



TSMONDO

IT-SECURITY & COMPLIANCE

KI-MANAGER

KI-Compliance, lokal und nachweisbar.

Software für die EU-KI-Verordnung und ISO/IEC 42001. Sie läuft auf dem eigenen Rechner, ohne Cloud-Konto, und legt die Nachweise an, nach denen Aufsicht, Kunden und Auditoren fragen.

• EU-KI-Verordnung

• ISO/IEC 42001

• Windows · portabel · signiert

• AES-256 zuschaltbar

AUSGANGSLAGE

Zwei Regelwerke fragen nach denselben Angaben.

Die **EU-KI-Verordnung** ist das europäische Gesetz für den Einsatz von KI. Sie ordnet jedes KI-System in eine Risikoklasse ein und knüpft daran Pflichten.

ISO/IEC 42001 ist die Norm für ein KI-Managementsystem — die Organisation drumherum, zertifizierbar, freiwillig.

Beide verlangen dieselbe Grundlage: Wer setzt welche KI wofür ein, mit welchen Daten, unter wessen Verantwortung. Wer das getrennt führt, pflegt es doppelt. Der KI-Manager erfasst es einmal und erzeugt daraus die Nachweise für beide Seiten.

ABLAUF

Neun Schritte je Anwendungsfall

Der Assistent führt durch die Fragen und lässt am Ende einen Maßnahmenplan mit Balkendiagramm über die Zeit stehen. Erledigte Schritte bleiben sichtbar, offene auch.

1 Projekt

Zweck, Prozess, Verantwortung, geplanter Produktivstart

2 Rolle

Betreiber, Anbieter oder beides — davon hängen die Pflichten ab

3 Ist das ein KI-System?

Abgrenzung nach der Begriffsbestimmung in Art. 3

4 Risiko-Triage

Einstufung in die Risikoklasse, mit Begründung je Antwort

5 Pflichten

Was aus der Einstufung folgt, Punkt für Punkt abhakbar

6 Risikomanagement

Risiken, Bewertung, Maßnahmen, Restrisiko

7 Querschnittspflichten

Transparenz, menschliche Aufsicht, Datenschutz

8 Vorlagen

Dokumente aus den erfassten Angaben erzeugen

9 Plan & Gantt

Maßnahmen mit Terminen als Balkendiagramm

SCHRITT 4

Fünf Wege, und am Ende genau eine Einstufung

PRÜFUNG	WAS GEFRAGT WIRD	FUNDSTELLE	ERGEBNIS
Verbotene Praktiken	Acht Fragen zu manipulativen Techniken, Ausnutzung von Schutzbedürftigkeit, Sozialbewertung, Emotionserkennung am Arbeitsplatz und biometrischer Fernidentifizierung	Art. 5	untersagt
Hochrisiko-Bereich	Acht Einsatzfelder mit besonderer Grundrechtsrelevanz, etwa Personalauswahl, Kreditvergabe, kritische Infrastruktur oder Bildung	Anhang III	hoch
Sicherheitsbauteil	KI als sicherheitsrelevanter Bestandteil eines Produkts, das ohnehin eine externe Konformitätsbewertung braucht — Maschine, Medizinprodukt, Fahrzeug	Anhang I	hoch
Ausnahme	Eng begrenzte Verfahrensaufgabe ohne Profiling: Der Fall liegt zwar im Hochrisiko-Bereich, die Pflichten greifen aber nicht in vollem Umfang	Art. 6 Abs. 3	begrenzt
Allgemeine KI-Modelle	Eigene Entwicklung oder Anpassung eines Modells mit allgemeinem Verwendungszweck, dazu die Frage nach systemischem Risiko	Art. 51 ff.	GPAI

STARTPUNKT

46 vorklassifizierte Anwendungsfälle aus 12 Fachbereichen

Statt vor einem leeren Formular zu sitzen, wählt man den Fall, der dem eigenen am nächsten kommt. Zweck, Rolle und Triage-Antworten sind vorgelegt, die Begründung der Einstufung steht dabei – und alles lässt sich ändern.

Personal & HR	5	Marketing & Kommunikation	4	Vertrieb & Sales	3
Kundenservice & Support	4	Finanzen & Buchhaltung	5	IT & Softwareentwicklung	4
Produktion & Fertigung	4	Logistik, Einkauf & Supply Chain	4	Recht, Compliance & Datenschutz	3
Geschäftsleitung & Verwaltung	5	Forschung, Entwicklung & Produkt	2	Gebäude, Sicherheit & Facility	3

DARUNTER FÄLLE ALLER KLASSEN – VOM VERBOTENEN BIS ZUM MINIMALEN RISIKO

ERGEBNIS

30 Dokumentvorlagen, gefüllt aus den erfassten Angaben

Kein leeres Muster zum Abschreiben: Firmendaten, Einstufung, Risiken und Maßnahmen stehen bereits im Text. Rot Gesetztes ist das, was noch zu ergänzen ist.

