



# Einsatz Künstlicher Intelligenz im Recruitingprozess

INES TACKE & ANTONIA STOLL



Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

Mittelstand-Digital 

aufgrund eines Beschlusses  
des Deutschen Bundestages

Der folgende Beitrag stellt die Anforderungen der KI-Verordnung der Europäischen Union (KI-VO) sowie der Datenschutzgrundverordnung (DSGVO) an KI-Systeme im Recruitingprozess beispielhaft anhand einer KI-gestützten Recruiting- und Matching-Plattform, der „Recruiting und Matching-App“ dar. Der Beitrag ist in zwei Teile untergliedert. In Teil 1 werden die Anforderungen der KI-Verordnung analysiert: Wer gilt als Anbieter, wer als Betreiber und welche Pflichten treffen beide. In Teil 2 wird untersucht, welche datenschutzrechtlichen Vorgaben zu beachten sind – von der Rechtsgrundlage für die Verarbeitung von Bewerberdaten über Scoring und Profiling bis hin zu Transparenzpflichten, Datenschutz-Folgenabschätzung und dem rechtskonformen Betrieb eines Talentpools.

Im Detail erfahren Sie in diesem Nachgelesen:

### Teil 1: Anforderungen der KI-Verordnung

- Welche Anforderungen die KI-VO an eine KI-gestützte Recruiting- und Matching-App stellt
- Welche Akteure die KI-VO kennt (Anbieter und Betreiber)
- Wie KI-Systeme nach der KI-VO in Risikoklassen eingeordnet werden
- Welche Ausnahmen von der Klasse des hohen Risikos bestehen

- Welche Anbieter- und Betreiberpflichten greifen
- Welche Pflichten konkret den Betreiber treffen
- Wie der Plattformbetreiber die Betreiberpflichten erfüllen kann

### Teil 2: Datenschutzrechtliche Anforderungen

- Welche datenschutzrechtlichen Anforderungen an eine KI-gestützte Recruiting- und Matching-App gelten
- Wer datenschutzrechtlich verantwortlich ist
- Wann eine gemeinsame Verantwortlichkeit vorliegt
- Auf welcher Rechtsgrundlage Bewerberdaten verarbeitet werden dürfen
- Was bei Scoring, Matching und Profiling zu beachten ist
- Welche Transparenzpflichten gegenüber Bewerbenden bestehen
- Wann eine Datenschutz-Folgenabschätzung erforderlich ist
- Wie Datenminimierung, Zweckbindung und Löschung umzusetzen sind
- Wie Diskriminierung und fehlerhafte Bewertungen vermieden werden können
- Welche technischen und organisatorischen Schutzmaßnahmen erforderlich sind
- Welche besonderen Anforderungen an einen Talentpool gelten
- Wie Verantwortlichkeiten vertraglich abgesichert werden können

## Impressum

### HERAUSGEBER

Mittelstand-Digital Zentrum Chemnitz  
c/o TU Chemnitz  
Erfenschlager Str. 73, 09125 Chemnitz  
Tel: 0371 531 19935 Fax: 0371 531 819935  
info@digitalzentrum-chemnitz.de  
www.digitalzentrum-chemnitz.de

### REDAKTION Anikó Lessi

### GESTALTUNG UND PRODUKTION

PUNKT191 – Marketing und Design  
www.punkt191.de

### BILDNACHWEIS TITEL creativeart - Magnific.com

### VERÖFFENTLICHUNG August 2026





↑ © syda\_productions - Magnific.com

# Teil 1: Anforderungen der KI-Verordnung beim Einsatz einer KI-gestützten Recruiting- und Matching-App

Die Verwendung Künstlicher Intelligenz (KI) hat inzwischen in allen Bereichen des geschäftlichen Lebens Einzug gehalten – so auch im Recruiting. Die Besonderheit beim Einsatz KI-gestützter Anwendungen im Recruiting liegt in seiner Vielfalt. Ein solches Beispiel ist die Verwendung von KI, um Bewerber auf Plattformen anhand von Kompetenzen und Testergebnissen mit passenden Stellenangeboten zusammenzubringen (Recruiting- und Matching-App). Die KI analysiert hierfür verschiedene Informationen wie Qualifikationen, Berufserfahrung, Fähigkeiten und persönliche Präferenzen der Bewerber. Arbeitsuchende können außerdem digitale Kompetenztests absolvieren. Die dabei erzielten Ergebnisse werden durch die KI ausgewertet, mit den Anforderungen der jeweiligen Stelle abgeglichen und mögliche Übereinstimmungen etwa in Form eines Scores berechnet. Auf dieser Grundlage können Bewerber passende Stellen finden und Unternehmen Entscheidungen über die Einladung zu Bewerbungsgesprächen treffen. Hierdurch kann die anstrengende Recherche im Bewerbungsprozess sowohl für Bewerber als auch für Unternehmen effizienter gestaltet werden. Welche rechtlichen Anforderungen stellt aber die Rechtsordnung an solche Systeme und welche Pflichten treffen Plattformbetreiber und ausschreibende Unternehmen?

Bei der Beurteilung von Anforderungen rechtlicher Pflichten in Verbindung mit KI-Systemen ist stets an die KI-Verordnung

zu denken.<sup>[1]</sup> Die Pflichten, die ein Unternehmen nach der KI-Verordnung treffen, hängen grundlegend von zwei Faktoren ab:

1. welche Rolle das Unternehmen als Akteur im Rahmen der KI-Verordnung einnimmt sowie
2. welcher Risikoklasse des KI-Systems im konkreten Anwendungsfall zuzuordnen ist.

Der folgende Beitrag widmet sich der Frage, welche Rolle sowohl der Plattformbetreiber als auch Unternehmen, welche die Plattform nutzen, nach der KI-Verordnung einnehmen und wie die beschriebenen Systeme in die Risikoklassen der KI-Verordnung und damit in den deren Pflichtenkanon einzuordnen sind.



# Akteure nach der KI-Verordnung

Die KI-Verordnung weist verschiedenen Akteuren Pflichten zu. Dabei liegt der Fokus im vorgenannten Fall auf dem Anbieter sowie dem Betreiber von Systemen.

| Anbieter (Art. 3 Nr. 3 KI-VO)                                                                                                                        | Betreiber (Art. 3 Nr. 4 KI-VO)                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System oder ein Allzweck-KI-Modell entwickeln oder entwickeln lassen | natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen |
| die KI-Systeme oder Allzweck-KI-Modelle im eigenen Namen oder unter eigener Marke in der EU in Verkehr bringen oder das KI-System in Betrieb nehmen  | eigenverantwortliche Verwender von KI-Systemen in der EU                            |

**Anbieter** ist nach der KI-VO jede natürliche oder juristische Person\*, Behörde, Einrichtung oder sonstige Stelle, die ein KI System entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich (Art. 3 Nr. 3 KI-VO). Ziel dieser Regelung ist, dass für weitere Akteure in der Wertschöpfungskette, der Verantwortliche für das System und damit der Ansprechpartner bei Problemen durch das Anbringen des Namens oder der Marke zu jedem Zeitpunkt erkennbar sein soll. Einer Verschleierung von Verantwortlichkeiten, und sei sie noch so unbeabsichtigt, soll vorgebeugt werden.

*Beispiel:*

*Entwickelt der Plattformbetreiber das Recruiting-KI-System und nimmt es anschließend im eigenen Namen bzw. unter eigener Marke in Betrieb, handelt er als Anbieter des KI-Systems.*

Dies gilt unbeschadet dessen, dass zur Entwicklung des KI-Systems u. U. KI-Modelle von dritten Anbietern Verwendung finden<sup>[2]</sup>. In dem Fall ist der Plattformbetreiber jedoch u. U.

Praxistipp:

Die natürliche oder juristische Person, deren Name oder Marke mit dem KI-System verbunden ist, gilt als Anbieter. Insbesondere im Rahmen von Auftragsarbeiten bildet dies damit eine wichtige Stellschraube, um im Rahmen von Verträgen die eigenen Pflichten nach der KI-Verordnung zu beeinflussen.

zur Erfüllung der eigenen Pflichten auf Zuarbeit des Anbieters der Modelle angewiesen. Um spätere Probleme zu verhindern, sollte die Zusammenarbeit bereits im Entwicklungsprozess in Verträgen garantiert und geregelt werden.

**Betreiber** ist jede natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI System in eigener Verantwortung verwendet, es sei denn, das KI System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet (Art. 3 Nr. 4 KI-VO). Der Betreiber grenzt sich vom Nutzer, den keine Pflichten nach der KI-VO treffen, anhand des Kriteriums der Eigenverantwortlichkeit ab. Betreiber ist, wer die Kontrolle über den Betrieb ausübt, unter dessen Verantwortung ein KI-System verwendet wird<sup>[3]</sup>, S. 146].

