DGUV
Deutsche Gesetzliche Unfallversicherung
Spitzenverband

Januar/Februar 1/2026

DGUV forum

Schwerpunkt

Digitalisierung und KI im Arbeitsschutz

Chancen und Herausforderungen von KI im Arbeitsschutz 2 | KI und soziale Sicherung global 6 | Gesunde Führung und KI 14 | Psychische Belastung durch KI in der Arbeitswelt 20 | KI in der Schule: Chancen und Risiken 25 | Digitale Anwendungen beim BGM 32 | Maschinensicherheit und KI 35 | Trust in Automation 38 | Sicherer Umgang mit Multikoptern 43 | Industrial Security in KMU 47

Weitere Themen Interview mit den DGUV-Vorstandsvorsitzenden 51 | Rechtskolumne 54

Künstliche Intelligenz im Arbeitsschutz: Chancen und Herausforderungen

Künstliche Intelligenz (KI) verändert die Arbeitswelt in rasantem Tempo. Für die Arbeitsschutzakteurinnen und -akteure entstehen neue Chancen für Prävention und Arbeitsschutz – aber auch Risiken, die ein vorausschauendes und menschenzentriertes Handeln erfordern.

Die Diskussion um KI prägt zunehmend die Arbeitswelt. Während der Begriff Digitalisierung häufig klassische Themen wie Automatisierung und Vernetzung beschreibt, geht KI einen Schritt weiter: Laut der KI-Verordnung sind KI-Systeme auf einen autonomen Betrieb ausgelegt, können nach der Inbetriebnahme Anpassungsfähigkeit zeigen und sowohl physische als auch virtuelle Umgebungen beeinflussen. Für den Arbeitsschutz besitzt dieses Thema besondere Relevanz: KI verändert Arbeitssysteme, Prozesse, Rollenprofile und Anforderungen an Beschäftigte. Damit eröffnet sie neue Chancen für Sicherheit und Gesundheit, birgt jedoch zugleich Risiken, die systematisch beurteilt und aktiv gestaltet werden müssen. Darüber hinaus bietet KI neue Möglichkeiten für das Präventionshandeln der Unfallversicherungsträger (UVT).

Handlungsfelder für die Unfallversicherung

Für die UVT ergeben sich zentrale Handlungsfelder, um die Potenziale der KI im Arbeitsschutz zu nutzen und zugleich Risiken zu minimieren.

Analyse, Bewertung und menschenzentrierte Gestaltung von KI

Eine zentrale Fragestellung des Arbeitsschutzes lautet: Wie können KI-Anwendungen sicher und gesundheitsgerecht in Unternehmen eingesetzt werden? Dies betrifft alle Herstellenden von Maschinen und Arbeitsmitteln. Im Vordergrund stehen dabei technologische Aspekte wie funktionale Sicherheit und der Schutz vor Fehlfunktionen. Diesbezügliche Einflussmöglichkeiten der UVT bestehen hier etwa über die Mitwirkung in nationalen und internationalen Gremien sowie Forschungsprojekten. Eine rein technologische Betrachtung greift jedoch zu kurz. Für eine wirksame Prävention ist es entscheidend, die menschenzentrierte Perspektive einzubeziehen. Dazu gehören partizipative Ansätze bei der Einführung von KI-Systemen, die ergonomische Gestaltung der Mensch-Maschine-Schnittstellen sowie die Berücksichtigung KI-spezifischer Belastungen in der Gefährdungsbeurteilung.

Key Facts

- Ein sicherer und gesunder KI-Einsatz erfordert menschenzentrierte Gestaltung, Forschung und gezielte Qualifizierung von Fachkräften
- KI kann selbst ein Präventionsinstrument werden
- Eine Online-Sifa-Befragung zeigt: Private KI-Erfahrung fördert berufliche Nutzung signifikant; betriebliche Anwendung im Arbeitsschutz bleibt noch gering – hier liegt großes Schulungs- und Transferpotenzial

Arbeitspsychologische Perspektive auf die Gestaltung des KI-Einsatzes

Veränderung von Aufgaben, Verantwortung und Kontrolle: Der Einsatz von KI verändert Zuschnitt und Wahrnehmung von Arbeitsaufgaben und Verantwortlichkeiten. Automatisierte Entscheidungsvorschläge können Kontroll- und Entscheidungsspielräume reduzieren. Erforderlich sind klare Verantwortungsdefinitionen, Eskalationspfade und nachvollziehbare Zuständigkeiten.

Akzeptanz und Vertrauen: Nachhaltige Einführung gelingt, wenn Beschäftigte Vertrauen in Funktion und Grenzen der Systeme entwickeln. Transparente Informationen, Erklärbarkeit der Entscheidungslogiken sowie frühe Einbindung fördern Akzeptanz.

Verhaltensadaption und Automatisierungsbias: Beschäftigte neigen dazu, automatisierten Vorschlägen übermäßig zu vertrauen. Schulungen, Checklisten und das Vier-Augen-Prinzip helfen, Fehlhandlungen durch unkritische Übernahme zu vermeiden.

Vertrauenskalibrierung: Ziel ist ein angemessenes, situationsabhängig reguliertes Vertrauen – weder blindes Vertrauen noch generelle Ablehnung. Partizipative Ansätze bei der Einführung und praxisnahe Trainings mit Feedback unterstützen die Kalibrierung.

Einschränkungen von Handlungsspielräumen: Stark vorstrukturierte KI-Workflows können Handlungsspielräume einengen und psychisch belasten. Arbeitsgestaltung sollte Eingriffsmöglichkeiten, Umsetzung des durch die KI-Verordnung geforderten „Human in the loop“-Ansatzes durch Override-Regeln und gestaltbare Freiheitsgrade sichern.[1]

Kompetenzverschiebungen und Weiterbildung: KI verändert Kompetenzprofile. Technische, analytische aber auch Metakompetenzen wie zum Beispiel kommunikative und reflektive Fähigkeiten sowie die Bereitschaft zum lebenslangen Lernen gewinnen an Gewicht. Qualifizierungskonzepte sollten diese Verschiebungen adressieren und alle Beschäftigtengruppen mitnehmen.

Bedeutung und Selbstwirksamkeit: Wenn Entscheidungen vermehrt durch KI vorbereitet werden, droht ein Bedeutungs- und Wirksamkeitsverlust. Soziale Anerkennung von Expertise, Feedbackschleifen und partizipative Gestaltung fördern Selbstwirksamkeit und Motivation.

» Wenn Entscheidungen vermehrt durch KI vorbereitet werden, droht ein Bedeutungs- und Wirksamkeitsverlust. «

Entwicklung KI-basierter Anwendungen für den Arbeitsschutz

KI kann selbst zu einem wirksamen Instrument des Arbeitsschutzes werden. Beispiele hierfür sind Sensorik und Frühwarnsysteme, automatisierte Datenanalysen für die Gefährdungsbeurteilung, adaptive Lernsysteme oder vertiefte

Analysen großer Datenmengen, die neue Risiken und Zusammenhänge sichtbar machen. Solche Anwendungen bieten erhebliche Potenziale zur Verbesserung der Prävention in Unternehmen.

Befähigung betrieblicher Arbeitsschutzakteurinnen und -akteure

Damit KI-Anwendungen im Arbeitsschutz wirksam eingesetzt werden können, benötigen betriebliche Akteurinnen und Akteure – insbesondere Fachkräfte für Arbeitssicherheit (Sifa) – entsprechendes Wissen und Kompetenzen. Eine Befragung unter 277 Sifa (Teilnehmende an Sifaforen der BGHM in 2025) zeigt deutliche Unterschiede zwischen beruflicher und privater Nutzung von KI.

Während 68 Prozent der Sifa eine gewisse private Nutzung und 20 Prozent eine starke private Nutzung (Mittelwert 1,89) angaben, lag die persönliche berufliche Anwendung als Sifa bei allen Befragten mit einem Mittelwert von 1,40 statistisch signifikant (gepaarter t-Test) niedriger. Es gab bei nur 31,5 Prozent der Befragten eine gewisse persönliche berufliche Nutzung und bei 7,9 Prozent eine starke persönliche berufliche Nutzung. Dies weist auf ein erhebliches Transferpotenzial hin.

Die Antworten erfolgten auf einer Likert-Skala (1 = nie–selten, 2 = manchmal, 3 = regelmäßig, 4 = häufig–immer; 0 = keine Nutzung oder keine Angabe).

Für die weitere Auswertung wurden die Antworten (277 gültige Antworten mit Angabe zur privaten Nutzung) in zwei Gruppen unterteilt:

Häufige private Nutzung: Private Nutzung ≥ 3 (auf der Skala 1 = trifft nicht zu, 4 = trifft voll zu; entspricht eher/stark zustimmend). Diese Gruppe umfasste 56 Sifa (circa 20 Prozent).

Seltene private Nutzung: Private Nutzung ≤ 2 (eher nicht/überhaupt nicht zustimmend, inkl. 0 = keine Angabe). Diese Gruppe umfasste 221 Sifa (circa 80 Prozent).

Die Tabelle (nächste Seite) zeigt die verwendeten Fragen zur persönlichen beruflichen KI-Nutzung durch die Sifa und KI-Nutzung durch die Unternehmen mit zugehöriger Auswertung für Gruppen mit häufiger und seltener privater Nutzung (t-Test).

Die Auswertung zeigt signifikante Unterschiede ($p < 0{,}001$) zwischen Sifa mit häufiger und seltener privater KI-Nutzung für alle Fragen zur persönlichen beruflichen Nutzung. Diese Ergebnisse verdeutlichen: Private KI-Erfahrungen fördern die berufliche Nutzung erheblich, während die institutionelle Integration bislang gering bleibt. Daraus ergibt sich ein klarer Auftrag zur Entwicklung praxisnaher Schulungs- und Qualifizierungsangebote für betriebliche Arbeitsschutzakteurinnen und -akteure.

» Private KI-Erfahrungen fördern die berufliche Nutzung erheblich, während die institutionelle Integration bislang gering bleibt. Daraus ergibt sich ein klarer Auftrag zur Entwicklung praxisnaher Schulungs- und Qualifizierungsangebote. «

Frage	Mittelwert (häufig)	Mittelwert (selten)	Bewertung des Unterschiedes
Persönliche berufliche KI-Nutzung:			
KI unterstützt mich bei meiner Arbeit	2,63	1,59	Signifikant
KI zur Textzusammenfassung	2,26	1,40	Signifikant
KI zur Gefahrenidentifikation	1,48	1,07	Signifikant
KI zur Gefährdungsbeurteilung	1,72	1,16	Signifikant
KI zur Automatisierung von Routineaufgaben	1,89	1,19	Signifikant
KI zur Schulungsvorbereitung	2,18	1,31	Signifikant
KI zur Datenauswertung	1,45	1,08	Signifikant
Unternehmensseitige KI-Nutzung:			
KI bei Audits	1,18	0,96	Signifikant
KI für video-/sensorbasierte Maßnahmen	1,02	0,92	Nicht signifikant
KI zur prädiktiven Instandhaltung	0,91	0,83	Nicht signifikant
KI bei der Softwareentwicklung	1,07	0,87	Nicht signifikant

Quelle: Eigene Untersuchung

Tabelle: Befragung unter 277 Sifa zeigt deutliche Unterschiede zwischen beruflicher und privater Nutzung von KI.

Wirkung von KI auf Beschäftigte

KI-Anwendungen halten zunehmend Einzug in Betriebe – von Produktionsassistenzsystemen über bildbasierte Qualitätsprüfung bis zu Chatbots in der Verwaltung. Damit eröffnen sich Potenziale für die Effizienzsteigerung und Fehlerreduktion. Gleichzeitig zeigen Befragungen, dass viele Beschäftigte der Einführung von KI mit Unsicherheit begegnen. Eine erfolgreiche Implementierung erfordert daher nicht nur technische sondern auch soziale und kommunikative Begleitmaßnahmen.

Ausblick: die Rolle der Unfallversicherung

Die Einführung von KI stellt auch die Unfallversicherungsträger vor neue Herausforderungen. Es genügt nicht, ausschließlich technische Aspekte zu betrachten. Ebenso wichtig sind psychologische, organisatorische und soziale Dimensionen. Daraus ergeben sich Aufgaben hinsichtlich der Präventionsleistungen: Zum Beispiel sind KI-spezifische Gefährdungen zu identifizieren und zu beurteilen, Handlungshilfen bereitzustellen und Qualifizierungsangebote anzupassen. Die Ergebnisse der Sifa-Befragung verdeutlichen dabei, dass die Förderung von arbeitsschutzspezifischen KI-Kompetenzen und Transferwissen zu einem präventionswirksamen Aufgabenfeld der Unfallversicherungsträger werden kann. KI bietet große Chancen für Prävention, wenn sie menschengerecht gestaltet und verantwortungsvoll eingesetzt wird. ●

Autor

Ulrich Zilz,
Berufsgenossenschaft Holz und Metall (BGHM)

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/01/#fussnoten

Literaturhinweise

Sie finden die Literaturhinweise zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/01/#literaturhinweise

Die Rolle von KI in Systemen der sozialen Sicherung aus globaler Perspektive

KI verändert nicht nur einzelne Tätigkeiten, sondern ganze Institutionen und Verwaltungsmodelle. Singapur und die skandinavischen Staaten zeigen, wie strategische Rahmenbedingungen, standardisierte Datenplattformen und gezielte KI-Initiativen soziale Sicherungssysteme effizienter, flexibler und bürgerorientierter gestalten können.

„Digitale Technologien und insbesondere KI haben eine disruptive Innovationskraft, die mit der historischen Bedeutung der Dampfmaschine vergleichbar ist“[1], schrieben Brynjolfsson und McAfee bereits 2014. Die US-amerikanischen Wissenschaftler argumentieren weiter, dass digitale Technologien – insbesondere KI – exponentiell leistungsfähiger werden, wodurch gesellschaftliche und wirtschaftliche Strukturen wesentlich schneller transformiert werden als Organisationen ihnen folgen können. Die Autoren betonen, dass KI nicht nur einzelne Tätigkeiten verändert, sondern ganze Institutionen, Branchen und Verwaltungsmodelle umgestaltet. Dadurch entstehen grundlegend neue Formen der Wertschöpfung, die bestehende Strukturen herausfordern.

Der vorliegende Artikel versucht Antworten auf diese Entwicklung aus der Perspektive von Singapur sowie der skandinavischen Länder zu geben, die sehr unterschiedliche strukturelle Strategien gefunden haben, die Potenziale von KI für die soziale Sicherung zu nutzen. Gemein ist ihnen allen, dass sie im Sinne Joseph Schumpeters einen disruptiven Rahmen zur Entfaltung der Potenziale von KI geschaffen haben, welcher die Sicherheit von Verwaltungsprinzipien mit der Innovationskraft marktorientierter Strukturen vereint. „Dieser Prozess (...)“, so schreibt Schumpeter, „(...) ist seiner Natur nach eine Form ökonomischen Wandels, die unaufhörlich die wirtschaftliche Struktur von innen heraus revolutioniert, unaufhörlich die alte zerstört und unaufhörlich eine neue schafft.“[2] Schumpeter sieht Innovation nicht als optionalen Luxus, sondern als zentralen Treiber für gesellschaftlichen und wirtschaftlichen Wandel. Damit lässt sich argumentieren: KI-Technologien sind nicht nur neue Tools, sondern – vorausgesetzt die politischen, gesellschaftlichen und wirtschaftlichen Rahmenbedingungen sind entsprechend adjustiert – potenzielle Motoren für einen strukturellen Wandel im Sozialstaat.

Key Facts

- Künstliche Intelligenz (KI) hat das Potenzial, einen fundamentalen Beitrag für die Zukunftsfähigkeit der Systeme der sozialen Sicherung zu leisten
- Dieses Potenzial kommt besonders zur Geltung, wenn sich Innovationsfreudigkeit, nationale KI-Strategien und unternehmerische Prinzipien verbinden
- Dies zeigen verschieden ausgerichtete KI-Strategien im internationalen Vergleich

Singapurs KI-Strategie für soziale Sicherung

Singapur gilt als ein Beispiel für die gezielte Nutzung staatlicher Strukturen zur Förderung von technologischer Innovation, insbesondere im Bereich der sozialen Sicherung beziehungsweise im Gesundheitsbereich. Cheang und Lim (2023) argumentieren, dass Singapurs institutionelles Gefüge – geprägt durch eine enge Verzahnung von Staat, Markt und gesellschaftlichen Akteuren – eine spezifische Variante des Kapitalismus darstellt, die stark auf staatlich gesteuerte Entwicklungsstrategien setzt.[3] Diese „institutionelle Vielfalt“ ermöglicht es dem Stadtstaat, technologische Fortschritte, wie den Einsatz von Künstlicher Intelligenz, systematisch in bestehende Sozial- und Governance-Strukturen zu integrieren.

» Singapur zeigt beispielhaft, wie institutionelle Rahmenbedingungen den Einsatz von KI im sozialen Sektor entscheidend prägen können. «

Vor diesem Hintergrund lässt sich der Erfolg Singapurs bei der Implementierung von KI in der sozialen Sicherung nicht isoliert betrachten, sondern muss in Verbindung mit seinen institutionellen Arrangements verstanden werden. Die Kombination aus zentraler Steuerung, flexiblen politischen Instrumenten und der Fähigkeit zur engen Kooperation zwischen staatlichen und privaten Akteuren schafft ein Umfeld, in dem KI-Anwendungen effizient entwickelt, getestet und skaliert werden können.

Eine zentrale Rolle spielt dabei die aktualisierte nationale KI-Strategie Singapurs – NAIS 2.0, die im Dezember 2023 offiziell vorgestellt wurde. Sie baut auf der ersten Version der Strategie aus 2019 auf, geht aber deutlich über punktuelle KI-Projekte hinaus und verfolgt einen systemischen, gesamtgesellschaftlichen Ansatz. Der zentrale Leitgedanke dieser Strategie ist die Schöpfung von „AI for the Public Good, for Singapore and the World“[4] – also KI als Mittel, um gesellschaftlichen Nutzen zu generieren und Singapur langfristig als global relevante KI-Nation zu etablieren.

Dazu will Singapur gezielt „Spitzen“ im Bereich KI aufbauen und Kompetenzen und Forschungskapazitäten in ausgewählten KI-Bereichen fördern. Darüber hinaus sollen Gesellschaft, Individuen und Unternehmen mit KI vertraut gemacht werden, um KI kompetent, reflektiert und verantwortungsbewusst einsetzen zu können.

Um die Vision und Ziele umzusetzen, gliedert sich NAIS 2.0 in drei „Systems“, durch die insgesamt zehn „Enabler“ wirken, konkret umgesetzt mit etwa 15 definierten „Actions“. Die drei Systeme sind:

1. Activity Drivers: Treiber für KI-Innovation und -Anwendung. Industrie, Regierung und Forschung sollen KI-Projekte gemeinsam vorantreiben.
2. People & Communities: Fokus auf Talentaufbau, Ausbildung, Kompetenzen und gesellschaftliche Einbindung.
3. Infrastructure & Environment: Bereitstellung von technischer Infrastruktur (zum Beispiel Rechenkapazitäten, Datenzugang) und Schaffung eines vertrauenswürdigen, verantwortungsbewussten Rahmens für KI (Governance, Datenschutz, Sicherheit).

Zu den konkreten Maßnahmen zählen beispielsweise der Aufbau von „Centres of Excellence“ für KI, die Förderung des Start-up-Ökosystems, der Ausbau des KI-Talentpools (mit dem Ziel, rund 15.000 KI-Fachkräfte zu erreichen), der Zugang zu Hochleistungsrechnern, die Förderung von KI-Einsatz im öffentlichen Sektor und die Nutzung öffentlicher Daten für gemeinwohlorientierte KI-Projekte.

Damit bietet Singapur ein Beispiel dafür, wie institutionelle Rahmenbedingungen den Einsatz von Künstlicher Intelligenz im sozialen Sektor entscheidend prägen können.

