KI-Governance Policy Industrie

Industrie & Fertigungsbetriebe | KMU mit ca. 200 Mitarbeitenden

RECHTLICHER HINWEIS

Dieses Dokument stellt keine Rechtsberatung dar. Die Qimpuls AG schliesst jegliche Haftung für die betriebliche Implementierung aus. Vor Inkraftsetzung ist eine juristische Prüfung zwingend erforderlich.

Version: 1.0 | April 2026

Herausgeber: ki-vr.ch | Qimpuls AG, Pfäffikon SZ

Branche: Industrie & Fertigungsbetriebe | KMU mit ca. 200 Mitarbeitenden

Geltungsbereich: Alle Mitarbeitenden, Kader, Verwaltungsrat

Hinweis: Anpassung auf Firmenname und spezifische Situation erforderlich. Interne Implementierung nur nach juristischer Freigabe.

Inhaltsverzeichnis

ABSCHNITT 1 Zweck und Geltungsbereich

1.1 Zweck

Diese KI-Governance Policy (nachfolgend "Policy") legt verbindliche Regeln für den Einsatz von Künstlicher Intelligenz (KI) und KI-gestützten Werkzeugen in [Firmenname] fest. Sie dient der Erfüllung der Oberaufsichtspflicht des Verwaltungsrats nach Art. 716a OR, dem Schutz von Mitarbeitenden und Kunden sowie der rechtssicheren Verankerung von KI-Prozessen im internen Kontrollsystem (IKS).

1.2 Geltungsbereich

Diese Policy gilt für alle Mitarbeitenden, Kader und Mitglieder des Verwaltungsrats von [Firmenname], einschliesslich Temporärangestellter, Freelancer und externer Dienstleister mit Zugang zu Unternehmenssystemen und Daten.

Als KI-Werkzeuge im Sinne dieser Policy gelten insbesondere:

- Generative KI-Modelle (ChatGPT, Claude, Copilot, Gemini und vergleichbare)
- KI-Module in MES, SCADA, ERP und Produktionsmanagementsystemen
- KI-gestützte Qualitätskontroll- und Sensorik-Auswertungssysteme
- Automatisierte Entscheidungssysteme in der Fertigungsplanung

ABSCHNITT 2 Rechtliche Grundlagen

2.1 Verwaltungsratshaftung (OR Art. 716a und Art. 754)

Art. 716a OR verpflichtet den Verwaltungsrat zur unübertragbaren Oberaufsicht über das Management, einschliesslich der Kontrolle über wesentliche Risiken. Der unkontrollierte Einsatz von KI in Kernprozessen stellt ein materielles Risiko dar, das die Oberaufsichtspflicht unmittelbar berührt. Fehlt eine dokumentierte KI-Policy, liegt ein Organisationsverschulden vor, das nach Art. 754 OR zur persönlichen Haftung von VR-Mitgliedern führen kann.

2.2 Arbeitnehmerpflichten (OR Art. 321e)

Mitarbeitende haften gegenüber dem Arbeitgeber nach Art. 321e OR für Schäden, die durch grobe Fahrlässigkeit im Umgang mit KI-Werkzeugen entstehen. Grobe Fahrlässigkeit liegt insbesondere vor bei der Weitergabe von vertraulichen Produktions- oder Kundendaten an nicht genehmigte KI-Systeme, der Verwendung von KI-Outputs ohne Prüfung in sicherheitsrelevanten Prozessen sowie der mutwilligen Umgehung dieser Policy.

2.3 Datenschutz (nDSG Art. 16ff. und Art. 21)

Das neue Datenschutzgesetz (nDSG, in Kraft seit 1. September 2023) verlangt, dass Personendaten nur für festgelegte Zwecke bearbeitet werden. Art. 16 nDSG regelt die Anforderungen an automatisierte Einzelentscheidungen. Art. 21 nDSG begründet eine Informationspflicht bei automatisierten Einzelentscheidungen mit erheblichen Folgen für betroffene Personen. Dies ist besonders relevant bei KI-gestützten HR-Entscheiden wie automatischer Schichtplanung und Leistungsbeurteilung. Personendaten von Mitarbeitenden und Kunden dürfen nicht ohne datenschutzrechtliche Grundlage in externe KI-Systeme eingegeben werden.

