nicht nur erfahren darf, welche Daten über sie gespeichert werden, sondern auch eine Reihe von Informationen über deren Verarbeitung (etwa zu Zwecken, Datenkategorien, Empfängern, Speicherdauer, Herkunft, Beschwerderecht und automatisierten Entscheidungen). Beim „Recht auf Berichtigung“ wird nicht erklärt, wann Daten als „unrichtig“ gelten. Bei der „Lösung“ wird zwar kurz und knapp erwähnt, dass die Lösung an bestimmte Bedingungen geknüpft ist, die Formulierung „können gelöscht werden“ macht jedoch weder deutlich, dass die betroffene Person verlangen kann, dass ihre Daten gelöscht werden, noch dass eine Pflicht besteht die Daten zu löschen, wenn diese bestimmten Bedingungen erfüllt sind. Zudem fehlt die Abgrenzung zum (ausdrücklich erwähnten) „Recht auf Vergessenwerden“ nach Abs. 2. Beim „Recht auf Einschränkung“ fehlt ein Hinweis darauf, dass die Einschränkung nur unter bestimmten Voraussetzungen erfolgen muss, etwa bei Bestreiten der Richtigkeit, unrechtmäßiger Verarbeitung oder zur Geltendmachung bzw. Verteidigung von Rechtsansprüchen. Ergänzend fehlen Verfahrenshinweise einschließlich der einmonatigen Frist nach Art. 12 Abs. 3 DSGVO, Hinweise auf Dokumentationspflichten sowie praxisnahe Beispiele zur Erkennung echter Anfragen.

6. Ihre Pflichten als Mitarbeiter

Sehr gelungen sind die Botschaften „Sie sind kein Datenschutzexperte – aber Sie tragen Mitverantwortung“, die klaren Do-/Don't-Listen mit konkreten Handlungsanweisungen, die Hinweise zur Meldung von Vorfällen („Verdachtsfälle melden“) sowie die Sicherheitshinweise, etwa zur Verschlüsselung oder zum Passwortschutz. Die Handlungsempfehlungen sind ansprechend formuliert und praxisnah. Die Beispiele greifen typische Alltagssituationen auf (Laptop, USB-Stick, E-Mail), was die Anwendbarkeit erhöht. Problematisch ist, dass die Handlungsanweisungen teilweise auf technische Infrastrukturen Bezug nehmen (z. B. verschlüsselte Festplatten, firmeneigenes Cloud-System, verschlüsselte E-Mails), die nicht zwingend in jeder Organisation verfügbar sind. Zudem hätten die Handlungsanweisungen stellenweise präziser sein können. Beispielsweise hätte der Hinweis „Geräte sichern“ durch die Empfehlung ergänzt werden können, eine automatische Bildschirmsperre nach Inaktivität einzurichten. Des Weiteren wäre der Hinweis „Verdachtsfälle melden“ deutlich besser einzuordnen und datenschutzkonform umzusetzen, wenn die Schulung auch auf Datenschutzverletzungen und deren Meldepflichten nach Art. 33, 34 DSGVO eingehen würde. Dies versäumt die Schulung, was dazu führen könnte, dass Mitarbeitende nicht einordnen können, was mit Verdachtsfällen gemeint ist, wann eine Meldepflicht besteht und an wen zu melden ist. Es fehlt die Definition, ab welcher Risikoschwelle eine Datenpanne meldepflichtig ist – Art. 33. Auch fehlt der Hinweis auf die 72-Stunden-Frist, innerhalb derer die Organisation an die Aufsichtsbehörde melden muss. Ebenso fehlt die Klarstellung, dass die interne Meldung an eine zuständige Stelle (z. B. Datenschutzbeauftragter, Geschäftsführung) erfolgen soll, die dann die Risikobewertung und gegebenenfalls die externe Meldung vornimmt. Ohne diese Informationen besteht die Gefahr, dass Verdachtsfälle nicht rechtzeitig, unvollständig oder gar nicht gemeldet werden. Die Leitregel „Wenn Sie unsicher sind – fragen Sie nach!“ unterstützt eine offene Unternehmenskultur und fördert die aktive Auseinandersetzung der Mitarbeitenden mit datenschutzrelevanten Fragestellungen. Der Verweis auf den Datenschutzbeauftragten wird jedoch nicht zu jeder Organisation passen, einerseits, weil nicht jede Organisation dazu verpflichtet ist, einen Datenschutzbeauftragten zu benennen, andererseits, weil die organisationsinterne

Umsetzung des Datenschutzes in manchen Organisationen anders organisiert sein wird (so dass z. B. der Datenschutzkoordinator oder die Datenschutz-Ansprechperson bei der Umsetzung von Betroffenenrechten unterstützt und nicht der Datenschutzbeauftragte).

7. Typische Praxisbeispiele

Die Reaktionsweisen sind richtig und datenschutzkonform, die Fallauswahl (E-Mail, Homeoffice, Kollegenanfrage) ist realitätsnah und zeitgemäß (inkl. Remote-Arbeit). Jede Situation enthält klare, gut umsetzbare Hinweise, macht typische Fehler sichtbar und adressiert diese präventiv. Sowohl technische als auch organisatorische Regeln werden angesprochen. Präzisierungspotenzial besteht bei der Formulierung „Laptop verschlüsseln“. Gemeint sein könnte die Festplattenverschlüsselung des Geräts, welche jedoch i. d. R. nicht durch einzelne Mitarbeiter, sondern durch die Organisation umgesetzt wird. Gemeint könnte außerdem sein, dass der Zugriff auf den Account auf dem Laptop durch ein Passwort geschützt wird; in diesem Fall sollte die Formulierung präzisiert und durch einen konkreten Hinweis hinsichtlich sicherer Passwörter ergänzt werden. Ebenso denkbar ist, dass eine Verschlüsselung der Daten selbst gemeint ist, wozu allerdings konkrete Hinweise zur praktischen Umsetzung fehlen.

8. Was passiert bei Verstößen?

Richtig dargestellt sind die möglichen Folgen bei Verstößen: Bußgelder, Imageverlust und persönliche Konsequenzen. Die konkreten Summen (bis 20 Mio. € oder 4 % des Umsatzes) verdeutlichen die Tragweite und appellieren an das eigene Pflicht- und Verantwortungsbewusstsein. Besonders positiv ist der Hinweis auf persönliche Konsequenzen bei vorsätzlichem oder grob fahrlässigem Handeln im Rahmen des innerbetrieblichen Schadensausgleich (leichte Fahrlässigkeit: keine Haftung, mittlere Fahrlässigkeit: anteilige Haftung, grobe Fahrlässigkeit oder Vorsatz: grundsätzlich volle Haftung)³⁰. Ebenso wichtig ist die Erwähnung der Sanktionierbarkeit unbeabsichtigter Verstöße: Auch fahrlässiges oder unbeabsichtigtes Verhalten kann sanktioniert werden, da die DSGVO keine klassische Schuldfrage voraussetzt.

9.-11. Zusammenfassung, Wissensüberprüfung, Kontakt, Abschluss

Die fünf klaren Regeln dienen als eingängige Merkhilfe (Datensparsamkeit, Sicherheit, Weitergabekontrolle, Meldepflicht, Rückfragen). Besonders positiv ist, dass der Hinweis, bei Unsicherheiten lieber nachzufragen, die Zurückhaltung reduziert und eigenverantwortliches Handeln fördert. Der Selbsttest motiviert zur Wiederholung und vertieft das Wissen. Die Fragen sind gut gewählt, da sie die Theorie effektiv wiederholen. Die Kontaktdata des Datenschutzbeauftragten sind sinnvoll platziert und leicht auffindbar, setzt jedoch voraus, dass die Organisation, die die Schulung einsetzen möchte, über einen Datenschutzbeauftragten verfügt. Hier hätten Platthalter eine gute Möglichkeit zur einfachen Anpassung an die Organisation geboten. Der Satz „Sie sind nicht allein!“ signalisiert Verfügbarkeit von Hilfe und baut Vertrauen auf. Zusätzliche positive Akzente setzen Formulierungen wie „Herzlichen Glückwunsch!“ und „Willkommen im Team!“, die ein positives Gefühl erzeugen und zur Umsetzung motivieren. Die Bitte, den Abschluss zu bestätigen, erhöht die Verbindlichkeit, dokumentiert die Teilnahme und unterstützt die Rechenschafts- und Dokumentationspflichten des Verantwortlichen.

Kritisch bleibt jedoch, dass die fünf Regeln zu allgemein gehalten sind („Daten sicher speichern und schützen“, „nur erforderliche Daten erfassen“) und konkrete technische Maßnahmen (z. B. Verschlüsselung, Zugriffsbeschränkung) fehlen. Auch der Hinweis „Verdachtsfälle sofort melden“ ist ohne Angabe eines Adressaten unvollständig. Zudem ist er mangels theoretischen Fundaments hinsichtlich dessen, was Verdachtsfälle sind und welche Meldepflichten und -fristen hierbei gelten, ist fehleranfällig. Hinweise auf die

³⁰ Baumgärtner, in: BeckOK BGB, § 611a Rdnr. 97.

4. Gegenüberstellung der Schulungen

regelmäßige Überprüfung und Aktualisierung der Prozesse fehlen. Zudem ist im Selbsttest erneut die Definition der Zweckbindung zu eng gefasst („nur für ursprünglich festgelegte Zwecke“).

Zusammenfassend ist die Schulung in vielerlei Hinsicht überzeugend. Besonders positiv sind die Übersichtlichkeit und Struktur, die optische Aufbereitung mit Fettschrift, farblicher Absetzung und Icons sowie die Vielzahl praxisnaher Beispiele und adressatengerechter Formulierungen. Die Schulung ist optisch und didaktisch sehr gelungen und vermittelt neuen Mitarbeitenden ohne Datenschutzvorwissen grundlegendes datenschutzrechtliches Wissen auf motivierende, klar strukturierte und praxisnahe Weise. Allerdings weist die Schulung punktuelle Ungenauigkeiten und Lücken auf. Insbesondere fehlt eine umfassende Erläuterung des Begriffs der personenbezogenen Daten. Ebenso nicht definiert wird der Begriff der Verarbeitung. Darüber hinaus fehlt eine Darstellung der besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO), des Verbots mit Erlaubnisvorbehalt, der Transparenz- und Informationspflicht (Art. 13, 14 DSGVO), der technischen und organisatorischen Maßnahmen (Art. 24, 25 und 32 DSGVO), der Melde- und Benachrichtigungspflichten im Falle von Datenschutzverletzungen (Art. 33, 34 DSGVO), der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO). Es werden keine konkreten Artikel der DSGVO genannt, wodurch es Mitarbeitenden erschwert wird, bei Bedarf weiterführende Informationen zu finden. Zudem bleibt der Selbsttest oberflächlich. Die Einheit ist daher als vollständige DSGVO-Schulung unzureichend.

4. Gegenüberstellung der Schulungen

Die vorhergehende Einzelbewertung der KI-generierten Schulungseinheiten zeigt, dass die Schulungen jeweils eine unterschiedliche Qualität aufweisen.

Um die Qualität der KI-generierten Schulungsinhalten vergleichbar zu machen, werden die Schulungen im Folgenden hinsichtlich Vollständigkeit, Richtigkeit und Verständlichkeit gegenübergestellt. Grundlage dieser Bewertung sind die folgenden dreizehn Kategorien, welche nach der hier vertretenen Meinung (in unterschiedlichem Detailgrad) den Mindestinhalt einer Grundlagenschulung zum Datenschutz definieren: DSGVO-Relevanz; Kernbegriff „personenbezogene Daten“; Kernbegriff „Verarbeitung“; Rollen im Datenschutzrecht (Verantwortlicher, gemeinsam Verantwortliche, Auftragsverarbeiter, betroffene Person); Grundsätze der Verarbeitung; Rechtsgrundlagen der Verarbeitung; Rechte der betroffenen Person; technische und organisatorische Maßnahmen (insb. Art. 25, 32 DSGVO); Datenschutz-Folgenabschätzung; Meldepflichten bei Vorfällen; Verzeichnis von Verarbeitungstätigkeiten; Drittstaatenübermittlungen; Sanktionen bei Verstößen.

Für jede der vorgenannten Kategorien gelten für die Bewertung und Gegenüberstellung der Vollständigkeit, Richtigkeit und Verständlichkeit der Schulungen die folgenden Leitfragen:

- **Vollständigkeit:** Sind alle für die jeweilige Kategorie relevanten Inhalte enthalten?
- **Richtigkeit:** Sind die Inhalte juristisch korrekt und frei von irreführenden Aussagen?

- **Verständlichkeit:** Wird das jeweilige Thema für die Zielgruppe nachvollziehbar vermittelt (z.B. durch anschauliche und treffende Beispiele, die das Verständnis fördern (soweit erforderlich))? Sind inhaltliche Lücken oder Fehler unkritisch, führen also zu keiner Beeinträchtigung des Verständnisses?³¹

Dabei führen die vorgenannten Fragen je betrachteter Kategorie jeweils zu einer von vier möglichen Ergebnissen: „Ja“, „Teilweise“, „Nein“ oder „(-)“.

Vollständigkeit

- „Ja“: Nahezu alle relevanten Inhalte sind enthalten. Es fehlen allenfalls sehr wenige, klar untergeordnete Aspekte.
„Teilweise“: Ein überwiegender Teil der relevanten Inhalte ist enthalten. Es fehlen einzelne relevante Teilespekte.
„Nein“: Es sind nicht alle relevanten Inhalte enthalten. Es fehlen wesentliche Inhalte, sodass kritische Lücken entstehen.
„(-)“: Es wurden keine Aussagen zu der Kategorie getroffen.

Richtigkeit

- „Ja“: Die Inhalte sind nahezu alle sachlich und rechtlich korrekt. Es bestehen allenfalls sehr geringfügige, in der Bewertung unerhebliche Ungenauigkeiten.
„Teilweise“: Die Inhalte sind überwiegend sachlich und rechtlich korrekt. Es liegen einzelne kleinere Fehler oder relevante Ungenauigkeiten vor.
„Nein“: Es sind kritische Fehler vorhanden.
„(-)“: Es wurden keine Aussagen zu der Kategorie getroffen.

Verständlichkeit

- „Ja“: Die Inhalte sind nahezu alle verständlich dargestellt und vorhandene Lücken oder Fehler beeinträchtigen nicht das Verständnis.
„Teilweise“: Die Inhalte sind überwiegend verständlich dargestellt und vorhandene Lücken oder Fehler führen zu keinen kritischen Missverständnissen.
„Nein“: Die Inhalte sind unverständlich dargestellt oder Lücken bzw. Fehler führen zu kritischen Missverständnissen.
„(-)“: Es wurden keine Aussagen zu der Kategorie getroffen.

Um bei der Bewertung und Gegenüberstellung der KI-generierten Schulungsinhalte eine einheitliche Bewertungsgrundlage zu schaffen, wurden je Kategorie überprüfbare Kriterien festgelegt, die als Maßstab für die Bewertung und Beantwortung der jeweiligen Leitfragen dienen. Die jeweiligen Bewertungskriterien stellen keinen abschließenden Maßstab, sondern einen Orientierungsrahmen dar, der nachvollziehbar macht, worauf bei der Beantwortung der Leitfragen je Kriterium geachtet wurde.

Begründung der Kategorienauswahl (Mindestinhalt)

Die Auswahl der dreizehn Kategorien stützt sich auf vier Grundlagen: Den Aufbau und die Regelungssystematik der DSGVO,³² den Abgleich mit etablierten Angeboten aus der

³¹ Die Verständlichkeit wird insoweit auch durch die Vollständigkeit und Richtigkeit der Schulungen beeinflusst. So können fehlende Inhalte und falsche Erklärungen auch das Verständnis beeinträchtigen. (Kritische) Lücken und Fehler, die sich auf das Verständnis auswirken, werden insoweit nicht nur bei der Vollständigkeit bzw. Richtigkeit berücksichtigt, sondern auch bei der Verständlichkeit.

³² Abgleich mit normativen Verankerung (DSGVO-Systematik): Die Kategorien bilden die zentralen Pflichtfelder ab: Anwendungsbereiche/Schutzzweck (Art. 1–3 DSGVO), Begriffe (Art. 4 DSGVO), Grundsätze und Rechenschaft (Art. 5 DSGVO), Rechtsgrundlagen einschließlich besonderer Kategorien (Art. 6, 9 DSGVO), Rechte der betroffenen Person (Art. 12–22 DSGVO), Technische und organisatorische Maßnahmen (Art. 24, 25 DSGVO) und Sicherheit der Verarbeitung (Art. 32 DSGVO), Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), Meldung/Benachrichtigung bei Datenschutzverletzungen (Art. 33/34 DSGVO), Datenschutzfolgeabschätzung (Art. 35 DSGVO), Drittstaatenübermittlungen (Kap. V) sowie Sanktionen (Art. 58, 82, 83 DSGVO).

4. Gegenüberstellung der Schulungen

Praxis,³³ den Abgleich mit öffentlich finanzierten Grundkursen (u. a. Berliner Beauftragte für Datenschutz und Informationsfreiheit)³⁴ und den Abgleich mit einschlägiger Fachliteratur³⁵. Ausgehend von diesen vier Grundlagen konnten die der vorliegenden Bewertung zugrundeliegenden Kategorien als sinnvoller Mindestinhalt einer Grundlagenschulung zum Datenschutz abgeleitet werden.

Die der Bewertung zugrundeliegenden 13 Kategorien bilden dabei den kleinsten gemeinsamen Nenner eines normativ und praktisch belastbaren Mindestinhalts.