So ist ein zentrales Beispiel für den Einsatz von KI im Gesundheitswesen Singapurs die KI-Lösung „Note Buddy“. Durch den Einsatz von generativer KI werden zeitaufwändige, repetitive Aufgaben wie das Verfassen von ärztlichen Briefen, die Dokumentation von Gesprächen mit Patientinnen und Patienten oder administrative Notizen automatisiert. Dies verschafft medizinischem Personal mehr Zeit für die direkte Versorgung der Menschen und entlastet vor allem bei bürokratischen Aufgaben. Die dadurch gewonnene Zeit kann für direkte Arbeit mit den Patientinnen und Patienten genutzt werden und führt zu Kostenreduktionen für das Gesundheitssystem Singapurs.

Laut aktuellen Berichten verwenden mehr als 2.100 Mitarbeitende im Gesundheitswesen Note Buddy; das System hat bereits über 16.000 klinische und administrative Notizen generiert. Die Regierung Singapurs hat erklärt, dass bis spätestens 2026 alle öffentlichen Gesundheitseinrichtungen vergleichbare KI-Tools einführen sollen. Zudem wird unter dem Namen „HealthHub AI“ eine zentrale Gesundheitsplattform etabliert werden, die künftig auch personalisierte Gesundheitsberatung bieten soll.

Während in Deutschland der Fokus des Datenschutzes (zum Beispiel unter der Datenschutz-Grundverordnung (DSGVO)) tendenziell stark auf individueller Kontrolle und Restriktion liegt, zeigt Singapur, wie ein balancierter Ansatz – mit verpflichtender Datenteilung im Gesundheitswesen, aber klaren Sicherheits- und Zugriffsbeschränkungen (zum Beispiel mit dem Personal Data Protection Act (PDPA) oder dem National Electronic Health Record (NEHR)) – dazu beitragen kann, Versorgungslücken zu schließen, Doppeluntersuchungen zu vermeiden und die klinische Entscheidungsfindung zu verbessern, ohne die Privatsphäre vollständig aufzugeben.

Skandinavien als digitaler KI-Vorreiter

Die skandinavischen Länder gelten international als Vorreiter bei der Digitalisierung des öffentlichen Sektors und setzen in zunehmendem Maße KI zur Effizienzsteigerung, Bürgerorientierung und Qualitätssicherung staatlicher Leistungen ein. Dabei verfolgt jedes Land eigene strategische Schwerpunkte, die jedoch durch gemeinsame Prinzipien wie Transparenz, Datenschutz, Interoperabilität und eine hohe Vertrauenskultur gegenüber der Nutzung von Daten und KI-basierten Lösungen gekennzeichnet sind.

So ist allen skandinavischen Ländern gemeinsam, dass sie umfangreiche ethische und rechtliche Rahmenwerke für den Einsatz von KI geschaffen haben – mit einem noch viel stärkeren Fokus auf ethischen Prinzipien als bei dem beschrieben Beispiel aus Singapur. Dazu zählen verpflichtende Folgenabschätzungen, Anforderungen an die Erklärbarkeit von Modellen sowie strikte Datenschutzstandards, die über rein technische Aspekte hinausgehen und den Schutz der Bürgerrechte in den Mittelpunkt stellen. Zudem investieren die Länder stark in offene Datenplattformen und Interoperabilitätsstandards, um die Entwicklung von KI-Anwendungen im öffentlichen Sektor systematisch zu ermöglichen.

Standardisierte Daten- und Austauschplattformen

Ein zentrales Fundament für den erfolgreichen Einsatz von KI in sozialen Sicherungssystemen und im Gesundheitswesen skandinavischer Länder liegt in der Existenz standardisierter, sicherer und interoperabler Daten- und Austauschplattformen.[5] Diese Plattformen ermöglichen den verlässlichen, datenschutzkonformen und systemübergreifenden Austausch von Gesundheits-, Sozial- und Verwaltungsdaten zwischen verschiedenen Behörden, Leistungserbringern und Dienstleistern.

Ein besonders gutes Beispiel hierfür ist X-Road. Die Plattform funktioniert sowohl in Estland als auch in Finnland als „Data Exchange Layer“: eine dezentral verwaltete Middleware, über die unterschiedliche Informationssysteme auf standardisierte Weise miteinander kommunizieren können. Dabei werden Daten verschlüsselt übertragen, Zugriffe authentifiziert und protokolliert, was Integrität, Vertraulichkeit und Nachvollziehbarkeit garantiert.

Architekturen wie diese erleichtern in Skandinavien nicht nur den reinen Datenaustausch, sondern schaffen auch eine solide Grundlage für KI-gestützte Anwendungen. Denn KI-Modelle, etwa zur Vorhersage von Pflegebedarf, Risikoanalysen im Sozialwesen oder personalisierter Gesundheitsversorgung, benötigen große, konsolidierte und aktuelle Datensätze – mit Informationen zu Demografie, Versicherungsstatus, Gesundheits- und Pflegedaten.

Eine Plattform wie X-Road erlaubt es, dass relevante Datenquellen (zum Beispiel Bevölkerungsregister, Sozialversicherungsträger, Gesundheitsämter, Pflegeanbietende) miteinander verknüpft werden können, ohne redundante Datenhaltung oder unsichere Schnittstellen. Dank dieser Datenintegration lassen sich KI-basierte Vorhersagemodelle realistischer und wirkungsvoller entwickeln. Beispielsweise kann eine Kommune oder Sozialversicherung Behördendaten, Pflegedaten und demografische Informationen kombinieren, um den zukünftigen Pflegebedarf vorherzusagen – und entsprechend früh Kapazitäten wie Heimplätze, ambulante Dienste oder Pflegepersonal ausbauen. Wenn Daten über X-Road permanent aktualisiert und abrufbar sind, erhöht das zudem die Aktualität und Genauigkeit solcher Prognosen und reduziert administrative Verzögerungen.

» Eine Plattform wie X-Road erlaubt es, dass relevante Datenquellen miteinander verknüpft werden können. So lassen sich KI-basierte Vorhersagemodelle realistischer und wirkungsvoller entwickeln. «

Darüber hinaus ermöglicht eine Plattform wie X-Road – durch ihre standardisierte, offene und interoperable Architektur – eine relativ einfache Skalierung und Erweiterung der KI-Anwendungen: Neue Services, Analysen oder Cross-Sector-Anwendungen (beispielsweise zwischen Gesundheit, Sozialversicherung und öffentlicher Verwaltung) können angeschlossen werden, ohne jede Schnittstelle neu entwickeln zu müssen. Das senkt Entwicklungskosten und fördert Innovation.

Datenschutz, Sicherheit und Transparenz sind eingebaut, Zugriff und Nutzung werden protokolliert – das verstärkt in Ländern mit hohem Vertrauen gegenüber öffentlichen Institutionen wie in jenen Skandinaviens wiederum die Akzeptanz für datengetriebene KI-Services.

KI-basierte Anwendungen in Dänemark

Dänemark zählt zu den international führenden Ländern bei der Implementierung datengetriebener Verwaltungsmodernisierung und dem gezielten Einsatz von Künstlicher Intelligenz im Bereich der sozialen Sicherung.[6] In dänischen Sozialbehörden werden KI-basierte Anwendungen zunehmend eingesetzt, um Entscheidungsprozesse zu unterstützen, Risiken frühzeitig zu erkennen und Ressourcen effizienter zu verteilen.

Die Nutzung solcher Technologien wird durch eine hochgradig integrierte digitale Infrastruktur, einschließlich nationaler Register und interoperabler Datenzugangssysteme, strukturell ermöglicht. Gleichzeitig gewährleisten umfassende Governance-Rahmen, ethische Leitlinien und Transparenzpflichten, dass Innovationen im Einklang mit den Prinzipien des Wohlfahrtsstaates – Fairness, Rechenschaftspflicht und Schutz der Bürgerrechte – implementiert werden.

Dieses Zusammenspiel von technologischem Fortschritt und politisch-institutioneller Steuerung positioniert Dänemarks Strategie als ein Vorzeigemodell für die verantwortungsvolle Integration von KI in soziale Sicherungssysteme. Beispielsweise hat Dänemark früh begonnen, KI in Verwaltungsprozessen zu erproben, insbesondere zur Automatisierung wiederkehrender Aufgaben. Ein häufig zitiertes Beispiel ist der Einsatz von Machine-Learning-Systemen in Kommunalverwaltungen zur Bearbeitung von Sozialleistungsfällen. Hier dienen KI-Modelle dazu, Dokumente zu klassifizieren, relevante Informationen aus Anträgen zu extrahieren und Mitarbeitende bei der Erstbewertung zu unterstützen. Ziel ist die Reduktion administrativer Belastungen und die Beschleunigung des Verfahrens.

Besonders bemerkenswert ist auch das Ambitionslevel, KI-basierte „world-class public services“ für einen modernen Wohlfahrtsstaat zu entwickeln, wie dies bereits 2019 in der Danish National Strategy for Artificial Intelligence der dänischen Regierung zum Ausdruck kommt[7]. Dabei strebt Dänemark eine aktive Rolle in der europäischen und globalen KI-Governance an. Die Strategie betont daher auch Kooperationen mit Institutionen wie der Europäischen Union und der OECD, um

gemeinsame Standards und ethische Rahmenbedingungen für den Einsatz von KI in der sozialen Sicherung zu fördern.

Automatisierte Bearbeitung in Schweden

Schweden setzt KI vor allem als Entscheidungsunterstützungssystem in Behörden ein. Ein prominentes Beispiel liefert die schwedische Steuerverwaltung, die seit mehreren Jahren Machine-Learning-Modelle verwendet, um Unregelmäßigkeiten und potenziellen Steuerbetrug zu identifizieren. Die Modelle analysieren große Mengen historischer Daten, um Muster zu erkennen, die auf risikobehaftete Fälle hindeuten könnten. Die finale Entscheidung liegt jedoch stets bei menschlichen Sachbearbeitenden, was im Einklang mit Schwedens starker Betonung auf Transparenz und Nachvollziehbarkeit steht.

Auch die Arbeitsverwaltung setzt KI ein, etwa zur automatisierten Analyse von Stellenanzeigen und zur Erstellung von Kompetenzprofilen, um Arbeitssuchende mit passenden Beschäftigungsmöglichkeiten zu matchen. Zudem setzt die schwedische Sozialversicherungsbehörde KI-gestützte Systeme ein, um Anträge auf Sozialleistungen wie Arbeitslosen- oder Krankengeld zu prüfen. KI-Algorithmen analysieren eingehende Anträge auf Vollständigkeit, erkennen Muster typischer Dokumente und unterstützen Mitarbeitende bei der schnellen Identifikation von fehlerhaften oder unvollständigen Angaben. Dadurch konnten Bearbeitungszeiten deutlich reduziert und die Effizienz der Behörden gesteigert werden, während gleichzeitig menschliche Kontrolle weiterhin für die endgültige Entscheidung sorgt.

Eine zentrale Rolle spielt dabei das 2019 gegründet Nationale Zentrum AI Sweden mit Sitz in Göteborg. Es dient als zentrale Plattform für den Einsatz von Künstlicher Intelligenz in der schwedischen öffentlichen Verwaltung. Es bündelt Ressourcen, Daten und Fachwissen, um gemeinsame KI-Lösungen zu entwickeln, die über einzelne Behörden hinaus genutzt werden können. Durch Initiativen wie den digitalen Assistenten für Kommunen und das Netzwerk für den öffentlichen Sektor fördert AI Sweden nicht nur Effizienz und Qualität in Verwaltungsprozessen, sondern ermöglicht auch eine koordinierte, strategische Einführung von KI, die Bürgerinnen und Bürger direkt unterstützt.

KI-basierte Kundenprozesse in Norwegen

Norwegen konzentriert sich besonders auf KI-gestützte digitale Bürgerdienste, häufig integriert in die nationale Plattform Altinn. Ein Beispiel hierfür ist der Einsatz von KI-basierten Chatbots in verschiedenen Behörden, etwa bei der Steuerbehörde oder dem norwegischen Arbeits- und Sozialamt. Diese Systeme beantworten Anfragen von Bürgerinnen und Bürgern automatisiert, erkennen Anliegen semantisch und leiten komplexere Fälle an menschliche Mitarbeitende weiter. Im Gesundheitswesen werden KI-Systeme darüber hinaus zur Priorisierung von Krankenakten und zur Unterstützung bei Diagnosen in der Radiologie eingesetzt, wobei große nationale Gesundheitsdatensätze eine besonders wertvolle Grundlage bilden.

» Der größten norwegischen Rentenorganisation ist es gelungen, papierbasierte Prozesslaufzeiten von oftmals mehreren Monaten auf Sekunden zu reduzieren. «

Ein weiteres Beispiel ist der Einsatz von KI bei der größten norwegischen Rentenorganisation (KLP). Im Rahmen einer grundlegenden digitalen Transformation ist es KLP gelungen, papierbasierte Prozesslaufzeiten von oftmals mehreren Monaten auf die automatisierte Bearbeitung von Anliegen in Sekunden zu reduzieren, wobei eine Vielzahl von kundenrelevanten Prozessen mittlerweile mit KI unterstützt wird. Dies wird auch durch den Pension-Calculator für individuelle Rentenplanung unterstrichen. Mit diesem Tool hat KLP einen digitalen Rentenrechner eingeführt, der es Mitgliedern erlaubt, anhand verschiedener Parameter (zum Beispiel Erwerbsdauer, Rentenbeginn, Kombination von Arbeit und Pension) und mit Unterstützung von Künstlicher Intelligenz die finanziellen Konsequenzen eigener Entscheidungen zu simulieren.

Auch für die besondere Leistungsfähigkeit des skandinavischen Systems der sozialen Sicherung ist das Organisationsmodell der KLP neben der konsequenten, strategisch motivierten digitalen Transformation ein besonders gutes Beispiel. Denn die KLP stellt ein hybrides Organisationsmodell dar, in dem öffentliche Verantwortung und privatwirtschaftliche Effizienzmechanismen miteinander verzahnt werden.

Als Rentenversicherer im Besitz norwegischer Kommunen und öffentlicher Einrichtungen agiert KLP zwar in staatlicher Trägerschaft, unterliegt jedoch zugleich einer marktwirtschaftlich orientierten Unternehmensführung, die Wettbewerb, Innovation und Effizienzsteigerung fördert. Dies zeichnet sich durch vier zentrale Faktoren aus:

1. Staatliche Stabilität und privatwirtschaftliche Effizienz: Die kommunale Eigentümerschaft garantiert langfristige finanzielle Stabilität, politische Kontinuität und Vertrauen. Zugleich operiert KLP wie ein professionelles Finanzunternehmen, das seine Kapitalanlagen marktorientiert diversifiziert, Risiken aktiv managt und die Erträge optimiert. Die Kombination aus öffentlicher Sicherheit und privatwirtschaftlichem Risikomanagement führt zu robusten, stabilen Pensionsleistungen, die weniger anfällig für politische, wirtschaftliche oder gesellschaftliche Schwankungen sind, welches das norwegische Rentensystem zu einem der erfolgreichsten der Welt macht.[8]
2. Gemeinwohlorientierung und Innovationsfähigkeit: KLP verfolgt keine Gewinnmaximierung zugunsten externer Anteilseigner, stattdessen fließen Effizienzgewinne und Investitionserträge direkt an die Mitglieder – die Kommunen – zurück. Gleichzeitig ermöglicht die unternehmerische Struktur die Implementierung moderner Technologien wie Automatisierung, KI-gestützte Entscheidungsunterstützung oder digitale Self-Service-Tools, wodurch Servicequalität und Kostenstruktur verbessert werden.
3. Wettbewerb als Qualitätstreiber: Obwohl KLP öffentlich getragen wird, konkurriert es im norwegischen Markt mit privaten Pensionsanbietern. Dieser Wettbewerb zwingt KLP, kontinuierlich Effizienz, Kundenzufriedenheit und digitale Dienstleistungen zu verbessern – bei gleichzeitig stark regulierten sozialen Mindeststandards. Der Wettbewerb sorgt somit für höhere Qualität, ohne dass die soziale Grundsicherung privatisiert wird.

4. Transparenz und partizipative Governance: Als öffentliches Unternehmen ist KLP verpflichtet, offen über seine Finanzstrategien und Risikomodelle zu berichten. Die Eigentumsstruktur stellt sicher, dass die Kommunen und damit die Bürgerinnen und Bürger Norwegens Einflussmöglichkeiten auf die Geschäftsentwicklung haben.

Fazit

Zusammengenommen unterstreichen diese Beispiele, dass KI nicht nur technologische Innovation bedeutet, sondern ein zentraler Hebel ist, um soziale Sicherung flexibel, effizient und zukunftsfähig zu gestalten. So zeigt das Beispiel der norwegischen KLP mit ihrem leistungsfähigen Hybridmodell, wie sich öffentliche Verantwortung und privatwirtschaftliche Innovationslogik zu einem leistungsstarken, resilienten und serviceorientierten Rentensystem verbinden lassen.

Eine der zentralen und besonders spannenden Fragen der Zukunft wird sein, welche innovativen Strategien, organisationalen Strukturen und prozessualen Anpassungen sich aus den in diesem Artikel skizzierten Entwicklungen für die Systeme der sozialen Sicherung in Deutschland ergeben werden und wie diese zur Flexibilisierung, Effizienzsteigerung und zukunftsorientierten Gestaltung der Leistungen beitragen können. Vor diesem Hintergrund liegt es nahe, den Austausch und die Kooperation mit Ländern wie Norwegen bis hin zur Schaffung gemeinsamer Kooperationsstrukturen zu intensivieren, um die dabei gewonnenen Erkenntnisse für die deutsche Praxis nutzbar zu machen. ●

Autor

Jakob Kort,
Berufsgenossenschaft der Bauwirtschaft (BG BAU)

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/02/#fussnoten

Quellen

Sie finden die Literaturhinweise zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/02/#quellen

Künstliche Intelligenz und gesunde Führung im Gesundheits- und Sozialwesen

Das Gesundheits- und Sozialwesen ist ein sensibler Bereich für den Einsatz von Künstlicher Intelligenz. Beschäftigte tragen eine besondere Verantwortung für die ihnen anvertrauten Personen und die Datenschutzanforderungen sind hoch. Gleichzeitig macht der Fachkräftemangel eine Entlastung von Routineaufgaben dringend nötig.

Zwar ist das Gesundheits- und Sozialwesen ein bedeutsames Feld für den Einsatz von Künstlicher Intelligenz, doch ist dieser Einsatz auch mit verschiedenen Chancen und Risiken verbunden. Typische Anwendungen der Künstlichen Intelligenz liegen im therapeutischen, diagnostischen, administrativen oder präventiven Bereich.[1] Die folgenden Beispiele zeigen Anwendungsbereiche für Künstliche Intelligenz im Gesundheits- und Sozialwesen.

Administrative Bereiche: Digitale Sprachassistenten unterstützen in Pflegeeinrichtungen. Als App auf dem Smartphone ermöglicht die Software das freie Einsprechen der Pflegedokumentation. Die Daten werden in das Dokumentationssystem übertragen.

Diagnostische Bereiche: Die Tools basieren auf überprüften medizinischen Datenbanken, die auf wissenschaftliche medizinische Literatur, Lehrbücher, regionale Epidemiologie, Krankheitsmodelle und Fallberichte verweisen. Sie werden in Arztpraxen oder Kliniken für die diagnostische Unterstützung eingesetzt.

Therapeutische Bereiche: Chatbot-assistierte ambulante Nachsorge wird bei Jugendlichen und jungen Erwachsenen nach einem Klinikaufenthalt eingesetzt. Die App bietet ergänzende psychotherapeutische Trainingseinheiten an, unterstützt am Ball zu bleiben und hilft passende ambulante Therapien und Selbsthilfegruppen zu finden.

Präventive Bereiche: Künstliche Intelligenz unterstützt in der Kommunikation von Einrichtungen der sozialen Arbeit im Migrationsbereich. Über Videos mit KI-generierten Avataren können Einrichtungen Klientinnen und Klienten in verschiedenen Sprachen ansprechen.