2.4 Urheberrecht (URG)

KI-generierte Inhalte geniessen nach schweizerischem Urheberrecht (URG) keinen automatischen Schutz. Reiner KI-Output ohne signifikante menschliche Schöpfungshöhe ist urheberrechtlich nicht geschützt und kann von Dritten grundsätzlich frei verwendet werden. Für externe Dokumente, technische Berichte und Kundendokumentationen mit KI-generierten Inhalten ist dies zu berücksichtigen.

ABSCHNITT 3 Definitionen und Anwendungsbereich

Begriff	Definition
Generative KI	KI-Systeme, die neue Inhalte erzeugen (Text, Bild, Code, Sprache).
MES/SCADA-KI	KI-Funktionen in Manufacturing Execution Systems und Supervisory Control and Data Acquisition-Systemen.
Produktive Nutzung	Einsatz von KI für Aufgaben, deren Output in Geschäfts- oder Fertigungsprozesse einfliessen kann.
Personendaten	Alle Informationen zu einer identifizierten oder identifizierbaren natürlichen Person (Art. 5 lit. a nDSG).

Schatten-KI	KI-Werkzeuge, die ohne Wissen oder Freigabe der Unternehmensleitung eingesetzt werden.
KI-Register	Interne Dokumentation aller produktiv eingesetzten KI-Werkzeuge mit Risikoklasse und Verantwortlichem.

ABSCHNITT 4 Risikoklassifikation

Alle KI-Werkzeuge werden einer von drei Risikoklassen zugewiesen. Die Klassifikation bestimmt Freigabeprozess und Nutzungsbedingungen.

Klasse	Niveau	Freigabe	Industrie & Fertigung: Beispiele
Klasse 1	Geringes Risiko	Freigegeben nach Schulung	Produktionsplanung-Assistenz (intern), interne Reportings, Texterstellung für Berichte, KI-gestützte Fehlersuche in Dokumentation
Klasse 2	Erhöhtes Risiko	Freigabe Bereichsleiter / GL	KI-gestützte Fertigungsplanung mit Auftragsdaten, vorausschauende Wartung (Sensordaten ohne Personenbezug), KI-Kunden-Kommunikation (Lieferzeitkonfirmation)
Klasse 3	Hohes Risiko	VR-Beschluss erforderlich	Automatisierte Qualitätsabweichungs-Eskalation mit Kundenkommunikation, KI-Personalbeurteilung in der Schichtplanung, vollautomatische Produktionssteuerung ohne menschliche Kontrolle

4.1 Freigabeprozess Klasse 2

Vor dem produktiven Einsatz eines Klasse-2-Werkzeugs muss der Bereichsleiter schriftlich bestätigen: (a) KI-Register-Erfassung, (b) Human-in-the-Loop definiert, (c) nDSG-Anforderungen geprüft.

4.2 Freigabeprozess Klasse 3

KI-Werkzeuge der Klasse 3 erfordern einen dokumentierten VR-Beschluss mit: Beschreibung des KI-Systems, Risikoabschätzung, Kontrollmechanismen, Abbruchkriterien und Verantwortlichem für Monitoring.

ABSCHNITT 5 Branchenspezifische Regelungen Industrie & Fertigung

5.1 ERP-gestützte Produktionskalkulation

KI-Assistenten in ERP-Systemen (z.B. SAP mit KI-Modulen, Microsoft Dynamics) für Produktionskalkulation und Kapazitätsplanung gelten als Klasse-2-Werkzeuge. KI-generierte Produktionskalkulationen müssen vor Auftragsbestätigung durch den verantwortlichen Produktionsplaner geprüft werden. Die Prüfung ist im Produktionsauftrag zu dokumentieren. Bei Nutzung proprietärer Fertigungsdaten (Rezepturen, Prozesskennwerte) in externen KI-Systemen ist der Schutz von Betriebsgeheimnissen sicherzustellen.

5.2 MES/SCADA-Integration und vorausschauende Wartung

KI-Funktionen in Manufacturing Execution Systems (MES) und SCADA-Systemen sind im KI-Register zu erfassen und zu klassifizieren. Vorausschauende Wartungsalgorithmen auf Basis von Sensordaten ohne Personenbezug gelten als Klasse 2. Kritisch: KI-generierte Sicherheits- oder Wartungsempfehlungen für sicherheitsrelevante Produktionsanlagen dürfen nicht ohne Freigabe durch einen zertifizierten Instandhaltungsfachmann und ggf. den Maschinenhersteller umgesetzt werden. Die Produkthaftungsrisiken (Produktehaftpflichtgesetz) sind bei KI-gesteuerten Fertigungsprozessen explizit zu bewerten.