*Beispiel:*

*Setzt ein Unternehmen KI-Systeme, die mit dem Namen oder der Marke eines Dritten versehen sind, im Rahmen des Recruitingprozesses in der Personalabteilung ein, indem etwa Bewerber sortiert werden, verwendet es diese Systeme in eigener Verantwortung und damit als Betreiber. Der Mitarbeitende hingegen, der das System lediglich bedient, kontrolliert den Betrieb nicht und ist mithin nicht als Betreiber zu qualifizieren<sup>[1]</sup>.*

Praxistipp:

Ist das Unternehmen zugleich Anbieter und Betreiber, muss es sowohl die Anbieter- als auch die Betreiberpflichten erfüllen<sup>[4]</sup>.

\* Bei natürlichen Personen handelt es sich um Menschen im Gegensatz zu juristischen Personen, Personenvereinigungen oder Zweckverbänden mit vom Gesetz anerkannter rechtlicher Selbständigkeit, wie Unternehmen.



**Die Rolle des Betreibers auf Plattformen,** wie der Recruiting- und Matching-App lässt sich nicht einfach zuordnen, weil je nach technischer Ausgestaltung der Plattform die Kontrolle über den Betrieb des KI-Systems u. U. variieren kann. Dem Betreiber des KI-Systems werden in der KI-Verordnung verschiedene Pflichten zur Überwachung des Betriebs zugeschrieben. Um analysieren zu können, welchem Beteiligten (Plattformbetreiber oder Unternehmen, die die Plattform nutzen) im Rahmen der Recruiting-Plattform die Kontrolle über den Betrieb zugeordnet werden kann, lohnt sich ein Blick auf die Betreiberpflichten, welche sich maßgeblich an der Risikoklassifizierung des KI-Systems bemessen.

KI-Systeme, die im Bereich des Recruitings eingesetzt werden, fallen insbesondere immer dann in diese Risikoklasse, wenn sie bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen (Nr. 4 Anh. III zur KI-VO). Das kann beispielsweise der Fall sein, wenn Stellenanzeigen gezielt geschaltet oder Bewerbungen gesichtet oder gefiltert oder Bewerber bewertet werden (Nr. 4 Anh. III zur KI-VO). Hierunter fällt auch die Prüfung von Bewerbern<sup>[8, Rn. 245]</sup>.

Werden auf der Plattform also mittels KI Bewertungen von Bewerbern etwa über einen Score auch mittels eines Eignungstests durchgeführt (Recruiting- und Matching-App), fällt das KI-System grundsätzlich in die Klasse des hohen Risikos.

*Beispiel:*

*Anders liegt der Fall, wenn ein KI-Chatbot lediglich für Fragen der Bewerber zum Bewerbungsprozess, zur Stellenausschreibung oder zur Vereinbarung von Bewerbungsterminen Verwendung findet. In dem Fall geht von der Anwendung kein besonders hohes KI-spezifisches Risiko für natürliche Personen aus und das System fällt nicht in die Klasse des hohen Risikos nach der KI-Verordnung, obwohl es bestimmungsgemäß im Rahmen eines Bewerbungsprozesses Anwendung findet.*

## Die Risikoklasse nach der KI-Verordnung

Die konkreten Pflichten von Anbietern und Betreibern bestimmen sich nach der Einordnung des Systems in seinem konkreten Anwendungsfall (KI-Praktik) in eine der Risikostufen: Minimal, begrenzt, hoch oder inakzeptabel. [5] KI-Praktiken werden anhand des Risikos eingeordnet, das sie für die Sicherheit, die Gesundheit sowie die Grundrechte natürlicher Personen darstellen.

| Risikoklasse | Beschreibung                                     | Regulierung                                                                     | Beispiel                                                           |
|--------------|--------------------------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------|
| inakzeptabel | Bedrohung grundlegender Rechte                   | Verbot                                                                          | Social Scoring, Schädliche Manipulation und Täuschung              |
| hoch         | potenziell hohes Risiko für Betroffene           | weitreichende Anforderungen (menschliche Aufsicht, hochwertige Datensätze etc.) | Kreditwürdigkeitsprüfung, KI im Personalbereich, Emotionserkennung |
| begrenzt     | Interaktion mit Menschen & KI generierte Inhalte | Transparenzpflicht                                                              | Chatbots, Deepfakes                                                |
| minimal      | alle anderen Systeme                             | keine rechtlichen Anforderungen (freiwillig Verhaltenskodizes)                  | Spamfilter                                                         |

Ist der Einsatz von KI-Systemen im konkreten Anwendungsfall mit einem hohen Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von Menschen verbunden, werden sie als Hochrisiko-KI eingestuft<sup>[6, S. 396]</sup>. Die Anwendungsbereiche, in denen ein solches hohes Risiko angenommen wird, sind in Anhang III zur KI-Verordnung aufgeführt (Art. 6 Abs. 2 KI-VO).<sup>[7]</sup> Dazu gehört insbesondere der Bereich „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“ (Art. 6 Abs. 2 und Nr. 4 Anh. III zur KI-VO).

**Praxistipp:**

Zur Einordnung von KI-Systemen in Risikoklassen sollte immer anhand des Einzelfalls vorgenommen werden. Orientierung kann hier der [KI-Compliance-Kompass](#) der Bundesnetzagentur bieten.





# Ausnahmen in der Klasse des hohen Risikos

Fallen Systeme nach einem Anwendungsszenario nach Anhang III in die Klasse des hohen Risikos, wie das konkrete Recruiting-KI-System, besteht die Möglichkeit, dass dennoch ein Ausnahmefall vorliegt (Art. 6 Abs. 3 KI-VO). Eine Einstufung als Hochrisiko-KI entfällt, wenn die Verwendung des KI-Systems im Anwendungsfall kein hohes KI-spezifisches Risiko für Menschen begründet (Art. 6 Abs. 3 KI-VO)<sup>[7]</sup>. Voraussetzung ist, dass die KI u. a. nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst (Art. 6 Abs. 3 KI-VO). [9, p. 58 f.] Eine Ausnahme liegt vor, wenn (Art. 6 Abs. 3 lit. a-d KI-VO):

- das System lediglich eine eng umgrenzte verfahrenstechnische Aufgabe wahrnimmt.
- das System lediglich der Verbesserung des menschlichen Ergebnisses dient.
- das System lediglich Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkennen soll und kein Ersatz für die zuvor durchgeführte menschliche Bewertung darstellen soll, ohne dass eine menschliche Überprüfung des KI-Ergebnisses stattfindet.
- das System lediglich vorbereitende Aufgaben für eine Bewertung durchführt.
- Um zu bewerten, ob ein System unter eine Ausnahme nach Abs. 3 fällt, ist entscheidend, die potenziellen Auswirkungen des KI-Systems auf die Beschäftigungs- und Karrieremöglichkeiten potenzieller oder tatsächlicher Bewerber sowie das Diskriminierungsrisiko zu prüfen. <sup>[8, Rn. 247]</sup>

## Beispiel:

Beispiele für Ausnahmefälle können im Erkennen von Duplikaten in Bewertungsbögen, dem Verbessern der Sprache in zuvor durch den Menschen verfassten Ausschreibungen, dem nachträgliche KI-gestützte Überprüfen von Bewertungsmus-

tern mit dem Ziel, Abweichungen von vorherigen Entscheidungen festzustellen oder dem KI-gestützte Aufzeichnen von Bewerbungsgesprächen liegen. Die Abgrenzung zwischen Hochrisiko-KI und Ausnahme muss immer anhand des Einzelfalls erfolgen, da die Grenze fließend sein kann. Sind in einem Unternehmen mehrere Stellen vakant und somit mehrere Stellenanzeigen veröffentlicht, kann KI verwendet werden, um eingehende Bewerbungen und damit Bewerber in die entsprechenden Kategorien einzuordnen, ohne dass die KI hierdurch zur Hochrisiko-KI wird.<sup>[8, Rn. 92]</sup> Werden jedoch Bewerbungen und damit Bewerber durch KI danach kategorisiert, wie gut sie zu einer angebotenen Stellenausschreibung passen, liegt eine Ausnahme vom hohen Risiko nicht mehr vor. Gleiches gilt, wenn Bewerber auf Plattformen mittels KI-erstelltem Score für von Unternehmen geschaltete Stellenausschreibungen bewertet werden.