Abgrenzung „kritisch“ vs. „nicht-kritisch“

Weil Fehler und Lücken unterschiedliche Auswirkungen auf das Verständnis haben können, wird zwischen kritischen und unkritischen unterschieden. Maßgeblich sind die inhaltliche Relevanz und die Auswirkung auf das Verständnis. Kritisch sind insbesondere rechtlich falsche Kernaussagen (z. B. „Einwilligung ist immer erforderlich“), Verwechslung von Rollen (Verantwortlicher/Auftragsverarbeiter), falsche Aussage zu Art. 33/34 DSGVO (Meldepflichten), sowie erhebliche Verkürzungen, oder gänzlich fehlende wesentliche Inhalte innerhalb eines Kriteriums die ein Grundverständnis dessen nicht mehr ermöglichen. Nicht-kritisch sind z. B. fehlende Beispiele, oberflächliche oder unpräzise, aber nicht falsche Vereinfachungen, sofern sie keine Missverständnisse erwarten lassen.

³³ mit kommerziellen Marktangeboten Inhalte eines kommerziellen Angebots („Datenschutzeinführung für Mitarbeiter und Führungskräfte“): Personenbezogene Daten; Pflichten; Schutz der Daten/technische und organisatorische Maßnahmen; Unternehmensrichtlinien; Rechte der betroffenen Person; Sanktionen; Datenschutzbeauftragter etc. Inhalte eines anderen kommerziellen Angebots („Einführung in den Datenschutz für die Privatwirtschaft“): Grundlagen; Datenverarbeitung einschließlich Beschäftigtendaten; Informationspflichten; Kundendatenschutz – Zulässigkeit der Verarbeitung und Interventionsrechte; Datenschutzbeauftragter etc. Über den Datakontext-Shop werden vortragsfähige Schulungsfolien „Datenschutzeinführung für Mitarbeiter und Führungskräfte“ (Inhalte: personenbezogene Daten; Pflichten; Schutz der Daten/technische und organisatorische Maßnahmen; Unternehmensrichtlinien; Rechte der betroffenen Person; Sanktionen; Datenschutzbeauftragter etc.). Beide Angebote decken einen Großteil der hier zugrunde gelegten Kategorien ab: personenbezogene Daten, Verarbeitung, Rollen/Organisation, Rechtsgrundlagen, Rechte der betroffenen Person, technische und organisatorische Maßnahmen sowie Sanktionen.

³⁴ Abgleich mit öffentlichen Basisprogrammen: Kostenfreie Einstiegsangebote wie z. B. von der Stiftung Datenschutz und dem Berliner Beauftragte für Datenschutz und Informationsfreiheit richten sich insbesondere an kleine Unternehmen, Vereine und junge Unternehmen (Inhalte Stiftung Datenschutz: Organisation und Verantwortlichkeiten; Verzeichnis der Verarbeitungstätigkeiten; Rechtsgrundlagen der Verarbeitung (Wann ist eine Verarbeitung erlaubt? Einwilligung, Vertrag, gesetzliche Pflicht); Datenschutzhinweise (Pflichtinformationen für Betroffene (z. B. Kunden, Mitarbeiter)); Technische und organisatorische Maßnahmen (Datensicherheit, Zugriffskontrolle, Verschlüsselung); Auftragsverarbeitung (Verträge mit Dienstleistern, die personenbezogene Daten verarbeiten), gemeinsame Verantwortlichkeit, Betroffenenrechte (Auskunft, Berichtigung, Löschung, Widerspruch); Datenpannen und Meldepflichten (Vorgehen bei Datenschutzverletzungen); Löschkonzept (Fristen und Verfahren zur Datenlöschung); Datenschutz-Folgenabschätzung (Wann erforderlich und wie durchführen); Datenschutz als laufender Prozess, abrufbar unter: <https://ds-kleinunternehmen.de/startseite>; (Inhalte Berliner Beauftragte für Datenschutz und Informationsfreiheit: Datenschutzgrundlagen, Basisüberblick DSGVO, Rechtsgrundlagen: Mehr als nur Einwilligung, Transparenz, Datenschutzerklärung & Verzeichnis der Verarbeitungstätigkeiten, Erstellung von Verzeichnissen und Datenschutzerklärungen, Cookies, Consent, Gestaltung, Cloud und andere Services, KI-Einsatz: Effizienz mit Verantwortung, Betroffenenrechte, Internationale Datenübertragung, Technisch-organisatorische Maßnahmen (Datenschutzmanagement, Speicherung, Zugriffsregelung, Löschkonzept), abrufbar unter: <https://www.datenschutz-berlin.de/service/starthilfe-datenschutz>). Diese Angebote decken einen Großteil der hier zugrunde gelegten Kategorien ab: Relevanz der Datenschutz-Grundverordnung, Rechtsgrundlagen, Verzeichnis von Verarbeitungstätigkeiten, Rechte der betroffenen Person (Auskunft), Übermittlungen in Drittländer sowie technische und organisatorische Maßnahmen; Meldepflichten bei Datenschutzverletzungen und Datenschutz-Folgenabschätzung.

³⁵ Abgleich mit Sekundärliteratur (Rath/Kraus in Godzierz, Compliance-Checklisten, § 6 Rdnr. 20): Als Mindestwissen werden gefordert: Schutzbereich („Was sind personenbezogene Daten?“), Grundprinzipien der Verarbeitung einschließlich Rechtsgrundlagen/Einwilligung sowie die Anpassung an unternehmensspezifische Situationen. Das stützt unsere Kategorien: personenbezogene Daten, Grundsätze und Rechtsgrundlagen sowie deren organisatorische Verankerung über technische und organisatorische Maßnahmen, das Verzeichnis von Verarbeitungstätigkeiten und die Rollen im Datenschutzrecht.

Themengerechte Zuordnung und Vermeidung von Doppelzählungen

Die Bewertung der Vollständigkeit, Richtigkeit und Vollständigkeit erfolgt strikt themenspezifisch. So werden die Aussagen der KI-generierten Schulungsinhalte der jeweils einschlägigen Kategorie zugeordnet. Das heißt: Jede Aussage wird genau einer Kategorie zugerechnet – und zwar derjenigen, deren Gegenstand sie inhaltlich hauptsächlich betrifft; bloße Kontext- oder Randbezüge sind für die Zuordnung unerheblich. Die Bestimmung der einschlägigen Kategorie orientiert sich am Kern der Aussage und an ihrem normativen Bezug (z. B. Art. 6 DSGVO → Rechtsgrundlagen; Art. 33/34 DSGVO → Meldepflichten). Feststellungen – positiv wie negativ – werden nicht auf andere Kategorien übertragen; Doppelzählungen sind damit ausgeschlossen (eine falsche Aussage zu Rechtsgrundlagen berührt z. B. nicht die Bewertung des Kernbegriffs „Verarbeitung“). Bei inhaltlichen Überschneidungen ist der Schwerpunkt der Aussage maßgeblich. Sachliche Lücken und Fehler werden primär in den Dimensionen Vollständigkeit bzw. Richtigkeit erfasst; sie können die Verständlichkeit jedoch zusätzlich beeinträchtigen und werden dort entsprechend mitberücksichtigt.

4.1 DSGVO-Relevanz

Für die Kategorie *DSGVO-Relevanz* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** kurze Darstellung des sachlichen und räumlichen Anwendungsbereichs der DSGVO; die Feststellung, dass die Verordnung für die jeweilige Organisation relevant ist.
- **Richtigkeit:** keine falsche Zielsetzung, etwa die Annahme, die DSGVO diene dem Schutz von Daten selbst.
- **Verständlichkeit:** Einbindung der Mitarbeitenden; Berücksichtigung etwaiger Lücken oder Fehler.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zur DSGVO-Relevanz wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Ja
Command-a-03-2025	Ja	Ja	Teilweise
DeepSeek V3	Teilweise	Ja	Ja
Gemma 3n E2B	Ja	Teilweise	Teilweise
GPT-4.1	Teilweise	Ja	Ja
Grok 3	Ja	Teilweise	Teilweise
LLaMA 4	Teilweise	Teilweise	Ja
Mistral Medium 3	Teilweise	Teilweise	Ja
Qwen 3-235B-A22B-2507	Ja	Teilweise	Ja

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Es fehlt ein Hinweis auf den räumlichen Anwendungsbereich der DSGVO. Die dargestellten Inhalte sind richtig und verständlich gestaltet. Die Lücke führt zu keinen Verständnisproblemen.

Command-a-03-2025: Es werden alle erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Die dargestellten Inhalte sind richtig. Die dargestellten Inhalte sind darüber hinaus überwiegend verständlich gestaltet, stellenweise können Verkürzungen (insbesondere zum „freier Datenverkehr“) jedoch zu einem Fehlverständnis führen. Zudem fehlt die Einbindung der Mitarbeitenden für eine bessere Verständlichkeit.

DeepSeek V3 Es wird ein überwiegender Teil der erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Es fehlt ein Hinweis auf den räumlichen Anwendungsbereich der DSGVO. Die dargestellten Inhalte sind richtig und verständlich gestaltet. Die Lücke führt zu keinen Verständnisproblemen.

Gemma 3n E2B: Es werden alle erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Die dargestellten Inhalte sind überwiegend richtig, greifen jedoch beim Schutzgegenstand zu kurz: Die DSGVO schützt primär die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten (Art. 1 Abs. 2 DSGVO), nicht „Daten“ an sich. Diese Darstellung führt jedoch zu keinen Verständnisproblemen. Die dargestellten Inhalte sind darüber hinaus überwiegend verständlich gestaltet, stellenweise können Verkürzungen (insbesondere zum räumlichen Anwendungsbereich) jedoch zu einem Fehlverständnis führen.

GPT-4.1: Es wird ein überwiegender Teil der erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Ein kurzer Hinweis auf den sachlichen und räumlichen Anwendungsbereich der DSGVO fehlt. Die dargestellten Inhalte sind richtig und verständlich gestaltet. Die Lücke führt zu keinen Verständnisproblemen.

Grok 3: Es werden alle erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Die dargestellten Inhalte sind überwiegend richtig, greifen jedoch beim Schutzgegenstand zu kurz: Die DSGVO schützt primär die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten (Art. 1 Abs. 2 DSGVO), nicht „Daten“ an sich. Der Schutz der Privatsphäre ist nur ein Teilaспект hiervon. Diese Darstellung führt jedoch zu keinen Verständnisproblemen. Die dargestellten Inhalte sind darüber hinaus überwiegend verständlich gestaltet, stellenweise können Verkürzungen (insbesondere zum räumlichen Anwendungsbereich) jedoch zu einem Fehlverständnis führen.

LLaMA 4: Es wird ein überwiegender Teil der erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Ein Hinweis auf räumlichen Anwendungsbereich der DSGVO fehlt. Die dargestellten Inhalte sind überwiegend richtig. Hinsichtlich des Schutzgegenstandes der DSGVO wäre jedoch richtig gewesen, dass die DSGVO primär die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten schützt (Art. 1 Abs. 2 DSGVO) und nicht „Daten“ an sich. Diese Darstellung führt jedoch zu keinen größeren Verständnisproblemen. Die dargestellten Inhalte sind darüber hinaus verständlich gestaltet.

Mistral Medium 3: Es wird ein überwiegender Teil der erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Ein Hinweis auf den räumlichen Anwendungsbereich der DSGVO und die Feststellung, dass die Verordnung für die eigene Organisation relevant ist, fehlt. Die dargestellten Inhalte sind überwiegend richtig. Hinsichtlich des Schutzgegenstandes der DSGVO wäre jedoch richtig gewesen, dass die DSGVO primär die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten schützt (Art. 1 Abs. 2 DSGVO) und nicht „Daten“ an sich. Diese Darstellung führt jedoch zu keinen größeren Verständnisproblemen. Die dargestellten Inhalte sind darüber hinaus verständlich gestaltet.

Qwen 3-235B-A22B-2507: Es werden alle erforderlichen Informationen zur DSGVO-Relevanz aufgeführt. Die dargestellten Inhalte sind überwiegend richtig. Hinsichtlich des Schutzgegenstandes der DSGVO wäre jedoch richtig gewesen, dass die DSGVO primär die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten schützt (Art. 1 Abs. 2 DSGVO) und nicht „Daten“ an sich. Diese Darstellung führt jedoch zu keinen Verständnisproblemen. Die dargestellten Inhalte sind darüber hinaus verständlich gestaltet.

4.2 Kernbegriff „Personenbezogene Daten“

Für die Kategorie *personenbezogenen Daten* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Erläuterung und Definition dessen, was personenbezogene Daten sind; Unterscheidung zwischen identifizierbaren und identifizierten Personen (gegebenenfalls indirekt durch Beispiele); Darstellung der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie die Abgrenzung zwischen pseudonymen und anonymen Daten.
- **Richtigkeit:** keine falschen oder unvollständigen Definitionen des Begriffs der personenbezogenen Daten und keine beispielhaften Aufzählungen, die ohne Kennzeichnung den Eindruck einer abschließenden Liste vermitteln.
- **Verständlichkeit:** Nutzung von Praxisbeispielen sowie Berücksichtigung möglicher Lücken oder Fehler. Zum besseren Verständnis, wenngleich nicht Voraussetzung für die Mindestanforderungen, trägt außerdem die Erläuterung der direkten und indirekten Identifizierung sowie der Begriff der „natürlichen Person“ bei.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den personenbezogenen Daten wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Teilweise
Command-a-03-2025	Nein	Ja	Teilweise
DeepSeek V3	Teilweise	Ja	Teilweise
Gemma 3n E2B	Teilweise	Teilweise	Teilweise
GPT-4.1	Nein	Ja	Teilweise
Grok 3	Teilweise	Ja	Teilweise
LLaMA 4	-	-	-
Mistral Medium 3	Nein	Ja	Teilweise
Qwen 3-235B-A22B-2507	Teilweise	Ja	Teilweise

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar und zur Unterscheidung personenbezogener, anonymer und pseudonymer Daten. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Darstellung der besonderen Kategorien ist jedoch unvollständig und kann durch die fehlende Kennzeichnung („z. B.“) fälschlich als vollständig verstanden werden. Die verkürzte Darstellung des Begriffs kann zu Verständnisproblemen führen, da zentrale Abgrenzungen fehlen.

Command-a-03-2025: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen wesentliche Inhalte, insbesondere Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar, zur Unterscheidung von direkten und indirekten Identifikatoren sowie zwischen personenbezogenen, anonymen und pseudonymen Daten. Ebenso fehlen Informationen zu der besonderen Kategorie personenbezogener Daten nach Art. 9 DSGVO. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die verkürzte Darstellung des Begriffs kann jedoch zu Verständnisproblemen führen, da zentrale Abgrenzungen fehlen. Zudem fehlen praxisnahe Beispiele aus den Unternehmensbereichen zur Veranschaulichung.

DeepSeek V3: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar, zur Unterscheidung von direkten und indirekten Identifikatoren sowie zwischen personenbezogenen, anonymen und pseudonymen Daten. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Einordnung der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO erfolgt indirekt („sensible Daten“). Die verkürzte Erläuterung der Begrifflichkeiten kann jedoch zu Verständnisproblemen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen praxisnahe Beispiele aus verschiedenen Unternehmensbereichen.

Gemma 3n E2B: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlt die Abgrenzung zwischen identifiziert und identifizierbar und die Unterscheidung zwischen personenbezogenen, pseudonymen und anonymen Daten. Die dargestellten Inhalte sind überwiegend richtig und überwiegend verständlich. Falsch ist die Darstellung, dass die Identifizierbarkeit davon abhängt, ob Daten öffentlich zugänglich sind. Diese Darstellung kann zu Verständnisproblemen führen. Ebenso kann die verkürzte Darstellung des Begriffs zu Verständnisproblemen führen, da zentrale Abgrenzungen fehlen.

GPT-4.1: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen wesentliche Inhalte, insbesondere Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar, zur Unterscheidung von direkten und indirekten Identifikatoren sowie zwischen personenbezogenen, anonymen und pseudonymen Daten. Ebenso fehlen die Definition und Einordnung der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die verkürzte Darstellung des Begriffs kann zu Verständnisproblemen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen praxisnahe Beispiele aus verschiedenen Unternehmensbereichen.

Grok 3: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar, zur Unterscheidung von direkten und indirekten Identifikatoren sowie zwischen personenbezogenen, anonymen und pseudonymen Daten. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Einordnung der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO erfolgt indirekt („sensible Daten“). Die verkürzte Erläuterung der Begrifflichkeiten kann zu Verständnisproblemen führen.

LLaMA 4: Es werden keine Informationen zum Kernbegriff „Personenbezogene Daten“ aufgeführt. Der Begriff wird nur erwähnt, aber nicht erklärt.

Mistral Medium 3: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen wesentliche Inhalte, insbesondere Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar, zur Unterscheidung von direkten und indirekten Identifikatoren sowie zwischen personenbezogenen, anonymen und pseudonymen Daten. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Einordnung der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO erfolgt rudimentär und nur indirekt („sensible Daten“). Die verkürzte Erläuterung der Begrifflichkeiten kann zu Verständnisproblemen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen praxisnahe Beispiele aus verschiedenen Unternehmensbereichen.

Qwen 3-235B-A22B-2507: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „personenbezogene Daten“ aufgeführt. Es fehlen

Erläuterungen zum Unterschied zwischen identifiziert und identifizierbar sowie zur Unterscheidung von direkten und indirekten Identifikatoren. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Abgrenzung zwischen personenbezogenen und anonymen Daten erfolgt indirekt. Ebenso werden die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO nur indirekt („sensible Daten“) eingeordnet. Die verkürzte Definition kann zu Verständnisproblemen führen.