5.3 Qualitätskontrolle und Sensorik-Auswertung

KI-gestützte Qualitätskontrollsysteme (automatische Bilderkennung, Sensorik-Auswertung für Fertigungsqualität) gelten als Klasse-2-Werkzeuge. Die Systemgrenzen und Fehlerraten sind zu dokumentieren und dem VR bekannt zu machen. Bei vollautomatischer Kundenkommunikation über Qualitätsabweichungen (Reklamationsbearbeitung ohne menschliche Prüfung) ist Klasse 3 vorzunehmen. In der Lebensmittel- und Pharmafertigung gelten zusätzlich die branchenspezifischen Regulatorien (GMP, HACCP), die KI-gestützten Prozessen übergeordnet sind.

5.4 Schichtplanung und Fertigungsdisposition

KI-gestützte Schicht- und Ressourcenplanung gilt als Klasse-2-Werkzeug, da Mitarbeiterdaten verarbeitet werden. Der Einsatz setzt eine entsprechende Grundlage im Arbeitsvertrag oder einer Betriebsvereinbarung voraus. Automatisierte Dispositionsentscheide ohne menschliche Prüfung sind als Klasse 3 zu behandeln. Betroffene Mitarbeitende sind nach Art. 21 nDSG über automatisierte Entscheide zu informieren, die erhebliche Folgen haben können (z.B. Schichtzuteilung, Überstundenanordnung).

5.5 Lieferanten-EDI und Supply-Chain-Management

KI-gestützte Lieferantenbewertung und automatische Bestellsysteme (EDI mit KI-Optimierung) gelten als Klasse-2-Werkzeuge. Lieferantenvertragskonditionen, Rabattvereinbarungen und strategische Einkaufspreise dürfen nicht in öffentliche KI-Systeme eingegeben werden. Bei vollautomatischen Bestellauslösungen über definierten Schwellenwerten ist eine menschliche Prüfung vor Bestellabsendung sicherzustellen. Supply-Chain-Risikodaten (Single-Source-Abhängigkeiten, kritische Lieferanten) sind vertraulich zu behandeln.

ABSCHNITT 6 Technische Vorgaben und IP-Schutz

6.1 Urheberrecht und Eigentum an KI-Output

Reiner KI-Output ohne signifikante menschliche Schöpfungshöhe ist nach schweizerischem URG urheberrechtlich nicht geschützt. Für externen Einsatz (Kundenberichte, technische Dokumentation) ist sicherzustellen, dass KI-generierte Inhalte durch urheberrechtlich schutzfähige eigene Beiträge ergänzt werden. Industrielle Schutzrechte (Patente, Gebrauchsmuster) auf KI-generierte Erfindungen sind nach Schweizer und internationalem Recht eingeschränkt: Die Erfinderschaft setzt eine natürliche Person voraus.

6.2 Verbotene Eingaben

Folgende Daten dürfen nicht in nicht genehmigte oder externe KI-Systeme eingegeben werden:

- Personendaten von Mitarbeitenden und Kunden
- Vertrauliche Fertigungs-Rezepturen, Prozesskennwerte und Prüfspezifikationen

- Strategische Einkaufskonditionen und Lieferantenpreise
- Kundenspezifische Produktanforderungen und Zeichnungen unter NDA
- Zugangsdaten, Passwörter und OT-Systemkonfigurationen

6.3 Genehmigte KI-Plattformen

Eine Liste der freigegebenen KI-Werkzeuge wird im KI-Register geführt und jährlich durch die GL überprüft. Für KI-Integrationen in OT-Systeme (Operational Technology) ist eine separate Freigabe durch den IT/OT-Sicherheitsverantwortlichen einzuholen.

ABSCHNITT 7 Datenschutz und nDSG-Compliance

7.1 Zweckbindung und Datensparsamkeit

Personendaten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden (Art. 6 nDSG). Produktionsdaten und Mitarbeiterdaten dürfen nicht ohne Grundlage in externe KI-Systeme eingegeben werden.