Wird ein KI-System verwendet, um aus vorgegebenen Anforderungen einen Eignungstest für Bewerber zu formulieren und hat das System selbst keinen Einfluss auf den Inhalt oder die Bewertung des Tests, kann davon ausgegangen werden, dass es lediglich eine eng umgrenzte verfahrenstechnische Aufgabe wahrnimmt. In dem Fall würde das System unter die Ausnahme fallen. Generiert ein KI-System jedoch die Inhalte für den Test und/oder führt eine Bewertung durch, hat es Einfluss auf die Beschäftigungs- und Karrieremöglichkeiten potenzieller oder tatsächlicher Bewerber und fällt somit nicht unter die genannte Ausnahme <sup>[vgl. 8, Rn. 247]</sup> Für die genaue Einschätzung des Risikos von KI-Systemen im Rahmen der Recruiting- und Matching-App kommt es daher auf den konkreten Einzelfall an.

Auch hier gilt allerdings: „Keine Regel ohne Ausnahme“ bzw. „Keine Ausnahme ohne **Gegenausnahme**“. Einen solchen Gegenausnahmefall stellt **Profiling**\*\* dar. Wird ein KI-System etwa zur Verarbeitung von Daten zur Bewertung von Aspekten bezüglich der Arbeitsleistung verwendet (Art. 4 Abs. 4 DSGVO), handelt es sich immer um ein Hochrisiko-KI-System (Art. 6 Abs. 3 S. 3 KI-VO).

## Beispiel:

Bestimmt das KI-System also anhand von Angaben in den Unterlagen oder von Tests einen Matching-Score für potenzielle oder tatsächliche Bewerber, der Aspekte bezüglich der Arbeitsleistung oder auch der wirtschaftlichen Lage, der Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel betrifft, handelt es sich immer um ein hochrisiko-KI-System.

---

\*\* Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 4 Abs. 4 DSGVO).



**Im Rahmen einer Gesamtbetrachtung** ist darüber hinaus in bestimmten Fällen bei der Bewertung von Ausnahmen nicht lediglich das konkrete KI-System zu betrachten. Wenn das KI-System als Modul neben weiteren im Rahmen eines komplexeren Gesamt-KI-Systems verwendet wird, ist in bestimmten Einzelfällen das gesamte System zu berücksichtigen. Unter Umständen kommt es also für die Risikoeinstufung eines bestimmten KI-Systems, etwa einem, das aus vorgegebenen Inhalten lediglich Fragen für Bewerbungstests generiert, nicht nur isoliert auf das bestimmte System an.

Werden verschiedene „Gesamtsystemmodule“ verwendet, um eine einzige Entscheidung in einem Hochrisikoo Anwendungsfall wesentlich zu beeinflussen, wird das Gesamtsystem einheitlich bewertet.<sup>[8]</sup> <sup>[8, Rn. 75]</sup> Gleiches gilt für verbundene Systeme (wie Agentensysteme).<sup>[8, Rn. 75]</sup> Anders liegt der Fall, bei KI-Systemen, die zwar mit Hochrisiko-KI-Systemen verbunden, jedoch von diesen tatsächlich trennbar sind und keinen Output einspeisen, welcher das Ergebnis des Hochrisiko-KI-Systems im riskanten Anwendungsfall erheblich beeinflusst.<sup>[8, Rn. 76]</sup> Im Einzelfall kommt es damit für die Risikoeinschätzung immer auf die konkrete Gestaltung des Systems an.

#### Praxistipp:

Komplexe KI-Systeme sowie verbundene Agentensysteme werden der Risikobewertung als einheitliches System unterzogen. Nur KI-Systeme, die nicht zur Entscheidung des Systems im riskanten Anwendungsfall beitragen und vom restlichen System abtrennbar sind, können einzeln einer Ausnahme unterfallen.

Ob von einem KI-System im konkreten vorgesehenen Anwendungsfall ein hohes Risiko ausgeht und es damit den Anforderungen an Hochrisiko-KI-Systeme genügen muss, muss der Anbieter bewerten.<sup>[10]</sup> Kommt er zu dem Ergebnis, dass kein hohes Risiko vorliegt, muss er dies dokumentieren (Art. 6 Abs. 4 KI-VO). Diese Dokumentation muss auf Verlangen der Bundesnetzagentur vorgelegt werden.

## Anbieter- und Betreiberpflichten

Liegt keine Ausnahme vor, müssen die Anforderungen der KI-Verordnung an Hochrisiko-KI-System erfüllt werden. KI-Systeme mit hohem Risiko sollen grundsätzlich in der Europäischen Union zum Einsatz kommen können. Zum Schutz der Betroffenen sind allerdings umfassende Sicherheitsanforderungen umzusetzen. Dabei trägt jeder Akteur die Verantwortung für Risiken, welchen er während seiner Tätigkeit am effektivsten begegnen kann. Die Verteilung der Pflichten sowie das Zusammenspiel verschiedener Akteure kann, insbesondere sollten mehrere Personen als Anbieter und Betreiber in Betracht kommen, hochkomplex sein.

### Anbieterpflichten\*\*\*

Der Anbieter ist für alle Pflichten verantwortlich, die während des Entwicklungsprozesses des Systems zu erfüllen sind. Hierunter fällt insbesondere die Pflicht, dafür zu sorgen, dass das System über den gesamten Lebenszyklus die Anforderungen der KI-VO (Art. 9-15 KI-VO) erfüllt (Art. 16 lit. a KI-VO). Dabei muss er auch alle technischen Voraussetzungen schaffen, die notwendig sind, damit nachgelagerte Akteure, wie der Betreiber, ihre Pflichten erfüllen können.

Hat ein Anbieter Grund zu der Annahme, dass ein bereits in Verkehr gebrachtes KI-System nicht (mehr) den Anforderungen der KI-VO entspricht, informiert er die Betreiber sowie nationale Marktüberwachungsstellen und ergreift entsprechende Korrekturmaßnahmen (Art. 16 lit. j, 20 KI-VO), etwa die Deaktivierung des Systems bzw. einzelner Funktionen oder das Zurverfügungstellen passender Updates.

\*\*\* Bei der KI-VO handelt es sich nach dem New Legislative Framework um eine Rahmenverordnung. Die Grundlegenden Anforderungen der Verordnung werden durch technische Standards weiter konkretisiert, die von den europäischen Normungsorganisationen CEN und CENELEC weiterhin entwickelt werden.

| Anbieterpflichten         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Qualitätsmanagementsystem | <p>Einrichten eines Qualitätsmanagementsystems (QMS) (Art. 16 lit. c, 17 KI-VO)</p> <p>→ Aufbewahrungsfrist der Dokumentation: 10 Jahre (Art. 16 lit. d, 18 KI-VO)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Risikomanagementsystem    | Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung eines Risikomanagementsystems (Art. 9 KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Datensätze                | Festlegen und Einhalten von Qualitätskriterien an Daten(-sätze) sowie Daten-Governance- und Datenverwaltungsverfahren für jene Daten(-sätze) (Art. 10 KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Technische Dokumentation  | <p>Erstellen der technischen Dokumentation (Art. 11 KI-VO)</p> <p>→ Aufbewahrungsfrist 10 Jahre (Art. 16 lit. d, 18 KI-VO)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Protokolle                | <p>Entwicklung einer Protokollierungsfunktion über den Betrieb des KI-Systems (Art. 12)</p> <p>→ Aufbewahren von Protokollen bei Zugriff: 6 Monate (Art. 16 lit. e KI-VO)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Transparenz               | <p>Bereitstellen erforderlicher, transparenter Informationen an Betreiber (Art. 13 KI-VO)</p> <p>→ Ziel: Der Betreiber kann die Ausgaben des Systems angemessen interpretieren und verwenden.</p> <p>→ Mittel: z. B. Betriebsanleitung</p>                                                                                                                                                                                                                                                                                                                                                                                |
| Menschliche Aufsicht      | <p>Schaffen technischer Voraussetzungen für die menschliche Aufsicht durch den Betreiber (Art. 14 KI-VO)</p> <p>→ Vorkehrungen, die in das KI-System eingebaut werden</p> <p>→ Vorkehrungen, die der Betreiber umsetzt</p> <p>→ <i>Beispiel: Bei KI-Systemen, die eingesetzt werden, um Bewerber durch Scores zu bewerten, sollte die technische Umsetzung sicherstellen, dass eine Prüfung der KI-Empfehlung durch den Menschen tatsächlich erfolgt, sie nicht nur optional, sondern verpflichtend ist. Es sollte daher im Idealfall nicht möglich sein, der KI-Empfehlung direkt „durch einen Klick“ zu folgen.</i></p> |
| Sicherheit des Systems    | Sicherstellen von Genauigkeit, Robustheit und Cybersicherheit des Systems über den gesamten Lebenszyklus (Art. 15 KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Barrierefreiheit          | Nachweis der Erfüllung der Barrierefreiheitsanforderungen durch das System (Art. 16 lit. l KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Name/Marke                | Angaben des Namens oder der Marke am System oder in der beigefügten Dokumentation (Art. 16 lit. b KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