Key Facts

- Der Einsatz von Künstlicher Intelligenz (KI) im Gesundheits- und Sozialwesen birgt besondere Herausforderungen
- Es bieten sich sowohl Chancen als auch Risiken für die gesundheitsfördernde Gestaltung von Arbeitsbedingungen
- Führungskräfte wirken als Ressource in Digitalisierungsprozessen, indem sie auf Beteiligung der Mitarbeitenden, effiziente Kommunikation sowie auf Transparenz setzen

Herausforderungen und Chancen

Der Einsatz von Künstlicher Intelligenz entwickelt sich rasant weiter. Das macht es herausfordernder, Chancen und Risiken für Sicherheit und Gesundheit am Arbeitsplatz zu beurteilen und die Arbeit menschengerecht zu gestalten. Das Gesundheits- und Sozialwesen ist ein sehr sensibler Anwendungsbereich, weil Beschäftigte eine besondere Verantwortung für Menschen in häufig schwierigen Lebenssituationen haben. Die zwischenmenschliche Kommunikation sowie das Erfassen von Bedürfnissen sind ein zentraler Bestandteil der Arbeit.

Digitalisierung kann dazu beitragen, die Arbeit gesundheitsfördernd zu gestalten: Wenn Arbeitsabläufe technikbedingt standardisiert werden, verbessert das häufig die Arbeitsorganisation. Übernimmt beispielsweise eine Künstliche-Intelligenz-Anwendung die Dokumentation, verringert dies die Arbeitsbelastung. Den Beschäftigten bleibt mehr Zeit für die direkte Arbeit an Patienten und Patientinnen oder den zu betreuenden Personen.

Technologiebedingter Stress kann zu negativen Auswirkungen auf die Sicherheit und Gesundheit von Beschäftigten bei der Arbeit führen: Verantwortungsdruck durch unvorhersehbare Algorithmen, ungeklärte Verantwortung bei Fehlern in der Dokumentation oder Diagnose und fehlendes Vertrauen in die Technik rufen Stress hervor. Digital gestützte Arbeit ist nicht automatisch gut gestaltete Arbeit. Beschäftigte erleben technische Unzuverlässigkeit beziehungsweise Störungen und technikbezogene Überanstrengung als besonders belastend.

Die wissenschaftlichen Erkenntnisse zu den positiven oder negativen Auswirkungen auf die Sicherheit und Gesundheit im Gesundheits- und Sozialwesen fallen unterschiedlich aus.[2,3]

» Die Herausforderung besteht darin, KI-Tools so zu wählen und einzusetzen, dass die Gestaltung von gesunden und sicheren Arbeitsplätzen nicht aus dem Blickfeld gerät. «

Anforderungen an Führungskräfte

Die digitale Transformation mit dem Einsatz von Künstlicher Intelligenz führt zu einer umfassenden strukturellen Reorganisation. Sie ist mit veränderten Arbeitsbedingungen verknüpft. Die Herausforderung besteht darin, Künstliche-Intelligenz-Tools so zu wählen und einzusetzen, dass die Gestaltung von gesunden und sicheren Arbeitsplätzen nicht aus dem Blickfeld gerät. Es gilt, die genannten Chancen und Risiken gegeneinander abzuwägen: Welche Stressoren und Ressourcen entstehen durch die digitalen Prozesse? Welche Maßnahmen können Stressoren reduzieren und Ressourcen fördern? Auch technische Lösungen müssen bestimmte Anforderungen erfüllen und gebrauchstauglich, fehlerrobust und transparent gestaltet sein. Laut Arbeitsschutzgesetz sind Führungskräfte dafür verantwortlich, Arbeitsbedingungen sicher und gesund zu gestalten.

Die Anforderungen unterscheiden sich entsprechend der verschiedenen Führungsebenen:

1. **Management:** Zentrale Aufgabe ist, eine Digitalisierungsstrategie zu erarbeiten und kontinuierlich weiterzuentwickeln. Dabei sind verschiedenen Stakeholder einzubeziehen, beispielsweise Mitarbeitendenvertretung, Arbeitsschutzexpertinnen und -experten, Personalabteilung, Qualitätsbeauftragte und Führungskräfte. Aufgenommen werden beispielsweise Aspekte der Ethik (Mensch im Mittelpunkt), Datensicherheit, Sicherheit und Gesundheit der Beschäftigten, Patientinnen und Patienten sowie der zu betreuenden Personen. Im Rahmen der Strategie erstellen die Verantwortlichen Leitlinien zu ethischen Grundsätzen, zur Datensicherheit und zur Beteiligung der Beschäftigten. Zudem ist eine Aktualisierung der Gefährdungsbeurteilung in Auftrag zu geben.
2. **Mittlere Führungsebene:** Zentrale Aufgabe ist, die Digitalisierung zu planen und die Nutzung von Künstlicher Intelligenz auf Arbeitsbereichsebene zu steuern. Der Einsatz von neuen Technologien erfolgt in einzelnen Pilotbereichen und wird anschließend auf den gesamten Arbeitsbereich übertragen. Zu planen sind die personellen und finanziellen Ressourcen für die Kommunikation, externe Unterstützung sowie Einarbeitung und Qualifizierung der Beschäftigten. Die Neuerungen machen es erforderlich, die Gefährdungsbeurteilung in der Abteilung zu aktualisieren.
3. **Direkte Führungsebene:** Zentrale Aufgabe ist, die Veränderungen in den Arbeitsaufgaben, -abläufen und Rollen entsprechend den Anforderungen mit dem Team abzustimmen. Zudem sind regelmäßige Feedbackrunden durchzuführen, Unsicherheiten zu berücksichtigen und Anpassungen vorzunehmen. Ebenfalls zu den Aufgaben gehört, die Mitarbeitenden zu qualifizieren, digitale Kompetenzen zu fördern und die Aktualisierung der Gefährdungsbeurteilung zu unterstützen.

» Jede Veränderung durchläuft gewisse Phasen. Es ist normal, dass dabei auch Ängste und Widerstände bei Beteiligten aufkommen. «

Im Sinne einer gesunden Gestaltung von Arbeitsbedingungen, sind die Beschäftigten frühzeitig durch verschiedene Schritte an den digitalen Veränderungsprozessen zu beteiligen. Dazu müssen Verantwortliche zunächst klären, ob die Veränderung notwendig ist und welche Ziele damit erreicht werden sollen.

Die Anforderungen der Beschäftigten, die mit Künstlicher Intelligenz arbeiten sollen, müssen ausreichend erhoben und berücksichtigt werden. Geht es beispielsweise um die Spracherkennung für die Dokumentation in der Pflege, muss geklärt sein, in welchen Sprachen dokumentiert wird. Zusätzlich braucht es Lösungswege für die Vorgehensweise bei technischen Störungen. Führungskräfte können die bestehende Arbeitsschutzorganisation nutzen, um digitale Prozesse und Tools gesundheitsfördernd auszuwählen und einzuführen.[4] Fachkräfte für Arbeitssicherheit sowie Betriebsärztinnen und Betriebsärzte können beispielsweise die Ergonomie von Tools beurteilen und dabei unterstützen, die psychische Belastung durch die erhöhte Nutzung von Technik zu ermitteln.

Vorbereitung und Planung	Kommunikation und Beteiligung als Erfolgsfaktor	Technische Einführung schrittweise gestalten, Beschäftigte qualifizieren
• Digitalisierungsstrategie • WARUM/WOFÜR wird dieser Ablauf, diese Aufgabe digitalisiert? Warum ist es notwendig, dies zu verändern? (Auch: Was sind die Vorteile?) • WIE und WAS ändert sich bei der Aufgabe/den Abläufen? • WEN betrifft die Veränderung? WEN muss man WANN beteiligen?	• Ziele und Nutzen transparent machen und kontinuierlich kommunizieren: Warum wird das Tool eingeführt? Was bedeutet das für den Arbeitsalltag? • Räume für Sorgen und Kritik schaffen. • Mitarbeitende bei der Entscheidungsfindung einbeziehen. • Erläutern welche Punkte aufgenommen und nicht aufgenommen wurden und warum. • Feedback der Mitarbeitenden zu den neuen Tools einholen und verwerten. • Erfolge sichtbar machen: Erste positive Effekte schnell kommunizieren („Quick Wins“).	• Rollout in Etappen: Nicht alle Bereiche gleichzeitig umstellen – Zeit für Eingewöhnung geben. • Technik testen, bevor sie Pflicht wird: Usability sicherstellen, Schnittstellen prüfen und technische Störungen minimieren. • Praxisnahe Schulungen anbieten: Nicht nur Technik erklären, sondern zeigen, wie das Tool im Alltag hilft. • Lernen ermöglichen statt überfordern: Schulungen staffeln, mit niedrigschwelligen Übungen starten, ggf. Peer-Learning organisieren. • Unterstützung dauerhaft sichern: Ansprechpersonen vor Ort oder „digitale Lotsen“ benennen, die bei Fragen helfen.

Quelle: BGW

Abbildung 1: Erfolgsfaktoren beim Einsatz von künstlicher Intelligenz, BGW 2025

Ablauf bei Veränderungsprozessen

Als Führungskraft kann es hilfreich sein, sich an der Change-Kurve (nach Kübler-Ross) zu orientieren, um die Beteiligten einzubinden und zu unterstützen.

Jede Veränderung durchläuft gewisse Phasen. Es ist normal, dass dabei auch Ängste und Widerstände bei Beteiligten aufkommen. Gerade in der Anfangsphase eines Veränderungsvorhabens sollten Führungskräfte sich auf diejenigen konzentrieren, die als Multiplikatoren oder Multiplikatorinnen dienen, die voranschreiten und andere mitnehmen können. Ein Team an Unterstützenden ist unerlässlich, um die Veränderungen nach und nach umzusetzen.

Gleichzeitig benötigen Führungskräfte einen Plan, wie sie mit den Mitarbeitenden umgehen, deren Einfluss auf die Umsetzung groß ist, die aber Zweifel haben, ob die Veränderung der richtige Weg ist. Auch hier können Unterstützende, gute Argumente und manchmal auch schlichtweg eine große Portion Geduld und Hartnäckigkeit helfen.

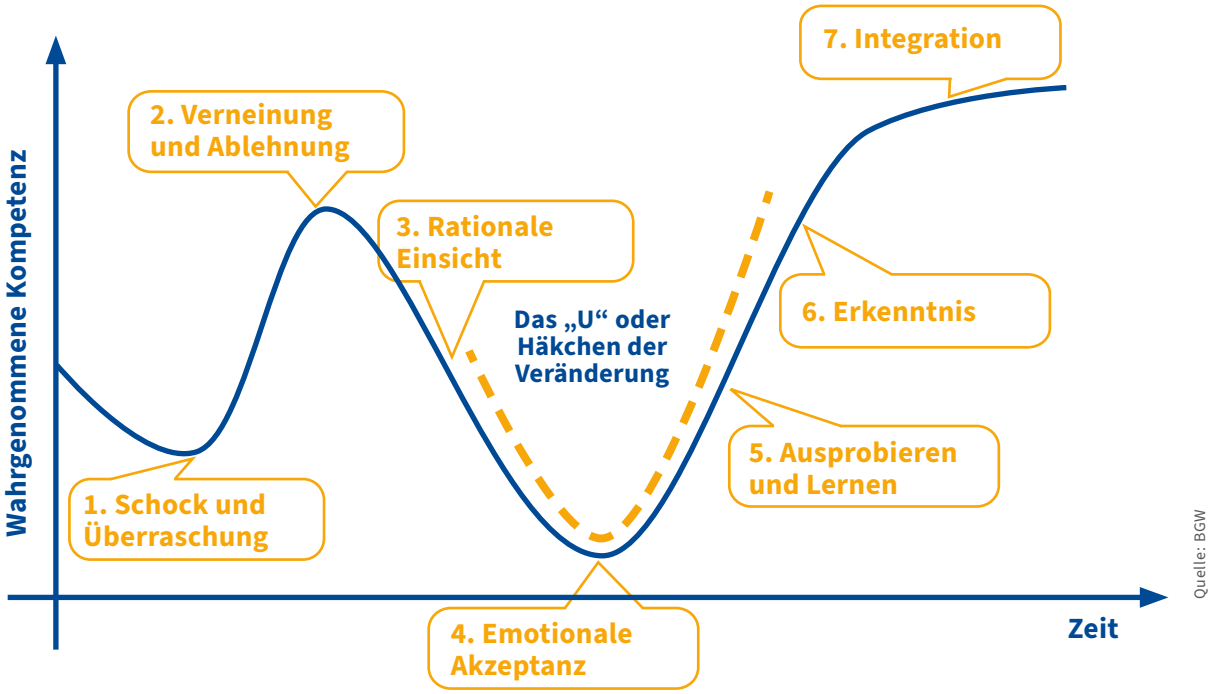


Abbildung 2: Change-Kurve in Anlehnung an Kübler-Ross, Changeleitfaden BV-Geschäftsführungen, BGW 2023

Schock und Überraschung

Nach Bekanntmachung der bevorstehenden Veränderungen herrscht oftmals Unruhe. Vermutungen werden aufgestellt und Ängste verbreitet.

Verneinung und Ablehnung

Nachdem Veränderungen, wie etwa interne Umstrukturierungen, verkündet werden, treffen diese nach der ersten Ablehnung gegebenenfalls auf Widerstand. Dies kann von langwierigen Diskussionen über Arbeitsverweigerung bis hin zu erhöhten Fehlzeiten führen.

Rationale Einsicht und emotionale Akzeptanz

Die Veränderung wird in die Praxis überführt. Die Mitarbeitenden hinterfragen, wollen Antworten und gegebenenfalls auch Einfluss nehmen auf die Art der Veränderung. Ängste oder Sorgen treten offensichtlicher hervor.

Ausprobieren und Lernen, Erkenntnis und Integration

Die Betroffenen lösen sich von alten Strukturen und akzeptieren die Veränderungen. Neue, notwendige Kompetenzen und neues Wissen werden erlernt.

Erkenntnis

Erfahrungen und Fähigkeiten werden gesammelt. Die neue Situation wird angenommen und es stellt sich ein Gefühl der Klarheit ein.

Integration

Die neuen Fähigkeiten werden umgesetzt, die Selbstwirksamkeit steigt und die Veränderung wird zur Normalität.

Veränderung als Chance nutzen

Im Sinne gesunder Arbeit ist es hilfreich, wenn Führungskräfte die Chance der Veränderung nutzen und den Einsatz von Künstlicher Intelligenz aktiv gestalten und kommunizieren. Dies bietet auch die Möglichkeit, bisherige Arbeitsabläufe neu zu denken und Beschäftigte aktiv in die Gestaltung einzubeziehen. Beim Einsatz Künstlicher Intelligenz im Gesundheits- und Sozialwesen können Führungskräfte als Ressource für die Gestaltung gesunder Arbeitsbedingungen wirken. Im Sinne gesunder Selbstführung kann es für Führungskräfte sinnvoll sein, sich Unterstützung für die Veränderungsprozesse durch Beratung oder Coaching zu holen. ●

Autorinnen

Kajsa Johansson,
Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW)

Dr. Sabine Gregersen,
Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW)

Christina Müller,
Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW)

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/03/#fussnoten

Psychische Belastung durch Künstliche Intelligenz in der Arbeitswelt

Künstliche Intelligenz ist mit physischer sowie psychischer Belastung verbunden. Psychische Belastung kann, je nachdem, wie sie gestaltet ist, Motivation und Gesundheit fördern oder zu Stress, Monotonie sowie langfristig Unfällen und Erkrankungen führen. Bei der Gestaltung von KI-Systemen sollte dies berücksichtigt werden.

Künstliche Intelligenz (KI) ist aktuell überall Thema, weil sie in immer mehr Bereichen eingesetzt wird. Zum Teil wird der Begriff jedoch undifferenziert genutzt. Dann stellt sich die Frage: Ist das noch Automatisierung oder schon KI? Im Folgenden sollen die Begriffe differenziert und anhand von Beispielen aus dem Pflegebereich veranschaulicht werden.

Bei der Automatisierung werden Technologien genutzt, um Prozesse ohne oder mit geringer menschlicher Unterstützung ablaufen zu lassen. Ein Beispiel sind automatisierte Medikamentenspender. Davon abzugrenzen ist KI, die in schwache und starke KI unterteilt werden kann.[1]

- **Schwache KI** oder auch spezialisierte KI beschreibt Systeme, die auf spezifische, klar definierte Aufgaben spezialisiert sind. Sie können sich in eingeschränktem Maße durch Datenverarbeitung an den Kontext anpassen, verfügen aber nicht über die Fähigkeit, neue Probleme zu lösen beziehungsweise über ein menschenähnliches Bewusstsein. Dazu gehört das Überwachen von Vitaldaten, um frühzeitig das Risiko einer Sepsis zu erkennen und dem Pflegepersonal präventive Maßnahmen vorzuschlagen.
- **Starke KI** oder auch allgemeine KI hingegen bezeichnet Systeme, die eigenständig komplexe Probleme in verschiedenen Kontexten lösen können. Ein Beispiel wäre ein Pflegeroboter, der allein Pflegebedürftige betreut, auf unvorhergesehene Situationen reagieren und empathisch kommunizieren kann. Solche Systeme übertreffen die menschliche Intelligenz in vielen Aspekten, konnten bisher aber noch nicht erstellt werden.

Verbreitung von KI

Schwache KI wird inzwischen in zahlreichen Branchen und Tätigkeiten eingesetzt. In Deutschland nutzten 2024 bereits 62 Prozent der Beschäftigten KI am Arbeitsplatz[2]. Laut Bitkom

Key Facts

- Anlagen und Software, die Künstliche Intelligenz nutzen, wirken psychisch auf die Beschäftigten ein
- Dadurch können sich positive sowie auch negative Auswirkungen auf die Sicherheit und Gesundheit ergeben
- Schon bei der Einführung von Künstlicher Intelligenz sollten mögliche negative Beanspruchungsfolgen mitbedacht werden

setzen 2025 36 Prozent der Unternehmen in Deutschland generative KI ein[3].

Psychische Belastung bei der Arbeit mit KI

KI wirkt psychisch auf uns Menschen ein, das bedeutet, sie beeinflusst unser Denken, Fühlen und Handeln. Sie geht also mit psychischer Belastung einher. Der Begriff wird in der Arbeitspsychologie unabhängig von der Wirkung und damit neutral betrachtet.[4]

Je nach Tätigkeitsbereich spielen verschiedene Belastungsfaktoren im Zusammenhang mit KI eine Rolle. Nicht jede KI-Anwendung ist mit allen Faktoren verbunden. Die GDA-Empfehlungen[5] geben einen strukturierten Überblick über die Vielfalt psychischer Belastungsfaktoren, wovon viele bei der Nutzung von KI am Arbeitsplatz relevant sind und somit frühzeitig betrachtet werden sollten.

Im Praxisfeld „Psychische Belastung mit Stresskammer“ der DGUV Akademie wird die Bedeutung psychischer Belastungsfaktoren praktisch erlebbar und es wird aufgezeigt, wie eine gute Gestaltung aussehen kann.

Psychische Belastungsfaktoren – Beispiele

Ob sich ein psychischer Belastungsfaktor positiv oder negativ auf den Menschen auswirkt, hängt davon ab, wie gut die Arbeit gestaltet ist und welche Tätigkeiten durch KI unterstützt oder ersetzt werden.

Für die einzelnen Gestaltungsbereiche psychischer Belastung der GDA sollen verschiedene Beispiele dargestellt werden.

Mit Blick auf die **Arbeitsaufgabe** ergeben sich sehr viele Belastungsfaktoren, die mit positiven oder negativen Auswirkungen verbunden sein können. So kann den Beschäftigten durch den Einsatz von KI langweilige Routinearbeit abgenommen werden. Unfälle können durch Risikoeinschätzung und Vorhersage schädigender Ereignisse vermieden werden, kognitive Beanspruchung (beispielsweise durch Vorselektion von Information) wird verringert und monotone Aufgaben werden durch KI übernommen.