7.2 Verzeichnis der Bearbeitungstätigkeiten

KI-Systeme, die Personendaten verarbeiten, sind im Verzeichnis der Bearbeitungstätigkeiten (Art. 12 nDSG) zu erfassen. Dies gilt insbesondere für KI-Systeme mit Kameraüberwachung in der Produktion.

7.3 Datenschutz-Folgenabschätzung

Bei KI-Systemen mit hohem Risiko für Grundrechte ist vorab eine Datenschutz-Folgenabschätzung (Art. 22 nDSG) durchzuführen. Priorität: KI-gestützte Mitarbeitendenüberwachung und HR-Entscheide (Klasse 3).

ABSCHNITT 8 KI-Register und Dokumentationspflicht

[Firmenname] führt ein internes KI-Register (Struktur gemäss Anhang B). Das Register enthält für jedes produktiv eingesetzte KI-Werkzeug mindestens:

- Name und Anbieter des KI-Werkzeugs
- Einsatzbereich und Prozessbeschreibung
- Risikoklasse (1, 2 oder 3)
- Freigabedatum und freigebende Person
- Datenschutzrelevanz (ja/nein) und Begründung
- Verantwortliche Person für laufenden Betrieb und Monitoring

Das KI-Register ist jährlich durch die GL zu aktualisieren. Dem Verwaltungsrat ist einmal jährlich ein aktualisierter Registerauszug vorzulegen. Die erstmalige Erfassung aller bereits eingesetzten KI-Werkzeuge hat innert 90 Tagen nach Inkrafttreten zu erfolgen.

ABSCHNITT 9 Schulung und Sensibilisierung

Alle Mitarbeitenden mit Zugang zu KI-Werkzeugen der Klassen 1 und 2 absolvieren innert 90 Tagen nach Inkrafttreten eine Grundlagenschulung. Inhalte:

- Risikoklassifikation und Freigabeprozesse
- Verbotene Dateneingaben und Haftungskonsequenzen
- Kritische Prüfung von KI-Outputs vor Weiterverwendung
- Meldepflicht bei ungenehmigten KI-Werkzeugen

Für Mitarbeitende an sicherheitsrelevanten Anlagen ist eine zusätzliche Schulung zu den spezifischen Risiken von KI in der OT-Umgebung durchzuführen. Neue Mitarbeitende werden im Onboarding in die KI-Governance eingeführt.

ABSCHNITT 10 Governance, VR-Beschluss und Berichterstattung

10.1 VR-Beschluss und Protokollierung

Diese Policy tritt mit einem formellen VR-Beschluss in Kraft. Der Beschluss ist im VR-Protokoll zu verankern und umfasst: Genehmigung der Policy, Beauftragung der GL mit der Umsetzung, Definition des Berichterstattungszyklus.

10.2 Berichterstattung an den VR

Die GL erstattet dem VR einmal jährlich Bericht: aktualisiertes KI-Register, Schulungsstand, aufgetretene Incidents, Massnahmen zur Risikominderung, Anpassungsbedarf der Policy.

10.3 Verantwortlichkeiten

Organ	Aufgabe
Verwaltungsrat	Oberaufsicht, Genehmigung Policy, Beschluss Klasse-3-Werkzeuge, jährlicher Review
Geschäftsleitung	Umsetzung, KI-Register-Führung, Schulungen, jährlicher Policy-Review
Bereichsleiter Produktion	Freigabe Klasse-2-Werkzeuge, Meldung von Policy-Verstössen und OT-Risiken
Mitarbeitende	Einhaltung Policy, Nutzung genehmigter Werkzeuge, Meldung von Schatten-KI
IT-Verantwortlicher	Technische Unterbindung von Schatten-KI, Bereitstellung genehmigter Enterprise-Lizenzen, technisches Audit des KI-Registers

ABSCHNITT 11 Inkrafttreten, Revision und Geltungsdauer

Diese Policy tritt mit dem VR-Beschluss in Kraft. Sie gilt bis auf Widerruf. Die GL überprüft die Policy jährlich auf Aktualität und Wirksamkeit. Bei wesentlichen Änderungen der rechtlichen Grundlagen oder der Produktionsinfrastruktur ist eine ausserordentliche Revision durchzuführen. Überarbeitete Versionen werden als neue Hauptversionsnummer veröffentlicht und erfordern einen neuen VR-Beschluss.

Version 1.0 | April 2026 | Herausgeber: ki-vr.ch | Qimpuls AG, Pfäffikon SZ | KI-Governance Policy. Vor Inkraftsetzung ist eine juristische Prüfung durch einen zugelassenen Anwalt zwingend.