4.3 Kernbegriff „Verarbeitung“

Für die Kategorie *Verarbeitung* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Darstellung und Definition dessen, was unter Verarbeitung im Sinne der DSGVO zu verstehen ist, einschließlich typischer Vorgänge wie Erheben, Speichern, Übermitteln oder Löschen von Daten.
- **Richtigkeit:** Herstellung eines klaren Bezugs zu personenbezogenen Daten; ein fehlender Bezug gilt als inhaltlicher Mangel.
- **Verständlichkeit:** Verwendung praxisnaher Beispiele sowie Berücksichtigung etwaiger Lücken oder Fehler in der Darstellung.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zur Verarbeitung wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Ja	Ja	Ja
Command-a-03-2025	Ja	Ja	Ja
DeepSeek V3	Nein	-	Teilweise
Gemma 3n E2B	Nein	-	Teilweise
GPT-4.1	Ja	Teilweise	Teilweise
Grok 3	Teilweise	Ja	Ja
LLaMA 4	Nein	-	Teilweise
Mistral Medium 3	Ja	Ja	Ja
Qwen 3-235B-A22B-2507	Nein	-	Teilweise

Claude Sonnet 4: Es werden alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Die dargestellten Inhalte sind richtig und verständlich. Zur Förderung der Verständlichkeit des Inhalts fehlen zwar praxisnahe Beispiele aus verschiedenen Unternehmensbereichen, dies beeinträchtigt das Verständnis im Gesamten aber nicht wesentlich.

Command-a-03-2025: Es werden alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Die dargestellten Inhalte sind richtig. Zur Förderung der Verständlichkeit des Inhalts fehlen zwar praxisnahe Beispiele aus verschiedenen Unternehmensbereichen, dies beeinträchtigt das Verständnis im Gesamten aber nicht wesentlich.

DeepSeek V3: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Es fehlen wesentliche Inhalte. Der Begriff wird zwar verwendet, jedoch weder erläutert noch durch Beispiele verständlich gemacht. Die thematische Einbettung in den übrigen Kapiteln ermöglicht zwar ein gewisses Grundverständnis, ohne eine eigene Definition und konkrete Beispiele bleibt das Verständnis jedoch lediglich rudimentär.

Gemma 3n E2B: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Es fehlen wesentliche Inhalte. Der Begriff wird zwar

4. Gegenüberstellung der Schulungen

verwendet, jedoch weder erläutert noch durch Beispiele verständlich gemacht. Die thematische Einbettung in den übrigen Kapiteln ermöglicht zwar ein gewisses Grundverständnis, ohne eine eigene Definition und konkrete Beispiele bleibt das Verständnis jedoch lediglich rudimentär.

GPT-4.1: Es werden alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Die dargestellten Inhalte sind überwiegend richtig und überwiegend verständlich. Die Schulung spricht bei der Definition der Verarbeitung explizit vom „Umgang mit Daten“. Problematisch ist dies insbesondere, da die Definition in der Schulung so den Eindruck erweckt, auch nicht personenbezogene Daten könnten unter den Begriff der Verarbeitung im Sinne der DSGVO fallen. Dies hat Auswirkung auf die Verständlichkeit des Themas. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele aus verschiedenen Unternehmensbereichen.

Grok 3: Es wird ein überwiegender Teil der erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Es fehlt jedoch die Definition des Kernbegriffs der „Verarbeitung“. Die dargestellten Inhalte sind richtig. Trotz der fehlenden Definition bleibt die Verständlichkeit durch die aufgeführten Beispiele typischer Verarbeitungsvorgänge in den Bereichen Personalwesen, Kundenmanagement, Marketing und IT gewährleistet.

LLaMA 4: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Es fehlen wesentliche Inhalte. Der Begriff wird zwar verwendet, jedoch weder erläutert noch durch Beispiele verständlich gemacht. Die thematische Einbettung in den übrigen Kapiteln ermöglicht zwar ein gewisses Grundverständnis, ohne eine eigene Definition und konkrete Beispiele bleibt das Verständnis jedoch lediglich rudimentär.

Mistral Medium 3: Es werden alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Die dargestellten Inhalte sind richtig und verständlich. Zur Förderung der Verständlichkeit des Inhalts fehlen zwar praxisnahe Beispiele aus verschiedenen Unternehmensbereichen, dies beeinträchtigt das Verständnis im Gesamten aber nicht wesentlich.

Qwen 3-235B-A22B-2507: Es werden nicht alle erforderlichen Informationen zum Kernbegriff „Verarbeitung“ aufgeführt. Es fehlen wesentliche Inhalte. Der Begriff wird zwar verwendet, jedoch weder erläutert noch durch Beispiele verständlich gemacht. Die thematische Einbettung in den übrigen Kapiteln ermöglicht zwar ein gewisses Grundverständnis, ohne eine eigene Definition und konkrete Beispiele bleibt das Verständnis jedoch lediglich rudimentär.

4.4 Rollen im Datenschutzrecht

Für die Kategorie *Rollen im Datenschutzrecht* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** zumindest implizite Definition des Verantwortlichen, des Auftragsverarbeiters sowie der betroffenen Person und eine klare Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter.
- **Richtigkeit:** keine Vermischung der Rollen oder fehlerhafte Rollenbeschreibungen.
- **Verständlichkeit:** Verwendung von Beispielen sowie die Berücksichtigung möglicher Lücken oder Fehler. Zum besseren Verständnis, wenngleich nicht Voraussetzung für die Mindestanforderungen, trägt die explizite Nennung der

gemeinsamen Verantwortlichkeit bei; sie ist jedoch entbehrlich, sofern aus der Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter deutlich wird, dass die Beteiligung einer weiteren Partei nicht zwangsläufig eine Auftragsverarbeitung bedeutet.

Auf Basis dieser Kriterien sind die AI-generierten Inhalte zu den Rollen im Datenschutzrecht wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Teilweise
Command-a-03-2025	Ja	Ja	Teilweise
DeepSeek V3	Ja	Teilweise	Teilweise
Gemma 3n E2B	Nein	Ja	Nein
GPT-4.1	Ja	Teilweise	Teilweise
Grok 3	Nein	Ja	Teilweise
LLaMA 4	Ja	Ja	Teilweise
Mistral Medium 3	Teilweise	Ja	Teilweise
Qwen 3-235B-A22B-2507	Ja	Ja	Teilweise

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Der Begriff des Auftragsverarbeiters wird nicht eingeführt und nicht definiert, und es erfolgt keine Abgrenzung zum Verantwortlichen. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Formulierungen „unsere Organisation ist Verantwortlicher“ und „wir entscheiden über Zweck und Mittel der Verarbeitung“ könnten aufgrund ihrer Absolutheit zu Missverständnissen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

Command-a-03-2025: Es werden alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Die dargestellten Inhalte sind richtig und überwiegend verständlich. Die Formulierungen „unsere Organisation ist Verantwortlicher“ könnten aufgrund ihrer Absolutheit zu Missverständnissen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele. Positiv für die Verständlichkeit ist jedoch, dass die gemeinsame Verantwortlichkeit zumindest indirekt angesprochen wird.

DeepSeek V3: Es werden alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen überwiegend richtig, es finden sich jedoch auch fehlerhafte oder verkürzte Darstellungen was der Verständlichkeit teilweise schadet. Der Begriff der „betroffenen Person“ wird nur implizit erläutert. Falsch ist die Formulierung „jede Person“ sei betroffene Person, da sie den Eindruck erwecken kann, dass auch Personen ohne Verarbeitung ihrer personenbezogenen Daten als betroffene Personen gelten würden. Die Verständlichkeit wird jedoch durch die Überschrift „Betroffenenrechte“ nicht kritisch beeinflusst. Die Definitionen des Verantwortlichen und des Auftragsverarbeiters sind nur implizit und zu oberflächlich enthalten, was die Verständlichkeit erschwert. Auch die Abgrenzung zwischen dem Auftragsverarbeiter und dem Verantwortlichen erfolgt nur implizit und unpräzise innerhalb der Definition des Auftragsverarbeiters. Ebenso könnte die Formulierung „unsere Organisation ist Verantwortlicher“ aufgrund ihrer Absolutheit zu Missverständnissen führen. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

Gemma 3n E2B: Es werden nicht alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Es fehlen wesentliche Inhalte; insbesondere die Definition des Verantwortlichen ist nicht enthalten, der Begriff wird lediglich im FAQ genannt, ohne

jede Erklärung. Der Begriff des Auftragsverarbeiters wird nicht eingeführt und nicht definiert, und die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt nicht. Der Begriff der betroffenen Person wird nicht, auch nicht implizit, erläutert. Zur Rollenverteilung sind keine inhaltlichen Fehler, sondern nur Auslassungen erkennbar. Da wesentliche Definitionen und Abgrenzungen der datenschutzrechtlichen Rollen fehlen, ist das Verständnis des Themas erheblich erschwert. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

GPT-4.1 Es werden alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen überwiegend richtig, jedoch größtenteils verkürzt dargestellt, was der Verständlichkeit teilweise schadet. Falsch ist die Formulierung „jede Person“ habe nach DSGVO bestimmte Rechte. Die Verständlichkeit wird jedoch durch die Überschrift „Betroffenenrechte“ und die Definition der betroffenen Person nicht kritisch beeinflusst. Die Definition des Verantwortlichen und des Auftragsverarbeiters ist nur implizit enthalten. Die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt ebenfalls nur implizit innerhalb der Definition des Auftragsverarbeiters, was die Verständlichkeit beeinträchtigen kann. Auch die Formulierungen „unsere Organisation ist Verantwortlicher“ könnten aufgrund ihrer Absolutheit zu Missverständnissen führen. Jedoch sind Beispiele zur Rollenabgrenzung teilweise enthalten und können das Verständnis fördern.

Grok 3: Es werden nicht alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Es fehlen wesentliche Inhalte; insbesondere die Begriffe des Verantwortlichen und des Auftragsverarbeiters werden weder eingeführt noch definiert. Eine Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt ebenso wenig. Inhaltlich sind die Aussagen richtig, jedoch größtenteils verkürzt dargestellt, was der Verständlichkeit teilweise schadet. Der Begriff der „betroffenen Person“ wird nur implizit erläutert. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

LLaMA 4: Es werden alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen richtig, jedoch größtenteils verkürzt dargestellt, was der Verständlichkeit teilweise schadet. Die Gleichsetzung des Verantwortlichen mit der durchführenden Stelle kann zu Missverständnissen führen. Die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt nur implizit innerhalb der Definition des Auftragsverarbeiters. Der Begriff der „betroffenen Person“ wird nur implizit erläutert. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

Mistral Medium 3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Der Begriff des Auftragsverarbeiters wird nicht definiert, und die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt nicht. Falsche Rollenbeschreibungen sind nicht erkennbar. Es finden sich jedoch verkürzte Darstellungen was der Verständlichkeit teilweise schadet. So ist bspw. die Erläuterung des Begriffs des Verantwortlichen nur impliziert enthalten. Zur Förderung der Verständlichkeit des Inhalts fehlen zudem praxisnahe Beispiele.

Qwen 3-235B-A22B-2507: Es werden alle erforderlichen Informationen zu den Rollen im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen richtig, jedoch größtenteils zu verkürzt dargestellt, was der Verständlichkeit teilweise schadet. Der Begriff des Auftragsverarbeiters und die Abgrenzung zwischen Auftragsverarbeiter und Verantwortlichem erfolgt nur implizit innerhalb der Beschreibung der Auftragsverarbeitung. Falsche Rollenbeschreibungen sind nicht erkennbar. Die Formulierungen „Verantwortlicher: In Ihrer Organisation ist das Ihre Firma“ könnten

jedoch aufgrund ihrer Absolutheit zu Missverständnissen führen. Beispiele zur Rollenabgrenzung sind enthalten und können das Verständnis fördern.

4.5 Grundsätze der Verarbeitung

Für die Kategorie *Grundsätze der Verarbeitung* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Die Grundsätze der Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht werden jeweils erwähnt und zumindest sinngemäß erläutert.
- **Richtigkeit:** Die Grundsätze sind richtig benannt und zutreffend erklärt; unzutreffende Darstellungen (z. B. die Annahme, personenbezogene Daten müssten stets aktualisiert oder unrichtige Daten seien zwingend zu löschen, wenn keine Berichtigung möglich ist) gelten als Fehler.
- **Verständlichkeit:** Nutzung von Praxisbeispielen sowie Berücksichtigung möglicher Lücken oder Fehler.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den Grundsätzen der Verarbeitung wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Teilweise	Teilweise
Command-a-03-2025	Ja	Teilweise	Teilweise
DeepSeek V3	Teilweise	Ja	Teilweise
Gemma 3n E2B	Ja	Teilweise	Teilweise
GPT-4.1	Ja	Ja	Teilweise
Grok 3	Ja	Ja	Teilweise
LLaMA 4	Nein	Teilweise	Teilweise
Mistral Medium 3	Ja	Ja	Teilweise
Qwen 3-235B-A22B-2507	Ja	Ja	Ja

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Es fehlen die (Teil-)Grundsätze von Treu und Glauben und Transparenz. Inhaltlich sind die Aussagen überwiegend richtig, es finden sich jedoch auch fehlerhafte oder verkürzte Darstellungen, insbesondere im Zusammenhang mit dem Grundsatz der Zweckbindung, dem Grundsatz der Richtigkeit und dem Grundsatz der Integrität und Vertraulichkeit fehlen wichtige Informationen, die für das Verständnis wichtig wären. Der Grundsatz der Rechenschaftspflicht wird nur implizit erwähnt. Zudem sind die enthaltenen Empfehlungen, etwa, dass unrichtige Daten zu löschen sind, wenn keine Berichtigung möglich ist, falsch. Die Verständlichkeit wird durch praktische Tipps und Beispiele zwar grundsätzlich unterstützt, insbesondere die zuvor genannten Verkürzungen können jedoch zu Verständnisproblemen führen.

Command-a-03-2025: Es werden alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen überwiegend richtig, jedoch finden sich auch fehlerhafte oder verkürzte Darstellungen, insbesondere im Zusammenhang mit den Grundsätzen der Rechtmäßigkeit, Zweckbindung sowie Integrität und Vertraulichkeit. So werden bspw. fälschlicherweise die (Teil-)Grundsätze Rechtmäßigkeit, Zweckbindung und Transparenz als ein Grundsatz zusammengefasst. Diese Fehler und Verkürzungen können zu Verständnisproblemen

4. Gegenüberstellung der Schulungen

führen. Zur Verständlichkeit fehlen ebenso praktische Tipps und Beispiele.

DeepSeek V3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Es fehlt der (Teil-)Grundsatz Treu und Glauben sowie die Rechenschaftspflicht. Inhaltlich sind die Aussagen richtig, jedoch finden sich größtenteils verkürzte Darstellungen, insbesondere im Zusammenhang mit den Grundsätzen der Rechtmäßigkeit, Zweckbindung, Richtigkeit sowie Integrität und Vertraulichkeit. Diese Verkürzungen können zu Verständnisproblemen führen. Im Übrigen wird die Verständlichkeit jedoch durch die tabellarische Darstellung mit Kurzbeschreibungen und Praxisbeispielen sowie durch den abschließenden Praxistipp unterstützt.

Gemma 3n E2B: Es werden nahezu alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Es fehlt allein der (Teil-)Grundsatz von Treu und Glauben. Inhaltlich sind die Aussagen überwiegend richtig, jedoch finden sich auch fehlerhafte, verkürzte oder zu ungenaue Darstellungen. Falsch ist insbesondere, dass der Grundsatz „Rechtmäßigkeit, Transparenz und Treu und Glauben“ „Rechtmäßigkeit, Angemessenheit und Zweckbindung“ genannt wird und der (Teil-)Grundsatz der Transparenz als isolierter Grundsatz aufgeführt ist. Auch im Zusammenhang mit dem Grundsatz der Zweckbindung, dem Grundsatz der Richtigkeit und dem Grundsatz der Integrität und Vertraulichkeit fehlen wichtige Informationen, die für das Verständnis wichtig wären. Zur Verständlichkeit fehlen ebenso praktische Tipps und Beispiele.

GPT-4.1: Es werden alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen richtig, jedoch finden sich größtenteils verkürzte Darstellungen, insbesondere im Zusammenhang mit den Grundsätzen der Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit sowie Integrität und Vertraulichkeit. Die Rechenschaftspflicht wird nur implizit erwähnt (z. B. fehlende Dokumentation). Diese Verkürzungen können zu Verständnisproblemen führen. Zur Verständlichkeit fehlen ebenso praktische Tipps und Beispiele.

Grok 3: Es werden alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen richtig, jedoch finden sich größtenteils verkürzte Darstellungen. So wird der Grundsatz der „Rechtmäßigkeit, Fairness und Transparenz“ in einem Satz zusammengefasst, ohne die einzelnen Elemente zu erklären oder durch Beispiele zu veranschaulichen. Auch die Grundsätze der Zweckbindung, Richtigkeit, sowie Integrität und Vertraulichkeit werden inhaltlich unzureichend ausgeführt. Der Grundsatz der Rechenschaftspflicht wird nur implizit erwähnt. Diese Verkürzungen können zu Verständnisproblemen führen. Zur Verständlichkeit fehlen ebenso praktische Tipps und Beispiele.