| Anbieterpflichten              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Konformität und CE-Kennzeichen | <p>Durchlaufen des Konformitätsbewertungsverfahrens sowie Anbringen des CE-Kennzeichens am System oder der beigefügten Dokumentation (Art. 16 lit. f, g, h, 43, 47, 48 KI-VO)</p> <p>→ <i>Beispiel: Im Anwendungsfall einer Verwendung von KI im Recruiting führt der Anbieter die Konformitätsbewertung auf der Grundlage einer internen Kontrolle durch (Art. 43 Abs. 2 KI-VO), indem er überprüft, dass das QMS und die Informationen aus der technischen Dokumentation die Anforderungen der KI-VO erfüllen, sowie dass der Entwurfs- und Entwicklungsprozess des KI Systems und das System zur Beobachtung der KI nach dem Inverkehrbringen mit der technischen Dokumentation im Einklang stehen.</i></p> <p>→ Aufbewahrungsfrist der Konformitätserklärung: 10 Jahre (Art. 16 lit. d, 18 KI-VO)</p> <p>→ Werden Systeme vom Anbieter lediglich digital bereitgestellt, wird eine digitale CE-Kennzeichnung angebracht (ErwGr. 129 S. 3 KI-VO).</p> |
| Registrierung                  | Registrieren des Systems in der hierfür vorgesehenen EU-Datenbank (Art. 16 lit. i, 49 KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Neben den Pflichten, die sich aus der KI-VO durch die Einordnung in die Klasse des hohen Risikos ergeben, sind die Anforderungen an den Aufbau eines ausreichenden Maßes an KI-Kompetenz (Art. 4 KI-VO) sowie u. U. je nach Gestaltung des Systems auch Transparenzanforderungen (Art. 50 KI-VO) einschlägig.

# Betreiberpflichten

Der Betreiber ist für alle Pflichten verantwortlich, die während des Betriebs des Systems zu erfüllen sind.

| Betreiberpflichten     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebsanleitung      | Handeln nach der Betriebsanleitung (Art. 26 Abs. 1 KI-VO)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| → Menschliche Aufsicht | <ul style="list-style-type: none"> <li>→ Wahrnehmen der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht (Art. 26 Abs. 3 KI-VO)</li> <li>→ Übertragen der menschlichen Aufsicht an eine kompetente Person <ul style="list-style-type: none"> <li>▪ U. U. sind Schulungen anzubieten und durchzuführen <sup>[11, p. 39]</sup></li> </ul> </li> <li>→ Ausstatten der menschlichen Aufsicht mit den notwendigen Befugnissen <ul style="list-style-type: none"> <li>▪ <i>Beispiel: Die menschliche Aufsicht muss die Befugnis haben, das System zu stoppen oder Ausgaben des Systems außer Acht zu lassen, in dem Anwendungsfall der Recruiting- und Matching-App etwa, wenn ein Score auffällig ist.</i></li> </ul> </li> <li>→ Die menschliche Aufsicht muss: <ul style="list-style-type: none"> <li>▪ die Fähigkeiten und Grenzen des Systems verstehen.</li> <li>▪ sich eines möglichen „Automatisierungsbias“<sup>****</sup> bewusst sein.</li> <li>▪ die Ausgaben des Systems richtig interpretieren können.</li> <li>▪ entscheiden können, die Ausgaben des Systems nicht zu verwenden oder rückgängig zu machen.</li> <li>▪ den Betrieb des Systems stoppen können.</li> </ul> </li> </ul> |
| Eingabedaten           | <p>Sicherstellen, dass die Eingabedaten passend sind (bei Kontrolle des Betreibers) (Art. 26 Abs. 4 KI-VO)</p> <ul style="list-style-type: none"> <li>→ Sicherstellung der Repräsentativität</li> <li>→ Sicherstellen der Übereinstimmung mit der Zweckbestimmung des Systems <ul style="list-style-type: none"> <li>▪ Die Zweckbestimmung ist beispielsweise der Betriebsanleitung, Werbe- oder Verkaufsmaterialien und/oder der technischen Dokumentation zu entnehmen</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Protokolle             | <p>Aufbewahren von Protokollen über den Betrieb des Systems bei Zugriff (Art. 26 Abs. 6 KI-VO)</p> <ul style="list-style-type: none"> <li>→ Aufbewahrungsfrist: 6 Monate</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Betreiberpflichten            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Grundrechte-Folgenabschätzung | <p>Durchführung der Grundrechtfolgenabschätzung durch Private lediglich für:</p> <ul style="list-style-type: none"> <li>→ Private, die vom Staat mit Hoheitsgewalt betraut sind (Beliehene) wie der TÜV oder Notare</li> <li>→ Private Einrichtungen, die öffentliche Dienste erbringen wie Dienste der Bildung, Gesundheitsversorgung, Sozialdienste oder das Wohnungswesen <sup>[12]</sup></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Schwerwiegender Vorfall       | <p>Information von Anbieter und zuständigen Marktüberwachungsbehörden</p> <ul style="list-style-type: none"> <li>→ <i>Beispiel: Ein schwerwiegender Vorfall liegt z. B. vor, wenn die Fehlfunktion eines KI-Systems zur Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte führt (Art. 3 Nr. 49 lit. c KI-VO). Nur solche Verstöße, die die durch die Charta geschützten Rechte in großem Umfang erheblich beeinträchtigen, sollten meldepflichtig sein</i> <sup>[13, Rn. 26]</sup>. Dies wäre der Fall, wenn das KI-basierte Rekrutierungssystem wie die Recruiting- und Matching-App Bewerber aufgrund ihrer ethnischen Herkunft oder ihres Geschlechts durch einen schlechten Score ausschließen würde.</li> <li>→ Es wird ein Formular zur einheitlichen Meldung bereitgestellt. <sup>[14]</sup></li> </ul> |
| Information von Betroffenen   | <p>Information von Betroffenen, dass sie einer KI-gestützten Entscheidung unterliegen mit dem Inhalt (Art. 26 Abs. 11 KI-VO):</p> <ul style="list-style-type: none"> <li>→ Zweckbestimmung der getroffenen Entscheidung</li> <li>→ Art der getroffenen Entscheidung</li> <li>→ Recht, Erläuterungen über die Entscheidung zu erhalten</li> <li>→ Recht, Erläuterungen über die Rolle der KI zu erhalten (ErwGr. 93 S. 5 f.)</li> </ul> <p>Die Information ist bereits zu erteilen, wenn KI-Output in die Entscheidung einfließt.</p>                                                                                                                                                                                                                                                                                                              |
| Erläuterung der Entscheidung  | <p>Bereitstellung klarer und aussagekräftiger Erläuterung zur Rolle des KI Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung im Fall eines Antrags durch den Betroffenen (Art. 86 KI-VO)</p> <ul style="list-style-type: none"> <li>→ Die Erläuterung muss durch Betroffene gut verständlich sein.</li> <li>→ <i>Beispiel: Im Anwendungsfall der Recruiting- und Matching-App könnten Bewerber etwa Protokolle ihrer Antworten und Bewertungsergebnisse erhalten sowie Informationen darüber, wie die einzelnen Antworten gewichtet wurden, um den Score zusammenzusetzen</i></li> </ul>                                                                                                                                                                                                              |

\*\*\*\* Unter Automatisierungsbias ist in diesem Fall übermäßiges Vertrauen in die Empfehlungen von KI zu verstehen, selbst wenn diese fehlerbehaftet sein sollten.



Außerdem überwacht der Betreiber anhand der Betriebsanleitung, dass das KI-System während des Betriebs weiterhin zu jeder Zeit den Anforderungen der KI-VO entspricht (Art. 26 Abs. 5 KI-VO). Erkennt der Betreiber eine Abweichung, informiert er den Anbieter (Art. 26 Abs. 5 S. 1, 72 KI-VO). Bei unverhältnismäßigen Risiken für die Gesundheit, die Sicherheit oder Grundrechte (i. S. d. Art. 79 Abs. 1 KI-VO), stoppt er die Verwendung des Systems unverzüglich und informiert neben dem Anbieter u. a. auch die zuständige Marktüberwachungsbehörde (Art. 26 Abs. 5 S. 2 KI-VO).

Neben den Pflichten, die sich aus der KI-VO durch die Einordnung in die Klasse des hohen Risikos ergeben, sind die Anforderungen an den Aufbau eines ausreichenden Maßes an KI-Kompetenz (Art. 4 KI-VO) einschlägig.