Anhang A

VR-Haftungs-Check KI-Governance

Beantworten Sie die folgenden fünf Fragen. Jede "Nein"-Antwort identifiziert eine offene Haftungslücke nach Art. 716a OR.

Frage 1: VR-Beschluss und Dokumentation

Hat der Verwaltungsrat einen formellen Beschluss zur KI-Nutzung in Ihrem Unternehmen gefasst und im Protokoll dokumentiert?

□ Ja, VR-Beschluss vorhanden und protokolliert	□ In Vorbereitung	□ Nein

Frage 2: KI-Governance Policy

Existiert eine schriftliche KI-Governance Policy, die Risikoklassen, Freigabeprozesse und Verantwortlichkeiten für alle Mitarbeitenden verbindlich regelt?

□ Ja, Policy in Kraft	□ In Erarbeitung	□ Nein

Frage 3: IP-Rechte an KI-Output

Sind die Urheberrechte und IP-Rechte an KI-generierten Arbeitsergebnissen (Berichte, technische Dokumentation, Kundenkommunikation) in den Arbeitsverträgen und AGB geregelt?

□ Ja, vertraglich geregelt	□ Teilweise	□ Nein

Frage 4: KI-Register

Wird ein aktuelles KI-Register geführt, das alle produktiv eingesetzten KI-Systeme mit Risikoklasse, Verantwortlichem und Datenschutzrelevanz erfasst?

□ Ja, Register aktuell	□ Unvollständig	□ Nein

Frage 5: Eskalationsmatrix

Liegt eine dokumentierte Eskalationsmatrix vor, die definiert, welche KI-Entscheide eine Freigabe durch GL oder VR erfordern, und ist diese dem Verwaltungsrat bekannt?

□ Ja, Matrix definiert und kommuniziert	□ Informell vorhanden	□ Nein

"Nein" oder "In Vorbereitung" angekreuzt?

Jede offene Antwort ist eine identifizierbare Haftungslücke nach Art. 716a OR. Klären Sie Ihren konkreten Handlungsbedarf in einem Erstgespräch (30 Minuten).

ki-vr.ch/standortbestimmung

Anhang B

KI-Risikoregister (Struktur)

KI-Werkzeug	Anbieter	Einsatzbereich	Risikoklasse	Freigabe durch	Datum	Personendaten
ChatGPT / GPT-4o	OpenAI	Texterstellung, interne Recherche	**Klasse 1**	GL	___.__.__	Nein (Policy beachten)
Microsoft Copilot	Microsoft	Office-Integration, E-Mails	**Klasse 1**	GL	___.__.__	Ggf. (MS-Vertrag prüfen)
[MES KI-Modul]	[Anbieter]	Fertigungsplanung, Wartung	**Klasse 2**	Bereichsleiter Prod.	___.__.__	Nein (nur Maschinendaten)
[KI-Qualitätskontrolle]	[Anbieter]	Bildauswertung Qualität	**Klasse 2**	Bereichsleiter Prod.	___.__.__	Nein
[Weiteres Werkzeug]						

Anhang C

Eskalationsmatrix KI-Governance

KI-Entscheid / Situation	Klasse	Freigabestufe	Dokumentation
KI für interne Texterstellung / Reportings	**Klasse 1**	Keine Einzelfreigabe	KI-Register-Eintrag
KI-Fertigungsplanung (Auftragsdaten)	**Klasse 2**	Bereichsleiter Produktion	Genehmigungsvermerk
Vorausschauende Wartung (Sensordaten)	**Klasse 2**	Bereichsleiter + IT-Sicherheit	Protokoll OT-Freigabe
Neues KI-Werkzeug produktiv einsetzen	**Klasse 2**	GL-Beschluss	KI-Register + Schulung
Automatisierte Qualitäts-Eskalation Kunden	**Klasse 3**	VR-Beschluss	VR-Protokoll
KI-gestützte Schichtplanung (HR-Daten)	**Klasse 3**	VR-Beschluss + DSFA	VR-Protokoll + nDSG Art. 21
Vollautomatische Produktionssteuerung	**Klasse 3**	VR-Beschluss	VR-Protokoll
Meldung Policy-Verletzung durch MA	N/A	GL-Meldung, ggf. VR-Eskalation	Incident-Report