Häufig negativ wirkt sich KI aus, wenn der Handlungs- und Entscheidungsspielraum für die Nutzenden verringert wird. Beispielsweise nutzt ein Unternehmen KI-Software, um eingehende Bewerbungen zu analysieren und zu sortieren. Die KI bewertet Lebensläufe, Anschreiben und Online-Profile anhand vordefinierter Kriterien wie Schlüsselwörter, Ausbildung, Berufserfahrung und sogar Sprachstil. Personalverantwortliche verlieren einen Teil ihrer Entscheidungsfreiheit, weil sie oft nur noch mit den von der KI vorselektierten Kandidatinnen und Kandidaten arbeiten.

Eine Herausforderung beim Einsatz von KI in Arbeitsprozessen besteht darin, dass Beschäftigte zunehmend als abstrakte Datenpunkte gesehen werden. Verhaltensweisen und Emotionen können durch algorithmische Verfahren analysiert, prognostiziert und in bestimmten Fällen sogar kontrolliert werden. So ermöglichen tragbare Sensortechnologien die kontinuierliche

Erfassung physiologischer Parameter sowie die Bestimmung der räumlichen Nähe zu bekannten Gefahrenquellen am Arbeitsplatz.[6] Dies kann zu Sorgen bezüglich Überwachung oder der Verletzung der Privatsphäre führen.

Darüber hinaus kann das Problem diskriminierender Effekte bestehen, etwa bei der automatisierten Bewertung von Bewerbungsunterlagen. Dies resultiert häufig aus Verzerrungen im Trainingsmaterial der Systeme. Ein weiteres Beispiel hierfür ist die unzureichende Erkennung dunklerer Hauttöne bei der Kollisionsvermeidung zwischen Mensch und Roboter, die auf eine überwiegende Berücksichtigung hellerer Hauttöne im Trainingsprozess zurückzuführen ist.[7]

Im Bereich **Arbeitsorganisation** können positive Effekte zum Beispiel dadurch entstehen, dass Beschäftigte in der Pflege KI-Dokumentationsassistenten nutzen und dadurch mehr Zeit haben, Bewohnerinnen und Bewohner in Heimen direkt zu betreuen.

Durch die Nutzung von KI-Arbeitsmanagementsystemen kann sich aber auch die Arbeitsintensität höhen. Diese können zum Beispiel in Logistikzentren genutzt werden, um Fertigstellungszeiten von Bestellungen zu verfolgen, Bewegungen, Wege und Fehler zu überwachen und dadurch Zeitverzögerungen zu eliminieren. Wenn die Systeme nicht an die physischen und kognitiven Fähigkeiten der Menschen angepasst sind und diese übersteigen, kann dies zu Zeit- und Leistungsdruck führen.

Der Fokus auf Effizienz und die steigende Zahl der Möglichkeiten, Beschäftigte zu überwachen, kann die Gestaltung der **Arbeitszeit** negativ beeinflussen. Werden Leistungsdaten systematisch ausgewertet und zum Beispiel durch Bestenlisten für alle sichtbar gemacht, kann das dazu führen, dass Wettbewerb zwischen Beschäftigten verschärft wird und diese eher Pausen ausfallen lassen, um die eigene Position im Ranking zu verbessern.[8]

Gleichzeitig können **soziale Beziehungen** am Arbeitsplatz leiden, wenn der Fokus auf Produktivität und Effizienz liegt und Kommunikation sowie Kooperation nicht mehr möglich sind. Lieferanten von Online-Essenslieferdiensten, die von einer KI per App über ihre nächste Auslieferung informiert werden, haben möglicherweise keinen direkten Kontakt mehr zu Kolleginnen und Kollegen oder Vorgesetzten. Die KI kann sogar verhindern, dass sich Lieferanten bei der Arbeit treffen, indem ein Warten vor dem gleichen Restaurant unterbunden wird.

Wenn durch KI Effizienzgewinne erzielt werden, kann aber auch mehr Zeit für Austausch, Führung und soziale Unterstützung entstehen. Das kann sich nachhaltig positiv auf das Betriebsklima und die Leistungsfähigkeit des Unternehmens auswirken.

» Um eine sichere und gesundheitsgerechte Gestaltung der Arbeit mit KI zu ermöglichen, ist eine Beurteilung der Arbeitsbedingungen, die die psychische Belastung einschließt, schon bei der Einführung von KI sinnvoll. «

Weiterhin ist es möglich, dass **Arbeitsmittel** ungünstig gestaltet sind, da das technische System bei Funktionsfehlern ungenügende oder unklare Antworten liefert. Immer häufiger werden bei Fragen und Problemen der Beschäftigten Chatbots eingesetzt, statt mit einem Menschen differenzierte Lösungen für ein Problem zu finden. Arbeitsplätze können durch KI aber auch für Menschen mit besonderen Bedürfnissen zugänglicher werden[9]. So profitieren gehörlose Menschen bereits durch Autotranskription von Gesprächen oder Vorlesungen.

Bezüglich der **Arbeitsumgebung** lassen sich viele Potenziale von KI feststellen. Die physische Arbeitsbelastung durch schwere Lasten und ungesunde Haltung sowie auch schmutzige und gefährliche Tätigkeiten können weiter verringert werden. So können selbstfahrende LKWs und Bohrmaschinen das Risiko für Menschen in Minen reduzieren. KI-gestützte Systeme sind in der Lage, toxische Materialien zu identifizieren und zu handhaben.

Folgen für Sicherheit und Gesundheit

Belastungsfaktoren, wie die hier beschriebenen, können sich negativ auf die Sicherheit und Gesundheit der Beschäftigten auswirken. So kann eine hohe Arbeitsintensität die Gesundheit verschlechtern[10] und Isolation das Wohlbefinden am Arbeitsplatz verringern.[11] Fallen Pausen häufig aus, kann sich sowohl das Unfallrisiko erhöhen[12] als auch das Auftreten von Nacken-, Rücken- und Schulterschmerzen, Müdigkeit sowie physischer und emotionaler Erschöpfung begünstigt werden.[13]

Maßnahmen für einen guten Umgang mit KI

Um eine sichere und gesundheitsgerechte Gestaltung der Arbeit mit KI zu ermöglichen, ist eine Beurteilung der Arbeitsbedingungen, die die psychische Belastung einschließt, schon bei der Einführung von KI sinnvoll.

Grundsätzlich sollte ein menschenzentrierter Ansatz verfolgt werden. Damit wird bewusst Abstand von einer technikzentrierten Gestaltung von KI-Systemen genommen, die vor allem Effizienzsteigerung in den Vordergrund stellt. Stattdessen rückt der Mensch wieder in den Mittelpunkt[14], indem er gemeinsam mit KI arbeitet, kreativ gestaltet und eigenverantwortlich Entscheidungen trifft. KI soll die Arbeit unterstützen, nicht ersetzen.

Aus diesem Grund sollte zunächst geprüft werden, in welchen Bereichen auf die Einführung von KI verzichtet werden sollte, wenn deren Nutzen die Risiken nicht übersteigt oder eine gute Gestaltung nicht gewährleistet werden kann. Fällt die Entscheidung für eine Einführung von KI, bieten die folgenden Beispiele einen ersten Einblick und Impulse für technische, organisatorische und personenbezogene Maßnahmen.

Als **technische Maßnahmen** ist „Explainable AI“ (erklärbare KI) eine besondere Unterstützung. Dabei macht die KI ihre

internen Informationsverarbeitungsschritte nachvollziehbar, statt nur die Ergebnisse der Verarbeitung zu liefern. Dies versetzt den Menschen in die Lage, das System besser zu verstehen und erhöht somit Vertrauen in das System sowie dessen Effizienz.[15] Das oben genannte System, das vor einer Sepsis warnt, könnte beispielsweise die konkreten Vitalparameter sowie deren Gewichtung transparent machen, die zu einer Warnmeldung und Handlungsempfehlungen geführt haben.

Aus **organisatorischer Sicht** ist es hilfreich und sinnvoll, die KI-Einführung als Change Management zu verstehen. KI beeinflusst potenziell sehr verschiedene Arbeitstätigkeiten in der Organisation und hängt somit mit vielen Belastungsfaktoren zusammen. Somit eignet sich ein systematisch gestalteter Veränderungsprozess, der schon bei der Analyse und der Planung die Beschäftigten einbindet und kontinuierlich die Chancen und Herausforderungen für die Arbeit sowie Sicherheit und Gesundheit der Beschäftigten im Blick hat, besonders.

Auf **personenbezogener Ebene** spielt KI-Kompetenz („AI literacy“) eine wichtige Rolle, um „KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“[16]. Laut europäischer KI-Verordnung müssen alle Personen, die in einer Organisation mit dem Betrieb oder der Nutzung von KI-Systemen zu tun haben, über solche Kompetenzen verfügen.[17]

Fazit

Eine gute Gestaltung von KI auf technischer, organisatorischer und personenbezogener Ebene ermöglicht es, die zahlreichen Chancen der Technologie zu nutzen, Herausforderungen frühzeitig im Blick zu haben und somit negative Auswirkungen auf Sicherheit und Gesundheit zu vermeiden. ●

Die DGUV Information 206-053 „Sicherheit & Gesundheit in Veränderungsprozessen“ gibt hilfreiche Tipps, wie Beschäftigte im gesamten Prozess eingebunden werden können.

Autorinnen

Dr. Christina Heitmann,
DGUV Akademie

Dr. Marlen Cosmar,
DGUV Akademie

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/04/#fussnoten

Künstliche Intelligenz in der Schule: Psychische Auswirkungen

Mehr als die Hälfte aller Schülerinnen und Schüler wünscht sich, dass Software auf Basis von Künstlicher Intelligenz (KI) fester Unterrichtsbestandteil wird. Noch wird sie meist punktuell genutzt. Ein Blick auf die möglichen psychischen Auswirkungen kann dabei helfen, zukünftige Einsatzmöglichkeiten besser zu beurteilen.

Die Vodafone Stiftung hat 2024[1] eine Befragung mit mehr als 1500 Jugendlichen im Alter von 14 bis 20 Jahren aus Deutschland durchgeführt. Demnach nutzen bereits 75 Prozent der Befragten textgenerierende KI oder auch KI-basierte Lernplattformen für die Schule. Am häufigsten wurden hierfür frei zugängliche Chatbots primär der großen amerikanischen Anbieter verwendet.

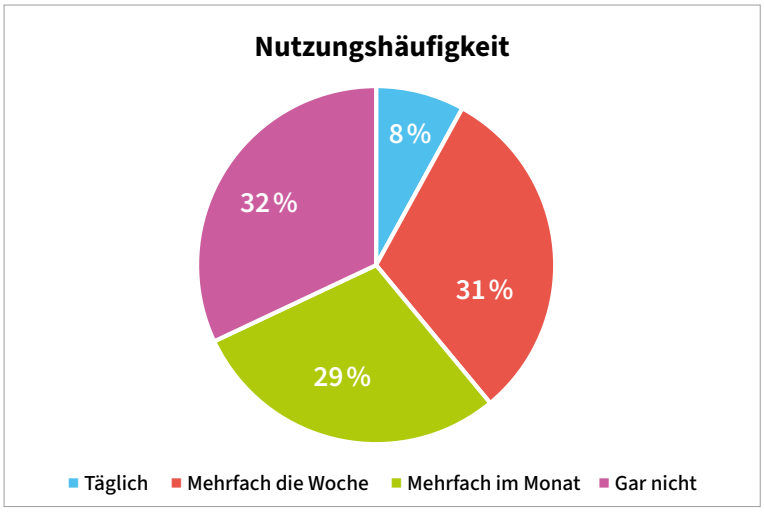
In Abbildung 1 ist ersichtlich, dass fast 40 Prozent der Befragten KI täglich bis mehrmals in der Woche nutzen.

Mehr als 70 Prozent der Befragten sahen die Nutzung von KI als Chance oder als eindeutige Chance, während nur 4 Prozent die Nutzung als eindeutiges Risiko wahrnahmen.

58 Prozent der Befragten wünschen sich, dass KI ein fester Unterrichtsbestandteil wird, vor allem in Fremdsprachen und Mathematik sowie in den Naturwissenschaften.

Key Facts

- Schülerinnen und Schüler nutzen bereits verbreitet Software, die auf Künstlicher Intelligenz basiert
- Chatbots, adaptive Lernprogramme oder tutorielle Systeme können den Lernerfolg fördern
- Studien zeigen, dass die psychischen Auswirkungen der Nutzung sowohl positiv als auch negativ sein können



Quelle: Vodafone, 2024

Abbildung 1: Häufigkeit der Nutzung von KI durch Schülerinnen und Schüler

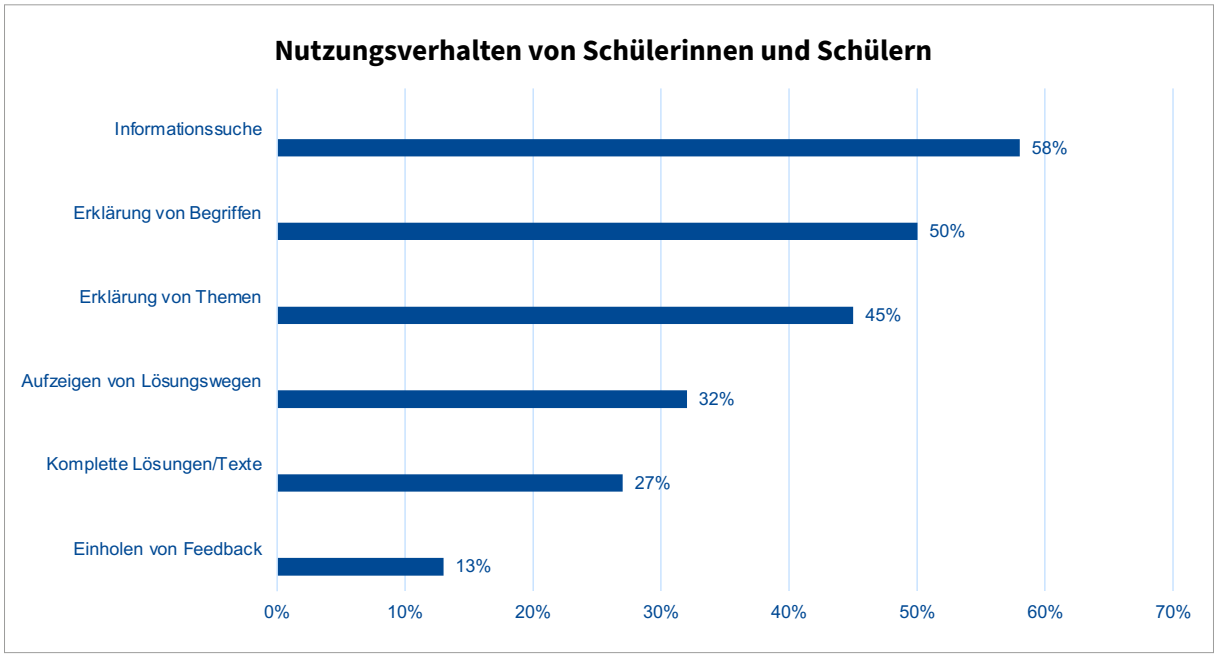


Abbildung 2: Anlässe für die Nutzung von KI durch Schülerinnen und Schüler

In Abbildung 2 kann man das Nutzungsverhalten von Schülerinnen und Schülern erkennen. So nutzt über die Hälfte der Befragten KI zur Informationssuche. Etwa ein Drittel lässt sich Lösungswege aufzeigen und erklären. Über ein Viertel lässt sich auch komplette Lösungen und Texte ausgeben und erstellen.

Darüber hinaus würden sich Schülerinnen und Schüler laut der Studie von KI bei der Bilderstellung, Literaturrecherche, Übersetzungen sowie der Plagiatssuche unterstützen lassen.

Neben Chatbots stellen Intelligente Tutorielle Systeme (ITS) einen wichtigen Bereich KI-basierter Lernunterstützung im Schulkontext dar. ITS vermitteln Wissen in verschiedenen Bereichen mit individuellen Lernstrategien. Der Lernfortschritt wird immer wieder geprüft und Lerninhalte werden dann zum Niveau passend zugewiesen. Lehrende können so Lernen und Üben teilweise an die Software übertragen und gezielter auf Schwierigkeiten einzelner Schülerinnen und Schüler eingehen. In Fächern, in denen es klare richtige und falsche Lösungen gibt, wie in Mathematik, kommt solche Software bereits zum Einsatz.

Lehrende können zudem auf interaktive KI-basierte Klassenverwaltungssysteme zurückgreifen. Die Software dokumentiert das Verhalten jeder Schülerin und jedes Schülers einzeln und erstellt daraus Vorschläge für die optimale Förderung.

Welche psychischen Auswirkungen die Nutzung von KI auf Schülerinnen und Schüler hat, recherchierte die DGUV Akademie in einem wissenschaftlichen Projekt. Aus den Ergebnissen wurden Handlungsempfehlungen abgeleitet. Mehr als 30 Studien – darunter Metaanalysen und Reviews – wurden in die Zusammenstellung einbezogen, die über Google Scholar und das

Discovery-System „JOST“ der Universität Osnabrück gefunden wurden. Die Studien beziehen sich auf Grundschulkinder, Jugendliche in den Sekundarstufen und Studierende, wobei die Ergebnisse als übertragbar angesehen werden.

Positive Auswirkungen und Chancen

Die Nutzung von ITS ermöglicht eine individuelle Lernförderung. Beispielsweise können durch direktes Feedback Fehler und Verbesserungsvorschläge sowie Wissenslücken und deren Behebung angezeigt werden. Hierbei werden unterschiedliche Lernstile berücksichtigt. Dies ist besonders relevant für Schülerinnen und Schüler mit Lernschwierigkeiten wie beispielsweise Leserechtschreibschwäche oder auch Aufmerksamkeits-Defizitsyndromen, weil eine leichtere Integration ermöglicht wird.[2]

Weiterhin dient die Nutzung von KI der Motivationsförderung durch abwechslungsreiche und personalisierte Lerninhalte. Empfinden Schülerinnen und Schüler mehr Spaß und Erfolg, so haben sie auch mehr Motivation sich auf Lernmaterial einzulassen und bei schwierigen Aufgaben nicht aufzugeben. Henze et al.[3] zeigten dies am Beispiel von Physikstudierenden, welche im Laufe des Studiums KI nutzen konnten, und deshalb auch bei schwierigen Aufgaben nicht so schnell aufgaben.

Auch zur Förderung des Selbstvertrauens kann KI beitragen. Durch positiv formuliertes Feedback, Lernunterstützung sowie die Motivationsförderung, fällt das Lernen leichter. Dies spiegelt sich in besseren Leistungen wider. Durch die Erfolgserlebnisse trauen sich Schülerinnen und Schüler außerdem mehr zu, ihr Selbstvertrauen steigt also. Hierdurch kann auch Prüfungsangst verringert werden.[4]

Bei Stress und Einsamkeit kann die Bindung an Chatbots positive Effekte haben.[5] Diese bieten emotionale Unterstützung, Ermutigung und psychologische Sicherheit. Wahrgenommene emotionale Sicherheit wurde von Henze et al. auch bei der Arbeit mit KI-Tools im Bildungsbereich gemessen. Studierende, die KI-Tools nutzten, berichteten von weniger Stress und Frustration.

Die Nutzung von KI-Tools kann auch zur Chancengleichheit beitragen. Durch den freien Zugang zu qualitativ hochwertigen Bildungsressourcen kann man von einer Demokratisierung von Bildung sprechen.

» Die Nutzung von KI-Tools kann auch zur Chancengleichheit beitragen. Durch den freien Zugang zu qualitativ hochwertigen Bildungsressourcen kann man von einer Demokratisierung von Bildung sprechen. «

Negative Auswirkungen

Es lassen sich in den Studien jedoch auch Risiken durch die Nutzung von Künstlicher Intelligenz finden.

Spitzer[6] verweist auf Studien, die belegen, dass Chatbots beziehungsweise Large Language Models die Fähigkeit für Textverständnis und -erzeugung reduzieren. Er warnt davor, sie in höheren Schulklassen einzusetzen.

Bastani et al.[7] konnten eine Leistungsverschlechterung durch KI-Nutzung in einer Studie belegen. Verwendeten die Teilnehmenden einen Chatbot, kam es zu einer anfänglichen Leistungsverbesserung (48 Prozent). Wurde die KI entfernt, kam es zu einer 17-prozentigen Leistungsreduktion im Vergleich zu einer Kontrollgruppe, die keine KI genutzt hat.

