KI-Sicherheitsrichtlinie

Stand 15.07.2025
Version 1.0

Inhaltsverzeichnis

1 Einleitung

Die Möglichkeiten Künstlicher Intelligenz (KI) eröffnen neue Wege für die Arbeitswelt – auch in unserem Unternehmen. Sie kann Routineaufgaben automatisieren, kreative Prozesse bereichern, fundierte Entscheidungen unterstützen und die Effizienz nachhaltig steigern.

Wir schätzen das Interesse und die Offenheit unserer Mitarbeitenden gegenüber diesen Entwicklungen und möchten sie ausdrücklich dazu ermutigen, die Potenziale von KI aktiv zu erkunden und verantwortungsvoll in den Arbeitsalltag einzubinden.

Gleichzeitig bringt der Einsatz von KI auch neue Herausforderungen mit sich – insbesondere im Hinblick auf Datenschutz, Transparenz und Verantwortung. Deshalb ist es wichtig, dass KI-Systeme umsichtig, nachvollziehbar und verantwortungsbewusst eingesetzt werden.

Diese Richtlinie schafft einen klaren Rahmen für den sicheren und rechtskonformen Einsatz von KI im Sinne der DSGVO und des EU AI Acts – mit dem Ziel, eine offene, verantwortungsvolle und zukunftsorientierte Nutzungskultur im Unternehmen zu fördern.

2 Geltungsbereich

Die Richtlinie gilt für alle Mitarbeitenden der Abacus Experten GmbH. Weitere Vereinbarungen, wie z.B. der jeweilige Arbeitsvertrag oder andere einschlägige Richtlinien, bleiben hiervon unberührt und gelten zusätzlich.

3 Freigegebene KI-Systeme

Die Nutzung von KI-Systemen ist seitens des Unternehmens grundsätzlich erwünscht. Allerdings sind hieran bestimmte Rahmenbedingungen geknüpft, um potenzielle Risiken für das Unternehmen zu vermeiden.

Die Nutzung von KI-Systemen ist unzulässig, wenn sie geeignet ist, die Interessen oder das Ansehen des Unternehmens zu gefährden, die IT-Sicherheit zu beeinträchtigen oder gegen geltende Rechtsvorschriften zu verstoßen.

Es sind daher ausschließlich KI-Systeme zu verwenden, die vom Unternehmen als sicher eingestuft und zur Nutzung freigegeben wurden. Die Liste dieser Systeme ist in **Anlage 1** dokumentiert.

Das Unternehmen überprüft diese Liste regelmäßig und aktualisiert sie bei Bedarf – durch Aufnahme neuer Systeme oder Streichung nicht mehr zugelassener Anwendungen.

Mitarbeitende sind ausdrücklich dazu aufgerufen, Hinweise auf Schwachstellen oder

Sicherheitslücken freigegebener Systeme sowie Vorschläge für neue KI-Anwendungen aktiv einzubringen, um Qualität und Sicherheit kontinuierlich zu verbessern. Zuständig für die Bewertung und Koordination entsprechender Hinweise ist der zuständige KI- und Cloud-Compliance-Ausschuss.

Die Nutzung von KI-Systemen, die nicht in **Anlage 1** aufgeführt sind, ist untersagt. Über die Aufnahme weiterer Systeme in diese Liste entscheidet ausschließlich der zuständige KI- und Cloud-Compliance-Ausschuss. Dieser ist ebenfalls allein befugt, Ausnahmen von der Vorgabe zu bewilligen oder anzuordnen – vorausgesetzt, die datenschutzrechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten werden eingehalten.

4 Nutzungsrisiken von KI-Systemen

KI-Systeme verarbeiten große Datenmengen für Lern- und Analysezwecke. Dabei kann es vorkommen, dass von Nutzenden eingegebene Inhalte – insbesondere bei öffentlich zugänglichen oder cloudbasierten Lösungen – in das Training einfließen. So besteht das Risiko, dass vertrauliche Informationen in späteren Ausgaben erneut erscheinen und Dritten unbeabsichtigt offengelegt werden. Der Schutz solcher Daten ist daher essenziell.