## Erfüllung der Betreiberpflichten durch den Plattformbetreiber

Betreiber eines KI-Systems ist, wer die Kontrolle über den Betrieb ausübt, unter dessen Verantwortung ein KI-System verwendet wird (s. o. 1. „Akteure nach der KI-Verordnung“). Dem Betreiber werden in der KI-Verordnung insbesondere bei dem Betrieb von Hochrisiko-KI-Systemen umfassende Pflichten zur Überwachung des sicheren Betriebs auferlegt (s. o. 4.2. „Betreiberpflichten“). Diese Zuordnung der Pflichten zum Betreiber statt zum Anbieter liegt u. a. darin begründet, dass der Betreiber dem Betrieb des Systems im konkreten Anwendungsfall nähersteht als der Anbieter und insofern die Risiken des Betriebs besser erkennen sowie die Überwachung am effizientesten durchführen kann.

Im vorliegenden Fall der Recruiting- und Matching-App kommen als Betreiber des Systems zunächst – in Anlehnung zur Nutzung von Chatbots für Social-Media-Beiträge, das interne Wissensmanagement oder auch die Verwendung von Recruiting KI-Tools direkt im Unternehmen – Unternehmen, welche die Plattform zum Recruiting nutzen, in Betracht. Das Unternehmen entscheidet, die Plattform zur Verbreitung der eigenen Stellenanzeigen und zur Suche nach geeigneten Bewerbern zu nutzen oder eine Nutzung zu unterlassen und hat damit entscheidenden Einfluss darauf, ob die konkrete Stellenausschreibung mit Hilfe von KI bearbeitet und die Stelle mit Hilfe von KI besetzt wird. Unternehmen haben auch die vollständige Kontrolle darüber, sich an die Betriebsanleitung bzw. die Nutzungsbedingungen der Plattform zu halten. Je

nach Aufbau der Plattform wäre es auch denkbar, dass das nutzende Unternehmen vom Anbieter Erläuterungen zum Zustandekommen des konkreten einzelnen Scores zur Verfügung gestellt bekommt, etwa über lokale Erklärungen im Rahmen von XAI-Methoden. Lokale Erklärungen stellen für eine KI-Entscheidung wichtige Attribute wie Ausbildung der Bewerber oder vorherige Berufserfahrung sowie deren Gewichtung also deren Bedeutung für die KI-Entscheidung dar<sup>[15, S. 702]</sup>. Hierdurch würden Unternehmen, welche die Plattform nutzen, in die Lage versetzt, Bewerbern aussagekräftige Erläuterungen über die KI-Entscheidung zur Verfügung zu stellen. Außerdem könnten sie den Betrieb des Systems für die eigenen Stellenausschreibungen überwachen.

Andere der Betreiberaufgaben können jedoch durch das Unternehmen, das die Plattform nutzt, nicht erfüllt werden. Dies gilt etwa für die initiale Information von potenziellen zukünftigen Bewerbern darüber, dass sie einer KI-gestützten Entscheidung unterliegen, wenn sie ihre Unterlagen auf der Plattform hochladen. Zu diesem Zeitpunkt besteht keine Verbindung zwischen dem Bewerber und dem einzelnen Unternehmen. Auch die Überwachung des Systems im Gesamten über verschiedene plattformnutzende Unternehmen hinweg kann nur durch die Plattformanbieter selbst wahrgenommen werden. Nur durch diese Überwachung des Systems im Gesamten kann aber die Sicherheit garantiert werden. Vorfälle, die Unternehmen, welche lediglich eine Stellenanzeige schalten, wie unbedeutende Zwischenfälle oder zufällige Ausfälle erscheinen, können durch eine Gesamtaufsicht in ein übergeordnetes Muster z. B. der Diskriminierung eingeordnet werden. Erst hierdurch können systematische Fehler erkannt werden. Der Plattformbetreiber hat übergeordnete Übersicht und übergeordneten Einfluss auf das System und kann den Gesamtbetrieb am effektivsten überwachen. Daher muss er in dieser Hinsicht als Betreiber gelten.

### Praxistipp:

Die Erfüllung der einzelnen Betreiberpflichten sollte in Verträgen oder im Anwendungsfall z. B. in den Nutzungsbedingungen der Plattform geregelt und plattformnutzenden Unternehmen klar kommuniziert werden, soweit die technischen Voraussetzungen für die Erfüllung der Pflichten gegeben sind.



# Fazit

Schon zum jetzigen Zeitpunkt werden vielfach KI-Systeme im Recruitingprozess eingesetzt und können zu erheblichen Effizienzgewinnen führen. KI-Systeme stellen KMU allerdings sowohl als Anbieter als auch als Betreiber vor vielfältige (neue) Herausforderungen.

Zentral zur Einschätzung der Anforderungen aus der KI-Verordnung ist insbesondere die Einschätzung der Risikostufe der Systeme. Hierfür stehen vielfältige Hilfestellungen und Tools zur Verfügung, die sich zur ersten Einschätzung eignen wie der KI-Compliance-Kompass der Bundesnetzagentur. Sie ersetzen jedoch nicht die genaue Analyse u. U. durch einen Rechtsanwalt im konkreten Anwendungsfall, da sich diese durchaus als komplex darstellen kann. Gerade KI-Systeme, die dazu beitragen, Bewerber zu bewerten, können als Hochrisiko-KI-Systeme zu klassifizieren sein. Ausnahmen von der Klasse des hohen Risikos sind im Bereich des Recruitings zwar möglich, müssen jedoch sorgfältig geprüft und dokumentiert werden. Auch die genaue Bestimmung der eigenen Rolle im Rahmen der KI-Verordnung ist bei zahlreichen Beteiligten nicht in jedem Fall trivial und trägt maßgeblich zur Bestimmung der eigenen Pflichten bei.

Für Unternehmen bedeutet dies: Der rechtssichere Einsatz von KI im Recruiting wie der Recruiting- und Matching-App setzt ein strukturiertes Vorgehen voraus. Dazu gehören eine frühzeitige rechtliche Bewertung, klare vertragliche Regelungen zwischen Plattformbetreibern und nutzenden Unternehmen, transparente Informationen gegenüber Bewerbern, wirksame menschliche Aufsicht sowie eine fortlaufende Überwachung des Systems.

Mit einem geplanten, gewissenhaften Vorgehen und unter Beachtung der in diesem Beitrag genannten Punkte steht dennoch der rechtssicheren Entwicklung und Nutzung von KI im KMU nichts im Wege.







↑ © creativeart - Magnific.com

## Teil 2: Datenschutzrechtliche Anforderungen beim Einsatz einer KI-gestützten Recruiting- und Matching-App

KI-gestützte Anwendungen im Recruiting können auf sehr unterschiedliche Weise eingesetzt werden. Im Mittelpunkt der folgenden datenschutzrechtlichen Betrachtung steht eine Anwendung, die Arbeitssuchende und Unternehmen anhand von Kompetenzen, Testergebnissen und Stellenanforderungen passgenau zusammenführen soll. Die Grundidee besteht darin, dass Unternehmen zunächst eine Branche, eine Tätigkeit oder ein konkretes Jobprofil angeben. Auf dieser Grundlage erstellt das System ein passendes Anforderungsprofil, das anschließend bei Bedarf angepasst oder weiter konkretisiert werden kann. Arbeitssuchende können daraufhin digitale Kompetenztests absolvieren. Die dabei erzielten Ergebnisse werden ausgewertet und mit den Anforderungen der jeweiligen Stelle abgeglichen.

Eine solche Anwendung geht damit über ein klassisches Bewerbermanagementsystem hinaus. Sie dient nicht nur dazu, Bewerbungen digital zu organisieren oder Unterlagen zu verwalten, sondern unterstützt aktiv die Einschätzung, welche Personen für bestimmte Tätigkeiten fachlich geeignet erscheinen. Dazu verbindet sie Kompetenzanalyse, automatisierte Bewertung und KI-gestütztes Matching. Gerade diese Kombination macht die Anwendung zu einem geeigneten Ausgangsbeispiel für die rechtliche Analyse: Es werden personenbezogene Daten verarbeitet, Testergebnisse erzeugt, Scores oder Eignungseinschätzungen gebildet und diese

Ergebnisse anschließend im Recruitingprozess nutzbar gemacht.

### Datenschutzrechtliche Rollen: Wer ist verantwortlich?

Zunächst ist zu klären, wer datenschutzrechtlich für die einzelnen Verarbeitungsschritte verantwortlich ist. Nach Art. 4 Nr. 7 DSGVO ist Verantwortlicher, wer über die **Zwecke und Mittel** der Verarbeitung personenbezogener Daten **entscheidet**.

