Künstliche Intelligenz im HR-Bereich: Sicherheitsleitlinie für Unternehmen

Mhel Laurent Soria

Betreuerin: Ursula Uttinger

6. Juni 2025

Kategorisierung

Die vorliegende Leitlinie ist in neun zentrale Kategorien unterteilt, die sich an den typischen Lebenszyklen und Kontrollbedarfen von KI-Systemen im Personalwesen orientieren. Innerhalb jeder Kategorie sind spezifische Massnahmen (Leitlinien) definiert. Dabei wurden auch die möglichen Zuständigkeiten im Unternehmen festgelegt.

Nr.	Bezeichnung
1	Organisatorische Massnahmen
2	Schulung und Bewusstseinsbildung
3	Technische Massnahmen
4	Transparenz und Erklärbarkeit
5	Datenschutz und Informationssicherheit
6	Ethik
7	Externe Lösungen
8	Risikomanagement und Compliance
9	Evaluation und kontinuierliche Verbesserung

1. Organisatorische Massnahmen

Die organisatorische Massnahmen bilden das Fundament für den systematischen Einsatz von KI in einem Unternehmen. Zu den Leitlinien zählen Bedarfsanalysen, klare Zuständigkeiten, Change Management sowie Strukturen für Beteiligung und Steuerung.

Massnahme	Beschreibung	Zuständigkeiten
Bedarfsanalyse von KI	Bewertung der Notwendigkeit, ob und in welchen Bereichen der Einsatz von KI im HR sinnvoll, notwendig und realisierbar ist.	• HR • KI-Verantwortliche
Change Management	Frühzeitige Einbindung der Mitarbeitenden von Beginn an, aktive Kommunikation, Schulung, Feedbackmechanismen und transparente Prozesse. Change Management ist eine zentrale Voraussetzung für die erfolgreiche Einführung von KI im HR-Bereich.	• HR • Projektteam • KI-Verantwortliche • Kommunikation
Prozesskultur & Datenpflege	Die aktive Beteiligung der Mitarbeitenden an der kontinuierlichen Datenpflege, um die Verlässlichkeit der KI-Systeme langfristig und bei zukünftigen Einsatz sicherzustellen. Ein zentraler Aspekt ist dabei die Durchführung regelmässiger Mitarbeitenden Gespräche zur Datenerfassung und Anpassung der HR-Prozesse.	• HR • Data Owner
Mitarbeitereinbindung in KI-Einführung	Frühzeitige und transparente Kommunikation über Ziel und Nutzen der KI, Mitarbeiterschulungen sowie aktive Beteiligung am Einführungsprozess zur Förderung von Akzeptanz und Verständnis.	• HR • KI-Verantwortliche • Projektteam • Kommunikation
Einführung eines KI-Gremiums	Aufbau eines interdisziplinären KI-Gremiums mit Fachpersonen aus verschiedenen Bereichen zur strategischen und ethischen Steuerung des KI-Einsatzes im HR.	• HR • Geschäftsleitung • KI-Verantwortliche • Datenschutz

***Tabelle 1**: Leitlinie - Organisatorische Massnahmen*

2. Schulung und Bewusstseinsbildung

Diese Leitlinien tragen zur Stärkung des Wissens und der Akzeptanz hinsichtlich des Umgangs mit KI bei. Schulungen, interne Informationsangebote und die Funktion der KI-Botschafter fördern den verantwortungsvollen und sicheren Einsatz durch alle Mitarbeitenden.

Massnahme	Beschreibung	Zuständigkeiten
Allgemeine KI-Schulungen	Sensibilisierungsmassnahmen wie Schulungen, Informationsveranstaltungen und E-Learning-Plattformen sollen ein Grundverständnis für KI schaffen.	• KI-Verantwortliche • Kommunikation
Tool bezogene Schulungen	Vermittlung konkreter Kenntnisse zur Funktionsweise und zum sicheren Einsatz einzelner KI-Tools an die betroffenen.	• KI-Verantwortliche • Projektteam • Datenschutz • IT
Interne Wissensdatenbank zu KI	Aufbau interner Informationsquellen wie Wikis, Dokumentationen und Anleitungen zu KI-Systemen. Ziel ist es, benötigte aber auch freiwillige Informationsangebote bereitzustellen und Transparenz zu schaffen.	• KI-Verantwortliche • Kommunikation • HR
KI-Botschafter	Interne Ansprechpersonen begleiten Teams beim Einsatz von KI-Tools, bieten informelle Schulungen an und unterstützen bei Fragen. Sie arbeiten eng mit Datenschutzexperten zusammen, pflegen eine Übersicht geplanter und eingesetzter KI-Anwendungen und dienen als direkte Kontaktstelle. Zusätzlich organisieren sie Workshops, um Mitarbeitende über bestehende Tools zu informieren und neue Ideen in die Organisation einzubringen.	• KI-Verantwortliche • HR

Tabelle 2: Leitlinie - Schulung und Bewusstseinsbildung

3. Technische Massnahmen

Es lässt sich festhalten, dass technische Massnahmen für den Betrieb, die Sicherheit und die Fairness von KI-Systemen Sorge tragen. Zu den relevanten Faktoren zählen demnach die Qualität der Daten, Testverfahren, IT-Sicherheit, Dokumentation sowie Monitoring über MLOps.