Zudem beruhen KI-generierte Inhalte auf Wahrscheinlichkeiten und sind nicht immer korrekt, vollständig oder rechtlich unbedenklich. Mögliche Risiken sind unter anderem:

- **Fehlerhafte oder unvollständige Ergebnisse** – z. B. unzutreffende Fakten, fehlerhafte Übersetzungen oder irreführende Schlussfolgerungen.
- **Verletzungen von Rechten Dritter** – etwa durch die unberechtigte Nutzung urheberrechtlich geschützter Inhalte oder geschützter Marken.
- **Verzerrte oder diskriminierende Aussagen** – aufgrund voreingenommener oder unzureichend diverser Trainingsdaten.

Die Weitergabe solcher fehlerhaften oder rechtlich problematischen Inhalte kann nicht nur zu finanziellen Schäden führen, sondern auch das Vertrauen in das Unternehmen nachhaltig beeinträchtigen.

5 Unzulässige Eingaben in KI-Systeme

Bei der Nutzung von KI-Systemen sind besondere Vorsichtsmaßnahmen zu treffen. Unsachgemäße oder unbedachte Eingaben können die Rechte Dritter verletzen oder dem Unternehmen erheblichen Schaden zufügen.

Daher dürfen die nachfolgenden Informationen nicht in KI-Systeme eingegeben werden – es sei denn, das jeweilige System ist gemäß **Anlage 1** ausdrücklich zur

Verarbeitung dieser Informationen freigegeben.

- **Personenbezogene Daten** – z. B. Namen, E-Mail-Adressen, Standortdaten oder andere identifizierbare Informationen.

- **Vertrauliche Unternehmensdaten** – z. B. Strategien, Geschäftsgeheimnisse oder interne Finanz- und Managementdaten.

- **Geheimhaltungsbedürftige Informationen** – z. B. Inhalte aus Projekten mit Geheimhaltungsverträgen (NDAs).

- **Urheberrechtlich geschützte Werke** – z. B. Texte, Bilder oder Quellcode ohne klare Nutzungserlaubnis.

6 Umgang mit KI-Ergebnissen

Ergebnisse, Analysen oder Vorschläge, die durch KI-Systeme erzeugt werden (nachfolgend zusammenfassend **„**KI-Ergebnisse**“** genannt), dienen grundsätzlich als unterstützende Entscheidungsgrundlage – nicht als alleinige Entscheidungsinstanz – und dürfen nur nach menschlicher Prüfung weiterverwendet oder weiterverarbeitet werden. Folgende Grundsätze sind zu beachten:

- **Prüfpflicht**: Alle durch KI erzeugten Ergebnisse sind von der nutzenden Person vor Verwendung oder Weitergabe eigenverantwortlich auf Richtigkeit, Vollständigkeit, Angemessenheit und rechtliche Zulässigkeit zu prüfen. Ein blindes Vertrauen auf die Korrektheit von KI-Ergebnissen ist unzulässig.

- **Kontextbezug**: Ergebnisse müssen im jeweiligen fachlichen und inhaltlichen Zusammenhang beurteilt werden. Dies gilt insbesondere bei sensiblen Themen wie Personalentscheidungen, rechtlichen Einschätzungen oder vertraulichen Sachverhalten.

- **Transparenz**: Wenn KI-Ergebnisse in interne oder externe Kommunikation einfließen, ist ihre Herkunft offenzulegen – soweit dies für Nachvollziehbarkeit und Transparenz erforderlich ist.

- **Keine alleinige Entscheidungsgrundlage**: Entscheidungen mit rechtlicher oder erheblicher tatsächlicher Wirkung für Dritte dürfen nicht ausschließlich auf KI-Ergebnissen beruhen.