Bei einer **Recruiting- und Matching-App** kommen vor allem der **App-Betreiber** und das **suchende Unternehmen** in Betracht. Der Betreiber stellt die technische Infrastruktur bereit, ermöglicht Tests, berechnet Scores, betreibt das Matching und speichert Daten. Das Unternehmen nutzt die Anwendung, um Bewerbende für konkrete Stellen zu finden, Ergeb-

nisse einzusehen, Kandidat\*innen zu kontaktieren oder Auswahlentscheidungen vorzubereiten.

Entscheidet der App-Betreiber selbst darüber, wie Tests aufgebaut sind, wie Scores berechnet werden, nach welchen Kriterien Matching-Ergebnisse entstehen oder wie lange Daten im Talentpool gespeichert werden, spricht viel für eine eigene Verantwortlichkeit. Nutzt ein Unternehmen die App für eine konkrete Stellenausschreibung und entscheidet auf Grundlage der Ergebnisse über Kontaktaufnahme oder weitere Auswahl, ist es hierfür regelmäßig ebenfalls verantwortlich. Maßgeblich ist nicht allein die vertragliche Bezeichnung, sondern die tatsächliche Entscheidung über Zwecke und Mittel<sup>[16][17]</sup>.

## Gemeinsame Verantwortlichkeit

Je nach Ausgestaltung kann auch eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegen, etwa wenn App-Betreiber und Unternehmen gemeinsam festlegen, welche Daten erhoben oder wie Matching-Ergebnisse genutzt werden. Werden Daten dagegen ausschließlich nach Weisung eines Unternehmens verarbeitet, kann eine **Auftragsverarbeitung nach Art. 28 DSGVO** vorliegen. Gerade bei webbasierten Bewerbermanagement-Tools ist dies praktisch bedeutsam; der Arbeitgeber bzw. Auftraggeber bleibt dann für die Einhaltung der Datenschutzvorschriften verantwortlich<sup>[18][17]</sup>.

Bei Plattformmodellen, Talentpools oder unternehmensübergreifendem Matching wird eine reine Auftragsverarbeitung jedoch oft nicht passen, sobald der Plattformbetreiber eigene Zwecke verfolgt, etwa den Aufbau eines allgemeinen Talentpools oder die Vermittlung an verschiedene Unternehmen.

### Praxistipp:

Die Rollen sollten für jeden Verarbeitungsschritt getrennt geprüft werden: Registrierung, Testdurchführung, Scoring, Matching, Talentpool, Kontaktaufnahme, Speicherung, Löschung und Weiterentwicklung des Systems.

# Rechtsgrundlage: Wann dürfen Bewerberdaten verarbeitet werden?

Jede Verarbeitung personenbezogener Daten benötigt eine Rechtsgrundlage. Für Datenverarbeitungen im Zusammenhang mit einem konkreten Bewerbungsverfahren kommt vor allem § 26 Abs. 1 BDSG in Betracht. Danach dürfen personenbezogene Daten von Bewerbern verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Ergänzend kann Art. 6 Abs. 1 lit. b DSGVO relevant sein, wenn die Verarbeitung zur Durchführung vorvertraglicher Maßnahmen erforderlich ist<sup>[16][17]</sup>.

Nutzt ein Unternehmen die App für eine **konkrete Stelle** und absolvieren Bewerben hierfür einen **fachbezogenen Kompetenztest**, können hierfür erforderliche Daten grundsätzlich verarbeitet werden. Anders ist die Lage bei Funktionen, die über ein konkretes Bewerbungsverfahren hinausgehen, etwa langfristige Speicherung, Talentpool, Matching mit mehreren Unternehmen, spätere Stellenangebote oder weitergehende Persönlichkeits-, Potenzial- oder Soft-Skill-Profile.

Für solche Zusatzfunktionen wird häufig eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich sein. Im Bewerbungs- und Beschäftigungskontext ist die Freiwilligkeit jedoch kritisch zu prüfen (§ 26 Abs. 2 BDSG). Bewerben dürfen nicht faktisch gezwungen sein, zusätzlichen Verarbeitungen zuzustimmen, nur um an einem Bewerbungsverfahren teilnehmen zu können. Gerade beim KI-Profiling im Recruiting wird die Einwilligung daher als datenschutzrechtlich herausfordernd eingeordnet<sup>[15][16]</sup>.

### Praxistipp:

Pflicht- und Zusatzfunktionen sollten klar getrennt werden. Ein Test für eine konkrete Stelle sollte nicht automatisch zur Aufnahme in einen allgemeinen Talentpool führen.



# Scoring, Matching und Profiling

Besonders sensibel ist der Kern der Anwendung: die automatisierte Bewertung von Kompetenzen und das Matching mit Stellenprofilen. Wird aus Testergebnissen oder sonstigen Bewerberdaten ein Score gebildet, der die fachliche Eignung oder Passgenauigkeit beschreibt, kann darin ein Profiling im Sinne von Art. 4 Nr. 4 DSGVO liegen. Profiling bedeutet, dass personenbezogene Daten automatisiert verarbeitet werden, um persönliche Aspekte zu bewerten oder vorherzusagen, etwa Fähigkeiten, berufliche Eignung, Leistung, Interessen oder Verhalten (vgl. Art. 4 Nr. 4 DSGVO)<sup>[15][16]</sup>.

Profiling ist nicht per se verboten, muss aber transparent, erforderlich, verhältnismäßig und durch eine Rechtsgrundlage gedeckt sein. Bewerbende dürfen zudem grundsätzlich nicht einer ausschließlich automatisierten Entscheidung unterworfen werden, wenn diese rechtliche Wirkung entfaltet oder sie ähnlich erheblich beeinträchtigt. Eine vollautomatische Ablehnung oder Auswahl allein aufgrund eines KI-Scores wäre daher regelmäßig unzulässig (vgl. Art. 22 Abs. 1 DSGVO)<sup>[15][16]</sup>.

Zulässig kann dagegen eine Empfehlung, Vorbewertung oder strukturierte Einschätzung sein, wenn anschließend ein Mensch die Entscheidung eigenständig prüft. Diese Kontrolle muss tatsächlich stattfinden und darf nicht nur formal vorgesehen sein. Lang/Schwaab betonen, dass eine menschliche Letztentscheidung hinreichende Informationen und eigenen Entscheidungsspielraum voraussetzt; Arbeitgeber sollten diese dokumentieren<sup>[16]</sup>. Auch Holthausen weist darauf hin, dass People-Analytics-Software nur als Entscheidungshilfe eingesetzt werden sollte<sup>[15]</sup>.

Gerade bei Matching-Systemen besteht das Risiko des Automation Bias. Ein angezeigter Wert wie „95 % Passung“ kann Entscheidungen stark beeinflussen. Deshalb sollte ein Score nicht als endgültige Wahrheit erscheinen, sondern durch Kompetenzbereiche, Einzelbewertungen, Unsicherheiten oder Antwortprotokolle ergänzt werden.

## Praxistipp:

Ein Score sollte nie alleinige Entscheidungsgrundlage sein. Unternehmen sollten verpflichtet werden, KI-Ergebnisse kritisch zu prüfen und ihre eigene Entscheidung zu dokumentieren.

# Transparenz gegenüber Bewerbenden

Bewerbende müssen klar und verständlich darüber informiert werden, was mit ihren Daten geschieht. Die Informationspflichten ergeben sich insbesondere aus Art. 12, 13 und 14 DSGVO. Transparenz ist zudem ein zentraler Datenschutzgrundsatz aus Art. 5 Abs. 1 lit. a DSGVO<sup>[15]</sup>.

Bei einer Recruiting- und Matching-App sollten Nutzerinnen und Nutzer insbesondere darüber informiert werden,

- welche Daten erhoben werden,
- zu welchen Zwecken diese Daten verarbeitet werden,
- ob ein Kompetenztest durchgeführt wird,
- ob aus den Testergebnissen ein Score oder Matching-Ergebnis erstellt wird,
- ob ein Profiling im Sinne der DSGVO stattfindet,
- welche Unternehmen oder sonstigen Stellen Zugriff auf die Daten erhalten,
- ob und unter welchen Voraussetzungen Daten in einen Talentpool aufgenommen werden,
- wie lange die Daten gespeichert werden,
- welche Rechte den betroffenen Personen zustehen.