In einer Studie mit mehr als 3800 chinesischen Jugendlichen fanden Huang et al. (2024)[8] heraus, dass bereits fast ein Viertel der Jugendlichen eine Abhängigkeit von KI zeigte. Während eine Bindung an Chatbots positive Effekte haben kann, stellen Trennungsängste und Abhängigkeit die Kehrseite dar. Diese können die psychologische Entwicklung unterbrechen und zu Langzeitfolgen wie einer reduzierten Leistungsfähigkeit und einem erhöhten Stresslevel führen. Chatbots verdrängen außerdem echte soziale Beziehungen. Diese soziale Isolation führt zu einer Verschlechterung der mentalen Gesundheit und kann auch die emotionale Intelligenz beeinträchtigen. Die soziale Dimension des Lernens ist gerade im schulischen Kontext wichtig.

Auch Falschaussagen von KI, sogenanntes „Halluzinieren“, stellen ein großes Risiko dar. Dies kann zu Verwirrung und Frustration führen. Bei ungenauen Antworten können Schülerinnen und Schüler verunsichert werden. Dadurch können sie Angst entwickeln, Fehler zu machen.[9]

Weiterhin kann KI Vorurteile und Rassismus verstärken. So wurden beispielsweise ethnisch-linguistische Stereotype von KI gegenüber Dialekten wie African-American English festgestellt. Dies geschieht vor allem durch die Nutzung alter Datensätze, wodurch „Vorurteile der Vergangenheit zu Vorurteilen der Zukunft führen“[10]. Auch in Bildungstools konnte rassistische Voreingenommenheit festgestellt werden: In akademischen Algorithmen wurden ethnische Minderheiten als weniger erfolgreich eingeschätzt. Generell wurde Diskriminierung gegenüber dem Geschlecht, sozioökonomischen Hintergrund und der Ethnie festgestellt. Dies führt zu einer Aufrechterhaltung von diskriminierenden Strukturen im Bildungswesen und reduziert die Chancengleichheit.

Diese Diskriminierung kann sich polarisierend in der Folge auf die Meinungsbildung von Schülerinnen und Schülern auswirken. Laut Wollersheim[11] ist dies eine „Gefährdung für die Entwicklung einer zutreffenden Weltorientierung“.

Lehrkräfte sorgen sich auch vor Plagiaten und dem daraus entstehenden Verlust an akademischer Integrität. Etwa 37 Prozent der Lehrkräfte verbietet KI-Nutzung laut einer Umfrage von Bitkom.[12] 57 Prozent können nicht einzuschätzen, ob KI genutzt wurde. Auch Schülerinnen und Schüler haben Angst vor Plagiaten: Die Vodafone Stiftung berichtet, dass 43 Prozent der Jugendlichen sich Sorgen machen, unbegründet des Schummelns beschuldigt zu werden.

» Verlassen sich Schülerinnen und Schüler beim Lernen und bei den Hausaufgaben übermäßig auf KI, fehlt der aktive Kompetenzerwerb. Im schlimmsten Fall erwerben sie kaum Fähigkeiten, selbstständig zu denken und eigene Selbstwirksamkeit zu erleben. «

Verlassen sich Schülerinnen und Schüler beim Lernen und bei den Hausaufgaben übermäßig auf KI, fehlt der aktive Kompetenzerwerb. Im schlimmsten Fall erwerben sie kaum Fähigkeiten, selbstständig zu denken und eigene Selbstwirksamkeit zu erleben. Dadurch wiederum erhöht sich das Abhängigkeitsrisiko. Auch weitere kognitive Fähigkeiten, wie zum Beispiel das Erinnerungsvermögen sowie das kreative Denken, können betroffen sein.

Weiterhin stellt sich die Frage: Wenn man alle Aufgaben an die KI delegiert werden können, warum sollte man sich noch mit ihnen beschäftigen. Wenn Schülerinnen und Schüler keine Selbstwirksamkeit und keinen Stolz für die eigene Arbeit empfinden, geht die intrinsische Lernmotivation verloren. Dies führt zu Frust, Unsicherheit, Langeweile und im späteren Verlauf tendenziell zu Prokrastination und Demotivation.

Überforderung bei der Nutzung von KI-basierten Tools kann auch „Techno-Stress“ erzeugen. Durch fehlendes Training und mangelnde technische Kenntnisse erleben Betroffene teilweise Überforderung, Stress und Angst. Laut der Vodafone Studie[13] geben 38 Prozent der europäischen Jugendlichen an, dass sie sich überfordert von KI fühlen, weil man „viel wissen muss, um [sie] zu nutzen“. Die erhöhte Bildschirmzeit kann außerdem zu digitaler Ermüdung führen.

Die dauerhafte Erreichbarkeit von Wissen kann zu erhöhtem Leistungsdruck führen und zu der Angst, mit der KI mithalten zu müssen.[14] Es gibt einen erhöhten Leistungsdruck durch Vergleiche auf Online-Plattformen und Learning Analytics. KI kann auch zu Zukunftsängsten und Einschränkungen in der Karrierewahl führen.

Auch Deindividuation ist ein möglicher Kritikpunkt: Haben Schülerinnen und Schüler den Eindruck, in Klassenverwaltungssystemen nur noch ein Datenpunkt zu sein, besteht die Gefahr, sich nicht länger als eigenständige Person innerhalb des Bildungssystems zu fühlen.[15]

Die Nutzung guter KI ist häufig auch an finanzielle Möglichkeiten der Familie gebunden. Gute intelligente tutorielle Systeme und Laptops sind teuer. Laut Vodafone Stiftung haben 38 Prozent der europäischen Jugendlichen die Befürchtung, KI weniger zu ihrem Vorteil nutzen zu können als ihre Mitschülerinnen und Mitschüler.

Weitere Vorsicht gilt dem Einfluss von KI auf die Umwelt. Eine Anfrage an eine KI verbraucht 0,0029 kWh – so viel Energie wie es braucht, um eine Energiesparlampe 15 Minuten leuchten zu lassen. Nach 345 Anfragen ist eine Kilowattstunde verbraucht. Sollte KI im Schulalltag vollends Einzug halten, muss der Energieverbrauch berücksichtigt werden.

Positive Auswirkungen	Negative Auswirkungen
Motivationsförderung	Oberflächliches Lernen und kognitiver Abbau
Förderung von Selbstvertrauen	Abhängigkeitspotential
Psychologische Unterstützung	Fehlinformation und mangelnde Zuverlässigkeit
Individuelle Lernförderung und adaptive Tutorien	Begrenzte Bewertungsfähigkeit
Unterstützung bei Lernschwierigkeiten	Förderung von Vorurteilen, Rassismus und polarisierte Meinungsbildung
Chancengleichheit	Plagiate, Verlust von Integrität und Selbstwirksamkeit
Stressreduktion	Prokrastination und Verlust von (intrinsischer) Lernmotivation
	Erhöhter Leistungsdruck
	Soziale Isolation, digitale Ermüdung
	Fehlende emotionale Unterstützung
	Finanzielle und soziale Ungerechtigkeit
	Zukunftsangst und Überforderung
	Verlust von Autonomie und Selbstbestimmung
	Deindividuation

Quelle: eigene Darstellung

Tabelle 1: Überblick über positive und negative Auswirkungen von KI-Nutzung

Die Tabelle 1 zeigt mögliche positive und negative Auswirkungen von KI-basierten Tools auf Schülerinnen und Schüler im Überblick.

Handlungsempfehlungen

Es ist wichtig, dass KI-Kenntnisse frühzeitig im Lehrplan verankert werden. KI-basierte Software darf aber nicht zu einer Ablösung der gezielten Verinnerlichung und Anwendung von Wissen führen. Selbst schreiben, lesen und rechnen bleiben bis in die Abschlussjahrgänge von größter Bedeutung.

Schülerinnen und Schüler müssen einen kritischen Umgang mit den Ergebnissen erlernen, die von KI-basierten Werkzeugen, vor allem von Chatbots, erstellt werden. Intelligente tutorielle Systeme sind hier anders einzuordnen, weil sie Denkprozesse nicht ersetzen oder verkürzen, sondern eher herkömmliches Lernen unterstützen. Im Schulalltag sollte auf eine Kombination aus KI und der Vermittlung und Betreuung durch Lehrkräfte gesetzt werden, da vor allem Letztere wichtig für die Entwicklung emotionaler Intelligenz und zwischenmenschlicher Fähigkeiten der Kinder und Jugendlichen ist.

Zudem sollte über das Abhängigkeitsrisiko besonders auch mit Blick auf Chatbots aufgeklärt werden.

Vor dem Hintergrund der zunehmenden Integration von KI in schulische Lernprozesse erscheint es erforderlich, Lehrmethoden und Prüfungsformate kritisch zu reflektieren und gegebenenfalls neu zu gestalten. Dabei stellt sich insbesondere die Frage, ob Formate wie Hausaufgaben und schriftliche Arbeiten weiterhin einen Beitrag zu Kompetenzentwicklung leisten können.

Sehr bedeutsam ist ein gleichberechtigter Zugang zu KI-basierter Lernsoftware. Auch darf KI nicht zu einer Einsparung von Lehrkräften führen. Vielmehr kann der derzeitige Mangel an Lehrkräften durch KI teilweise kompensiert werden. Die aktive Auseinandersetzung mit Wissen vor Ort in der Schule ist aber unersetzbar.

Das folgende Zitat fasst den Stand sehr gut zusammen: „KI ‚macht' keine Bildung, kann aber sehr wohl Bildung ermöglichen und Bildungsprozesse unterstützen."[16]

Autorinnen

Dr. Marlen Cosmar,
DGUV Akademie

Greta Nepp,
TU Dresden

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/05/#fussnoten

Orientierung in der Vielfalt digitaler betrieblicher Gesundheitstools

Digitale Tools bereichern zunehmend das Betriebliche Gesundheitsmanagement. Doch welche Anwendungen sind qualitativ geeignet, sicher und praxistauglich? Eine neue DGUV Information bietet Orientierung bei der Auswahl und Bewertung digitaler Anwendungen im Präventionsfeld „Gesundheit bei der Arbeit“.

Digitale Technologien verändern die Arbeitswelt und eröffnen auch neue Möglichkeiten, um die Gesundheit bei der Arbeit zu stärken. Gesundheits-Apps, Wearables oder webbasierte Coachings werden zunehmend im Rahmen des Betrieblichen Gesundheitsmanagements eingesetzt.

Laut einer Studie des Instituts für Betriebliche Gesundheitsberatung (IFBG), der Techniker Krankenkasse und der Haufe Group aus dem Jahr 2025 verwenden bereits 42,3 Prozent der befragten Unternehmen und Einrichtungen des Öffentlichen Dienstes bundesweit digitale Angebote der Betrieblichen Gesundheitsförderung (BGF).[1] Die Bandbreite reicht von einzelnen Anwendungen bis hin zu umfassenden Komplettsystemen für das Betriebliche Gesundheitsmanagement (BGM).

Vorteile und Herausforderungen

Digitale Tools bieten viele Vorteile. Sie ermöglichen eine orts- und zeitunabhängige Nutzung, sind niedrigschwellig und sprechen Beschäftigte durch interaktive oder spielerische Elemente an.[2] Die Tools berücksichtigen persönliche Bedürfnisse, können die individuelle Gesundheitskompetenz stärken und gesundheitsgerechtes Verhalten im Arbeitsalltag erleichtern – etwa durch Erinnerungen an Pausenübungen bei überwiegend statischen Tätigkeiten oder durch Stress-Checks und gezielte Tipps.

Auch BGM-Verantwortliche können sich bei der Umsetzung eines BGM von digitalen Tools unterstützen lassen: BGM-Komplettsysteme erfassen Teilnahmezahlen, Fehlzeiten oder erfragen Arbeitsbelastungen. Sie erleichtern die Dokumentation und Organisation von Prozessen und bieten Möglichkeiten für die Evaluation.

Gleichzeitig sind Herausforderungen zu beachten. Technische Probleme, fehlerhafte Inhalte oder mangelhafte Akzeptanz bei den Beschäftigten können die Wirksamkeit einschränken.

Key Facts

- Digitale Gesundheitsanwendungen bieten Chancen, bringen aber auch Herausforderungen für ein Betriebliches Gesundheitsmanagement mit sich
- Qualitätskriterien helfen bei der Auswahl geeigneter Tools
- Die DGUV Information 206-058 bietet eine praxisorientierte Checkliste, die Transparenz, Datenschutz, Technik, Inhalte und Gebrauchstauglichkeit bewertet

Daten könnten missbraucht werden und Fehler beim Gebrauch auftreten.[3] Besonders kritisch ist der Umgang mit sensiblen Gesundheitsdaten – hier sind Datenschutz und IT-Sicherheit gefragt. Zudem existierten bereits im Jahr 2015 weltweit „mehr als 160.000 Digital-Health-Anwendungen für mobile Endgeräte und unzählige gesundheitsbezogene Web-Anwendungen“.[4]

DGUV Information als Orientierungshilfe

Welche dieser vielen Tools sind nun qualitativ hochwertig, datenschutzkonform und tatsächlich geeignet, gesundheitsbezogene Ziele im Betrieb zu unterstützen? Welche Kriterien sollten bei der Auswahl und Einführung herangezogen werden?

Die „DGUV Information 206-058: Digitale Anwendungen im Präventionsfeld ‚Gesundheit bei der Arbeit‘ – eine Orientierungshilfe“[5] bietet hierfür Unterstützung. Sie stellt Qualitätskriterien in Form einer Checkliste bereit, mit der Organisationen Tools strukturiert bewerten können. Dabei konzentriert sie sich ausdrücklich auf Anwendungen im Präventionsfeld „Gesundheit bei der Arbeit“, die sich von medizinischen Apps abgrenzen, welche bereits durch das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) nach § 139e SGB V geprüft und im DiGA-Verzeichnis[6] gelistet sind.

» Die Checkliste erhebt keinen Anspruch auf Vollständigkeit. Sie soll als eine pragmatische Entscheidungshilfe dienen. «

Entwicklung der Checkliste

Grundlage der DGUV-Orientierungshilfe war eine umfangreiche, systematische Literaturrecherche.[7] Bestehende Qualitätskriterien für digitale Anwendungen im Bereich Sicherheit und Gesundheit aus verschiedenen Quellen wurden recherchiert – unter anderem:

- die Qualitätskriterien des Leitfaden Prävention des GKV-Spitzenverbandes[8],
- die häufig herangezogenen Qualitätskriterien von Albrecht[9] sowie
- das Gütekriterien-Kernset von Thranberend und Bittner[10].

Alle Qualitätskriterien wurden in einer Synopse erfasst und hinsichtlich ihrer Häufigkeit in allen Bewertungskatalogen, der Relevanz für den Bereich Gesundheit im Betrieb sowie der Erfüllung in den digitalen Anwendungen der Träger der gesetzlichen Unfallversicherung gewichtet und auf den betrieblichen Kontext übertragen.

Die Checkliste erhebt keinen Anspruch auf Vollständigkeit. Sie soll als eine pragmatische Entscheidungshilfe dienen. Um die Anwendung zu erleichtern, wurden die Kriterien in drei Kategorien unterteilt:

- Must-have: Mindestanforderungen, die ein Tool zwingend erfüllen sollte
- Should-have: Kriterien, die die Praxistauglichkeit und Akzeptanz des Tools erhöhen

- Nice-to-have: Zusatzmerkmale, die einen Mehrwert bieten können, aber nicht zwingend erforderlich sind

Aufbau und Anwendung der Checkliste

Die Bewertung erfolgt entlang von fünf zentralen Qualitätsdimensionen, die jeweils durch spezifische Kriterien und Indikatoren operationalisiert sind:

- Transparenz: Bewertet wird, ob das Tool klare Informationen zu Zielsetzung, Zielgruppen, Kosten und Angebotsidentität bereitstellt.
- Datenschutz: Die sichere und transparente Verarbeitung personenbezogener Daten bezieht sich auf die Gewährleistung grundlegender Faktoren des Datenschutzes sowie die Einhaltung der individuellen Datenschutzvorgaben des Unternehmens. Bei Bedarf wird die Einholung von Expertise empfohlen. Die aufgelisteten Punkte zeigen gleichzeitig wesentliche Aspekte auf, die berücksichtigt werden sollten, wenn eine Prüfung durch Fachkräfte nicht möglich oder nicht gewünscht ist.
- Technik und Interoperabilität: Hier geht es um die technische Zuverlässigkeit und die Kompatibilität mit bestehenden Systemen im Unternehmen. Auch Aspekte wie Barrierefreiheit und Updates werden berücksichtigt.
- Qualität der Inhalte: Die bereitgestellten Informationen sollten fachlich fundiert, aktuell, evidenzbasiert und für die Zielgruppe verständlich aufbereitet sein. Dies betrifft sowohl Textinhalte als auch audiovisuelle Elemente.
- Gebrauchstauglichkeit: Eine intuitive Bedienung, attraktive Gestaltung und niedrigschwelliger Zugang sind entscheidend für die Akzeptanz bei den Beschäftigten. Auch die Möglichkeit zur Individualisierung sowie Motivationselemente spielen eine Rolle.

Je nach Ziel und Funktion der Anwendung – etwa Informationsvermittlung, Verhaltensförderung oder Monitoring – können einzelne Indikatoren unterschiedlich relevant sein. Die Checkliste ermöglicht eine flexible Gewichtung und unterstützt eine bedarfsgerechte Entscheidung. Durch ihre systematische Struktur bietet sie eine praktische Unterstützung für Unfallversicherungsträger im Beratungskontext und für Organisationen, die digitale Tools in ihr BGM integrieren möchten.

DGUV Information

publikationen.dguv.de
Webcode: p206058
Digitale Anwendungen im Präventionsfeld „Gesundheit bei der Arbeit“ – eine Orientierungshilfe | DGUV Publikationen

Autorin

Anja Mücklich,
DGUV Akademie

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/06/#fussnoten

KI in der Maschinensicherheit: Potenziale, Grenzen und sichere Einbindung

Gerade dort, wo klassische Schutzkonzepte an ihre Grenzen stoßen, eröffnet der Einsatz von künstlicher Intelligenz neue Möglichkeiten für den Arbeitsschutz. Gleichzeitig kann KI jedoch zu unvorhersehbaren Entscheidungen führen. Für die Sicherheit der Beschäftigten unterliegt ihr Einsatz daher strengen Anforderungen.

Die rasante Entwicklung von KI eröffnet auch für die Maschinensicherheit neue Perspektiven. KI-Systeme können Arbeitsumgebungen interpretieren, Verhaltensmuster erkennen und potenziell gefährliche Situationen frühzeitig melden. So lassen sich Gefährdungen adressieren, die bisher nicht durch konventionelle Sicherheitsfunktionen abgedeckt waren, etwa durch unvorhergesehenes menschliches Verhalten, komplexe Arbeitsumgebungen oder variable Prozesse. Dies ermöglicht die Vermeidung von Arbeitsunfällen.

Regulatorische Rahmenbedingungen

Um diese Potenziale zu nutzen und dabei die Sicherheit und Gesundheit der Beschäftigten zu erhalten, werden klare rechtliche Anforderungen benötigt. Die KI-Verordnung (EU) 2024/1689 (KI-VO)[1] bildet den zentralen europäischen Rechtsrahmen für KI-Systeme. Sie stuft KI-Anwendungen nach Risiken ein und fordert für „Hochrisiko-KI-Systeme“, zu denen KI-basierte Sicherheitsfunktionen in Maschinen zählen, insbesondere:

- ein Risikomanagement über den gesamten Lebenszyklus,
- hohe Datenqualität, Robustheit und Transparenz,
- technische Dokumentation und menschliche Aufsicht
- sowie Verfahren zum Qualitätsmanagement und Fehlerbehandlung.