- **Dokumentation**: Bei geschäftskritischen oder risikobehafteten Vorgängen ist nachvollziehbar zu dokumentieren, ob und in welchem Umfang KI-Ergebnisse in die Entscheidung eingeflossen sind. Die Dokumentation kann z. B. in Form eines kurzen Vermerks im Projektprotokoll, eines Kommentars in einer Datei oder eines Hinweises im jeweiligen Dokument erfolgen.

- **Urheberrechtliche Vorsicht**: KI-Ergebnisse können bestehenden

urheberrechtlich geschützten Werken ähneln oder entsprechen. Solche Inhalte dürfen nicht verwendet werden, sofern keine rechtssichere Klärung vorliegt.

- **Verbot rechtswidriger Nutzung**: Die Verwendung von KI-Systemen für illegale Zwecke oder zur Umgehung rechtlicher Vorgaben ist streng untersagt.

- **Verlaufshistorie prüfen**: Viele KI-Systeme speichern Eingaben automatisch. Diese Historien können – je nach Anbieter – auch für Dritte einsehbar sein. Mitarbeitende sind verpflichtet, regelmäßig zu kontrollieren, ob dort vertrauliche oder personenbezogene Daten gespeichert sind, und diese ggf. zu löschen.

7 Änderungsvorbehalt

Das Unternehmen behält sich das Recht vor, diese KI-Sicherheitsrichtlinie jederzeit zu ändern oder zu ergänzen, insbesondere sofern gesetzliche, organisatorische oder technische Anforderungen dies erforderlich machen. Die jeweils aktuelle Version wird den Mitarbeitenden in geeigneter Form (z. B. über das Netzlaufwerk oder per E-Mail) zur Verfügung gestellt und ist für alle verbindlich. Die Mitarbeitenden sind verpflichtet, sich regelmäßig über den aktuellen Stand der Richtlinie zu informieren und die Änderungen zeitnah zu beachten und umzusetzen.

8 Verantwortlichkeiten und Konsequenzen

Als Unternehmen sind wir verpflichtet, die ordnungsgemäße Verwendung von KI-Systemen entsprechend dieser Richtlinie zu überwachen. Es können daher Kontrollen der Einhaltung dieser Richtlinie stattfinden, z. B. stichprobenhaft durch Protokollauswertungen. Falls dies technisch nicht möglich ist, sind auch personenbezogene Prüfungen zulässig.

Die Verantwortung für eine regelkonforme Nutzung von KI-Systemen liegt bei allen Mitarbeitenden. Wer KI-generierte Inhalte weiterverwendet, trägt die Verantwortung für deren sachliche und rechtliche Angemessenheit.

Sicherheitsrelevante Vorfälle – insbesondere das unbefugte Auslesen, Verwenden oder Offenlegen vertraulicher Informationen – sind unverzüglich dem KI- und Cloud-Compliance-Ausschuss zu melden. Gleiches gilt für die Meldung potenzieller Risiken oder Störungen im Zusammenhang mit freigegebenen KI-Systemen.

Das Unternehmen unterstützt seine Mitarbeitenden durch regelmäßige Schulungen, klare Richtlinien und technische Hilfsmittel im sicheren Umgang mit KI.

Verstöße gegen diese Richtlinie können arbeitsrechtliche Konsequenzen nach sich ziehen – etwa Abmahnungen oder, bei schwerwiegenden oder wiederholten Verstößen, eine Kündigung. Dabei wird jeder Einzelfall unter Berücksichtigung von

Vorsatz, Fahrlässigkeit, Schwere und Folgen des Verstoßes sowie etwaiger Wiederholungen geprüft. Es gilt das Prinzip der Verhältnismäßigkeit.

Ort, Datum: _____

Unterschrift Mitarbeiter/in: _____

Name in Druckbuchstaben: _____