LLaMA 4: Es werden nicht alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Es fehlen wesentliche Inhalte, insbesondere der Grundsatz der Rechtmäßigkeit der Verarbeitung wird nicht herausgearbeitet. Ebenso fehlt der Grundsatz der Richtigkeit und die Rechenschaftspflicht. Inhaltlich sind die Aussagen überwiegend richtig, jedoch finden sich größtenteils verkürzte und unvollständige Darstellungen. Der (Teil-)Grundsatz der Transparenz wird fälschlicherweise als isolierter Grundsatz dargestellt. Auch die Grundsätze der Zweckbindung, Richtigkeit, sowie Integrität und Vertraulichkeit werden inhaltlich unzureichend ausgeführt. Diese Verkürzungen können zu Verständnisproblemen führen. Im praktischen Teil werden zudem anderslautende Begrifflichkeiten (bspw. „Datenvermeidung“) genutzt, was zu erheblichen Missverständnissen führen kann.

Mistral Medium 3: Es werden nahezu alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Es fehlt die Rechenschaftspflicht. Inhaltlich sind die Aussagen richtig, jedoch finden sich auch verkürzte Darstellungen. So wird insbesondere der Grundsatz „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz“ nur oberflächlich dargestellt. Diese Verkürzungen können zu Verständnisproblemen führen. Zur Verständlichkeit fehlen ebenso praktische Tipps und Beispiele.

Qwen 3-235B-A22B-2507: Es werden alle erforderlichen Informationen zu den Grundsätzen der Verarbeitung im Datenschutzrecht aufgeführt. Inhaltlich sind die Aussagen richtig, jedoch finden sich auch verkürzte Darstellungen. So werden insbesondere die Grundsätze der Zweckbindung, Speicherbegrenzung, Richtigkeit, sowie Integrität und Vertraulichkeit inhaltlich verkürzt ausgeführt. Diese Verkürzungen können zu Verständnisproblemen führen. Die „Rechenschaftspflicht“ wird zwar als „Nachweisbarkeit“ bezeichnet, was begrifflich nicht präzise ist, jedoch der Verständlichkeit des Inhalts nicht wesentlich schadet, da die gemeinte Pflicht zur Dokumentation erkennbar bleibt. Im Übrigen wird die Verständlichkeit jedoch durch die praxisnahen Beispiele erheblich unterstützt.

4.6 Rechtsgrundlagen für die Verarbeitung

Für die Kategorie *Rechtsgrundlagen der Verarbeitung* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Hinweis auf die Notwendigkeit einer Rechtsgrundlage; Nennung und zumindest beispielhafte Erläuterung der in Art. 6 Abs. 1 lit. a bis f DSGVO genannten Rechtsgrundlagen sowie Darstellung und Erklärung der Besonderheiten des Art. 9 DSGVO zu besonderen Kategorien personenbezogener Daten.
- **Richtigkeit:** keine falschen Vorrangbehauptungen zugunsten der Einwilligung und keine unzutreffende Darstellung des berechtigten Interesses als Generalerlaubnis.
- **Verständlichkeit:** Verwendung von Beispielen sowie der Hinweis darauf, dass einzelne Rechtsgrundlagen an spezifische Voraussetzungen gebunden sind; zudem Berücksichtigung möglicher Lücken oder Fehler in der Darstellung.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den Rechtsgrundlagen der Verarbeitung wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Teilweise
Command-a-03-2025	Teilweise	Ja	Ja
DeepSeek V3	Nein	Ja	Nein
Gemma 3n E2B	Nein	Teilweise	Nein
GPT-4.1	Nein	Ja	Nein
Grok 3	Teilweise	Ja	Teilweise
LLaMA 4	-	-	-
Mistral Medium 3	-	-	-
Qwen 3-235B-A22B-2507	Nein	Ja	Nein

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Es fehlen die Rechtsgrundlagen des Art. 6 Abs. 1 lit. d und e DSGVO. Ebenso werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten

4. Gegenüberstellung der Schulungen

nicht berücksichtigt. Inhaltlich sind die Aussagen richtig, jedoch ist die Darstellungen größtenteils verkürzt, was dem Verständnis schadet. Die Ausführungen beschränken sich auf eine oberflächliche Aufzählung der Rechtsgrundlagen, ohne inhaltliche Erläuterung. Die Verständlichkeit wird durch praktische Tipps und Beispiele grundsätzlich unterstützt. Allerdings fehlt ein konkretes Beispiel für die Einwilligung als Rechtsgrundlage. In Kombination mit ihrer Nennung an erster Stelle kann dies zu dem Missverständnis führen, dass die Einwilligung die bevorzugte Rechtsgrundlage sei. Das Beispiel zum berechtigten Interesse ist stark vereinfacht, sodass es den falschen Eindruck erwecken könnte, Videoüberwachung zur Sicherheit sei automatisch auf berechtigte Interessen stützbar.

Command-a-03-2025: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Nicht berücksichtigt werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Inhaltlich sind die Aussagen richtig. Zur Verständlichkeit fehlen praktische Tipps und Beispiele, dies beeinträchtigt das Verständnis im Gesamten aber nicht wesentlich.

DeepSeek V3: Es werden nicht alle erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff „Rechtsgrundlage“ nicht genutzt, sondern lediglich allgemein formuliert, dass „Daten legal verarbeitet werden müssen“. Es fehlt der Hinweis, dass die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage unzulässig ist. Rechtsgrundlagen sind nur beispielhaft und nicht vollständig aufgezählt. Nicht berücksichtigt werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Inhaltlich sind die Aussagen sofern vorhanden richtig, aber zu oberflächlich und mangels Erläuterung insgesamt unverständlich. Die Verständlichkeit wird auch durch das Beispiel nicht unterstützt.

Gemma 3n E2B: Es werden nicht alle erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Es fehlen wesentliche Inhalte, insbesondere sind die Rechtsgrundlagen nur beispielhaft und nicht vollständig aufgezählt. Es fehlt der Hinweis, dass die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage unzulässig ist. Inhaltlich sind die Aussagen überwiegend richtig, die Darstellung erfolgt jedoch zu oberflächlich. Falsch ist, die Darstellung der Einwilligung als alleinige Rechtsgrundlage bei besonderen Kategorien personenbezogener Daten. Dies kann zu Missverständnissen führen. Die nur beispielhaft genannten Rechtsgrundlagen werden nicht näher erläutert, wodurch sie nahezu unverständlich sind. Die Verständlichkeit wird auch durch die Übung nicht unterstützt.

GPT-4.1: Es werden nicht alle erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Es fehlen wesentliche Inhalte, insbesondere sind die Rechtsgrundlagen nur beispielhaft und nicht vollständig aufgezählt. Nicht berücksichtigt werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Inhaltlich sind die Aussagen richtig, aber zu oberflächlich und mangels Erläuterung insgesamt unverständlich.

Grok 3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Nicht berücksichtigt werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Inhaltlich sind die Aussagen richtig, die Darstellung erfolgt jedoch insgesamt zu oberflächlich, was der Verständlichkeit schadet. Insbesondere werden das „öffentliche Interesse“ und „berechtigte Interesse“ vermischt, was zu Verständnisschwierigkeiten führen kann. Ebenso wird bei den „Tipps zur praktischen

Umsetzung“ der Punkt „Einwilligung einholen“ genannt, was fälschlicherweise den Eindruck erwecken könnte, dass Einwilligung die Standardrechtsgrundlage ist.

LLaMA 4: Es werden keine Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt.

Mistral Medium 3: Es werden keine Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt.

Qwen 3-235B-A22B-2507: Es werden nicht alle erforderlichen Informationen zu den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt. Es fehlen wesentliche Inhalte, insbesondere sind die Rechtsgrundlagen nur beispielhaft und nicht vollständig aufgezählt. Nicht berücksichtigt werden die Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Inhaltlich sind die Aussagen richtig, aber zu oberflächlich, was der Verständlichkeit schadet. So werden die beispielhaft genannten Rechtsgrundlagen nicht näher erläutert, wodurch sie nahezu unverständlich sind.

4.7 Rechte der betroffenen Person

Für die Kategorie *Rechte der betroffenen Person* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Erwähnung und zumindest sinngemäße Erläuterung der Rechte auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit sowie Widerruf der Einwilligung, zudem Hinweise auf Fristen, interne Meldewege und darauf, dass Anfragen nicht unmittelbar selbst beantwortet werden sollen.
- **Richtigkeit:** richtige Darstellung der einzelnen Rechte, insbesondere in Bezug auf Fristen, Umfang und Adressatenkreis; keine falschen oder erfundenen Rechte, keine fehlerhafte Einordnung als austauschbare Alternativen (z. B. Berichtigung oder Löschung) und keine unzutreffende Adressierung (etwa „Rechte der Mitarbeitenden“ statt „Rechte der betroffenen Person“).
- **Verständlichkeit:** Verwendung von Beispielen und Praxistipps sowie Bezugnahme auf Voraussetzungen und Ausnahmen (mindestens Formulierungen wie „unter bestimmten Voraussetzungen“ oder „in manchen Fällen“). Zu vermeiden sind stark vereinfachte oder vom Gesetzeswortlaut zu weit entfernte Aussagen, die Missverständnisse begünstigen (z. B. „Daten können gelöscht werden, wenn ...“, „betroffene Person kann ihre Daten ändern“, „kann grundsätzlich Widerspruch einreichen“). Zum besseren Verständnis, wenngleich nicht Voraussetzung für die Mindestanforderungen, tragen ergänzende Erläuterungen zur Beschwerdemöglichkeit und zum Umfang der einzelnen Rechte bei.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den Rechten der betroffenen Person wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Teilweise	Teilweise
Command-a-03-2025	Teilweise	Ja	Teilweise
DeepSeek V3	Nein	Ja	Teilweise
Gemma 3n E2B	Teilweise	Teilweise	Teilweise
GPT-4.1	Nein	Teilweise	Teilweise
Grok 3	Teilweise	Teilweise	Teilweise

4. Gegenüberstellung der Schulungen

LLaMA 4	Nein	Ja	Nein
Mistral Medium 3	Teilweise	Ja	Teilweise
Qwen 3-235B-A22B-2507	Teilweise	Ja	Teilweise

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten sowie der Widerruf der Einwilligung werden nicht erwähnt. Inhaltlich sind die Aussagen überwiegend richtig, jedoch finden sich auch falsche oder verkürzte Darstellungen. So ist die Angabe zur Aufbewahrungsfrist im Zusammenhang mit der Speicherbegrenzung falsch, was jedoch keine Auswirkungen auf die Verständlichkeit des Themas haben dürfte. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit beeinträchtigt. Die Rechte auf Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch werden lediglich stichpunktartig, ohne jede Erläuterung genannt. Dies kann zu Missverständnissen und Fehlinterpretationen führen. Die gegebenen Praxistipps unter „Ihr Vorgehen“ sind der Verständlichkeit grundsätzlich zuträglich. Die Beschreibung der internen Prozesse erfolgt jedoch zu absolut, was ebenfalls zu Missverständnissen führen kann.

Command-a-03-2025: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten werden nicht behandelt. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen richtig, jedoch sind die Darstellungen teilweise stark verkürzt. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit erheblich beeinträchtigt. Durch die absolute Formulierung der Betroffenenrechte („Betroffene können verlangen“) könnte der falsche Eindruck entstehen, dass diese Rechte grundsätzlich gelten. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

DeepSeek V3: Es werden nicht alle erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Es fehlen wesentliche Inhalte, insbesondere fehlt das Recht auf Einschränkung, Widerspruch und Widerruf der Einwilligung. Auch die Informations- und Mitteilungspflichten werden nicht behandelt. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen richtig, jedoch sind die Darstellungen stark verkürzt. Insgesamt mangelt es an Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit erheblich beeinträchtigt. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

Gemma 3n E2B: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten sowie der Widerruf der Einwilligung werden nicht behandelt. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen überwiegend richtig, jedoch finden sich auch verkürzte Darstellungen. Falsch ist, dass von den „Rechten der Mitarbeiter“ gesprochen wird. Zudem wird der Eindruck vermittelt, dass der Mitarbeitende seine Rechte selbst unmittelbar umsetzen darf. Dies kann zu Missverständnissen führen. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit beeinträchtigt. Die Verständlichkeit auch leidet darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

GPT-4.1: Es werden nicht alle erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Es fehlen wesentliche Inhalte, insbesondere fehlt das Recht auf Einschränkung, Widerspruch und Widerruf der Einwilligung. Auch die Informations- und Mitteilungspflichten werden nicht behandelt. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der explizite Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen überwiegend richtig, die Darstellungen sind jedoch insgesamt stark verkürzt. Falsch ist, dass das Recht auf Berichtigung und das Recht auf Löschung weitestgehend als Alternativen dargestellt werden. Das kann zu Missverständnissen führen. Insgesamt mangelt es an Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit erheblich beeinträchtigt. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

Grok 3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten sowie der Widerruf der Einwilligung werden nicht behandelt. Es fehlen Fristen. Inhaltlich sind die Aussagen überwiegend richtig, jedoch sind die Darstellungen insgesamt stark verkürzt. Falsch ist die Nennung eines „Rechts auf Nicht-Diskriminierung“. Dies kann zu Missverständnissen führen. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit beeinträchtigt. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

LLaMA 4: Es werden nicht alle Informationen zu den Rechten der betroffenen Person aufgeführt. Es fehlen wesentliche Inhalte, insbesondere fehlt die Nennung und Erläuterung der einzelnen Betroffenenrechte, allein die Informationspflicht wird implizit angesprochen. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen – soweit überhaupt vorhanden – richtig, jedoch deutlich verkürzt. Die Verständlichkeit leidet darunter, dass die jeweiligen Rechte weder aufgezählt noch erläutert werden. Die gewählten Praxistipps tragen nicht zur Verständlichkeit bei, da insgesamt die theoretische Grundlage zu den Betroffenenrechten fehlt, um sie umsetzen zu können.

Mistral Medium 3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten sowie der Widerruf der Einwilligung werden nicht behandelt. Es fehlen Fristen und Hinweise auf interne Meldewege bzw. der Hinweis darauf, dass Anfragen nicht selbst beantwortet werden sollten. Inhaltlich sind die Aussagen richtig, jedoch sind die Darstellungen verkürzt. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit beeinträchtigt. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden.

Qwen 3-235B-A22B-2507: Es wird ein überwiegender Teil der erforderlichen Informationen zu den Rechten der betroffenen Person aufgeführt. Die Informations- und Mitteilungspflichten sowie der Widerruf der Einwilligung werden nicht behandelt. Inhaltlich sind die Aussagen richtig, jedoch sind die Darstellungen teilweise verkürzt. Insgesamt mangelt es an tiefergehenden Erläuterungen zu den einzelnen Rechten und deren Voraussetzungen, was die Verständlichkeit beeinträchtigt. Die Verständlichkeit leidet auch darunter, dass zu den jeweiligen Rechten keine Praxisbeispiele oder Praxistipps bereitgestellt werden. Im Übrigen wird die Verständlichkeit jedoch durch die tabellarische Darstellung unterstützt.

4.8 Technische und organisatorische Maßnahmen

Für die Kategorie *Technische und organisatorische Maßnahmen* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** zumindest eine grobe Erläuterung der technischen und organisatorischen Maßnahmen; Nennung von *Privacy by Design* und *Privacy by Default*; Hinweis darauf, dass technische und organisatorische Maßnahmen nicht ausschließlich der Sicherheit dienen, sondern generell zur Umsetzung der Datenschutz-Grundverordnung erforderlich sind. Zudem werden Sicherheitsmaßnahmen gemäß Art. 32 DSGVO sowie der Risikobezug thematisiert und auch organisatorische Maßnahmen einbezogen.
- **Richtigkeit:** Die genannten Beispiele für technische und organisatorische Maßnahmen sind zutreffend und richtig eingeordnet; insbesondere werden typische Fehler bei der Unterscheidung zwischen Zugriffsschutz und Zugangsschutz vermieden.
- **Verständlichkeit:** Nutzung von Praxisbeispielen sowie Berücksichtigung möglicher Lücken oder Fehler.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den technischen und organisatorischen Maßnahmen wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Teilweise
Command-a-03-2025	Nein	Ja	Nein
DeepSeek V3	Nein	Ja	Nein
Gemma 3n E2B	Teilweise	Ja	Teilweise
GPT-4.1	Nein	Ja	Nein
Grok 3	Nein	Ja	Nein
LLaMA 4	Nein	Ja	Nein
Mistral Medium 3	Teilweise	Ja	Teilweise
Qwen 3-235B-A22B-2507	Teilweise	Ja	Teilweise

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlt der Hinweis, dass die Auswahl der Maßnahmen risikobasiert erfolgen muss. Ebenso wird nicht deutlich, dass technische und organisatorische Maßnahmen nicht nur der Sicherheit der Verarbeitung dienen, sondern auch generell zur Umsetzung der DSGVO erforderlich sind. Der Grundsatz „Privacy by Design“ und „Privacy by Default“ bleibt ebenfalls unberücksichtigt. Inhaltlich sind die Aussagen richtig, jedoch teilweise verkürzt dargestellt. Es fehlen nähere Erläuterungen zu den Kategorien der technischen und organisatorischen Maßnahmen. Die Verständlichkeit wird jedoch durch konkrete, praxisnahe Beispiele deutlich gesteigert.

Command-a-03-2025: Es werden nicht alle erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff der technischen und organisatorischen Maßnahmen weder erwähnt noch explizit oder implizit erläutert. Im Rahmen der praktischen Tipps wird lediglich auf einzelne Aspekte wie Datensicherheit, Dokumentation und Schulungen eingegangen, ohne diese als Teil der technischen und organisatorischen Maßnahmen im Sinne der DSGVO einzuordnen. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch deutlich verkürzt dargestellt. Dadurch bleibt das Thema insgesamt unverständlich.