Je KI-System

Steckbrief, technische Dokumentation, Risikoakte, Betriebsanleitung, Transparenzhinweis, Logbuch, Konformitätsbericht — und die Grundrechte-Folgenabschätzung, wo sie verlangt ist.

EU-KI-VERORDNUNG

Einmal je Unternehmen

KI-Leitlinie, Anwendungsbereich, Kontext, Rollen, Ziele, Datenmanagement, Lieferantenprüfung, Anwendbarkeitserklärung, internes Audit, Managementbewertung, Überwachungsplan, Umsetzungsübersicht und weitere.

ISO/IEC 42001

Fassung und Freigabe

Jedes Dokument trägt eine Fassungsnummer, einen Stand — Entwurf, in Kraft, abgelöst — und ein Datum zur Wiedervorlage. Solange „Entwurf“ steht, gilt es als nicht in Kraft.

NACHVOLLZIEHBARKEIT

ISO/IEC 42001

Die Norm ist Punkt für Punkt hinterlegt

HAUPTKAPITEL

7

Kapitel 4 bis 10, die Managementanforderungen

ABSCHNITTE DARIN

32

von „Kontext der Organisation“ bis
„Verbesserung“

ANNEX - A - MASSNAHMEN

38

alle Maßnahmen des Anhangs A der Norm

Zusammen **70 Normpunkte**. Zu jedem steht in eigenen Worten, wie die Software ihn umsetzt und wo im Programm das passiert. Je Normpunkt halten Sie fest, wer ihn prüft, in welchem Rhythmus, **woran man es prüft** und was dabei herauskam — und welches Dokument ihn trägt.

Alles, was ein Auditor am Normpunkt fragt

- Stand: noch offen, umgesetzt oder nicht anwendbar
- Umgesetzt durch: bei allen 70 Punkten vorbelegt
- Ergänzung für das, was außerhalb der Software geschieht
- Jeder Klick auf Geprüft legt einen datierten Nachweis mit Ergebnis ab

REGULATORIK · ANHANG A.7.4 · DATENQUALITÄT

SCHRITT 7 · DATENSCHUTZ

Zehn Angaben für die Datenschutzstelle

Der Block öffnet sich erst, wenn die Eingangsfrage nach personenbezogenen Daten mit „ja“ beantwortet ist. Steht dort „nein“, entfällt der Rest — und die Feststellung bleibt trotzdem dokumentiert.

- Rechtsgrundlage nach Art. 6, besondere Kategorien nach Art. 9
- Datenkategorien, Betroffenengruppen, Empfänger
- Datenstandort und Grundlage für den Drittlandtransfer
- Speicherdauer, Informationspflichten, Eintrag im Verarbeitungsverzeichnis

TSMONDO KI-Manager

EU-KI-Verordnung & ISO/IEC 42001 · lokal, ohne Cloud

←

→

↶

↷

Alles durchsuchen...

📧

Lizenziert · Muster Maschinenbau GmbH

Übersicht

KI-Projekte

Berichte

Verzeichnisse

Dokumente

Fristen

Zuständige

Regulatorik

Schulung

Stammdaten

System

Hilfe

✓ Projekt

✓ Rolle

✓ KI-System?

✓ Risiko-Triage

✓ Pflichten

✓ Risikomanagement

7 Querschnitt

8 Vorlagen

9 Plan & Gantt

Datenschutz – Übergabe an den Datenschutzbeauftragten

Diese Angaben gehen an die Datenschutzstelle, damit sie ohne Rückfragen entscheiden kann. Der KI-Manager führt selbst keine Datenschutz-Folgenabschätzung durch.

Verarbeitet das System personenbezogene Daten?

ja

Rechtsgrundlage der Verarbeitung

Berechtigtes Interesse (Art. 6 Abs. 1 lit. f)

Besondere Kategorien nach Art. 9 DSGVO betroffen?

nein

Kategorien personenbezogener Daten

Name, Kontaktdaten, Lebenslauf, Zeugnisse, Anschreiben, Angaben zu Qualifikation und Berufserfahrung

Betroffene Personengruppen

Bewerberinnen und Bewerber auf ausgeschriebene Stellen

Empfänger und eingebundene Dienstleister

Personalabteilung, einstellender Fachbereich, Anbieter des Auswertungsdienstes als Auftragsverarbeiter

Datenstandort und Drittlandtransfer

Drittland mit Standardvertragsklauseln (SCC)

Speicherdauer oder Löschfrist

6 Monate nach Abschluss des Verfahrens

ASSISTENT · SCHRITT 7 · QUERSCHNITTSPFLICHTEN

SCHRITT 7 · SCHWELLWERT

Neun Kriterien, und eine ehrliche Antwort

Die Schwellwertanalyse klärt, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nötig ist. Drei Kriterien stammen aus der Verordnung selbst, sechs aus der Liste der Aufsichtsbehörden. Zu jedem angekreuzten gehört eine Begründung.