Auch die Maschinenverordnung (EU) 2023/1230 (MVO)[2], gültig ab 20. Januar 2027, betrifft KI-Systeme, wenn sie sicherheitsrelevante Funktionen übernehmen. Die MVO ersetzt die Maschinenrichtlinie 2006/42/EG (MRL)[3] und verlangt, dass für solche KI-Systeme im Rahmen des Konformitätsbewertungsverfahrens für die Maschine neben den Anforderungen der MVO auch die Anforderungen der KI-VO betrachtet werden.

Key Facts

- Künstliche Intelligenz (KI) eröffnet neue Möglichkeiten für den Arbeitsschutz und die Maschinensicherheit
- Aufgrund unvollständiger normativer und regulatorischer Anforderungen kann KI Sicherheitsfunktionen derzeit unterstützen, aber nicht ersetzen
- Die Einbindung von KI in Sicherheitsfunktionen erfordert eine gesamtsystemische Betrachtung

Normung und funktionale Sicherheit

Zur Umsetzung der Anforderungen der MRL, und zukünftig der MVO, gelten in der Maschinensicherheit die Grundsätze der funktionalen Sicherheit. Sicherheitsfunktionen müssen deterministisch, nachvollziehbar und validierbar sein. KI-Systeme verhalten sich dagegen probabilistisch. Ihr Entscheidungsprozess ist häufig nicht vollständig erklärbar. Das erschwert den Nachweis der funktionalen Sicherheit im Rahmen des Konformitätsbewertungsprozesses. Normen bilden den Stand der Technik ab und erleichtern die Umsetzung der Anforderungen von MRL und MVO an sichere Maschinen. Relevante Normen auf dem Gebiet der funktionalen Sicherheit sind IEC 61508[4] und ISO 13849[5], die Anforderungen an sicherheitsgerichtete Steuerungen festlegen. Diesen Anforderungen müssen auch KI-basierte Sicherheitsfunktionen genügen. Zudem werden die Prüfung und Zertifizierung, zum Beispiel durch notifizierte Stellen, beeinflusst. Neue Bewertungsansätze sind erforderlich.

Während die funktionale Sicherheit auf definierte Sicherheitsintegritätslevel (SIL) oder Performance Level (PL) setzt, lassen sich solche Kennwerte auf dynamische KI-Systeme nur eingeschränkt anwenden. Erste Ansätze zur Überbrückung dieser Lücke finden sich im ISO/IEC TR 5469:2024 „Functional Safety and AI Systems“[6]. Weiterführende Arbeiten erfolgen derzeit im Normungsprojekt ISO/IEC TS 22440[7].

» Nur ein gesamtsystemischer Ansatz kann sicherstellen, dass die Maschine auch unter veränderten Bedingungen vorhersehbar reagiert. «

Gesamtsystemische Absicherung

Damit KI sicher eingesetzt werden kann, muss sie in das gesamte Maschinensystem integriert werden, von der Sensorik über die Steuerung bis zur Mensch-Maschine-Schnittstelle und der Arbeitsumgebung. Entscheidend ist das Zusammenspiel aller Komponenten: Nur wenn ihre Wechselwirkungen verstanden und kontrolliert werden, lässt sich ein sicherer Gesamtzustand gewährleisten.

Eine isolierte Bewertung einzelner KI-Modelle greift dabei zu kurz. Veränderungen an der Datenerfassung oder der Auswertung können das Verhalten des Gesamtsystems beeinflussen. Daher ist es notwendig, die Sicherheit nicht nur auf Funktionsebene, sondern systemisch auf mögliche Rück- und Nebenwirkungen und über den gesamten Lebenszyklus der Maschine hinweg zu betrachten, von der Entwicklung über die Inbetriebnahme bis zum Betrieb, zur Wartung und zum Rückbau.

Nur ein gesamtsystemischer Ansatz kann sicherstellen, dass die Maschine auch unter veränderten Bedingungen vorhersehbar reagiert. So kann KI zu einem Bestandteil eines sicher gestalteten Gesamtsystems werden; unterstützend, aber eingebettet in nachvollziehbare Strukturen und Verantwortlichkeiten.

KI-gestützte Assistenzsysteme

Bereits heute unterstützt KI Beschäftigte direkt, etwa durch Systeme, die gefährliche Körperhaltungen erkennen oder bei

riskanten Arbeitsschritten warnen. Diese Assistenzsysteme haben keinen rechnerisch nachweisbaren Einfluss auf die Risikominderung, wirken aber ergänzend zu bestehenden Schutzmaßnahmen. Sie können Fehlverhalten, Ablenkung, Überlastung oder gefährliche Situationen erkennen und so präventiv zur sicheren Arbeit beitragen.

Ein Beispiel ist eine KI-gestützte Objekt- oder Personenerkennung. Diese kann feststellen, wenn Personen ungeschützte Bereiche betreten oder Schutzeinrichtungen umgehen, und dann Warnungen ausgeben oder eine Maschine anhalten, bevor ein Unfall geschieht.

Wesentlich ist, dass solche Systeme nachvollziehbar eingebunden werden. Die DGUV Test Prüfgrundsätze GS-BAU-70[8] beschreiben grundlegende Anforderungen an den sicheren Einsatz von Assistenzsystemen an Maschinen und Nutzfahrzeugen. Ergänzend wurden in der DGUV Test Information 5[9] allgemeine Grundsätze für die sicherheitstechnische Bewertung von KI erarbeitet, die künftig als Grundlage für Prüfungen von KI-Systemen in Maschinen dienen können.

Zukunftsperspektive

Die Zukunft der Maschinensicherheit liegt in der Kombination bewährter Sicherheitsprinzipien mit neuen datengetriebenen Verfahren. KI kann dort einen Mehrwert bieten, wo klassische Systeme an Grenzen stoßen, etwa durch vorausschauende Gefährdungserkennung oder adaptive Sicherheitszonen. KI ist in der Lage, Risiken zu erkennen und Maßnahmen vorzuschlagen, aber sicherheitsrelevante Entscheidungen müssen für Betreiberinnen und Betreiber jederzeit überprüfbar bleiben.

Für den Arbeitsschutz bedeutet das: KI kann die sicherheitstechnische Beurteilung unterstützen, diese aber nicht ersetzen. Es braucht klare Zuständigkeiten, eine lückenlose Dokumentation und nachvollziehbare Schritte und Mechanismen, um fehlerhafte Entscheidungen korrigieren zu können. Ziel bleibt, die Zahl der Arbeitsunfälle zu senken. Dies kann durch die Verbindung aus technischer Innovation und bewährter funktionaler Sicherheit geschehen. ●

Infokasten

Maschinensicherheit umfasst alle technischen und organisatorischen Maßnahmen, um Gefährdungen durch Maschinen zu vermeiden. Funktionale Sicherheit bezeichnet die verlässliche Wirkung von Steuerungs- und Schutzeinrichtungen, auch im Fehlerfall.

Autorin

Dr. Svenja Granderath, Berufsgenossenschaft Holz und Metall

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/07/#fussnoten

Vertrauen in Automatisierung: Das richtige Maß ist entscheidend

Das Konzept „Trust in Automation“ beschreibt das Ausmaß, in dem Menschen darauf vertrauen, dass automatisierte Systeme zuverlässig, kompetent und innerhalb ethischer Grundsätze agieren. Ist das Vertrauen zu groß oder zu gering, birgt dies spezifische Gefahren und Herausforderungen.

Stellen Sie sich vor: Sie lassen eine künstliche Intelligenz Ihre medizinische Diagnose stellen, einen Algorithmus Ihr Geld anlegen oder einen Roboter Ihr Haus bewachen. Würden Sie sich entspannt zurücklehnen – oder hätten Sie doch ein mulmiges Gefühl?

Solche Szenen waren noch vor wenigen Jahren Science-Fiction, heute sind sie schon fast Realität. Maschinen und Software assistieren dem Menschen und übernehmen Aufgaben, die früher fest in menschlicher Hand lagen. Sie unterstützen, entscheiden und steuern intelligent oft schneller und sicherer als wir.

So beeindruckend die Anwendungen auch sind: Der Mensch bleibt doch oft skeptisch. Warum fällt es uns so schwer, Kontrolle abzugeben? Was braucht es, damit wir uns auf Maschinen verlassen, ihnen Verantwortung überlassen – vielleicht sogar unser Leben beispielsweise im Auto anvertrauen? Und wieso bleiben Effekte von Assistenzsystemen oft hinter den Erwartungen zurück?

Was ist Vertrauen?

Im Bereich der Führung, des Managements und der Soziologie wurde Vertrauen konzeptionell sehr früh analysiert.[1] Schon 1922 formulierte der Soziologe Georg Simmel, dass Vertrauen eine Erwartung „zukünftigen Verhaltens [ist], die sicher genug ist, um praktisches Handeln darauf zu gründen“.[2] Bisher konnten sich die unterschiedlichen Disziplinen allerdings nicht auf eine allgemeingültige Definition von Vertrauen einigen. Denn Vertrauen kann man nicht direkt messen, sondern nur die Auswirkungen des Vertrauens beziehungsweise des mangelnden Vertrauens, also des Misstrauens.

Vertrauen eröffnet uns neue Möglichkeiten. Es unterstützt unsere begrenzte menschliche Wahrnehmung. Schon in Alltagssituationen kommen wir Menschen an unsere Grenzen. Wir übersehen etwas, reagieren nicht auf alle Umweltreize

Key Facts

- „Trust in Automation“ ist ein entscheidender Faktor, um die Vorteile von automatisierten Systemen nutzen zu können
- Dieses Vertrauen entwickelt sich über Wissen, Interaktion mit dem System, aber auch durch individuelle Voraussetzungen beim Menschen
- Zu großes oder mangelndes Vertrauen kann durch Interaktionen mit dem System, aber auch durch Arbeitsorganisation und Schulungen kalibriert werden

gleichermaßen, überhören zum Beispiel das Piepsen des Handys und treffen Entscheidungen, die nicht optimal sind. Beispiele, die zeigen, dass unsere menschliche Wahrnehmung begrenzt ist. Trotzdem bleiben wir handlungs- und entscheidungsfähig. Denn Vertrauen hilft dabei, die Komplexität von Szenarien abzumildern.

Vertrauen hat auch noch eine weitere Funktion: Es erweitert die menschlichen Möglichkeiten, Entscheidungen zu treffen. Mit Vertrauen werden plötzlich Entscheidungsalternativen möglich, die ohne Vertrauen nicht in Betracht gezogen werden würden. Menschen zeigen dabei eine subjektive Erwartung, dass „es schon klappen wird“.

» Vertrauen in die Automatisierung ähnelt stark dem Vertrauen gegenüber Menschen und ist ein dynamisches Zusammenspiel aus Vorwissen, Erfahrungen, kognitiven Urteilen und Emotionen, aber auch menschlichen Prädispositionen. «

Erwartungen an die Automatisierung

Das Konzept „Trust in Automation“ beschreibt das Ausmaß, in dem Menschen darauf vertrauen, dass automatisierte Systeme zuverlässig, kompetent und innerhalb ethischer Grundsätze agieren. Vertrauen wird insbesondere dann relevant, wenn komplexe Situationen zu bewältigen sind: Nur wenn der Mensch glaubt, dass das System seine Ziele auch unter unsicheren, unklaren Bedingungen unterstützt, wird er Aufgaben an die Automatisierung delegieren.

Vertrauen in die Automatisierung ähnelt stark dem Vertrauen gegenüber Menschen und ist ein dynamisches Zusammenspiel aus Vorwissen, Erfahrungen, kognitiven Urteilen und Emotionen, aber auch menschlichen Prädispositionen. Die Einschätzung der Vertrauenswürdigkeit erfolgt dabei anhand von Eigenschaften wie Leistungsfähigkeit, Integrität und guter Absicht des automatisierten Systems.[3, 4]

Entspricht die Erwartung des Menschen in die Automatisierung nicht den tatsächlichen Möglichkeiten der Automatisierung gibt es zwei Möglichkeiten: Das Vertrauen in die Automatisierung ist entweder zu groß (Overtrust) oder zu gering (Distrust). Jede dieser Ausprägungen birgt spezifische Gefahren und Herausforderungen.

Overtrust

Overtrust (zu großes Vertrauen) beschreibt den Zustand, in dem Nutzerinnen und Nutzer einer Automatisierung mehr zutrauen, als diese tatsächlich leisten kann. Overtrust verleitet dazu, Systemgrenzen zu ignorieren, Warnhinweise zu übersehen oder Kontrollaufgaben nicht auszuführen. Daraus können gravierende Sicherheitsrisiken entstehen. Overtrust beruht häufig auf fehlender Aufklärung über Systemgrenzen, einer falschen Kalibrierung des Vertrauens oder einer generalisierten positiven Einstellung („dispositional trust“). Wenn Menschen fälschlicherweise glauben, dass ein System völlig zuverlässig ist, kann das nach einem Systemversagen fatale Unfallfolgen haben – besonders in sicherheitsrelevanten Verkehrsanwendungen oder Hochrisikoindustrien. Die „Ironies of Automation“ beschreiben dieses Paradox: Je automatisierter ein System ist,

desto entscheidender wird die menschliche Fähigkeit, bei Ausfällen richtig zu reagieren. Overtrust schwächt genau diese Fähigkeit massiv und erhöht das Gefahrenpotenzial.

Distrust

Distrust (aktives Misstrauen) äußert sich in ablehnendem Verhalten gegenüber der Automatisierung – auch wenn die Technologie eigentlich leistungsfähig und zuverlässig wäre. Distrust führt dazu, dass Systeme nicht genutzt oder ständig überwacht werden, wodurch Effizienzgewinne verloren gehen. Distrust basiert oft auf negativen Erfahrungen, bekannt gewordenen Fehlfunktionen oder einem individuell ausgeprägten geringen Zutrauen zu technischen Neuerungen. Auch fehlende Transparenz der Automatisierung kann eine der Ursachen sein. Distrust verhindert eine optimale Mensch-Maschine-Interaktion und kann die Einführung sinnvoller Automatisierung hemmen – sie wird dann einfach nicht genutzt. Ist der Mensch aktiv misstrauisch, kostet es viele Mühen und Zeit, das verlorene Vertrauen wiederherzustellen, das bedeutet für Organisationen hohe Aufwände für Schulungen und Investitionen in transparente Kommunikation.

Kalibrierung des Vertrauens

Vertrauen ist kein statischer Wert, sondern entwickelt sich über Wissen, Erfahrung, Feedback und Beobachtungen des Systemverhaltens. Vertrauen gilt als optimal, wenn das Vertrauen des Menschen in die Automatisierung genau dem Leistungsvermögen der Maschine entspricht – wenn es „kalibriert“ ist. Unkalibriertes Vertrauen erschwert die sichere und effiziente Zusammenarbeit von Mensch und Maschine. Unkalibriertes Vertrauen wird auch oft als „mistrust“ bezeichnet.

Um eine gute Kalibrierung des Vertrauens zu erreichen, müssen die Menschen auch gut über Funktionen und die Systemgrenzen während der Interaktion aufgeklärt sein.

Industrie: Roboter und Mensch

In der Automobil-, Elektronik- und Fertigungsindustrie sind Roboter und Cobots allgegenwärtig. Forschungen zeigen, dass das Vertrauen von Mitarbeitenden durch transparente Kommunikation, einfache und verständliche Rückmeldungen sowie die individuelle Erfahrung eines zuverlässigen Systemverhaltens gestärkt wird. Ein anschauliches Beispiel ist der Einsatz von Cobots, die dem Bedienpersonal die eigenen Entscheidungen und Systemzustände über Displays oder Lichtsignale erklären. So werden Missverständnisse reduziert und Interaktionsbarrieren abgebaut.

Kommt es aber zu Fehlfunktionen, etwa durch Konstruktions-, Programmierfehler oder mangelhafte Sensorik, gerät das Vertrauen schnell ins Wanken. Ein einziger unerwarteter Stillstand der automatisierten Systeme lässt das Vertrauen der Mitarbeitenden signifikant sinken und die Überprüfungs- sowie Kontrollneigung stark ansteigen.[4]

Neuere Studien fordern eine gute Balance zwischen Anforderungen und Ressourcen der Arbeitsplätze, um so eine kontinuierliche Kalibrierung des Vertrauensniveaus während der Nutzung der automatisierten Systeme sicherzustellen. So haben Menschen beispielsweise in Zusammenarbeit mit Robotern mitunter kognitiv wenig anspruchsvolle Arbeiten und zu wenig Entscheidungsspielraum. Dadurch entsteht häufig das Gefühl von vollständiger Abhängigkeit von der Maschine. Hier können mehr direkte Rückmeldungen des Systems und zumindest Bestätigungsschleifen durch die Bedienenden vorgesehen werden. Das führt insgesamt zu besserer Motivation der Beschäftigten und damit auch zu geringerer psychischer Belastung.[5]

Verkehrssicherheit: Herausforderungen

Fahrerassistenzsysteme, wie automatische Notbremsassistenten oder Spurhalteassistenten, sind auf das „richtige Maß“ an Vertrauen angewiesen. Übermäßiges Vertrauen (Overtrust) in das Fahrassistenzsystem „Tesla Autopilot“ hat etwa bei den ersten Unfällen mit Tesla-Fahrzeugen dazu geführt, dass Fahrende alle Verantwortung abgaben – mit teils gravierenden Folgen.[6] Übermäßiges Vertrauen kann im ungünstigen Fall auch zu risikoreichem Verhalten verleiten. So wird in einer Studie[7] ein deutlich erhöhtes Unfallrisiko des klassischen Tempomaten erkannt (+12 Prozent). Aber auch die adaptive Geschwindigkeitsregelung erhöht das Unfallrisiko (+1,8 Prozent). In dieser Studie wurde auch die eingestellte Geschwindigkeit abgefragt – sie lag bei den Fahrzeugen mit adaptiver Geschwindigkeitsregelung deutlich über der geltenden Geschwindigkeitsbeschränkung.

In der aktuellen „Zufriedenheitsstudie Assistenzsysteme“[8] wurden mehr als 4000 Personen online zu Reifegrad und Nutzung der Assistenzsysteme in ihren jeweiligen Fahrzeugen befragt. Abhängig vom jeweiligen System berichtete die Studie von Reifegraden zwischen 61 und 88 Prozent, aber Nutzungsquoten von 25 Prozent bis über 90 Prozent (Mistrust/Distrust). Im Fall von hohen Reifegraden bei gleichzeitig geringer Nutzung können Assistenzsysteme ihr Potenzial zur Verhinderung von Unfällen nicht ausspielen.[9]

Diese Studien und Unfallanalysen zeigen, dass falsches Vertrauen das Unfallrisiko stark erhöht und die Technik missbraucht wird, zum Beispiel durch das Missachten von Warnhinweisen oder risikoreicheres Fahren.

Systeme mit klaren Rückmeldungen, wie automatisierte U-Bahnen in Nürnberg, London, Paris oder Kopenhagen, stärken das Vertrauen der Fahrgäste nachweislich. So öffnen die Doppeltüren auf dem Bahnsteig beispielsweise erst, wenn der Zug dahinter gehalten hat. Und Lautsprecher melden die Einfahrt eines Zuges. Solche regelmäßigen Informationen, sichtbare Überwachung und die Einbindung von Nutzenden verbessern die Akzeptanz und das Vertrauen langfristig.

» Systeme mit klaren Rückmeldungen, wie automatisierte U-Bahnen in Nürnberg, London, Paris oder Kopenhagen, stärken das Vertrauen der Fahrgäste nachweislich. «

Auch im Luftverkehr sind gute Beispiele für erfolgreiche Kalibrierung von „Trust in Automation“ zu finden: Autopiloten und Flight-Management-Systeme übernehmen komplexe Aufgaben, werden aber durch organisatorische Maßnahmen wie regelmäßige Schulungen und die bewusste Kompetenzstärkung der Piloten sicher ergänzt. So wird die dauerhafte Kalibrierung des Vertrauens unterstützt – die Sicherheit steigt.