DeepSeek V3: Es werden nicht alle erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff der technischen und organisatorischen Maßnahmen weder erwähnt noch explizit oder implizit erläutert. Im Rahmen der praktischen Tipps wird lediglich auf die Datensicherheit eingegangen, ohne diese als Teil der technischen und organisatorischen Maßnahmen im Sinne der DSGVO einzuordnen. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch deutlich verkürzt dargestellt. Dadurch bleibt das Thema insgesamt unverständlich.

Gemma 3n E2B: Es wird ein überwiegender Teil der erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Der Begriff „Technische und organisatorische Maßnahmen“ wird zwar genannt, jedoch ausschließlich auf Sicherheitsmaßnahmen wie Verschlüsselung und Zugriffskontrollen reduziert. Eine umfassende Darstellung, die auch organisatorische Aspekte und die risikobasierte Auswahl gemäß Art. 32 DSGVO berücksichtigt, fehlt. Ebenso bleibt der Zusammenhang zur DSGVO-Umsetzung sowie die Einordnung von Grundsätzen wie „Privacy by Design“ und „Privacy by Default“ unberücksichtigt. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch deutlich verkürzt dargestellt, was sich negativ auf die Verständlichkeit auswirkt.

GPT-4.1: Es werden nicht alle erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff der technischen und organisatorischen Maßnahmen weder erwähnt noch explizit oder implizit erläutert. Im Rahmen der praktischen Tipps werden zwar einzelne technische und organisatorische Maßnahmen angesprochen (bspw. starke Passwörter nutzen, dienstliche Systeme nutzen), diese werden jedoch nicht als Teil der technischen und organisatorischen Maßnahmen im Sinne der DSGVO eingeordnet. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch so verkürzt, dass das Thema insgesamt unverständlich bleibt.

Grok 3: Es werden nicht alle erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff der technischen und organisatorischen Maßnahmen weder erwähnt noch explizit oder implizit erläutert. Im Rahmen der praktischen Tipps wird lediglich auf die Datensicherheit eingegangen, ohne diese als Teil der technischen und organisatorischen Maßnahmen im Sinne der DSGVO einzuordnen. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch so verkürzt, dass das Thema insgesamt unverständlich bleibt.

LLAMA 4: Es werden nicht alle erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere wird der Begriff der technischen und organisatorischen Maßnahmen weder erwähnt noch explizit oder implizit erläutert. Im Rahmen der praktischen Tipps wird lediglich auf die Datensicherheit eingegangen, ohne diese als Teil der technischen und organisatorischen Maßnahmen im Sinne der DSGVO einzuordnen. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch so verkürzt, dass das Thema insgesamt unverständlich bleibt.

Mistral Medium 3: Es wird ein überwiegender Teil der erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Der Begriff wird zwar nicht explizit erläutert, im Rahmen der praktischen Tipps werden jedoch mehrere typische Maßnahmen angesprochen (z. B. starke Passwörter, Verschlüsselung sensibler Daten, Schulungsteilnahmen). Auch der Grundsatz „Privacy by Default“ wird erwähnt, jedoch ohne Einordnung in den Kontext der technischen und organisatorischen Maßnahmen im Sinne der DSGVO. Da sich aus den genannten Beispielen der thematische Zusammenhang zu den technischen und organisatorischen Maßnahmen auch ohne explizite Begriffsnennung gut erschließen, ist die Darstellung insgesamt vollständiger als bei anderen

4. Gegenüberstellung der Schulungen

Schulungen. Inhaltlich sind die Aussagen richtig, jedoch sehr verkürzt, was sich negativ auf die Verständlichkeit auswirkt.

Qwen 3-235B-A22B-2507: Es wird ein überwiegender Teil der erforderlichen Informationen zu den technischen und organisatorischen Maßnahmen aufgeführt. Der Begriff wird zwar nicht explizit erläutert, im Rahmen der praktischen Tipps werden jedoch mehrere technische und organisatorische Maßnahmen (z. B. starke Passwörter, Verschlüsselung sensibler Daten, Schulungen) genannt und erläutert. Da die Beispiele ein breites Spektrum typischer technischer und organisatorischer Maßnahmen abdecken, ergibt sich der inhaltliche Bezug auch ohne explizite Benennung des Begriffs, sodass die Vollständigkeit im Vergleich zu anderen Formaten höher ausfällt. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch sehr verkürzt, was sich negativ auf die Verständlichkeit auswirkt.

4.9 Datenschutzfolgenabschätzung

Für die Kategorie *Datenschutz-Folgenabschätzung* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Das Instrument der Datenschutz-Folgenabschätzung wird kurz dargestellt, und die Schwelle eines „hohen Risikos“ für die Rechte und Freiheiten betroffener Personen wird benannt.
- **Richtigkeit:** keine pauschalen oder missverständlichen Aussagen, etwa, dass vor jeder Verarbeitung zwingend eine Datenschutz-Folgenabschätzung durchzuführen sei (z. B. Formulierungen wie „Vor der Verarbeitung muss eine Datenschutz-Folgenabschätzung durchgeführt werden“ oder „Führen Sie eine Datenschutz-Folgenabschätzung durch, bevor Sie personenbezogene Daten verarbeiten“).
- **Verständlichkeit:** Nutzung von Beispielen sowie die Berücksichtigung möglicher Lücken oder Fehler in der Darstellung. Zum besseren Verständnis, wenngleich nicht Voraussetzung für die Mindestanforderungen, trägt die Erläuterung des Zwecks der Datenschutz-Folgenabschätzung bei.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zur Datenschutz-Folgenabschätzung wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	-	-	-
Command-a-03-2025	-	-	-
DeepSeek V3	-	-	-
Gemma 3n E2B	Nein	Ja	Nein
GPT-4.1	-	-	-
Grok 3	-	-	-
LLaMA 4	-	-	-
Mistral Medium 3	-	-	-
Qwen 3-235B-A22B-2507	-	-	-

Claude Sonnet 4: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Command-a-03-2025: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

DeepSeek V3: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Gemma 3n E2B: Es werden nicht alle erforderlichen Informationen zur Datenschutzfolgeabschätzung aufgeführt. Es fehlen wesentliche Inhalte; der Begriff wird zwar genannt, jedoch werden weder die Voraussetzungen nach Art. 35 DSGVO noch das Instrument als solches erläutert. Die zur Datenschutzfolgeabschätzung erwähnte Aussage („Maßnahmen zur Vermeidung von Datenschutzverletzungen: Durchführung von Datenschutz-Folgeabschätzungen bei neuen Verarbeitungsvorgängen“) ist inhaltlich korrekt. Mangels weiterer Erläuterung bleibt sie jedoch unverständlich.

GPT-4.1: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Grok 3: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

LLaMA 4: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Mistral Medium 3: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Qwen 3-235B-A22B-2507: Es werden keine Informationen zu der Datenschutzfolgeabschätzung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

4.10 Meldepflichten bei Vorfällen

Für die Kategorie *Meldepflichten bei Vorfällen* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Definition der Datenschutzverletzung sowie Erläuterung, welche Vorfälle gemeldet werden müssen und welche nicht (nicht sämtliche Verletzungen datenschutzrechtlicher Pflichten); Nennung und kurze Beschreibung von Art. 33 und Art. 34 DSGVO, insbesondere der Voraussetzungen „Risiko“ beziehungsweise „hohes Risiko“ und der 72-Stunden-Frist für die Behördenmeldung; interne Prozesse und Ansprechpersonen werden dargestellt (mindestens als Freifelder), und es erfolgt der Hinweis, nicht eigenständig nach außen tätig zu werden.
- **Richtigkeit:** keine Annahme einer pauschalen Meldepflicht.
- **Verständlichkeit:** Nutzung von Praxisbeispielen sowie Berücksichtigung möglicher Lücken oder Fehler.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zu den Meldepflichten bei Vorfällen wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Teilweise	Ja	Teilweise
Command-a-03-2025	-	-	-
DeepSeek V3	Nein	Ja	Nein
Gemma 3n E2B	Nein	Ja	Nein
GPT-4.1	Nein	Ja	Nein
Grok 3	Nein	Ja	Teilweise

4. Gegenüberstellung der Schulungen

LLaMA 4	-	-	-
Mistral Medium 3	Nein	Ja	Nein
Qwen 3-235B-A22B-2507	Nein	Ja	Nein

Claude Sonnet 4: Es wird ein überwiegender Teil der erforderlichen Informationen zur Meldepflicht bei Datenschutzvorfällen aufgeführt. Es fehlt jedoch die Erklärung, was gemeldet werden muss und was nicht; eine Darstellung der Anforderungen aus Art. 33 und Art. 34 DSGVO sowie der ausdrückliche Hinweis, dass externe Meldungen nicht eigenständig vorgenommen werden dürfen. Inhaltlich sind die Aussagen richtig, jedoch durch die fehlenden Inhalte verkürzt. Zu Verständnisproblemen könnte auch führen, dass die 72-Stunden-Frist nicht der Behördenmeldung zugeordnet wurde. Diese Lücken führen zwar nicht zu gravierenden Verständnisproblemen, da Praxisbeispiele und ein interner Meldeweg (wenn auch zu absolut formuliert) und praxisrelevante Beispiele vorhanden sind, jedoch können durch die Lücken Unsicherheiten entstehen, da zwar eine unmittelbare Meldung verlangt wird, aber nicht erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist.

Command-a-03-2025: Es werden keine Informationen zur Meldepflicht bei Vorfällen aufgeführt. Die Pflicht wird weder erwähnt noch explizit oder implizit erläutert.

DeepSeek V3: Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung, der ausdrückliche Hinweis, extern nicht selbst tätig zu werden sowie die Dokumentationspflicht aller Vorfälle. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch stark verkürzt. Interne Prozesse/Ansprechpartner sind nur implizit genannt. Die Lücken können zu erheblichen Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist. Für die Verständlichkeit fehlen ebenso Praxistipps und Beispiele zu Vorfällen.

Gemma 3n E2B: Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung, der ausdrückliche Hinweis, extern nicht selbst tätig zu werden sowie die Dokumentationspflicht aller Vorfälle. Inhaltlich sind die Aussagen – soweit vorhanden – richtig, jedoch stark verkürzt. Interne Prozesse/Ansprechpartner sind nur implizit in den FAQ genannt. Die Lücken können zu erheblichen Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist. Besonders kritisch ist die verkürzende „Definition“ („Verlust oder unrechtmäßiger Zugriff“), weil sie andere Datenschutzverletzungen i. S. d. Art. 4 Nr. 12 DSGVO ausblendet und Mitarbeitende denken könnten, dass nur diese Vorfälle Meldepflichten auslösen. Für die Verständlichkeit fehlen ebenso Praxistipps und Beispiele zu Vorfällen.

GPT-4.1 Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung, der ausdrückliche Hinweis, extern nicht selbst tätig zu werden sowie die

Dokumentationspflicht aller Vorfälle. Interne Prozesse/Ansprechpartner sind nicht genannt. Inhaltlich ist die Aussage richtig, jedoch stark verkürzt. Die Lücken können zu erheblichen Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist. Für die Verständlichkeit fehlen ebenso mehrere Praxistipps und Beispiele zu Vorfällen.

Grok 3: Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung sowie der ausdrückliche Hinweis, dass externe Meldungen nicht eigenständig vorgenommen werden dürfen. Inhaltlich sind die Aussagen richtig, jedoch teilweise verkürzt. Der Hinweis, den Datenschutzbeauftragten zu informieren, ist zu absolut formuliert und kann zu Verständnisproblemen führen. Ebenso können die genannten Lücken teilweise zu Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist.

LLaMA 4: Es werden keine Informationen zur Meldepflicht bei Vorfällen aufgeführt. Die Pflicht wird weder erwähnt noch explizit oder implizit erläutert.

Mistral Medium 3: Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung sowie der ausdrückliche Hinweis, dass externe Meldungen nicht eigenständig vorgenommen werden dürfen. Inhaltlich ist die Aussage richtig, jedoch stark verkürzt. Der Hinweis, den Datenschutzbeauftragten zu informieren, ist zu absolut formuliert und kann zu Verständnisproblemen führen. Die Lücken können zu erheblichen Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist. Für die Verständlichkeit fehlen ebenso Praxistipps und Beispiele zu Vorfällen.

Qwen 3-235B-A22B-2507: Es werden nicht alle erforderlichen Informationen zur Meldepflicht bei Vorfällen aufgeführt. Es fehlen wesentliche Inhalte, insbesondere die Definition und Erklärung einer Datenschutzverletzung, welche hier nur „Verdachtsfall“ genannt wird, sowie die klare Abgrenzung zwischen meldepflichtigen und nicht meldepflichtigen Vorfällen; die Darstellung und Erläuterung der Voraussetzungen von Art. 33 und Art. 34 DSGVO; die Nennung der 72-Stunden-Frist zur Behördenmeldung sowie der ausdrückliche Hinweis, dass externe Meldungen nicht eigenständig vorgenommen werden dürfen. Inhaltlich sind die Aussagen richtig, jedoch verkürzt. Die Lücken können zu erheblichen Verständnisproblemen führen, da zwar eine unmittelbare Meldung verlangt wird, aber weder der Adressat genannt noch erklärt wird, was unter einer „Datenschutzverletzungen“ zu verstehen ist. Für die Verständlichkeit fehlen ebenso mehrere Praxistipps und Beispiele zu Vorfällen.

4.11 Verzeichnis von Verarbeitungstätigkeiten

Für die Kategorie *Verzeichnis von Verarbeitungstätigkeiten* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Erklärung, wann die Pflicht zum Führen eines Verzeichnisses besteht; mindestens beispielhafte Nennung der Mindestangaben nach Art. 30 DSGVO (Zwecke der Verarbeitung, Kategorien personenbezogener Daten, Kategorien von Empfängern, Übermittlungen in Drittländer, Aufbewahrungsfristen sowie technische und organisatorische Maßnahmen).
- **Richtigkeit:** keine falsche Annahme, dass das Verzeichnis fakultativ sei oder nur für bestimmte Unternehmensgrößen erforderlich ist; ebenso falsch ist die Vorstellung, das Verzeichnis ersetze weitere Dokumentationspflichten.
- **Verständlichkeit:** Darstellung ausschließlich im Zusammenhang mit der Rechenschaftspflicht oder in Formulierungen wie „Dokumentieren Sie die Verarbeitung personenbezogener Daten im Verarbeitungsverzeichnis, damit die Dokumentationspflicht erfüllt wird“ kann den Eindruck erwecken, dass dies alles sei, was dokumentiert werden muss; solche Darstellungen bergen Verständnisprobleme. Lücken und Fehler in der Erklärung werden ebenfalls berücksichtigt.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zum Verzeichnis von Verarbeitungstätigkeiten wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	-	-	-
Command-a-03-2025	Teilweise	Ja	Teilweise
DeepSeek V3	-	-	-
Gemma 3n E2B	Teilweise	Ja	Teilweise
GPT-4.1	-	-	-
Grok 3	-	-	-
LLaMA 4	-	-	-
Mistral Medium 3	Teilweise	Ja	Teilweise
Qwen 3-235B-A22B-2507	-	-	-

Claude Sonnet 4: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert. Die Schulung erklärt zwar allgemein, dass Organisationen die DSGVO-Einhaltung nachweisen und dokumentieren müssen, bleibt dabei jedoch so unspezifisch, dass das Verzeichnis als konkretes Instrument nicht erkennbar wird. Die Ausführungen beziehen sich wohl eher auf die Rechenschaftspflicht im Allgemeinen.

Command-a-03-2025: Dokumentation: Es wird ein überwiegender Teil der erforderlichen Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Es fehlen die ausdrückliche Benennung von Art. 30 DSGVO sowie beispielhafte Mindestinhalte. Die Aussage „Dokumentieren Sie alle Verarbeitungstätigkeiten und halten Sie diese Dokumentation stets aktuell“ ist zwar nicht falsch, bleibt jedoch zu allgemein und kann zu dem Missverständnis führen, dass eine generische Dokumentation das Verzeichnis von Verarbeitungstätigkeiten ersetze. Kurze Beispiele oder eine Feldliste zum Verzeichnis von Verarbeitungstätigkeiten hätten die Verständlichkeit erhöht.

DeepSeek V3: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Gemma 3n E2B: Es wird ein überwiegender Teil der erforderlichen Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Es fehlen jedoch die ausdrückliche Benennung von Art. 30 DSGVO sowie beispielhafte Mindestinhalte. Inhaltlich sind die Aussagen richtig, aber ungenau. Die Darstellung kann zu dem Missverständnis führen, die generische „Dokumentation der Verarbeitung“ reiche zur Erfüllung der Anforderungen

an das Verzeichnis von Verarbeitungstätigkeiten aus. Kurze Beispiele oder eine Feldliste zum Verzeichnis von Verarbeitungstätigkeiten hätten die Verständlichkeit erhöht.

GPT-4.1: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Grok 3: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert. Die Schulung erklärt zwar allgemein, dass Organisationen die DSGVO-Einhaltung nachweisen und dokumentieren müssen, bleibt dabei jedoch so unspezifisch, dass das Verzeichnis nicht erkennbar wird. Die Ausführungen beziehen sich wohl eher auf die Rechenschaftspflicht im Allgemeinen.