Massnahme	Beschreibung	Zuständigkeiten
Datenqualität – Interne Prüfung	Regelmässige interne Überprüfung der HR-Daten auf Aktualität, Vollständigkeit, Fehler und Verzerrungen. Ziel ist die Sicherstellung einer fairen, objektiven und aktuellen Datenbasis.	• Data Science Team • HR
Datenqualität – Externe Prüfung	Externe oder unabhängige Prüfung der verwendeten Datensätze (z. B. durch externe Audits, Beratungen oder Tools) auf Bias, Repräsentativität und datenschutzkonforme Verarbeitung. Ergänzt die interne Kontrolle um eine objektive Qualitätssicherung.	• Externe Prüfstelle • Compliance • Datenschutz

Testing – Funktionalität des KI-Systems	Die Funktionalität des KI-Systems wird geprüft, um sicherzustellen, dass die geplanten Ergebnisse erzielt werden. Es wird überprüft, ob das System die definierten Anforderungen erfüllt, korrekt implementiert wurde und zuverlässig.	• Data Science Team • IT • HR
Testing – Bias im KI-System	Es werden gezielte Testszenarien entwickelt, um mögliche Diskriminierungen (Bias) frühzeitig zu erkennen und zu vermeiden (abhängig vom Use Case). Die Tests beinhalten das gezielte Einspielen von Testfällen mit kritischen demografischen Merkmalen. Ergebnisse werden hinsichtlich Ungleichbehandlung analysiert.	• Data Science Team • KI-Verantwortliche
Modelüberprüfung mit MLOps	Periodische technische Überprüfungen durch MLOps inkl. Modell-Monitoring, Validierung von Ergebnissen und Sicherstellung der Übereinstimmung mit dem ursprünglichen Einsatzzweck.	• Data Science Team • Datenschutz • IT
Explainability	Einführung von Prozessen und Methoden, um die Resultate der ML-Algorithmen zu verstehen und diese transparent zu gestalten.	• Data Science Team • IT
Dokumentation	Das Führen von einer Technische Dokumentation, inkl. Architektur, Systemtests, Change Management und Nachvollziehbarkeit der betroffenen KI-Systeme.	• IT • KI-Verantwortliche • Projektleitung
IT-Sicherheit - Infrastruktur	Die Server- und Netzwerkumgebung, auf der KI-Systeme betrieben werden, muss vor unbefugtem Zugriff und Manipulation geschützt sein. Dazu zählen die physische Absicherung von Rechenzentren (z. B. Zutrittskontrolle) sowie allgemeine IT-technische Massnahmen.	• Externer Hosting Partner • IT (Security)
IT-Sicherheit – Zugriff und Datensicherheit	Es müssen technische Massnahmen etabliert werden, um den Zugriff auf sensible Daten durch Identitäts- und Rechteverwaltung zu regulieren. Daten sind sowohl im Ruhezustand als auch bei Übertragung zu verschlüsseln. Zugriffskontrollen müssen rollenbasiert implementiert und regelmässig überprüft werden. Sicherheitsupdates müssen zeitnah durchgeführt werden.	• IT (Security)
Human Oversight	Etablierung des Zwei-Augen-Prinzips mit menschlicher Kontrolle bei der Anwendung von KI-Modellen, insbesondere bei sensiblen Entscheidungen.	• HR • KI-Verantwortliche

***Tabelle 3**: Leitlinie - Technische Massnahmen*

4. Transparenz und Erklärbarkeit

Ein nachvollziehbarer Einsatz von KI ist essenziell. Die Implementierung dieser Massnahmen gewährleistet, dass Entscheidungen und Prozesse in einer transparenten Weise kommuniziert werden und die Systemlogiken nachvollziehbar dargelegt werden können.