Messung und Gestaltung von Vertrauen

Vertrauen kann man nicht direkt messen, sondern nur die Auswirkungen von Vertrauen. Neben Fragebögen kommen zunehmend Verhaltensbeobachtungen und sogar physiologische Methoden wie Eye-Tracking oder Hautleitfähigkeitsmessungen zum Einsatz. Dabei werden Nutzungshäufigkeit und Interaktionen mit dem System erfasst. Transparenz des Systemzustands und -verhaltens, Wissen über Systemgrenzen, regelmäßige Rückmeldungen, Schulungen und Lernen aus Erfahrungen gelten als Schlüsselelemente für angemessene Vertrauensbildung.

Herausforderungen für die Zukunft

Angesichts der fortschreitenden Automatisierung – von KI-gestützten Robotern bis hin zu vollautonomen Fahrzeugen im öffentlichen Straßenverkehr – ist „Trust in Automation“ zentral für die Arbeitssicherheit. Neben technischen und rechtlichen Fragestellungen werden besonders die Kompetenz und Bereitschaft der Nutzenden, Kontrolle in komplexen Situationen an Assistenzsysteme abzugeben, zur entscheidenden Einflussgröße. Die kontinuierliche Weiterbildung, transparente Kommunikation[10], gut verständliche Rückmeldungen der Systemzustände, klare Fehlerkultur und schnelle Lernschleifen in der Praxis sind entscheidende Hebel, um Vertrauen dynamisch und verlässlich zu gestalten.

Autor

Christopher Frank,
DGUV Akademie

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/08/#fussnoten

Sicherer Umgang mit Multikoptern im gewerblichen Einsatz

In vielen Branchen sind unbemannte Luftfahrtsysteme heute unverzichtbare Helfer. Sie ermöglichen Inspektionen, Vermessungen und Überwachungen, die früher riskant, teuer oder schlicht unmöglich waren. Mit der wachsenden Verbreitung steigen auch die Anforderungen an Sicherheit und Professionalität beim Multikopterflug.

Durch die vielfältigen Anwendungsmöglichkeiten werden Multikopter (Drohnen) zunehmend für die unterschiedlichsten gewerblichen Zwecke genutzt. Insbesondere die einfache Handhabung, unterschiedlichste Bauformen, Verfügbarkeit, moderne Navigationstechnik sowie relativ niedrige Anschaffungs- und Betriebskosten machen ihre Anwendung so attraktiv. Multikopter können herkömmliche Arbeitsmittel ersetzen und erschließen vollkommen neue Anwendungsmethoden beziehungsweise Verfahren.

Die DGUV Information 208-058 „Sicherer Umgang mit Multikoptern (Drohnen)“[1] wird momentan überarbeitet und an die veränderten Rechtsgrundlagen angepasst. Sie stellt die neue Technik vor, gibt Hinweise zu deren Anwendungsmöglichkeiten sowie gesetzlichen Grundlagen und soll dazu beitragen, Risiken beim Betrieb von Multikoptern zu minimieren. In den Anlagen finden sich auch eine Vorlage für die Gefährdungsbeurteilung und eine Musterbetriebsanweisung für den Umgang mit Multikoptern.

Rechtliche Grundlagen: Wer darf was?

Der gewerbliche Betrieb von Multikoptern ist rechtlich streng geregelt. Grundlage ist die EU-Drohnenverordnung (EU) 2019/947[2] sowie die ergänzende Delegierte Verordnung (EU) 2019/945[3]. Sie definieren drei Betriebsarten:

- Offener Betrieb: Geringes Risiko, keine Einzelgenehmigung erforderlich, jedoch Gewichtsbeschränkungen (bis 25 Kilogramm) und Abstandspflichten zu Personen.

Key Facts

- Der gewerbliche Multikoptereinsatz unterliegt strengen EU-Vorschriften – Sicherheit, Genehmigungen und Schulungen sind gesetzlich verpflichtend
- Arbeitssicherheit beginnt bei der Einsatzplanung: Gefährdungsbeurteilung, Wartung und klare Teamkommunikation sind entscheidend
- Gut geschulte Pilotinnen und Piloten und gelebte Sicherheitskultur erhöhen Effizienz und senken Unfallrisiken dauerhaft

Begriffsklärung

UAS (Unmanned Aircraft System) ist der Oberbegriff für das gesamte System (Fluggerät plus Bodenstation etc.), **Drohne** ist der allgemeine Begriff für das Fluggerät selbst und **Multikopter** beschreibt eine spezifische Bauform mit mehreren Rotoren. Während „Drohne“ umgangssprachlich oft verwendet wird, ist „UAS“ der präzisere und in der EU-Gesetzgebung verwendete Begriff. Das DGUV-Sachgebiet „Postsendungen“ hat sich bei der Überarbeitung seiner Publikationen auf den Begriff „Multikopter“ festgelegt.

- Spezieller Betrieb: Mittleres Risiko, Betriebsgenehmigung erforderlich; eine Risikoanalyse (Specific Operations Risk Assessment, SORA) ist Pflicht.
- Zulassungspflichtiger Betrieb: Hohes Risiko, vergleichbar mit bemannter Luftfahrt, zum Beispiel Transport von Menschen oder gefährlichen Gütern.

Wichtig: Gewerbliche Multikopterpilotinnen und -piloten benötigen einen Kompetenznachweis (A1/A3 oder A2). Außerdem muss jedes Unternehmen eine Haftpflichtversicherung nach § 43 LuftVG[4] vorweisen können. Verstöße können Bußgelder und strafrechtliche Konsequenzen nach sich ziehen.

Wichtige Rechtsquellen:
- EU-Durchführungsverordnung (EU) 2019/947
- EU-Delegierte Verordnung (EU) 2019/945
- Luftverkehrsgesetz (LuftVG) § 43
- Luftverkehrs-Ordnung (LuftVO) §§ 21a–21k
- DGUV Information 208-058 „Sicherer Umgang mit Multikoptern (Drohnen)“

Arbeitssicherheit beginnt vor dem Start

Ein sicherer Multikoptereinsatz beginnt lange vor dem Abheben. Planung und Gefährdungsbeurteilung sind zentrale Bausteine der Arbeitssicherheit.

- Gefährdungsbeurteilung: Jede Einsatzumgebung birgt Risiken – etwa Hindernisse, Windböen, Magnetfelder oder Funkstörungen. Auch Dritte (Fußgänger, Fahrzeuge, Tiere) müssen berücksichtigt werden.
- Flugplanung: Digitale Luftraumkarten und Apps wie Droniq, AirMap oder Dronedesk helfen, Flugverbotszonen zu erkennen und Genehmigungen einzuholen.
- Kommunikation im Team: Pilot und Pilotin, Beobachterinnen und Beobachter sowie Einsatzleitung sollten klare Rollen haben. Absprachen verhindern Missverständnisse – besonders bei gleichzeitigen Einsätzen mehrerer Systeme.
- Notfallmanagement: Verfahren für technische Defekte, Signalverlust oder Abstürze müssen schriftlich festgelegt sein. Dazu gehören Notfallkontakte, Landebereiche und Erste-Hilfe-Ausrüstung.

PRAXISTIPP: Checkliste vor dem Flug
- Akku und Sensoren geprüft?
- Software-Updates installiert?
- Start- und Landefläche abgesichert?
- Wetter- und Sichtbedingungen geeignet?
- Sicherheitsabstände eingehalten?

Eine solche Checkliste sollte fester Bestandteil der Betriebsroutine sein – sie schützt Mensch, Material und Reputation.

Technische Sicherheit

Multikopter sind komplexe Arbeitsmittel – und unterliegen damit der Betriebssicherheitsverordnung (BetrSichV)[5]. Unternehmen müssen nachweisen, dass Geräte regelmäßig gewartet, geprüft und dokumentiert werden.

Ein technisches Sicherheitsmanagement umfasst:
- regelmäßige Inspektionen und Kalibrierungen,
- Dokumentation aller Wartungsarbeiten,

- Einsatzprotokolle (Flugstunden, Zwischenfälle, Softwarestände),
- definierte Zuständigkeiten für Prüfung und Freigabe.

Viele Betriebe nutzen mittlerweile digitale Flottenmanagement-Systeme, um Wartungsintervalle zu überwachen und Daten revisionssicher zu speichern.

BEISPIEL AUS DER PRAXIS:
Ein Energieversorger nutzt Multikopter zur Inspektion von Hochspannungsleitungen. Früher mussten Beschäftigte dafür auf Leitermasten steigen – heute erfolgt die Kontrolle kontaktlos aus der Luft. Das spart Zeit und reduziert Absturzrisiken. Der Betrieb dokumentiert jeden Einsatz digital, inklusive Wetterdaten, Flugroute und Akkustatus – ein Musterbeispiel für integriertes Sicherheitsmanagement.

» Multikopter schaffen neue Perspektiven, erleichtern gefährliche Arbeiten und liefern wertvolle Daten. Doch diese Chancen entfalten sich nur, wenn Sicherheit an erster Stelle steht. «

Schulung und Qualifikation

Die größte Sicherheitslücke ist oft der Mensch – genauer gesagt, dessen mangelhafte Schulung. Selbst moderne Assistenzsysteme können keine Erfahrung ersetzen.

Deshalb sind regelmäßige Unterweisungen Pflicht. Personen, die Drohnen bedienen, sollten über die gesetzlich geforderten Kompetenznachweise verfügen und folgende Inhalte kennen:
- Verhalten bei Störungen und Notfällen,
- Datenschutz und Persönlichkeitsrechte,
- Wetterkunde und Umwelteinflüsse,
- sichere Datenübertragung und -speicherung,
- Verhalten bei Einsätzen über sensiblen Arealen (zum Beispiel Industrieanlagen, Menschenansammlungen).

Unternehmen sollten Schulungen jährlich wiederholen und dokumentieren. Auch psychische Belastungen – etwa durch lange Konzentrationsphasen am Monitor – gehören in die Gefährdungsbeurteilung.

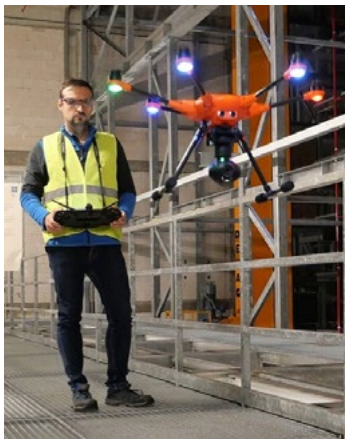
Das DGUV-Sachgebiet „Postsendungen“ erarbeitet gegenwärtig den DGUV Grundsatz „Ausbildung und Beauftragung des Bedienpersonals von Multikoptern“, der die Ausbildung und Beauftragung des Bedienpersonals von unbemannten Fluggeräten darstellt. Er ist vorrangig für die Ausbildung und zur Erlangung des Basiswissens von Betreibern von Multikoptern konzipiert und wird Mitte 2026 zur Verfügung stehen.

Arbeitssicherheit als Effizienzfaktor

Sicherer Multikoptereinsatz bedeutet nicht nur Risikominimierung, sondern auch Produktivitätsgewinn. Beispiele:
- Bauindustrie: Vermessung großer Areale ohne Betreten gefährlicher Baustellen.
- Windenergie: Rotorblattinspektion aus der Ferne, ohne Höhenarbeiten.

- Katastrophenschutz: Lageerkundung bei Bränden oder Hochwasser, ohne Einsatzkräfte zu gefährden.
- Landwirtschaft: Präzisionsanalyse von Pflanzenbeständen, reduziert Chemikalien und schützt Bodenpersonal.

In all diesen Fällen steigert Sicherheit die Effizienz – und umgekehrt. Unternehmen, die strukturiert planen, schulen und dokumentieren, arbeiten nicht nur sicherer, sondern auch wirtschaftlicher.



Quelle: velotech.de GmbH – Marco Brust

Multikopter erleichtern die Arbeit. Für ihre sichere Nutzung braucht es Qualifikation, Planung und passende Schutzmaßnahmen.

Sicherheitskultur im Unternehmen

Langfristig erfolgreich sind jene Betriebe, die Sicherheit nicht als Pflicht, sondern als Wert begreifen. Eine gelebte Sicherheitskultur bedeutet:

- offene Kommunikation über Risiken und Fehler,
- klare Verantwortlichkeiten,
- kontinuierliche Verbesserung,
- Integration von Sicherheitsaspekten in alle Projektphasen.

Ein betriebliches Multikopterhandbuch mit Einsatzregeln, Zuständigkeiten, Checklisten und Notfallplänen ist ein wirksames Werkzeug. Es fördert Transparenz und reduziert Unsicherheiten – besonders bei wechselnden Einsatzorten und Teams.

Fazit: Verantwortung trägt, wer fliegt

Multikopter sind aus der modernen Arbeitswelt nicht mehr wegzudenken. Sie schaffen neue Perspektiven, erleichtern gefährliche Arbeiten und liefern wertvolle Daten. Doch diese Chancen entfalten sich nur, wenn Sicherheit an erster Stelle steht.

Arbeitssicherheit beim Multikoptereinsatz ist keine lästige Vorschrift, sondern eine Investition in Qualität, Vertrauen und Zukunftsfähigkeit. Wer Planung, Schulung, Technik und Verantwortung systematisch verknüpft, nutzt das volle Potenzial der Technologie – sicher, effizient und nachhaltig. ●

Autor

Jens Becker,
BG Verkehr

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/09/#fussnoten

Industrial Security: Neue Regeln als Chance für Europas Unternehmen

Neue Regelwerke zu Security beschäftigen Unternehmen in Europa. Vor ihnen muss sich kein Unternehmen, wohl aber böswillige Hacker fürchten. Sie stärken Europa und schützen jedes einzelne Unternehmen. Entscheidend ist nun, die ersten Schritte anzugehen, die Deutsche Gesetzliche Unfallversicherung (DGUV) gibt dazu Hilfestellung.

Schwachstellen in Produkten und in Unternehmen haben über Jahrzehnte nicht genügend Aufmerksamkeit bekommen. Die Entwicklungsabteilungen bekamen oft nicht die notwendigen Ressourcen, um „Secure by Design“ zu entwickeln, also Security von Anfang an mitzubetrachten. Sogar Produkte mit Hintertüren wurden in den Markt eingeführt. So konnte es kommen, dass immer wieder über neue Schwachstellen berichtet wurde: Vom Herzschrittmacher, der sich über Funk hacken ließ, Krane, die auf fremde Fernbedienungen reagieren, bis hin zu manipulierbaren Industriesteuerungen.

Es zeigte sich, dass der Markt dies nicht selbst regeln konnte, denn Verbraucher hatten kaum eine Chance, Produkte vor dem Kauf mit Blick auf Security zu vergleichen. Und nach dem Kauf waren die Verbraucherrechte bei Bekanntwerden von Schwachstellen ungenügend. So galt das Produkthaftungsgesetz etwa nicht für Software, weil die Software allein kein Produkt war.

Eine Regelung durch den Markt war ebenfalls nicht möglich, weil Hersteller von Produkten mit Schwachstellen selten einen Nachteil hatten. Im Gegenteil konnte oft sogar das Nachfolgeprodukt leichter verkauft werden, wenn Schwachstellen im Vorgängerprodukt nicht behoben wurden. Unternehmen, die in Security investierten, hatten folglich auf kurze Zeit einen wirtschaftlichen Nachteil gegenüber Unternehmen mit hoher Risikobereitschaft.

Der Gesetzgeber hat nun mit einem ganzen Paket neuer Verordnungen europaweit alle Beteiligten in die Pflicht genommen. Die European Network and Information Security Agency (ENISA) bekommt durch den Cybersecurity Act (CSA) als europäische Behörde umfangreiche Aufgaben. Von der Mitwirkung bei nationalen Vorschriften bis hin zum Betrieb einer Europäischen Schwachstellendatenbank laufen hier die Fäden zusammen. Der Cyber Resilience Act (CRA) richtet sich an die Hersteller von Produkten mit digitalen Elementen und regelt, wie etwa mit Schwachstellen umgegangen werden muss. Auch

Key Facts

- Neue Regelwerke zu Security stärken alle Unternehmen in Europa
- Unternehmen sollten nicht untätig auf harmonisierte Standards warten
- Jedes Unternehmen sollte einen Notfallkontakt einrichten
- Security erfordert internationale Zusammenarbeit und gute Kommunikation

Europäische Schwachstellendatenbank
euvd.enisa.europa.eu

die neue europäische Maschinenverordnung (MVO) fordert deutlicher als bisher, dass Maschinen adäquat vor versehentlicher und böswilliger Korrumpierung geschützt werden müssen, wenn dadurch Menschen in Gefahr gebracht werden können. Einen Produktionsstillstand, bei dem niemand verletzt werden kann, berücksichtigen die Anforderungen aus der MVO jedoch nicht. Am Ende der Kette ist auch der Arbeitgeber in der Pflicht.

Für Arbeitgeber, die ein sicheres Arbeitsmittel zur Verfügung stellen müssen, sind die Anforderungen an die Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen in der Technischen Regel für Betriebssicherheit TRBS 1115 Teil 1[1] zusammengefasst.

Während früher nur Arbeitgeber von kritischer Infrastruktur konkrete Mindestvorgaben zu Security bekamen, richtet sich die NIS-2 Verordnung[2] nun von der Abfallbewirtschaftung bis zum Maschinenbau auch an Unternehmen, die bislang nicht betrachtet wurden.

Einfache Security-Maßnahmen für Unternehmen

Bei so vielen neuen Verordnungen kann man schnell den Überblick verlieren. Die DGUV hat daher eine Webseite mit Informationen und Links zu den neuen Verordnungen eingerichtet[3]. Wichtig ist, dass Unternehmen jetzt nicht untätig auf eine perfekte, vollständige Lösung warten, sondern schnell mit einfachen ersten Schritten starten. Ein Drei-Schritte-Plan, mit dem Unternehmen sofort beginnen können:

Schritt 1: Unternehmenswebseite scannen

Unternehmenswebseite auf typische Probleme scannen. Der Scanner Internet.nl listet nicht nur die Probleme auf, sondern gibt auch Lösungsvorschläge und Erklärungen für die IT-Abteilung. Der Onlinescanner wurde in einer Kooperation der Internetcommunity und den niederländischen Behörden erstellt. Unter den vielen Tests prüft einer auch, ob das Unternehmen schon über die „security.txt“ einen Notfallkontakt hinterlegt hat. Falls nicht, kann das in nur fünf Minuten in Schritt 2 erledigt werden.

Onlinescanner Internet.nl:
https://en.internet.nl

Schritt 2: Notfallkontakt einrichten

Wenn ein Unternehmen eine kritische IT-Schwachstelle im Betrieb oder in seinen Produkten hat, ist oft unklar, wer zu informieren ist. Niemand möchte, dass diese wertvolle Meldung kreuz und quer durch das Unternehmen weitergeleitet wird. Die Erfahrung zeigt, dass sich niemand verantwortlich fühlt, bis die Geschäftsführung eine Person benennt, welche die Warnmeldungen entgegennimmt. Sie entscheidet dann, was Spam ist und was eine Meldung, der man nachgehen sollte. Es ist dabei nicht schlimm, wenn im Unternehmen für diese Rolle keine Person mit Fachkenntnissen bereitsteht. Das Wichtigste ist, zunächst eine Erreichbarkeit zu schaffen. Gehen Meldungen ein, kann externe Hilfe hinzugezogen werden.

Die Entscheidung, den Notfallkontakt einzurichten und eine oder mehrere Personen zu benennen, muss von den Entscheidungstragenden des Unternehmens kommen. Daher hat das Institut für Arbeitsschutz (IFA) der DGUV einen Kurzfilm erstellt, in dem der Zusammenhang beschrieben wird. Für Hersteller, die unter den CRA fallen, wird ein Notfallkontakt sogar Pflicht. Sobald die Entscheidung gefallen ist, finden sich auf den Seiten des IFA eine Anleitung und ein Tool, das die Datei genau nach Spezifikation erstellt. Die Spezifikation RFC9116 wird bereits von mehreren Zehntausend Unternehmen weltweit umgesetzt. Viele bekannte Unternehmen wie Google, Facebook, Siemens und Bosch gehören zu den ersten, die nun über den Notfallkontakt erreichbar sind. Praktisch ist es, als Kontaktmailadresse etwa einen generischen Verteiler wie security@example.com zu verwenden. Wenn sich das Team ändert, bleibt die E-Mail-Adresse erhalten und wird nur intern an andere Personen weitergeleitet. Große Unternehmen möchten möglicherweise auch zwischen Meldungen zum Produkt und zur eigenen Infrastruktur unterscheiden. In diesem Fall wird ein sogenanntes Product Security Incident Response Team (PSIRT) etwa mit dem Kontakt psirt@example.com für Warnungen zu Schwachstellen im Produkt eingerichtet.