LLaMA 4: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Mistral Medium 3: Es wird ein überwiegender Teil der erforderlichen Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Es fehlt die ausdrückliche Benennung von Art. 30 DSGVO sowie beispielhafte Mindestinhalte. Die Aussage „Dokumentieren Sie alle Verarbeitungstätigkeiten und halten Sie diese Dokumentation stets aktuell“ ist nicht falsch, bleibt jedoch zu allgemein und kann zu dem Missverständnis führen, dass eine generische Dokumentation das Verzeichnis von Verarbeitungstätigkeiten ersetze. Kurze Beispiele oder eine Feldliste zum Verzeichnis von Verarbeitungstätigkeiten hätten die Verständlichkeit erhöht.

Qwen 3-235B-A22B-2507: Es werden keine Informationen zum Verzeichnis von Verarbeitungstätigkeiten aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert. Die Schulung erklärt zwar, dass Organisationen nachweisen müssen, dass sie die DSGVO einhalten, und weist in diesem Zusammenhang auch auf die erforderliche Dokumentation hin. Allerdings wird das Verzeichnis von Verarbeitungstätigkeiten in diesem Zusammenhang nicht erwähnt.

4.12 Drittstaatenübermittlungen

Für die Kategorie *Drittstaatenübermittlungen* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Erwähnung, dass die Übermittlung personenbezogener Daten in Drittstaaten, also in Staaten außerhalb der Europäischen Union, nur unter bestimmten Voraussetzungen zulässig ist.
- **Richtigkeit:** keine pauschalen Aussagen, dass Standardvertragsklauseln stets genügen.
- **Verständlichkeit:** Nutzung von Beispielen; Berücksichtigung möglicher Lücken oder Fehler in der Darstellung.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zur Drittstaatenübermittlungen wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	-	-	-
Command-a-03-2025	-	-	-
DeepSeek V3	-	-	-
Gemma 3n E2B	-	-	-
GPT-4.1	-	-	-

4. Gegenüberstellung der Schulungen

Grok 3	-	-	-
LLaMA 4	-	-	-
Mistral Medium 3	-	-	-
Qwen 3-235B-A22B-2507	-	-	-

Claude Sonnet 4: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Command-a-03-2025: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

DeepSeek V3: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Gemma 3n E2B: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

GPT-4.1: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Grok 3: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

LLaMA 4: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Mistral Medium 3: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Qwen 3-235B-A22B-2507: Es werden keine Informationen zur Drittstaatenübermittlung aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

4.13 Sanktionen bei Verstößen

Für die Kategorie *Sanktionen bei Verstößen* wurde insbesondere auf folgende Kriterien geachtet:

- **Vollständigkeit:** Erwähnung, dass Verstöße gegen datenschutzrechtliche Vorgaben Sanktionen nach sich ziehen können, mindestens die Nennung von Bußgeldern.
- **Richtigkeit:** keine falsche Angabe von Bußgeldhöhen.
- **Verständlichkeit:** Es darf nicht der Eindruck entstehen, dass Bußgelder den Mitarbeitenden persönlich drohen; praxisnahe Beispiele im Sinne von „Was kann passieren?“ werden genutzt. Mögliche Lücken oder Fehler in der Darstellung werden berücksichtigt. Zum besseren Verständnis, wenngleich nicht Voraussetzung für die Mindestanforderungen, können weitere Sanktionen wie Schadensersatzansprüche erläutert werden.

Auf Basis dieser Kriterien sind die KI-generierten Inhalte zur Sanktionen bei Verstößen wie folgt zu bewerten:

Modelle	Vollständig?	Richtig?	Verständlich?
Claude Sonnet 4	Ja	Ja	Teilweise
Command-a-03-2025	Ja	Ja	Teilweise

DeepSeek V3	Ja	Ja	Teilweise
Gemma 3n E2B	-	-	-
GPT-4.1	Ja	Ja	Teilweise
Grok 3	Ja	Ja	Teilweise
LLaMA 4	-	-	-
Mistral Medium 3	-	-	-
Qwen 3-235B-A22B-2507	Ja	Ja	Ja

Claude Sonnet 4: Es werden alle erforderlichen Informationen zu Sanktionen bei Verstößen genannt. Die Inhalte sind richtig, aber verkürzt. Es fehlt die explizite Adressatenklärstellung. Dies hat teilweise Auswirkungen auf die Verständlichkeit, weil ohne Adressat der Eindruck entstehen kann, Bußgelder trafen Mitarbeitende. Beispiele am Ende würden die Einordnung verbessern

Command-a-03-2025: Es werden alle erforderlichen Informationen genannt. Die Inhalte sind richtig, aber verkürzt. Es fehlt die explizite Adressatenklärstellung. Dies hat teilweise Auswirkungen auf die Verständlichkeit, weil ohne Adressat der Eindruck entstehen kann, Bußgelder trafen Mitarbeitende. Beispiele am Ende würden die Einordnung verbessern

DeepSeek V3: Es werden alle erforderlichen Informationen genannt. Die Inhalte sind richtig, aber verkürzt. Es fehlt die explizite Adressatenklärstellung. Dies hat teilweise Auswirkungen auf die Verständlichkeit, weil ohne Adressat der Eindruck entstehen kann, Bußgelder trafen Mitarbeitende. Beispiele am Ende würden die Einordnung verbessern.

Gemma 3n E2B: Es werden keine Informationen zu Sanktionen bei Verstößen aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

GPT-4.1: Es werden alle erforderlichen Informationen genannt. Die Inhalte sind richtig, jedoch verkürzt. Es fehlt die explizite Adressatenklärstellung. Dies hat teilweise Auswirkungen auf die Verständlichkeit, weil ohne Adressat der Eindruck entstehen kann, Bußgelder trafen Mitarbeitende. Beispiele am Ende würden die Einordnung verbessern

Grok 3: Es werden alle erforderlichen Informationen genannt. Die Inhalte sind richtig, aber verkürzt. Es fehlt die präzise Adressatenklärstellung; „rechtliche Konsequenzen“ bleibt unscharf. Dies hat teilweise Auswirkungen auf die Verständlichkeit. Beispiele am Ende würden helfen, die Folgen adressatengerecht zu verorten.

LLaMA 4: Es werden keine Informationen zu Sanktionen bei Verstößen aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Mistral Medium 3: Es werden keine Informationen zu Sanktionen bei Verstößen aufgeführt. Der Begriff wird weder erwähnt noch explizit oder implizit erläutert.

Qwen 3-235B-A22B-2507: Es werden alle erforderlichen Informationen genannt. Die Inhalte sind richtig, aber verkürzt, was vorliegend jedoch keine große Auswirkung auf die Verständlichkeit des Themas hat. Zwar bleibt der Hinweis auf „persönliche Konsequenzen für Mitarbeitende“ ohne nähere Einordnung, dennoch wird damit zutreffend auf die Unterscheidung zwischen persönlicher Haftung von Mitarbeitenden und der Haftung des Unternehmens bei DSGVO-Verstößen hingewiesen. Dadurch wird das Thema adressatengerecht verdeutlicht und trägt zur Verständlichkeit bei. Ein konkretes Beispiel am Ende hätte die Einordnung zusätzlich erleichtert.

4.14 Didaktische Qualität und Aufbau

Nachdem alle dreizehn Kategorien des inhaltlichen Mindeststandards einzeln bewertet wurden, ist ein weiterer Aspekt zu betrachten, der bislang bewusst nicht einbezogen wurde: Die didaktische Qualität und der Aufbau der Schulung. Diese Dimension wurden bisher nicht betrachtet, weil sie nicht zu den inhaltlichen Mindestanforderungen zählt, gleichwohl aber maßgeblich bestimmt, wie gut die Inhalte vermittelt werden.

Eine Schulung kann inhaltlich korrekt und vollständig sein, verliert aber deutlich an Verständlichkeit und Nutzen, wenn insbesondere Aufbau, roter Faden, Visualisierung, Praxisnähe oder Interaktionsmöglichkeiten fehlen oder unzureichend ausgearbeitet sind.³⁶ Anschauliche Darstellungen, eine klare Struktur, praxisnahe Beispiele sowie kurze Quiz- oder Anwendungsaufgaben erleichtern es Mitarbeitenden, Zusammenhänge zu erkennen und das Gelernte im Arbeitsalltag anzuwenden.

Vor diesem Hintergrund erfolgt nun eine übergreifende Bewertung der didaktisch-methodischen Gestaltung der Schulungen. Berücksichtigt wurden unter anderem Struktur und roter Faden, die Ansprache der Mitarbeitenden, Visualisierung, Praxisnähe, Interaktivität wie Quiz- oder Transferaufgaben sowie gestalterische Elemente, die die Orientierung unterstützen.

Begründungen der didaktischen Bewertung:

Claude Sonnet 4: Die Schulung ist klar entlang der Struktur der DSGVO aufgebaut und durchgehend logisch gegliedert. Lernziele, Praktische „Do's and Don'ts“, häufige Fragen und Antworten, ein motivierender Abschlusssteil sowie wichtige Kontaktinformationen mit individuell anpassbaren Platzhaltern und ein Selbsttest sind enthalten. Die Sprache ist adressatengerecht und verständlich, die direkte Ansprache unterstützt die Aktivierung der Mitarbeitenden. Visuelle Elemente wie Icons und optische Hervorhebungen steigern die Lesbarkeit. Der Praxisbezug ist im Aufbau erkennbar und methodisch gut eingebettet.

Command-a-03-2025: Die Schulung folgt einem systematischen Aufbau entlang der DSGVO und verwendet eine klare, adressatengerechte Sprache. Teilweise erfolgt eine direkte Ansprache der Mitarbeitenden. Abschnitte zur praktischen Umsetzung und Transferaufgaben erleichtern die Anwendung des Gelernten im Arbeitsalltag. Ein Selbsttest zur Lernkontrolle ist enthalten, jedoch ohne Lösungshinweise. Eine abschließende Zusammenfassung unterstützt die Wiederholung.

DeepSeek V3: Die Schulung weist eine strukturierte Gliederung anhand der DSGVO – teilweise im Tabellenformat – auf. Sie verwendet eine verständliche und adressatengerechte Sprache. Teilweise erfolgt eine direkte Ansprache der Mitarbeitenden. Abschnitte zur Anwendung im Arbeitskontext sind vorhanden, jedoch nicht konsequent integriert. Eine Zusammenfassung rundet die Einheit ab, der Abschnitt zu wichtigen Kontakten bleibt allerdings ohne Freitextfeld. Kritisch ist, dass die Verbindung zwischen theoretischen Grundlagen und Transferabschnitten nicht durchgängig hergestellt wird, wodurch der Lernfluss gelegentlich abreißt.

Gemma 3n E2B: Die Schulung ist strukturiert entlang der DSGVO aufgebaut. Lernziele und geschätzte Bearbeitungsdauer werden zu Beginn genannt, was zur Orientierung beiträgt. Abschnitte zur Umsetzung im Arbeitskontext (FAQ mit individuellen Anpassungsmöglichkeiten) fördern den Transfer. Sie verwendet eine verständliche und adressatengerechte Sprache. Teilweise erfolgt eine direkte Ansprache der Mitarbeitenden.

³⁶ Mandl/Kopp, in Nuissl: Vom Lernen zum Lehren, S. 118 ff.; Arnold, in Arnold/Nuissl/Schrader: Wörterbuch Erwachsenen- und Weiterbildung.

GPT-4.1: Die Schulung ist strukturiert entlang der DSGVO aufgebaut, mit klar definierten Lernzielen und Angabe der Dauer. Sie verwendet eine verständliche und adressatengerechte Sprache. Teilweise erfolgt eine direkte Ansprache der Mitarbeitenden. Einzelne Abschnitte zur Umsetzung im Arbeitskontext sowie „Do's and Don'ts“ fördern den Transfer. Ein Wissenstest mit Lösungsmöglichkeiten ermöglicht die Selbstkontrolle. Eine abschließende Zusammenfassung unterstützt die Wiederholung. Die gesamte Schulung wirkt dabei jedoch sehr überblicks- und stichpunktartig.

Grok 3: Die Schulung folgt einer klaren Gliederung und adressatengerechten Sprache. Teilweise erfolgt eine direkte Ansprache der Mitarbeitenden. Abschnitte zur Anwendung im Arbeitskontext sind vorhanden, jedoch nicht konsequent integriert. Eine Zusammenfassung und Checkliste am Ende runden die Schulung ab.

LLaMA 4: Die Schulung nutzt eine adressatengerechte, teilweise direkte Ansprache, bleibt aber didaktisch weit hinter den Anforderungen zurück. Die Trennung zwischen Theorie („Grundlagen“) und Praxis („Relevanz“) führt zu einer wenig verbundenen Darstellung ohne roten Faden. Zudem treten inkonsistente Begrifflichkeiten auf, der angekündigte interaktive Elemente (Test) fehlen.

Mistral Medium 3: Die Schulung folgt einer klaren Struktur entlang der DSGVO und bietet praxisnahe Umsetzungshinweise. Es fehlen jedoch interaktive Elemente wie Kontrollfragen oder Reflexionsaufgaben, wodurch der Lernprozess rein informativ bleibt. Ein motivierender Einstieg, etwa über die Frage „Warum betrifft mich das?“, ist nicht vorhanden. Viele Aussagen bleiben allgemein, ohne klare Handlungsanweisungen oder praxisnahe Szenarien.

Qwen 3-235B-A22B-2507: Die Schulung ist sehr klar und lernorientiert anhand der DSGVO aufgebaut. Lernziele und Bearbeitungsdauer werden angegeben. Durch direkte Ansprache, Do's and Don'ts, ein strukturierter Praxisbezug im Aufbau, Merksätze, Icons gelingt eine anschauliche und praxisnahe Vermittlung. Eine Wissensüberprüfung mit Lösungen fördert den Transfer. Icons, optische Hervorhebungen und teilweise Tabellenformate steigern die Lesbarkeit.

5. Gesamtvergleich der Schulungen

Um die Ergebnisse der zuvor dargestellten Einzelauswertungen in einen übergeordneten Zusammenhang stellen zu können, werden im Folgenden alle Bewertungen zusammengeführt und modellübergreifend analysiert.

5.1 Quantitative Auswertung

Die Bewertung der einzelnen Kategorien hinsichtlich „Vollständigkeit, Richtigkeit und Verständlichkeit“ der für eine Datenschutzschulung erforderlichen Mindestinhalte sowie die didaktische Qualität zeigt, dass alle KI-generierten Schulungen Schwachstellen aufweisen. Das Spektrum reicht von inhaltlichen Ungenauigkeiten über thematische Lücken und missverständliche Darstellungen bis hin zu gänzlich fehlenden Inhalten.

Um einen Gesamteindruck der neun KI-generierten Datenschutzschulung zu gewinnen und die neun KI-Modelle systematisch miteinander vergleichen zu können, wurden die Ergebnisse der drei Leitfragen „Vollständigkeit, Richtigkeit und Verständlichkeit“ in den

jeweiligen Kategorien für jedes KI-Modell zusammengeführt. Grundlage der Bewertung sind dreizehn Kategorien, die die inhaltlichen Mindestanforderungen, die eine DSGVO-Schulung abdecken muss, beschreiben. Jedes der neun KI-Modelle wurde in jeder dieser dreizehn Kategorien im Hinblick auf die jeweils einschlägigen Bewertungskriterien beurteilt. Die Erfüllung dieser Bewertungskriterien wurde jeweils mit „Ja“, „Teilweise“, „Nein“ oder „(–)“ beantwortet, wobei „(–)“ bei der Gesamtbetrachtung wie „Nein“ gewertet wurde. Da alle drei Leitfragen auf dieselben dreizehn Kategorien angewandt wurden, ergibt sich für jede dieser Bewertungsdimensionen ein fester Nenner von dreizehn. Die für ein Modell vergebenen Antworten wurden anschließend zusammengezählt und zu einer Gesamtdarstellung pro Leitfrage zusammengeführt.³⁷

Die Antworten auf die drei Leitfragen „Vollständigkeit, Richtigkeit und Verständlichkeit“ wurden mithilfe eines einheitlichen Ampelsystems eingeordnet. Für jede der drei Kategorien gilt jeweils:

- Grün: mindestens 11x „Ja“ ($\geq 84,62\%$)
- Gelb: mindestens 5x „Ja“ ($\geq 38,46\%$) oder mindestens 7x „Ja + Teilweise“ ($\geq 53,85\%$)
- Rot: höchstens 4x „Ja“ ($\leq 30,77\%$) und höchstens 6x „Ja + Teilweise“ ($\leq 46,15\%$)

Die *didaktische Qualität* wird im Rahmen dieser Zusammenfassung nicht über die gleiche Berechnungssystematik ermittelt. Sie wurde bereits im vorherigen Kapitel eigenständig und qualitativ bewertet, da sie nicht zu den inhaltlichen Mindestanforderungen gehört. Didaktische Aspekte wie Struktur, roter Faden, Visualisierung, Praxisnähe, Interaktivität und unmittelbare Anwendbarkeit im Arbeitsalltag lassen sich nicht sinnvoll über die Leitfragen „Ja/Teilweise/Nein“ abbilden. Die didaktische Bewertung wird daher lediglich als zusammenfassendes Ergebnis in die abschließende Ampelübersicht übernommen, steht methodisch aber eigenständig neben der quantitativen Bewertung der dreizehn Kategorien.

Die folgende tabellarische Gegenüberstellung enthält daher vier Elemente pro KI-Modell: Vollständigkeit, Richtigkeit, Verständlichkeit und – als gesondert ermitteltes, bereits im vorherigen Kapitel begründetes Ergebnis – didaktische Qualität.