Massnahme	Beschreibung	Zuständigkeiten
Nachvollziehbarkeit	Die Ergebnisse eines KI-Systems müssen verständlich begründet und dokumentiert werden können. Dies umfasst auch Kontrollmechanismen zur Fehlererkennung und Korrektur.	• Data Science Team • Datenschutz • HR
Transparente Kommunikation	Unternehmen müssen offenlegen, welche KI-Systeme in welchen HR-Prozessen verwendet werden und warum. Tools sollten mit klaren Hinweisen (Disclaimern) gekennzeichnet werden.	• Datenschutz • HR • Kommunikation
Layered Information	Informationen zur KI-Nutzung sollen in verschiedenen Detailstufen bereitgestellt werden: z. B. eine Kurzinfo (z. B. Hinweistext im Tool) und weiterführende Details auf interne Wissensdatenbanken.	• Datenschutz • IT • KI-Verantwortliche • Kommunikation
Zweckbindung	Es ist transparent darzustellen, zu welchem Zweck die gesammelten Daten verwendet werden und welche Nutzungen ausgeschlossen sind. Eine nachträgliche Zweckänderung ist nur mit Zustimmung erlaubt.	• Datenschutz • HR

***Tabelle 4**: Leitlinie - Transparenz und Erklärbarkeit*

5. Datenschutz und Informationssicherheit

In der nächsten Kategorisierung wird die rechtmässige und datenschutzkonforme Betrieb von KI-Systemen wird durch diese Massnahmen sichergestellt.

Massnahme	Beschreibung	Zuständigkeiten
Rechtsgrundlagen Schweiz	Bei der Implementierung und dem Betrieb von KI-Systemen müssen das revDSG beachtet werden.	• Data Owner • Datenschutz • KI-Verantwortliche
Rechtsgrundlage mit Anwendungsbezug EU	Bei der Implementierung und dem Betrieb von KI-Systemen müssen die geltenden europäischen Datenschutzgesetze beachtet werden. Dazu zählen die DSGVO sowie der EU AI Act bei Anwendungsbezug zur EU.	• Data Owner • Datenschutz • KI-Verantwortliche
Zweckbindung	Eine Weiterverarbeitung von personenbezogenen Daten darf nur dann erfolgen, wenn der ursprüngliche Verwendungszweck erfüllt ist oder die betroffene Person explizit zugestimmt hat.	• Data Owner • Datenschutz • KI-Verantwortliche
DSFA	Bei hohem Risiko (z. B. Bewerbungsverfahren oder Performanceanalysen) ist gemäss Art. 22 revDSG eine Datenschutz-Folgenabschätzung (DSFA) verpflichtend durchzuführen.	• Datenschutz • KI-Verantwortliche

***Tabelle 5**: Leitlinie - Datenschutz und Informationssicherheit*

6. Ethik

Die Implementierung ethischer Leitlinien, die Durchführung von Bias-Prüfungen sowie die Etablierung von Meldestellen fördern eine faire, diskriminierungsfreie und gesellschaftlich akzeptierte Nutzung von KI. Des Weiteren werden Prinzipien wie Verantwortung und Nachhaltigkeit an dieser Stelle verankert.

Massnahme	Beschreibung	Zuständigkeiten
Bias Prüfungen	Durchführung von Bias-Audits und Einsatz geeigneter Fairness-Metriken zur Erkennung und Vermeidung diskriminierender Muster in KI-Systemen.	• Data Science Team • HR • KI-Verantwortliche
Meldestelle	Einrichtung eines anonymen Feedback-/ Meldesystems bei Hinweisen, Bedenken oder ethischen Fragestellungen im Zusammenhang mit KI.	• Datenschutz • Ethikgremium • KI-Verantwortliche
Corporate Digital Responsiblitiy (CDR)	CDR umfasst die gesamtheitliche digitale Unternehmensverantwortung über gesetzliche Anforderungen hinaus. Sie adressiert Themen wie Datenschutz, digitale Inklusion, faire KI-Nutzung, Umwelteinflüsse durch IT-Infrastruktur sowie transparente Datennutzung. Ziel ist es, einen nachhaltigen und verantwortungsvollen digitalen Fussabdruck zu etablieren.	• Datenschutz • Ethikgremium • Geschäftsleitung • IT
Ethische Leitlinien für KI	Ethische Leitlinien regeln speziell den Umgang mit KI-Systemen im Unternehmen. Dazu zählen Prinzipien wie Fairness, Nichtdiskriminierung, Transparenz, Verantwortung und Erklärbarkeit. Sie orientieren sich an übergeordneten ethischen Frameworks (z. B. OECD) und sind im Unternehmen verbindlich zu dokumentieren und umzusetzen.	• Datenschutz • Ethikgremium • KI-Verantwortliche
Dokumentation Ethikrichtlinien	Darstellung, wie ethische Grundsätze, insbesondere Fairness und Nichtdiskriminierung, konkret im HR-Bereich umgesetzt werden. Dokumentation von Standards und Entscheidungswegen.	• Compliance • Ethikgremium
Human-in-the-loop (HITL)	Interaktive Trainings- und Optimierungsschleifen mit menschlicher Aufsicht: KI-Modelle werden durch gezieltes Feedback von Fachpersonen trainiert und bei kritischen Fällen manuell.	• HR • KI-Verantwortliche