» Unternehmen sollten heute ihre Schwachstellen schließen und nicht mit einer Glaskugel einen Hacker von übermorgen analysieren. «

Schritt 3: Inventarliste anlegen

Im dritten Schritt könnte eine Inventarliste der vernetzten Maschinen und Produkte angelegt werden. Diese kann dann für die Umsetzung der TRBS 1115 Teil 1 herangezogen werden. Darin werden Fragen beantwortet, wie sich die Maschine in einen sicheren Zustand versetzen lässt, wenn ihre Steuerung gehackt wurde und die Maschine unkontrolliert läuft. Auch für die Anforderungen aus NIS-2 kann die Liste eine wertvolle Grundlage darstellen. Viele Unternehmen wissen derzeit vermutlich nicht genau, welche vernetzten Geräte überhaupt existieren und es existiert oft auch kein Prozess zu ihren Security-Maßnahmen.

IFA-Kurzfilm „Erreichbarkeit im IT-Notfall“

Quelle: IFA

Der Kurzfilm zum Notfallkontakt richtet sich an Geschäftsführende, die ihr Unternehmen über den internationalen Standard RFC9116 erreichbar machen möchten. Das Video wurde bereits in Chinesisch, Deutsch, Englisch, Französisch, Japanisch, Niederländisch und Tschechisch übersetzt.

Link zum Erklärfilm

https://dguv.de/securitytxt_DE

Das IFA bietet zu Industrial Security jedes Jahr spezielle Seminare für Hersteller, aber auch Veranstaltungen für Arbeitgeber und Aufsichtspersonen oder Prüfstellen an[5].

Nicht nur für Unternehmen, die unter die NIS-2-Verordnung fallen, ist dabei die kostenlose NIS-2-Geschäftsleitungsschulung des BSI[4] ein guter Start. Darin wird der Geschäftsleitung der Start in das Thema vereinfacht. Es werden sogar schon hilfreiche Fragen vorformuliert, die helfen können, den Handlungsbedarf zu ermitteln. Unternehmen verschwenden oft wertvolle Ressourcen, indem sie versuchen zu analysieren, wer mit welchen Kenntnissen in fünf Jahren potenziell eine Steuerung angreifen könnte. Das ist nicht möglich, aber auch nicht notwendig, denn ein sicheres Design kann heute bereits umgesetzt werden. Für wie viele Jahre ein kryptographisches Verfahren geeignet ist, kann statistisch berechnet werden.

Kommunikation ist der Schlüssel für Security

Um die Produkte und Unternehmen mit der erforderlichen Geschwindigkeit vor Angriffen schützen zu können, ist die Kommunikation mit den Betroffenen über das Thema und untereinander zu Schwachstellen entscheidend.

Für die Kommunikation mit den Betroffenen hat es sich bewährt, die sehr abstrakte Thematik anhand anschaulicher Modellfabriken zu erklären und international mit den Arbeitsschutzorganisationen zusammenzuarbeiten. Die Grundprinzipien für Security sind wie ein Naturgesetz überall auf der Welt gleich. Gut ausgearbeitete Materialien müssen also nur noch übersetzt werden, damit die Information für alle leicht zugänglich ist. Dadurch werden nicht nur Kosten gespart, sondern auch schnell eine große Reichweite generiert.

Die Kommunikation untereinander wird durch den neuen Notfallkontakt und ein weltweites Netzwerk zu Schwachstellenmeldungen stark verbessert. Künftig können Unternehmen alle Handlungsempfehlungen für genau die Produkte, die im Unternehmen eingesetzt werden, vom Hersteller abonnieren. Während es bei der weltweit bekannten Schwachstelle Log4Shell teilweise noch mehr als sechs Monate dauerte, bis Hersteller wussten, ob ihre Steuerung in der Maschine betroffen ist, können diese Informationen künftig noch am gleichen Tag an alle Betroffenen verteilt werden. ●

Autor

Jonas Stein,
Institut für Arbeitsschutz
der Deutschen Gesetzlichen
Unfallversicherung (IFA)

Fußnoten

Sie finden die Fußnoten zu diesem Artikel online unter forum.dguv.de/ausgabe-1-2026/10/#fussnoten

„Die Selbstverwaltung muss ins Grundgesetz“

Am 4. Dezember hat die Mitgliederversammlung der DGUV ein Positionspapier mit Maßnahmen zur Stärkung der Sozialen Selbstverwaltung beschlossen. Die Vorstandsvorsitzenden der DGUV, Herr Volker Enkerts (VBG) und Herr Hans-Peter Kern (BG ETEM), stellen die wichtigsten Vorschläge vor.

Im Positionspapier setzt sich die Selbstverwaltung der gesetzlichen Unfallversicherung dafür ein, der Sozialen Selbstverwaltung Verfassungsrang zu verleihen. Was sind die Gründe hierfür und was könnte eine Selbstverwaltung mit Verfassungsrang bewirken?

Volker Enkerts: Um der Selbstverwaltung einen möglichst großen Gestaltungsspielraum einzuräumen und sie vor übermäßiger politischer Einflussnahme zu schützen, bedarf es einer verfassungsrechtlichen Garantie der Selbstverwaltung für die Sozialversicherungsträger. Die eigenverantwortliche Mitwirkung der Versicherten sowie Arbeitgeberinnen und Arbeitgeber sollte verfassungsrechtlich gewährleistet sein.

Hans-Peter Kern: Jedem einzelnen Träger der gesetzlichen Unfallversicherung sollte es möglich sein, sich im Rahmen einer Verfassungsbeschwerde gegen unzulässige Eingriffe in das Recht der Selbstverwaltung wirksam zur Wehr zu setzen. Dieses Recht muss geschaffen werden. Daher fordern wir, klarzustellen, dass den Trägern der Sozialversicherung der Rechtsweg gegen Akte anderer Träger hoheitlicher Gewalt eröffnet ist, soweit die von ihnen treuhänderisch wahrgenommenen Interessen oder Rechte ihrer Mitglieder betroffen sind. Die Möglichkeit zur Verfassungsbeschwerde ist auch in ihrer Wirkung auf den Stellenwert der Sozialen Sicherung und auf das Ansehen der Selbstverwaltung in der Gesellschaft nicht zu unterschätzen.

Die Selbstverwalterinnen und Selbstverwalter haben sich im Positionspapier für die Ausweitung ihrer Kompetenzen ausgesprochen. In welchen Bereichen müssen diese ausgeweitet werden und warum?

Hans-Peter Kern: Die gesetzliche Unfallversicherung ist im Vergleich zu anderen Zweigen der Sozialen Sicherung in Bezug auf ihre Kompetenzen gut aufgestellt. Wir entscheiden beispielsweise über den Beitragssatz sowie die Gefahrklassen für die bei den Unfallversicherungsträgern versicherten Gewerbezweige. Dennoch: Es bleibt Luft nach oben.

» Wir plädieren für mehr Autonomie im Bereich der Rehabilitation, für eine Erweiterung des Entscheidungsspielraums der Widerspruchsausschüsse und eigenständiges Wirtschaften. «

Volker Enkerts

Volker Enkerts: Konkret plädieren wir für mehr Autonomie im Bereich der Rehabilitation, für eine Erweiterung des Entscheidungsspielraums der Widerspruchsausschüsse und eigenständiges Wirtschaften nach dem Grundsatz der Wirtschaftlichkeit und Sparsamkeit im Bereich der Verwaltung. Diese Kompetenzen müssen zunächst erweitert und dann auch sichtbar gemacht werden.

Nur wenn ehrenamtliche Vertreterinnen und Vertreter der Selbstverwaltung ihre Entscheidungs-, Handlungs- und Gestaltungsspielräume erkennen können, werden sie sich engagieren. Ferner beeinflussen die Kompetenzen und Gestaltungsmöglichkeiten von Ämtern ihre Attraktivität. Das hat wiederum hohe Relevanz für die Nachwuchsgewinnung und das Interesse der Bevölkerung für die Sozialwahlen. Denn Interesse besteht vor allem für die Dinge, bei denen die Menschen mitwirken können oder einen konkreten Nutzen für sich und andere sehen.

Die Soziale Selbstverwaltung ist ein Strukturelement der Sozialen Sicherung und dennoch in großen Teilen der Bevölkerung nicht bekannt. Woran liegt das und welche Maßnahmen schlagen Sie vor, um einen größeren Bekanntheitsgrad zu erreichen?

Volker Enkerts: Die Unfallzahlen sind aufgrund der guten Präventionsarbeit der Unfallversicherungsträger seit Jahren rückläufig. Oft kommen die Menschen mit der gesetzlichen Unfallversicherung erst nach einem Unfall oder dem Auftreten einer berufsbedingten Erkrankung in Kontakt und lernen ihren Mehrwert kennen. Die Soziale Sicherung muss aber so früh wie möglich in das Bewusstsein der Menschen Eingang finden. Daher plädieren wir dafür, junge Menschen bereits im Schulalter über die gesetzliche Unfallversicherung und die Rolle der Selbstverwaltung im politischen System der Bundesrepublik Deutschland zu informieren und unsere Öffentlichkeitsarbeit zu intensivieren.

Hans-Peter Kern: Tue Gutes und rede darüber! Wir müssen vermitteln, was die gesetzliche Unfallversicherung für die Menschen tut und in welchen Bereichen die Selbstverwalterinnen und Selbstverwalter mitwirken – sowohl in der Prävention von Unfällen und berufsbedingten Erkrankungen als auch nach dem Eintreten eines Schadenfalls in der Rehabilitation. Wichtig ist, dass die Kommunikation zeitgemäß und adressatengerecht ist. So kann insbesondere jüngeren Menschen aufgezeigt werden, wie einflussreich und gestalterisch Selbstverwaltung sein kann – auch mit dem Ziel, sie für die Arbeit der Selbstverwaltung zu begeistern.

Das Positionspapier spricht sich für den Erhalt der Friedenswahlen in der gesetzlichen Unfallversicherung aus. Welchen Mehrwert bieten Friedenswahlen?

Hans-Peter Kern: Den Sozialwahlen in der gesetzlichen Unfallversicherung ist eine wichtige Handlung vorgeschaltet: Die

» Wir müssen vermitteln, was die gesetzliche Unfallversicherung für die Menschen tut und in welchen Bereichen die Selbstverwalterinnen und Selbstverwalter mitwirken. «

Hans-Peter Kern

Vorbereitung von gemeinsamen Wahllisten in einem umfangreichen Abstimmungs- und Aushandlungsprozess. An dessen Ende steht stets eine ausgewogene Wahlliste.

Volker Enkerts: Nur wenn der Einigungsprozess der Sozialpartner erfolgreich ist, kommt es zu Friedenswahlen. Diese vermeiden unnötigen Aufwand und sind wirtschaftlich. Die Wahllisten stellen eine ausgewogene Repräsentation der Arbeitgeberinnen und Arbeitgeber und der Versicherten, der Branchen sowie der Geschlechter in den Gremien der Selbstverwaltung sicher. Friedenswahlen haben sich bewährt und tragen zum Gelingen der Arbeit in der paritätischen Selbstverwaltung wesentlich bei.

———

Das Interview führte Dr. Anna Kavvadias.

Keine Haftungsprivilegien nach §§ 104 ff. SGB VII bei Werkverträgen

(Urteil des Oberlandesgerichtes Köln vom 29.10.2025, AZ 17 U 73/24)

Haftungsprivilegien außerhalb der Arbeitnehmerüberlassung gegenüber leiharbeitsähnlichen Dienst- und Werkvertragsmitarbeitenden gibt es im System der §§ 104 ff. SGB VII nicht. Selbst ein gewisser Organisationsgrad genügt nicht per se für die Annahme einer gemeinsamen Betriebsstätte.

Insbesondere in Werks- oder Lagerhallen kommt es häufiger vor, dass Mitarbeitende von Fremdfirmen auf Stammbeschäftigte von Unternehmen treffen, in deren Eigentum die Hallen stehen. Kommt es dann zu einem Arbeitsunfall, stellt sich die Frage, ob sich der Schädiger (zum Beispiel ein Gabelstaplerfahrer) oder dessen Arbeitgebender gegenüber den Geschädigten (zum Beispiel eine an- und überfahrene Fußgängerin) auf Haftungsprivilegien gemäß den §§ 104 ff. Sozialgesetzbuch (SGB) VII berufen können.

Handelt es sich bei den Geschädigten um Leiharbeitskräfte, ist die Rechtslage seit den beiden Urteilen des Bundesgerichtshofs (BGH) vom 18.11.2014, Aktenzeichen VI ZR 47/13 und VI ZR 141/13, im Sinne des Bestands von Privilegien nach den §§ 104, 105 SGB VII geklärt. Handelt es sich indes, wie im konkret zu entscheidenden Fall, nicht um Leiharbeitnehmerinnen und -arbeitnehmer, sondern um Arbeitnehmende von Drittfirmen, die aufgrund von Dienst- oder Werkverträgen andernorts auf Stammbeschäftigte treffen und von diesen geschädigt werden, gibt es seitens der Schädigenden, deren Arbeitgebenden und der dahinterstehenden Betriebshaftpflichtversicherer eindeutige Tendenzen, die Haftungsprivilegierungstatbestände der §§ 104 ff. SGB VII durch Behauptung leiharbeitsähnlicher Konstellationen auszudehnen. Dies würde eine Übertragung der beiden BGH-Entscheidungen vom 18.11.2014 als geboten erscheinen lassen. Die Rechtsfolge wäre, dass ein Regress bei den Unfallverursachenden deutlich erschwert wäre, weil die Unfallversicherungsträger ein mindestens grob fahrlässiges Tun oder Unterlassen, das zum Versicherungsfall geführt hat, nachweisen müssten.

Bereits das Landgericht Köln hatte in seinem Urteil vom 13.09.2024 der Idee eines leiharbeitsähnlichen Verhältnisses gegenüber einer als Qualitätsprüferin beschäftigten Geschädigten eines Fremdunternehmens, die von einem Gabelstaplerfahrer an- und überfahren wurde, zurecht eine Absage erteilt und Haftungsprivilegien des Schädigers und des Werkbestellers

gemäß den §§ 104, 105 SGB VII verneint. Einer analogen Anwendung der oben genannten BGH-Rechtsprechung zur Arbeitnehmerüberlassung auf die hier vorliegende Konstellation bedürfe es mangels einer Regelungslücke nicht. Das erstinstanzliche Gericht hatte indes ein Haftungsprivileg gemäß § 106 Abs. 3 Variante 3 SGB VII – Tätigwerden von Versicherten mehrerer Unternehmen auf einer gemeinsamen Betriebsstätte – angenommen.

Das Oberlandesgericht Köln hat in seinem Urteil vom 29.10.2025 indes auch dieses Haftungsprivileg zu Recht verneint. Allein ein Tätigwerden in derselben Werkshalle begründet keine gemeinsame Betriebsstätte. Denn die gemeinsame Betriebsstätte ist mehr als dieselbe Betriebsstätte und das bloße Zusammentreffen von Risikosphären mehrerer Unternehmen an einem Ort erfüllt den Tatbestand der Norm des § 106 Abs. 3 Variante SGB VII daher nicht.

Wenn die Unfallbeteiligten nur nebeneinander gearbeitet haben und ihre Arbeiten nicht aufeinander bezogen waren, sich die Beteiligten also nicht in irgendeiner Weise wechselseitig zugearbeitet haben, mag dies zwar für ein Mitwirken an einem einheitlichen Betriebsziel genügen. Ein solches einheitliches oder gemeinsames Ziel führt indes noch nicht zu einer gemeinsamen Aufgabe. Eine solche wird auch nicht dadurch begründet, dass die Geschädigte zur Erledigung ihrer Tätigkeiten eine Liste der auf ihre Qualität zu überprüfenden Werkstücke, einen Arbeitsbereich und Arbeitsmaterial von der Werkbestellerin zur Verfügung gestellt erhalten hatte. Schließlich vermittelt allein dies noch keine konkrete Beziehung zwischen den Tätigkeiten der Geschädigten und denen des Gabelstaplerfahrers, die in Kombination mit einer wechselseitigen Gefährdungslage aber eine gemeinsame Betriebsstätte gerade kennzeichnet.

Auch eine einzige gemeinsame Vorgabe der Werkbestellerin gegenüber eigenen und fremden Beschäftigten in Form der Nutzung des verschiedenfarbigen Wegenetzes begründet keine gemeinsame Betriebsstätte. Denn diese Vorgabe betrifft nicht nur die Unfallbeteiligten, sondern letztlich alle Personen, die eine Werkshalle zu betrieblichen oder privaten Zwecken betreten und benutzen. Sie ist lediglich Folge einer betrieblichen Verkehrssicherungspflicht, die der Vermeidung von Unfällen im Allgemeinen dient, ohne konkret einzelne Arbeitsabläufe zu erfassen.

Zurecht gibt es daher kein Haftungsprivileg für den schädigenden Gabelstaplerfahrer. Er haftet der geschädigten Qualitätsprüferin daher in vollem Umfang, wobei einfache Fahrlässigkeit genügt. Daneben haftet der Arbeitgeber des Schädigers als Werkbesteller für das Fehlverhalten des Mitarbeiters. Aufgrund der sehr umfangreichen Leistungen an die Verletzte sind die Ansprüche auf sachlich und zeitlich kongruenten Schadensersatz auf die Berufsgenossenschaft übergegangen. ●

Autor

Dr. Jerom Konradi

Die Inhalte dieser Rechtskolumne stellen allein die Einschätzungen des Autors dar.

Impressum

DGUV forum
Fachzeitschrift für Prävention, Rehabilitation, Versicherungsrecht, Forschung
13. Jahrgang. Erscheint ab dem 01.01.2026 sechsmal jährlich

Herausgeber der Fachzeitschrift *DGUV forum* und Betreiber der Website
Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)
Glinkastraße 40, 10117 Berlin
https://forum.dguv.de

vertreten durch die stellvertretende Hauptgeschäftsführerin
Frau Dr. Edlyn Höller
Telefon: 030 13001-0 (Zentrale)
Fax: 030 13001-9876
E-Mail: info@dguv.de
Vereinsregister-Nr. VR 751 B beim Amtsgericht Charlottenburg

Verantwortlich für redaktionelle Inhalte der Fachzeitschrift *DGUV forum* und der Website
https://forum.dguv.de
Stefan Boltz, DGUV

Chefredaktion
Stefan Boltz (DGUV), Sabine Herbst (DGUV), Dr. Anna Kavvadias (DGUV)

Redaktion
Elke Biesel (DGUV), Katharina Braun (DGUV), Susan Haustein (DGUV)

Technische Erstellung und Betreuung der einzelnen Ausgaben der Fachzeitschrift *DGUV forum* und der Website *DGUV forum* inklusive Redaktionsassistenz für die Chefredaktion
Raufeld Medien GmbH, Paul-Lincke-Ufer 42/43
10999 Berlin, Telefon: 030 695 665-0
E-Mail: info@raufeld.de

Rechtlicher Hinweis
Die mit Autorennamen versehenen Beiträge in dieser Zeitschrift geben ausschließlich die Meinungen der jeweiligen Verfasser wieder.

Zitierweise der Fachzeitschrift *DGUV forum*
DGUV forum, Ausgabe, Jahrgang, Link, Abrufdatum

ISSN (Online)
2699 – 7304

OS-Plattform
Die Plattform der EU-Kommission zur Online-Streitbeilegung kann hier eingesehen werden: www.ec.europa.eu/consumers/odr
Diese befindet sich jedoch auf dem Weg der Abschaltung und nimmt keine neuen Beschwerden mehr an.

Alle Autorinnen und Autoren online unter

forum.dguv.de/autorinnen-und-autoren/