Modelle	Vollständigkeit	Richtigkeit	Verständlichkeit	Didaktische Qualität
Claude Sonnet 4	●	●	●	●
Command-a-03-2025	●	●	●	●
DeepSeek V3	●	●	●	●
Gemma 3n E2B	●	●	●	●
GPT-4.1	●	●	●	●
Grok 3	●	●	●	●
LLaMA 4	●	●	●	●
Mistral Medium 3	●	●	●	●
Qwen 3-235B-A22B-2507	●	●	●	●

³⁷ Zu den detaillierten Einzelauswertungen der Modelle, siehe Anhang.

5.2 Qualitative Einordnung

Das Ergebnisse des Gesamtvergleichs zeigt, dass keine der geprüften KI-generierten Datenschutzschulungen in allen Kategorien vollständig überzeugen konnte. Im Gesamtergebnis liegt der Mittelwert der Ampelbewertung über alle dreizehn Bewertungskategorien hinweg deutlich im gelben Bereich. Keine Schulung erreichte in einem der drei Hauptkriterien (Vollständigkeit, Richtigkeit und Verständlichkeit) die grüne Stufe. Rund zwei Drittel aller Bewertungen lagen im mittleren Bereich (Gelb), das restliche Drittel im roten Bereich. Die inhaltliche Analyse offenbart wiederkehrende Schwachstellen. Am häufigsten beanstandet wurden fehlende oder nur rudimentäre Definitionen zentraler Grundbegriffe der DSGVO, verkürzte oder unverbundene Erläuterungen, fehlende Herleitungen, Passagen auf Stichwortniveau sowie Brüche zwischen Theorie und Praxis. Teilweise zeigte sich auch eine inkonsistente Begriffsnutzung. Diese Mängel beeinträchtigen die Verständlichkeit und begünstigen Fehlinterpretationen.

Eine Ausnahme bildet die didaktische Gestaltung. Drei von neun Schulungen weisen eine gelungene didaktische Aufbereitung auf und wurden insoweit „grün“ bewertet. Da jedoch Vollständigkeit, Richtigkeit und teilweise auch Verständlichkeit überwiegend nur gelb oder rot ausfallen, relativiert sich dieser Vorteil für die Schulungstauglichkeit insgesamt.

Die Gesamtbewertungen zeigen, dass die KI-Modelle hinsichtlich zweier Leitfragen – Richtigkeit und Verständlichkeit – weitestgehend mittelmäßig abschneiden, während die Vollständigkeit der Schulungsinhalte deutlich zurückfällt. Richtigkeit und Verständlichkeit erreichen jeweils rund 89 % gelbe Bewertungen, die Vollständigkeit erreicht hingegen nur 56 % gelbe Bewertungen. Die KI-Modelle liefern also mehrheitlich überwiegend richtige und verständliche Inhalte, verfehlen aber häufig die strukturelle Abdeckung aller erforderlichen Mindestinhalte.

Die Verteilung der Ampelwerte zeigt zudem, in welchen Bereichen KI-generierte Schulungen die gravierendsten Risiken bergen. Besonders deutlich wird hier erneut die Vollständigkeit: 44 % der Bewertungen fallen in den roten Bereich, während Richtigkeit und Verständlichkeit mit jeweils lediglich 11 % rotem Bereich deutlich risikoärmer sind. Das zentrale Problem KI-generierter Datenschutzschulungen liegt damit nicht in der fachlichen Unrichtigkeit, sondern im Weglassen relevanter Inhalte. Die Betrachtung der Ergebnistabilität stützt diese Einschätzung zusätzlich. Richtigkeit und Verständlichkeit verlaufen nahezu parallel (je 8 × Gelb, 1 × Rot). Dieses Muster zeigt, dass Modelle, die fachlich überwiegend korrekte Inhalte liefern, diese in der Regel auch verständlich formulieren. Umgekehrt tritt kein Fall auf, in dem ein Modell inhaltlich zutreffend, aber unverständlich wäre. Die Stabilität der beiden Kriterien unterstreicht somit, dass das Hauptdefizit nicht in der sprachlichen oder didaktischen Umsetzung liegt, sondern in der strukturellen Tiefe und Abdeckung der Inhalte.

Darüber hinaus zeigt sich ein in den Ergebnissen angelegter Zusammenhang zwischen inhaltlicher Qualität und didaktischer Aufbereitung. Modelle, die in den drei Leitfragen überwiegend vollständig, richtig und verständlich abschneiden, erzielen häufig auch eine höhere bis gute didaktische Qualität. Umgekehrt fällt bei Modellen, die bereits erhebliche inhaltliche Lücken oder Unstimmigkeiten aufweisen, regelmäßig auch die didaktische Bewertung schwächer aus. Insgesamt weist der Befund darauf hin, dass eine didaktisch überzeugende Schulung ohne eine gewisse inhaltliche Qualität kaum erreichbar ist: Erst wenn ein Modell die Mindestinhalte weitgehend abdeckt und richtig sowie verständlich darstellt, entsteht auch didaktisch ein tragfähiger Gesamteindruck.

Schließlich lohnt ein Blick darauf, inwieweit qualitativ problematische Bereiche gehäuft auftreten. Hier zeigt sich ein differenziertes Bild: Nur ein Modell (LLaMA 4) weist gleichzeitig mehrere rote Bereiche auf, während die übrigen Modelle ausschließlich punktuell scheitern. Die Mehrheit der Systeme zeigt also keine systematische Schwäche in mehreren Kriterien gleichzeitig, sondern verfehlt nur einzelne Anforderungen. Dies bestätigt das zentrale Muster des Modellvergleichs: Die KI-Systeme liefern weder durchgehend schlechte noch überwiegend hervorragende Ergebnisse, sondern ein durchweg mittleres Leistungsniveau mit klar erkennbaren strukturellen Lücken.

Diese Beobachtung markiert eine strukturelle Grenze der aktuell verfügbaren generativen KI-Systeme: Sie erzeugen zwar überwiegend brauchbare Inhalte (gelber Bereich), erreichen jedoch in keiner Dimension ein exzellentes Niveau (grüner Bereich).

6. Diskussion

Der übergeordnete Vergleich hat gezeigt, dass keine der Schulungen allein dazu geeignet ist, fehlerfrei, vollständig und unmissverständlich zum Datenschutz zu schulen. Die KI-generierten Schulungsinhalte sind zwar teilweise dazu geeignet ein solides Basiswissen zur DSGVO zu vermitteln, sie erfüllen jedoch wegen unvollständiger Darstellungen, begrifflicher Unschärfen und fehlendem Praxisbezug weitgehend nicht die Anforderungen an eine vollumfängliche Schulung. Wenn auch keine der KI-generierten Datenschutzschulung zu einem insgesamt guten Ergebnis gekommen ist, stellt sich dennoch die Frage, ob und unter welchen Voraussetzungen KI-generierte Schulungen juristische Expertise ersetzen oder ergänzen können.

6.1 Risikobasierter Ansatz und Qualitätsanforderungen nach DSGVO

Entscheidend ist die Frage, welches Qualitätsniveau die DSGVO für Datenschutzschulungen verlangt. Nach Art. 24 Abs. 1 DSGVO haben Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um die DSGVO-Konformität sicherzustellen und nachweisen zu können; hierzu gehört – jedenfalls implizit – die Schulung der Mitarbeitenden im Bereich des Datenschutzes.³⁸

Entlang des risikobasierten Ansatzes der DSGVO richtet sich das geforderte Qualitätsniveau der Schulung folglich nach dem im Einzelfall bestehenden Risiko für die Rechte und Freiheiten betroffener Personen. Je höher die Eintrittswahrscheinlichkeit und Schwere eines möglichen Schadens für die betroffene Person (Risiko), desto höher muss der Schutz durch technische und organisatorische Maßnahmen ausfallen.³⁹

Für Datenschutzschulungen bedeutet das konkret, dass KI-generierte Schulungen in risikobehafteten Umgebungen allein keinesfalls genügen. Hier sind eine fachliche Prüfung, Anpassung und gegebenenfalls Ergänzung zwingend erforderlich. In kleinen Organisationen mit seltenen, überschaubaren und risikoarmen Datenverarbeitungsvorgängen (z. B. in Handwerksbetrieben oder Vereinen) können KI-

³⁸ Enzmann/Selzer/Stummer, EuDIR 2025, 270 (270); Martini, in: Paal/Pauly, DSGVO/BDSG, Art. 24 Rn. 22; Hartung, in: in Kühling/Buchner, DSGVO/BDSG, Art. 25 Rn. 16; Jandt, in: in Kühling/Buchner, DSGVO/BDSG, Art. 32 Rn. 88.

³⁹ Selzer, EDPL 2021, 120 (120).

generierte Schulungen dagegen – nach inhaltlicher Prüfung und punktueller Anpassung – eine geeignete und verhältnismäßige Maßnahme darstellen.⁴⁰

6.2 Differenzierte Eignung nach Organisationsgröße und Risiko

Da die Untersuchungsergebnisse jedoch zeigen, dass KI-generierte Schulungen relevante Inhalte auslassen und Fehler enthalten, die zu Missverständnissen führen können, ist eine eigene Qualitätssicherung der KI-generierten Schulungsinhalte unerlässlich – auch in kleinen Organisationen mit nur wenigen und risikoarmen Verarbeitungen. Diese Nacharbeiten setzen sowohl datenschutzrechtliches Know-how als auch personelle Ressourcen voraus und können auch nur eingeschränkt von anderen KI-Modellen übernommen werden.⁴¹ Insofern wird die anfängliche Zeit- und Kosteneinsparung durch den Aufwand der fachlichen Prüfung und Anpassung zum Teil wieder aufgewogen.

Fraglich ist vor diesem Hintergrund, ob es für KI-generierte Datenschutzschulungen überhaupt eine sinnvolle Anwendung gibt. So existieren auch kostenfreie Online-Schulungen – etwa das Schulungsangebot des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Entsprechende Grundlagenschulungen decken mit den dieser Untersuchung zugrundeliegenden 13 Kategorien nicht nur den datenschutzrechtlichen Grundbedarf ab, sondern sind auch institutionell abgesichert und durch regelmäßige Aktualisierungen auf dem aktuellen Stand. Dabei werden die einzelnen Themen in der für Grundlagenschulungen üblichen Tiefe adressiert – zum Teil sogar ausführlicher als in den verschiedenen KI-generierten Schulungen. Zudem ist die inhaltliche Qualität kostenloser Schulungsangebote regelmäßig höher als die der untersuchten KI-generierten Schulungen. Entsprechende kostenlose kuratierte Angebote stellen gegenüber KI-generierten Datenschutzschulungen also grundsätzlich die wirtschaftlichere und rechtssicherere Lösung dar, insbesondere für Organisationen ohne eigene Datenschutzexpertise, bei denen i. d. R. auch kein großer organisationsspezifischer Anpassungsbedarf besteht.

Sofern Organisationen dennoch auf KI-generierte Datenschutzschulungen zurückgreifen möchten, ggf. auch nur in Ergänzung zu den kostenlosen Einstiegsangeboten (etwa, um bestimmte, für die Organisation besonders relevante Inhalte tiefergehend zu betrachten), setzt der Einsatz entsprechender KI-generierter Inhalte voraus, dass es sich um eine sehr kleine Organisation mit geringem und unkritischem Verarbeitungsvolumen handelt. Die Begründung hierfür liegt in der Verhältnismäßigkeitsabwägung zwischen dem Schulungsaufwand und dem tatsächlichen Risiko: Bei risikoarmen Verarbeitungstätigkeiten kann neben kostenlosen kuratierten Angeboten auch eine KI-gestützte Grundlagenschulung ohne eigene Datenschutzexpertise eine verhältnismäßige Maßnahme darstellen. Bei sehr geringem Verarbeitungsrisiko – etwa, wenn nur Kontaktdaten weniger Kunden verarbeitet werden, keine sensiblen Daten vorliegen und die Verarbeitungsprozesse einfach sind – reicht eine Sensibilisierung der Mitarbeitenden für datenschutzrechtliche Grundfragen aus. Dies können die meisten der in dieser Studie untersuchten KI-Chatbots grundsätzlich leisten. Kostenlose kuratierte Angebote sind hier zwar strukturell die sicherere Wahl, da sie inhaltlich geprüft sind. Wenn jedoch eine stärkere Anpassung an die spezifischen Gegebenheiten des Kleinstunternehmens gewünscht ist und die Kosten für eine externe Anpassung unverhältnismäßig wären, kann alternativ oder ergänzend eine KI-generierte Datenschutzschulung genutzt werden,

⁴⁰ So bereits Selzer, EDPL 2021, 120 (120); Enzmann/Selzer/Stummer, EuDIR 2025, 270 (271); Selzer/Kurchyna/Berndt/Timm, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten, 53 (64); Selzer/Berndt/Timm, DuD 2025, 539.

⁴¹ Enzmann/Selzer/Stummer, EuDIR 2025, 270 (271).

sofern eine bestmögliche Qualitätskontrolle durch die Unternehmensleitung erfolgt. Diese Lösung ist allerdings nur dann datenschutzrechtlich und betriebswirtschaftlich tragfähig, wenn die Kosteneinsparung nicht im Missverhältnis zum erforderlichen Anpassungsbedarf steht.⁴²

Für Organisationen mit vorhandener Datenschutzexpertise kann KI dagegen lediglich als Beschleuniger bei der Erstellung individualisierter Schulungsmaterialien dienen, insbesondere wenn sie durch gezielte Arbeitsaufträge auf die jeweiligen Anforderungen zugeschnitten werden. Hier liegt der Mehrwert nicht in der vollständigen Automatisierung, sondern in der Effizienzsteigerung bei der Erstellung von Rohentwürfen, die anschließend fachlich überarbeitet und an die spezifischen organisatorischen Gegebenheiten angepasst werden. Diese Vorgehensweise ist sowohl aus betriebswirtschaftlicher als auch aus datenschutzrechtlicher Verhältnismäßigkeitsperspektive sinnvoll: Da die erforderliche Datenschutzexpertise bereits im Haus vorhanden ist, können die Kosten für externe kommerzielle Schulungsangebote eingespart oder reduziert werden, während gleichzeitig eine individualisierte, auf die Organisation zugeschnittene Schulung erstellt wird. Allerdings ist zu berücksichtigen, dass für die fachliche Prüfung, Berichtigung und Anpassung der KI-generierten Inhalte ein nicht unerheblicher Zeitaufwand einzuplanen ist.

Für große Unternehmen mit meist komplexen Abläufen und höherem Risiko eignen sich KI-generierte Datenschutzschulungen nicht als alleinige Lösung, denn die dort erforderliche Tiefe, Präzision und Aktualität lässt sich – Stand heute – mit KI-generierten Inhalten nicht verlässlich sicherstellen. Hinzu kommt, dass bereits geringfügige inhaltliche Ungenauigkeiten oder unvollständige Darstellungen in sensiblen Bereichen – etwa bei Beschäftigtendaten – zu fehlerhaften Rechtsanwendungen und damit zu Datenschutzverstößen führen können. Ebenso benötigen große Organisationen regelmäßig differenzierte Schulungskonzepte, die an Rollen, Prozesse und Systeme sowie an unterschiedliche Abteilungen und Bereiche angepasst sind und laufend aktualisiert werden können. Aus Verhältnismäßigkeitsperspektive ist hier der Einsatz professioneller kommerzieller Schulungsangebote oder die Entwicklung individuell zugeschnittener Schulungskonzepte durch interne oder externe Datenschutzexpertise geboten, da das hohe Verarbeitungsrisiko entsprechend umfassende und qualitätsgesicherte Maßnahmen erfordert. KI-generierte Datenschutzschulungen können die erforderliche Tiefe, Präzision und rollenspezifische Differenzierung – Stand heute – nicht als alleinige Lösung gewährleisten, zumal der Aufwand für eine vollständige fachliche Überarbeitung den Kostenvorteil eliminieren würde. Sie können daher allenfalls unterstützend bei der Erstellung von Entwürfen eingesetzt werden.

Insgesamt zeigt sich, dass KI-generierte Datenschutzschulungen i. d. R. nicht dazu geeignet sind professionelle Schulungsangebote und juristische Expertise zu ersetzen. Potenzial haben KI-generierte Schulungsinhalte jedoch überall dort, wo sie ergänzend eingesetzt werden, um z. B. bestimmte Inhalte vertieft darzustellen oder eine Ausgangsbasis für Konkretisierungen zu bieten. An diesen Stellen haben KI-generierte Schulungsinhalte das Potenzial, die Effizienz zu steigern und den Erstellungsaufwand zu reduzieren. KI-generierte Inhalte sind jedoch stets zu prüfen, auf ihre Eignung für die jeweilige Organisation zu validieren und ggf. um organisationsspezifische Aspekte zu ergänzen. Eine vollständige Automatisierung des Schulungsprozesses ist weder rechtlich noch praktisch angezeigt.

⁴² So auch schon: *Enzmann/Selzer/Stummer*, EuDIR 2025, 270 (270); *Selzer/Kurchyna/Berndt/Timm*, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten, 53 (64); *Selzer/Berndt/Timm*, DuD 2025, 539.

7. Empfehlungen

Auf Grundlage der durchgeföhrten Untersuchung und der diskutierten Ergebnisse lassen sich differenzierte Empfehlungen für den praktischen Einsatz KI-generierter Datenschutzschulungen ableiten.