***Tabelle 6**: Leitlinie – Ethik*

7. Externe Lösungen

Im Falle zugekaufter KI-Systeme sind Transparenz, Vertragssicherheit und Risikobewertung von signifikanter Relevanz. Die vorliegenden Massnahmen dienen der Regelung der Auswahl, Integration und Überwachung externer Anbieter.

Massnahme	Beschreibung	Zuständigkeiten
Lieferantentransparenz	Bei der Auswahl und Nutzung externer KI-Dienstleister sollte das Unternehmen Einblick in wesentliche Aspekte wie verwendete Trainingsdaten, Modelllogik, Implementierungsverfahren sowie bekannte Risiken einfordern. Nur so kann eine fundierte Entscheidung über die Integration getroffen.	• Compliance • Datenschutz • Einkauf • IT
Compliance-Vorgaben	Bestehende interne Richtlinien und Compliance-Vorgaben müssen explizit auch für externe Anbieter gelten. Diese sind vertraglich zu verpflichten, etwa auf revDSG, Datenschutz oder ethische Standards.	• Compliance • Datenschutz
Bewertung vor Integration	Vor der produktiven Nutzung eines KI-Tools durch externe Anbieter sollte eine Risikoanalyse erfolgen, idealerweise ergänzt durch eine Pilotphase. So können technische, rechtliche und ethische Risiken frühzeitig erkannt und adressiert werden.	• Datenschutz • HR • IT • Projektleitung

__Tabelle 7__: Leitlinie - Externe Lösung

8. Risikomanagement und Compliance

Die vorliegende Kategorie gewährleistet eine systematische Bewertung, Dokumentation und Integration von Risiken und gesetzlichen Anforderungen in die Unternehmensprozesse, wobei klare Rollen und Prüfzyklen eine wesentliche Rolle spielen.

Massnahme	Beschreibung	Zuständigkeiten
Verantwortlichkeiten	Es ist festzulegen, wer für die Durchführung von Risikobewertungen und DSFAs zuständig ist. Die Rollenverteilung muss dokumentiert und bei Bedarf regelmässig überprüft werden.	• Compliance • Datenschutz • Geschäftsleitung
Compliance-Integration	Das Risikomanagement für KI muss verbindlich in interne Kontrollsysteme, Richtlinien und Governance-Strukturen eingebunden werden.	• Compliance • Datenschutz
Regelmässige Reviews	Risiken und Compliance-Vorgaben müssen regelmässig überprüft und angepasst werden – insbesondere bei Systemupdates oder geänderten Prozessanforderungen.	• Compliance • Datenschutz • IT • KI-Verantwortliche

__Tabelle 8__: Leitlinie - Risikomanagement und Compliance

9. Evaluation und kontinuierliche Verbesserung

Die kontinuierliche Evaluation und Optimierung von KI-Systemen trägt zur Steigerung von Qualität, Sicherheit und Akzeptanz bei. Mittels Monitoring, Feedback und Audits wird ein lernender Umgang mit KI etabliert.

Massnahme	Beschreibung	Zuständigkeiten
MLOps & Monitoring	Kontinuierliche Überwachung von KI-Modellen auf Genauigkeit, Daten-Drift und Einhaltung der Zweckbindung. Abweichungen werden analysiert und durch gezielte Auswertungen dokumentiert.	• Date Science • IT • KI-Verantwortliche
Audits	Regelmässige interne und externe Prüfungen zur Bewertung der technischen, datenschutzrechtlichen und organisatorischen Konformität der KI-Systeme.	• Compliance • Datenschutz • IT
Kontinuierliches menschliches Feedback	Systematisches Erfassen von Problemen, Nutzerfeedback und Verbesserungsvorschlägen aus dem operativen Einsatz der KI-Anwendungen um zur kontinuierlichen Verbesserung der Systeme beizutragen.	• HR • KI-Verantwortliche
Dokumentation zu KI-Ereignisse	Dokumentation von Änderungen, Erkenntnissen, Vorfällen und Lessons Learned, um zukünftige KI-Projekte effizienter und sicherer zu gestalten.	• KI-Verantwortliche • Qualitätsmanagement

***Tabelle 9**: Leitlinie - Evaluation und kontinuierliche Verbesserung*