Bei automatisierten Bewertungen müssen außerdem aussagekräftige Informationen über die involvierte Logik sowie über Tragweite und angestrebte Auswirkungen bereitgestellt werden (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h DSGVO). Der vollständige Algorithmus muss nicht offengelegt werden. Bewerbende müssen aber verstehen können, welche Faktoren wesentlich sind und welche Bedeutung das Ergebnis im Bewerbungsprozess hat. Bei KI-Analysen kann oft nicht der gesamte Algorithmus nachvollziehbar beschrieben werden; umso wichtiger sind klare Angaben zu System, Zwecken, Eingabedaten und zulässigen Verwendungen<sup>[15]</sup>.

Transparenz sollte nicht erst durch eine lange Datenschutzerklärung hergestellt werden. Bewerbende sollten bereits vor dem Test kurz erfahren, was passiert, wer das Ergebnis sehen kann und ob es nur für eine konkrete Stelle oder auch für weitere Matching-Prozesse genutzt wird.



#### Praxistipp:

Sinnvoll ist ein gestuftes Informationsmodell: kurze Hinweise direkt vor dem Test, ausführliche Datenschutzinformationen über einen Link und auf Anfrage eine verständliche Erläuterung des individuellen Ergebnisses.

## Datenschutz-Folgenabschätzung

Bei KI-gestütztem Scoring und Matching sollte regelmäßig geprüft werden, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist. Sie ist durchzuführen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen mit sich bringt. Das kann insbesondere bei neuen Technologien, Profiling, systematischer Bewertung persönlicher Aspekte oder automatisierter Vorauswahl der Fall sein (vgl. Art. 35 DSGVO) <sup>[15][16]</sup>.

Bei einer App, die Bewerbende bewertet, Kompetenzprofile erstellt, Scores berechnet und Ergebnisse Unternehmen zugänglich macht, spricht vieles für eine Datenschutz-Folgenabschätzung. Die Verarbeitung betrifft berufliche Chancen und kann Rückschlüsse auf Fähigkeiten, Herkunft, Bildungswege oder andere persönliche Merkmale ermöglichen. (vgl. BayLDA, „KI & Datenschutz“, abrufbar unter <https://www.lda.bayern.de/de/ki.html>).

Die Folgenabschätzung sollte beschreiben, welche Daten verarbeitet werden, wie Tests und Scores funktionieren, wer Zugriff erhält, welche Risiken bestehen und welche Schutzmaßnahmen vorgesehen sind. Dazu gehören insbesondere Maßnahmen gegen Fehlbewertungen, Diskriminierung, unberechtigte Zugriffe, zu lange Speicherung und intransparente Entscheidungen. Datenschutz sollte dabei bereits in der Entwicklung berücksichtigt werden („Privacy by Design“, Art. 25 DSGVO).

#### Praxistipp:

Die Datenschutz-Folgenabschätzung sollte als lebendes Dokument verstanden und bei neuen Funktionen wie Soft-Skill-Analysen, erweitertem Talentpool oder KI-generierten Interviewfragen aktualisiert werden.

## Datenminimierung, Zweckbindung und Löschung

Nach Art. 5 DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden (Art. 5 Abs. 1 lit. b DSGVO). Es dürfen nur erforderliche Daten erhoben werden (Art. 5 Abs. 1 lit. c DSGVO), und sie dürfen nicht länger gespeichert werden, als es für den jeweiligen Zweck notwendig ist (Art. 5 Abs. 1 lit. e DSGVO). Gerade bei Big Data und KI besteht ein Spannungsverhältnis zu diesen Grundsätzen <sup>[15]</sup>.

Für eine Recruiting- und Matching-App bedeutet das: Es sollte genau unterschieden werden, **welche Daten für welchen Zweck** benötigt werden. Daten aus einem konkreten Kompetenztest dürfen nicht automatisch für andere Zwecke genutzt, in einen Talentpool übertragen oder anderen Unternehmen zugänglich gemacht werden. Die Durchführung eines Bewerbungsverfahrens, die spätere Nutzung für Matching-Prozesse und die interne Systemverbesserung sind unterschiedliche Zwecke und benötigen jeweils eine passende Grundlage.

Auch das **Löschkonzept** ist zentral. Bewerbungsdaten sollten gelöscht werden, wenn sie für den ursprünglichen Zweck nicht mehr benötigt werden und keine gesetzlichen Aufbewahrungsinteressen entgegenstehen. Für Talentpool-Daten können längere Speicherfristen denkbar sein, wenn die betroffene Person wirksam zugestimmt hat. Auch dann sollten klare Fristen, Erinnerungen und einfache Löschmöglichkeiten vorgesehen werden.

Besondere Vorsicht gilt bei Daten, die Rückschlüsse auf geschützte Merkmale ermöglichen, etwa Alter, Geschlecht, Herkunft, Behinderung oder Religion. Auch scheinbar neutrale Daten können solche Rückschlüsse mittelbar zulassen. Daher sollten Maßnahmen wie Anonymisierung, Pseudonymisierung, Zugriffsbeschränkungen und klaren Löschkonzepten ergriffen werden. <sup>[15]</sup>.

#### Praxistipp:

Das Löschkonzept sollte zwischen Registrierungsdaten, Bewerbungsdaten, Testergebnissen, Scores, Talentpool-Daten, Kommunikationsdaten, Protokolldaten und anonymisierten Statistikdaten unterscheiden.



# Schutz vor Diskriminierung und fehlerhaften Bewertungen

Datenschutzrecht und Antidiskriminierungsrecht greifen bei KI-gestütztem Recruiting eng ineinander. Nach Art. 5 Abs. 1 lit. d DSGVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls aktuell sein. Fehlerhafte oder verzerrte Daten können zu falschen Bewertungen führen. Zugleich kann ein KI-System Bewerbende benachteiligen, wenn Trainingsdaten, Bewertungskriterien oder Gewichtungen bestimmte Gruppen systematisch schlechter stellen.

Nach dem AGG dürfen Bewerbende insbesondere nicht wegen **Geschlecht, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter oder sexueller Identität** benachteiligt werden (§ 1 AGG). Das gilt auch, wenn die Benachteiligung nicht ausdrücklich programmiert wurde, sondern mittelbar durch bestimmte Datenmuster entsteht.

Bei einer Kompetenz- und Matching-App können etwa bisherige Auswahlmuster, bestimmte Bildungswege, Sprachmuster oder Berufserfahrungen zu Verzerrungen führen. Auch fachliche Tests müssen tatsächlich berufsrelevante Kompetenzen messen und dürfen nicht unbeabsichtigt andere Faktoren wie Sprachstil, kulturelle Prägung oder Testvertrautheit bewerten. KI-Systeme werden auf vorhandenen, häufig menschlich geprägten Datensätzen trainiert werden und deshalb bestehende Verzerrungen fortführen können; Bias-Mitigation-Maßnahmen sind daher besonders wichtig<sup>[16]</sup>.

## Praxistipp:

Der App-Betreiber sollte regelmäßig prüfen, ob bestimmte Gruppen systematisch schlechter bewertet werden. Dazu gehören Bias-Prüfungen, Qualitätssicherung, Dokumentation der Bewertungskriterien, Beschwerdemöglichkeiten und Schulungen für Unternehmen.

# Technische und organisatorische Schutzmaßnahmen

Nach Art. 32 DSGVO müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Bei einer Recruiting- und Matching-App sind die Anforderungen regelmäßig hoch, weil sensible Informationen über berufliche Fähigkeiten, Karrierewege, Testergebnisse und Eignungseinschätzungen verarbeitet werden.

Wichtig sind rollenbasierte Zugriffskonzepte, sichere Authentifizierung, Verschlüsselung, Protokollierung von Zugriffen, klare Berechtigungskonzepte für Unternehmen, Trennung verschiedener Kundenbereiche, Schutz vor unberechtigter Weitergabe, regelmäßige Sicherheitsprüfungen und klare Prozesse für Auskunft, Berichtigung und Löschung<sup>[15]</sup>.

Unternehmen dürfen nur die Daten sehen, für die eine Rechtsgrundlage besteht. Ergebnisse aus einem Test für ein bestimmtes Unternehmen dürfen nicht automatisch anderen Unternehmen angezeigt werden. Für eine Sichtbarkeit im Talentpool braucht es eine eigene Freigabe. Bei Plattform-, White-Label- oder Personaldienstleistermodellen muss zudem klar geregelt sein, wer auf welche Daten zugreifen darf.

## Praxistipp:

Datenschutzfreundliche Voreinstellungen sind Pflicht (Art. 25 DSGVO). Standardmäßig sollten möglichst wenige Daten sichtbar sein; erweiterte Freigaben sollten aktiv bestätigt werden.



# Besondere Anforderungen an den Talentpool

Ein Talentpool ist praktisch attraktiv, aber datenschutzrechtlich besonders sensibel. Während ein Test für eine konkrete Stelle eng mit einem bestimmten Bewerbungsverfahren verbunden ist, geht ein Talentpool darüber hinaus. **Die Daten werden gespeichert**, um sie später für weitere Stellen, andere Unternehmen oder neue Matching-Prozesse zu nutzen.