Dabei gilt grundsätzlich, dass KI-generierte Datenschutzschulungen angesichts der zahlreichen fehlerhaften, lückenhaften und missverständlichen Inhalte nicht dazu geeignet sind juristische Expertise, professionelle Angebote oder kuratierte Inhalte zu ersetzen. Vor diesem Hintergrund dürfen KI-generierte Schulungen niemals unreflektiert übernommen werden. Sie sind stets kritisch auf ihre Richtigkeit zu prüfen, auf ihre Eignung für die jeweilige Organisation zu validieren und ggf., um organisationsspezifische Aspekte zu ergänzen.

Im Übrigen lassen sich je nach Unternehmensgröße, vorhandener Datenschutzexpertise und Risiko für die Rechte und Freiheiten natürlicher Personen verschiedene Empfehlungen ableiten:

Organisationen ohne eigene Datenschutzexpertise wird empfohlen, primär auf kostenlose, kuratierte Schulungsangebote zurückzugreifen. KI-generierte Schulungen bieten in diesem Kontext keinen erkennbaren Mehrwert, da der erforderliche Nachbearbeitungsaufwand den vermeintlichen Kostenvorteil aufzehrt und ohne entsprechende Fachexpertise schwer zu bewältigen ist.

Sofern im Einzelfall dennoch eine KI-generierte Schulung eingesetzt werden soll, ggf. auch nur ergänzend oder mit Fokus auf eine bestimmte Fragestellung, setzt dies bei sehr kleinen Organisationen voraus, dass die Verarbeitung personenbezogener Daten unkritisch ist und bloß in geringem Umfang erfolgt. Des Weiteren muss eine bestmögliche fachliche Prüfung der generierten Inhalte durch die Unternehmensleitung erfolgen, auch wenn diese keine Datenschutzexpertise besitzt.⁴³ Hierdurch können offensichtliche Fehler und Lücken erkannt und ggf. erforderliche Anpassungen vorgenommen werden.

Für mittlere bis große Organisationen mit vorhandener Datenschutzexpertise – etwa durch einen internen oder externen Datenschutzbeauftragten oder geschulte Mitarbeitende – kann KI als Beschleuniger bei der Erstellung individualisierter Schulungsmaterialien dienen. Der Mehrwert liegt nicht in der vollständigen Automatisierung, sondern in der Effizienzsteigerung bei der Erstellung von Rohentwürfen, die anschließend fachlich überarbeitet und an die spezifischen organisatorischen Gegebenheiten angepasst werden. Diesen Organisationen wird empfohlen, KI-Systeme (sofern gewünscht) zur Erstellung von Erstentwürfen zu nutzen und ausreichend Zeit für die fachliche Überarbeitung einzuplanen.

Für große Unternehmen mit komplexen Abläufen und erhöhtem Verarbeitungsrisiko eignen sich KI-generierte Schulungen nach heutigem Stand nicht als alleinige Lösung. Diesen Organisationen wird empfohlen, auf professionelle kommerzielle Schulungsangebote zu setzen oder mit interner oder externer Datenschutzexpertise individuell zugeschnittene Schulungskonzepte zu entwickeln. KI-Systeme können allenfalls unterstützend bei der Erstellung von Teilentwürfen eingesetzt werden.

⁴³ Ggf. auch mehrstufige Prüfung: Selzer/Kurchyna/Berndt/Timm, KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten, 53 (63).

8. Zusammenfassung

Im Rahmen der Untersuchung wurden neun KI-Modelle mit demselben Arbeitsauftrag beauftragt, eine Schulung für neue Mitarbeitende zu den Grundlagen des Datenschutzes zu erstellen. Die generierten Inhalte wurden zunächst einzeln analysiert und anschließend in einem systematischen Vergleich gegenübergestellt. Grundlage bildeten dreizehn von uns definierte Bewertungskategorien, die die Mindestinhalte einer datenschutzrechtlich angemessenen Schulung abbilden. Jede Schulung wurde in den Dimensionen Vollständigkeit, Richtigkeit und Verständlichkeit bewertet.

Der anschließende Gesamtvergleich zeigt ein heterogenes Bild: Die didaktische Gestaltung der meisten Schulungen fällt insgesamt zufriedenstellend aus – Aufbau, Struktur und Ansprache sind häufig nachvollziehbar und ansprechend umgesetzt. Inhaltlich besteht insbesondere im Bereich der Vollständigkeit deutlicher Verbesserungsbedarf. In vielen Fällen fehlen zentrale Definitionen oder grundlegende Begriffsbestimmungen; essenzielle Instrumente des Datenschutzes werden unzureichend oder gar nicht erläutert. Weitgehend fehlt eine rechtliche Einordnung von Begriffen. Erläuterungen bleiben häufig zu rudimentär, Praxisbeispiele sind selten oder gar nicht vorhanden. Dadurch entsteht das Risiko von Fehlinterpretationen und Missverständnissen.

In der Konsequenz müssen die von KI generierten Schulungsinhalte derzeit fachlich nachgearbeitet werden, um Lücken, Ungenauigkeiten und fehlerhafte Darstellungen zu beseitigen. Eine solche Überarbeitung erfordert jedoch juristische Expertise, über die insbesondere kleine Organisationen häufig nicht verfügen. Daher ist es für die meisten Organisationen gegenwärtig sinnvoller, auf kostenlose kuratierte Schulungsangebote (z. B. von Datenschutzaufsichtsbehörden) zurückzugreifen. Diese sind fachlich geprüft, regelmäßig aktualisiert und gewährleisten ein Mindestmaß an rechtlicher Verlässlichkeit. Eine Ausnahme können sehr kleine Organisationen mit geringem Verarbeitungsrisiko darstellen, bei denen die Verhältnismäßigkeit eine weniger intensive Schulung zulässt: Wenn nur einfache, risikoarme Datenverarbeitungsprozesse stattfinden und eine Plausibilitätsprüfung durch die Unternehmensleitung erfolgt, können KI-generierte Schulungen eine tragfähige und kostengünstige Lösung darstellen.

Der aktuelle Entwicklungsstand der Modelle erlaubt keine rechtssichere Nutzung ohne fachliche Kontrolle und Nachbearbeitung. Der Einsatz von KI zur Erstellung datenschutzrechtlicher Schulungen ist derzeit – je nach Organisationsgröße, Verarbeitungsrisiko und vorhandener Expertise – unterschiedlich geeignet und kann etablierte Schulungsformate ergänzen, aber nicht ersetzen.

Insgesamt zeigt sich, dass KI-generierte Datenschutzschulungen ein vielversprechendes, aber noch nicht ausgereiftes Instrument darstellen. Ihr Einsatz erfordert ein differenziertes Vorgehen, das Risiko, Organisationsgröße und vorhandene Expertise berücksichtigt. Mit fortschreitender Entwicklung der KI-Systeme könnte sich ihre Eignung künftig deutlich verbessern. Bis dahin bleibt die fachliche Prüfung, Anpassung und Ergänzung durch datenschutzrechtlich geschulte Personen unverzichtbar.

Anhang: Berechnung des Gesamtvergleichs⁴⁴

Vollständigkeit						
Modell	Ja	Teilw.	Nein	(-)	Ampel	Begründung
Claude Sonnet 4	2 = 15,38 %	8 = 61,54 %	0 = 0 %	3 = 23,08 %	Gelb	Ja+Teilweise=10 ≥ 7 .
Command-a-03-2025	5 = 38,46 %	3 = 23,03 %	2 = 15,38 %	3 = 23,03 %	Gelb	Ja=5 ≥ 5 und Ja+Teilweise=8 ≥ 7 .
DeepSeek V3	2 = 15,38 %	3 = 23,08 %	5 = 38,46 %	3 = 23,08 %	Rot	Ja=2 ≤ 4 und Ja+Teilweise=5 ≤ 6 .
Gemma 3n E2B	2 = 15,38 %	4 = 30,77 %	5 = 38,46 %	2 = 15,38 %	Rot	Ja=2 ≤ 4 und Ja+Teilweise=6 ≤ 6 .
GPT-4.1	4 = 30,77 %	2 = 15,38 %	4 = 30,77 %	3 = 3,08 %	Rot	Ja=4 ≤ 4 und Ja+Teilweise=6 ≤ 6 .
Grok 3	3 = 23,03 %	4 = 30,77 %	3 = 23,03 %	3 = 23,08 %	Gelb	Ja+Teilweise=7 ≥ 7 .
LLaMA 4	1 = 7,69 %	1 = 7,69 %	4 = 30,77 %	7 = 53,85 %	Rot	Ja=1 ≤ 4 und Ja+Teilweise=2 ≤ 6 .
Mistral Medium 3	2 = 15,38 %	5 = 38,46 %	2 = 15,38 %	4 = 30,77 %	Gelb	Ja+Teilweise=7 ≥ 7 .
Qwen 3-235B-A22 B-2507	4 = 30,77 %	3 = 23,08 %	3 = 23,08 %	3 = 23,08 %	Gelb	Ja+Teilweise=7 ≥ 7 .
Richtigkeit						
Modell	Ja	Teilw.	Nein	(-)	Ampel	Begründung
Claude Sonnet 4	8 = 61,54 %	2 = 15,38 %	0 = 0 %	3 = 23,08 %	Gelb	Ja=8 ≥ 5 und Ja+Teilweise=10 ≥ 7 .
Command-a-03-2025	9 = 69,23 %	1 = 7,69 %	0 = 0 %	3 = 23,08 %	Gelb	Ja=9 ≥ 5 und Ja+Teilweise=10 ≥ 7 .

⁴⁴ Die im Anhang enthaltenen Tabellen fassen für jedes der neun KI-Modelle zusammen, wie oft in den dreizehn Bewertungskategorien die Ausprägungen „Ja“, „Teilweise“, „Nein“ oder „(–)“ vergeben wurden. Jede Tabelle bezieht sich auf eine Leitfrage (Vollständigkeit, Richtigkeit oder Verständlichkeit) und zeigt, wie häufig das jeweilige Modell die entsprechenden Bewertungskriterien erfüllt hat. Die tabellarische Übersicht dient als rechnerische Grundlage für die Ampelzuordnung (Grün/Gelb/Rot) der Modelle. Die Ampelfarbe wird nach einer festen Schwellenlogik bestimmt: „Grün“ erfordert mindestens 11 „Ja“-Bewertungen ($\geq 84,62\%$). „Gelb“ wird vergeben, wenn mindestens 5 „Ja“-Bewertungen ($\geq 38,46\%$) oder alternativ mindestens 7 „Ja+Teilweise“-Bewertungen ($\geq 53,85\%$) vorliegen. „Rot“ wird zugeteilt, wenn sowohl höchstens 4 „Ja“-Bewertungen ($\leq 30,77\%$) als auch höchstens 6 „Ja+Teilweise“-Bewertungen ($\leq 46,15\%$) erreicht wurden.

DeepSeek V3	8 = 61,54 %	1 = 7,69 %	0 = 0 %	4 = 30,77 %	Gelb	Ja=8 ≥5 und Ja+Teilweise=9 ≥7.
Gemma 3n E2B	5 = 38,46 %	5 = 38,46 %	0 = 0 %	3 = 23,08 %	Gelb	Ja=5 ≥5 und Ja+Teilweise=10 ≥7.
GPT-4.1	7 = 53, 85 %	3 = 23,08 %	0 = 0 %	3 = 23,08 %	Gelb	Ja=7 ≥5 und Ja+Teilweise=10 ≥7.
Grok 3	8 = 61,54 %	2 = 15,38 %	0 = 0 %	3 = 23,08 %	Gelb	Ja=8 ≥5 und Ja+Teilweise=10 ≥7.
LLaMA 4	3 = 23,08 %	2 = 15,38 %	0 = 0 %	8 = 61,54 %	Rot	Ja=3 ≤4 und Ja+Teilweise=5 ≤6.
Mistral Medium 3	8 = 61,54 %	1 = 7,69 %	0 = 0 %	4 = 30,77 %	Gelb	Ja=8 ≥5 und Ja+Teilweise=9 ≥7.
Qwen 3-235B-A22 B-2507	8 = 61,54 %	1 = 7,69 %	0 = 0 %	4 = 30,77 %	Gelb	Ja=8 ≥5 und Ja+Teilweise=9 ≥7.
Verständlichkeit						
Modell	Ja	Teilweise	Nein	(-)	Ampel	Begründung
Claude Sonnet 4	2 = 15,38 %	8 = 61,54 %	0 = 0 %	3 = 23,08 %	Gelb	Ja+Teilweise=10 ≥7.
Command-a-03-2025	2 = 15,38 %	7 = 53, 85 %	1 = 7,69 %	3 = 23,08 %	Gelb	Ja+Teilweise=9 ≥7.
DeepSeek V3	1 = 7,69 %	6 = 46,15 %	3 = 23,08 %	3 = 23,08 %	Gelb	Ja+Teilweise=7 ≥7.
Gemma 3n E2B	0 = 0 %	7 = 53, 85 %	4 = 30,77 %	2 = 15,38 %	Gelb	Ja+Teilweise=7 ≥7.
GPT-4.1	1 = 7,69 %	6 = 46,15 %	3 = 23,08 %	3 = 23,08 %	Gelb	Ja+Teilweise=7 ≥7.
Grok 3	1 = 7,69 %	8 = 61,54 %	1 = 7,69 %	3 = 23,08 %	Gelb	Ja+Teilweise=9 ≥7.
LLaMA 4	1 = 7,69 %	3 = 23,08 %	2 = 15,38 %	7 = 53, 85 %	Rot	Ja=1 ≤4 und Ja+Teilweise=4 ≤6.
Mistral Medium 3	2 = 15,38 %	6 = 46,15 %	1 = 7,69 %	4 = 30,77 %	Gelb	Ja+Teilweise=8 ≥7.
Qwen 3-235B-A22 B-2507	3 = 23,08 %	5 = 38,46 %	2 = 15,38 %	3 = 23,08 %	Gelb	Ja+Teilweise=8 ≥7.

Gesamtübersicht der Ampelbewertungen aller KI-Modelle:

Bereich	Grün	Gelb	Rot
Vollständigkeit	0%	55,56%	44,44%
Richtigkeit	0%	88,89%	11,11%
Verständlichkeit	0%	88,89%	11,11%

Literatur

- Arnold, Rolf/Nuissl, Ekkehard/Schrader, Josef: Wörterbuch Erwachsenen- und Weiterbildung, 3. Auflage, Verlag Julius Klinghardt, Bad Heilbrunn 2023.
- Besgen, Nicolai (Hrsg.): Rechtshandbuch Leitende Angestellte, Geschäftsführer und Vorstände, 2. Auflage 2023, C.H.Beck, München 2023.
- Bunjes, Johann: Umsatzsteuergesetz, 25. Auflage, C.H.Beck, München 2025.
- Bürkle, Jürgen (Hrsg.): Compliance in Versicherungsunternehmen, 3. Auflage, C.H.Beck, München 2020.
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand: 17.12.2018.
- EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020.
- EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, angenommen am 29. Januar 2020.
- Ehmann, Eugen/Selmayr, Martin (Hrsg.): DSGVO – Kommentar, 3. Auflage, C.H. Beck, München 2024.
- Enzmann, Matthias/Selzer, Annika/Stummer, Sarah: Zur Qualität KI-generierter Selbstlerneinheiten – Kurzschulungen zu Anonymität, Pseudonymität und Personenbezug im Kontext der Verarbeitung von Gesundheits-, Personal- und Administrationsdaten, EuDIR 2025, S. 270-276.
- Godzierz, Cornelia (Hrsg.): Compliance-Checklisten, 6. Auflage, C.H.Beck, München 2025.
- Gola, Peter/Heckmann, Dirk (Hrsg.): Datenschutzgrundverordnung, Bundesdatenschutzgesetz – Kommentar, 3. Auflage, C.H.Beck, München 2022.
- Hau, Wolfgang/Poseck, Roman (Hrsg.): BeckOK BGB, 76. Edition, C.H.Beck, München 2025.
- Heberlein, Horst: Datenschutz und Meinungsfreiheit. Der Regelungsauftrag der Datenschutz-Grundverordnung für den nationalen Gesetzgeber, EuR 2021, S. 672-696
- Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutzgrundverordnung/BDSG – Kommentar, 4. Auflage, C.H.Beck, München 2024.
- Nuissl, Ekkehard: Vom Lernen zum Lehren, wbv, Bielefeld 2006.
- Paal, Boris/Pauly, Daniel (Hrsg.): Datenschutzgrundverordnung, Bundesdatenschutzgesetz – Kommentar, 3. Auflage, C.H.Beck, München 2021
- Selzer, Annika/Berndt, Jan Ole/Timm, Ingo J.: Einsatz KI-generierter Datenschutz-Schulungsmaterialien, DuD 2025, S.539-543.
- Selzer, Annika/Kurchyna, Veronika /Berndt, Jan Ole/Timm, Ingo J.: KI-generierte, Verarbeitungskontext-spezifische Mitarbeiterschulungen zum Datenschutz als Ausprägung der angemessenen Umsetzung datenschutzrechtlicher Pflichten. In: Selzer, Annika (Hrsg.) Aktuelle Entwicklungen des Rechtsrahmens der Cybersicherheit und Privatheit. ATHENE2025 2025. Rechtsrahmen der Cybersicherheit und Privatheit, S. 53-65. Springer Vieweg, Wiesbaden.
- Selzer, Annika: The Appropriateness of Technical and Organisational Measures under Article 32 GDPR, EDPL 01/2021, S. 120-128.

Literatur

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht – DSGVO/BDSG, Kommentar, 2. Auflage, Nomos, Baden-Baden 2025.

Sydow, Gernot/Marsch, Nikolaus (Hrsg.): DSGVO/BDSG – Handkommentar, 3. Auflage, Nomos, Baden-Baden 2022.