Für die Aufnahme in einen Talentpool sollte daher regelmäßig eine gesonderte Einwilligung eingeholt werden. Diese muss freiwillig, informiert und widerrufbar sein. Bewerbende sollten klar erkennen können, welche Daten aufgenommen werden, wer Zugriff erhält, für welche Stellen oder Unternehmen sie sichtbar sind und wie lange die Daten gespeichert werden. Wegen der kritisch zu prüfenden Freiwilligkeit im Bewerbungs- und Beschäftigungskontext sollte die Teilnahme an einem konkreten Bewerbungsverfahren nicht von der Aufnahme in einen Talentpool abhängig gemacht werden (vgl. § 26 Abs. 2 BDSG)<sup>[15][16]</sup>.

## Praxistipp:

Die Aufnahme in den Talentpool sollte nie automatisch erfolgen. Empfehlenswert ist ein aktiver Opt-in mit klarer Erklärung, einfacher Widerrufsmöglichkeit und regelmäßiger Erinnerung.

Der App-Betreiber sollte festlegen, für welche Zwecke die Anwendung bestimmt ist, wie Scores zu verstehen sind, welche Grenzen das System hat und dass Unternehmen Ergebnisse nicht als alleinige Entscheidungsgrundlage verwenden dürfen. Unternehmen sollten verpflichtet werden, eine eigene menschliche Prüfung vorzunehmen, Ergebnisse kritisch einzuordnen und arbeits- sowie datenschutzrechtliche Vorgaben einzuhalten.

Gleichzeitig bleibt der App-Betreiber für Bereiche verantwortlich, die er selbst kontrolliert, insbesondere technische Sicherheit, Scoring- und Matching-Logik, datenschutzfreundliche Voreinstellungen, Transparenz der Systemfunktionen und Umsetzung von Betroffenenrechten in seinem Einflussbereich.

Bei White-Label-Modellen, Branchenlösungen oder Personaldienstleister-Konstellationen sollten die Rollen besonders sorgfältig geregelt werden<sup>[15][16]</sup>.

## Praxistipp:

AGB und Verträge sollten konkrete Nutzungspflichten enthalten: keine vollautomatisierten Entscheidungen, Pflicht zur menschlichen Prüfung, kein zweckwidriger Export, keine Diskriminierung, Einhaltung von Löschfristen und klare Zuständigkeiten bei Betroffenenanfragen.

## Fazit

Der Einsatz einer KI-gestützten Recruiting- und Matching-App ist datenschutzrechtlich möglich, erfordert aber eine sorgfältige Gestaltung. Besonders sensibel sind die automatisierte Bewertung von Kompetenzen, die Bildung von Scores, das Matching mit Stellenprofilen und die Aufnahme in einen Talentpool. Je stärker ein Score oder Matching-Ergebnis die Auswahlentscheidung beeinflusst, desto höher sind die Anforderungen an Transparenz, Dokumentation, menschliche Kontrolle und Diskriminierungsschutz<sup>[15][16]</sup>.

Für den App-Betreiber empfiehlt es sich, Datenschutz von Anfang an in Technik, Nutzerführung, Verträge und interne Prozesse einzubauen. Entscheidend sind klare Verantwortlichkeiten, tragfähige Rechtsgrundlagen, verständliche Informationen, echte menschliche Kontrolle, ein differenziertes Löschkonzept und wirksame Schutzmaßnahmen gegen Fehlbewertungen und Diskriminierung.

# Verantwortlichkeit und Absicherung durch Verträge

Verträge, Nutzungsbedingungen und Datenschutzinformationen können gesetzliche Verantwortlichkeiten nicht beliebig verschieben, aber klarstellen, wer welche Pflichten übernimmt und wie die Anwendung genutzt werden darf.





# Literaturverzeichnis

- 1** G. Borges, „Die europäische KI-Verordnung (AI-Act): Teil 1,“ CR, pp. 497-507, 2024.
- 2** J. Kirschke-Biller und L. A. Füllsack, „Art. 3,“ in BeckOK KI-Recht, 6. Edition Stand: 01.11.2025, München, C. H. Beck, 2025, p. Rn. 79.
- 3** M. Schuh und H. Witt, „KI-Systeme und ihre Betreiber nach der KI-VO: Pflichten und Abgrenzung zum Endnutzer,“ EuDIR, pp. 142-148, 2025.
- 4** C. Wendehorst, „Art. 3,“ in KI-VO: Verordnung über Künstliche Intelligenz Kommentar, 1. Auflage, M. Martini und C. Wendehorst, Hrsg., München, C. H. Beck, 2024, p. Rn. 86.
- 5** U. Spiegel und M. Höving, „Die Klassifizierung von KI-Systemen nach der KI VO,“ KIR, pp. 231-239, 2025.
- 6** M. Ebers und C. Streitböcker, „Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung,“ RDi, pp. 393-400, 2024.
- 7** D. Gesmann-Nuissl und I. Tacke, „Compliance-Tipps für KMU: Rechtssichere Chatbots,“ in EU AI Act – Verständlich für Unternehmen und Institutionen, Stuttgart, Schäffer-Poeschel, im Erscheinen.
- 8** Europäische Kommission, „ANNEX to the COMMUNICATION FROM THE COMMISSION Draft Commission guidelines on the classification of high-risk AI systems under Article,“ Mai 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems>. [Zugriff am 24 Juni 2026].
- 9** P. Bronner, „Risikoklassifizierung, Risikobewertung und Risikominimierung nach der KI-Verordnung,“ KIR, pp. 55-62, 2024.
- 10** A. Lauber-Rönsberg, P. Meinel, J. Laux und H. Ruschmeier, „Hochrisiko oder Ausnahme? Zur Auslegung von Art. 6 Abs. 3 KI VO,“ KIR, pp. 399-407, 2025.
- 11** J. Lommatzsch und R. Albrecht, „Einsatz von KI im Personalwesen von Unternehmen – Neue Herangehensweise nach Geltung der KI-VO,“ GWR, pp. 37-40, 2025.
- 12** I. Eisenberger, „Art. 27,“ in KI-VO: Verordnung über Künstliche Intelligenz Kommentar, 1. Auflage, M. Martini und C. Wendehorst, Hrsg., München, C. H. Beck, 2024, p. Rn. 24 ff..
- 13** Europäische Kommission, „Draft Guidance Article 73 AI-Act – Incident Reporting (High-Risk-AI-Systems),“ September 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks>. [Zugriff am 24 06 2026].
- 14** Europäische Kommission, „Incident Report for Serious Incidents under the AI Act (High-risk AI systems) (Draft),“ September 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks>. [Zugriff am 24 06 2026].
- 15** M. Becker, P. Birnstill und A. Ebert, „Erklärbarkeit von KI-Systemen unter der KI-Verordnung - Vorgaben der KI-VO für Hochrisiko-KI-Systeme im Lichte aktueller Erklärverfahren aus dem Feld der Explainable AI (XAI),“ CR, pp. 701-707, 2025.
- 16** J. Holthausen, „Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen,“ Recht der Arbeit (RdA) 2021, 19.
- 17** Lang / Schwaab, Legal Tech Zeitschrift (LTZ) 2025, 28.
- 18** M. Lützel und D. Kopp, „Bewerbermanagement-Tools,“ Arbeitsrecht Aktuell (ArbRAktuell) 2015, 491.





## Teil 1 verfasst von

**INES TACKE** ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz ist sie als KI-Trainerin tätig und beschäftigt sie sich mit Innovations- und Technikrecht.

[ines-maria.tacke@digitalzentrum-chemnitz.de](mailto:ines-maria.tacke@digitalzentrum-chemnitz.de)

## Teil 2 verfasst von

**ANTONIA STOLL** ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz beschäftigt sie sich insbesondere mit datenrechtlichen Themen rund um IT und Digitalisierung.

[antonia.stoll@digitalzentrum-chemnitz.de](mailto:antonia.stoll@digitalzentrum-chemnitz.de)

## Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

### **WAS IST MITTELSTAND-DIGITAL?**

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren* und der Initiative *IT-Sicherheit in der Wirtschaft* umfassende Unterstützung bei der Digitalisierung mit dem Schwerpunkt Künstliche Intelligenz. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter [www.mittelstand-digital.de](http://www.mittelstand-digital.de).





Mittelstand-Digital  
**Zentrum  
Chemnitz**

Gefördert durch:



Mittelstand-Digital

aufgrund eines Beschlusses  
des Deutschen Bundestages