ERGEBNISVORSCHLAG DER SOFTWARE

„Ein Regelbeispiel nach Art. 35 Abs. 3 DSGVO ist erfüllt. Eine Folgenabschätzung ist durchzuführen — Entscheidung und Durchführung beim Datenschutzbeauftragten.“

 **TSMONDO KI-Manager**
EU-KI-Verordnung & ISO/IEC 42001 · lokal, ohne Cloud

←

→

↶

↷

🔍 Alles durchsuchen...

✉

Lizenziert · Muster Maschinenbau GmbH

Übersicht

KI-Projekte

Berichte

Verzeichnisse

Dokumente

Fristen

Zuständige

Regulatorik

Schulung

Stammdaten

System

Hilfe

✓ Projekt

✓ Rolle

✓ KI-System?

✓ Risiko-Triage

✓ Pflichten

✓ Risikomanagement

7 Querschnitt

8 Vorlagen

9 Plan & Gantt

Schwellwertanalyse nach Art. 35 DSGVO

Ankreuzen, was auf dieses KI-System zutrifft. Die drei Regelbeispiele der Verordnung lösen die DSFA-Pflicht unmittelbar aus; die übrigen Kriterien stammen aus der Liste der Aufsichtsbehörden.

☒ **Systematische und umfassende Bewertung persönlicher Aspekte, etwa Scoring, Profiling oder automatisierte Entscheidungen mit Rechtswirkung.**
Art. 35 Abs. 3 lit. a · Regelbeispiel der Verordnung

Das System bildet eine Rangfolge der Bewerbungen und bereitet damit eine Personalentscheidung vor.

☐ **Umfangreiche Verarbeitung besonderer Kategorien nach Art. 9 DSGVO oder von Daten über strafrechtliche Verurteilungen nach Art. 10.**
Art. 35 Abs. 3 lit. b · Regelbeispiel der Verordnung

☐ **Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.**
Art. 35 Abs. 3 lit. c · Regelbeispiel der Verordnung

☒ **Verarbeitung in großem Umfang oder mit hoher Zahl betroffener Personen.**
DSK-Positionspapier

Je Ausschreibung werden 150 bis 400 Bewerbungen ausgewertet, im Jahr rund 3.000.

☐ **Zusammenführung von Datensätzen aus unterschiedlichen Quellen.**
DSK-Positionspapier

☒ **Daten besonders schutzbedürftiger Personen, etwa Kinder, Patienten oder Beschäftigte.**
DSK-Positionspapier

Bewerberinnen und Bewerber stehen in einem Abhängigkeitsverhältnis zum Unternehmen.

☒ **Innovative Nutzung neuer Technologien. Trifft bei KI-Systemen regelmäßig zu.**
DSK-Positionspapier

Eingesetzt wird ein Sprachmodell des Anbieters, das Freitexte auswertet.

☐ **Betroffene können ein Recht oder eine Leistung nicht in Anspruch nehmen, wenn sie nicht einwilligen.**
DSK-Positionspapier

☒ **Übermittlung in ein Drittland ohne Angemessenheitsbeschluss.**
Kriterium DSGVO

SCHWELLWERTANALYSE NACH ART. 35 DSGVO

LIEFEROBJEKT

Das Papier, das beim Datenschutzbeauftragten ankommt

Ein Dokument statt einer Mail mit Rückfragen: Einstufung nach EU-KI-Verordnung, alle Angaben zur Verarbeitung, die Schwellwertanalyse mit Begründungen — und am Ende ein leerer Block für die Entscheidung der Datenschutzstelle.

- Folgenabschätzung erforderlich, ja oder nein, mit Begründung
- Auflagen für den Betrieb
- Freigabe aus Sicht Datenschutz, mit Datum und Unterschrift

Wer die Datenschutzstelle im Haus hat, spart sich den Umweg. Wer sie extern hat, schickt ein Dokument statt einer Anfrage.

Stand

Wieder ansehen am

Fassung 1.0

Entwurf

31.08.2027

Solange hier Entwurf steht, gilt das Dokument als noch nicht in Kraft.

DSGVO-Übergabe an den Datenschutzbeauftragten

Angaben zur Verarbeitung und Schwellwertanalyse (Art. 35 DSGVO)

Organisation	Muster Maschinenbau GmbH
Anschrift	Industriestraße 12, 59302 Oelde, Deutschland
KI-System	Bewerber-Vorauswahl (CV-Screening)
Rolle	Betreiber
Risikoeinstufung	Hochrisiko-KI
Erstellt am	30.8.2026
Fassung	1.0 – Entwurf

Zweck dieser Übergabe

Dieses Dokument fasst die datenschutzrechtlich erheblichen Angaben zu einem KI-System zusammen und übergibt sie an die Datenschutzstelle. Es ist keine Datenschutz-Folgenabschätzung, sondern deren Vorbereitung: Es hält fest, was geprüft wurde, was zutrifft und worüber die Datenschutzstelle zu entscheiden hat.

Einstufung nach EU-KI-Verordnung

Beschäftigung (Anhang III Nr. 4) · Profiling – Art.-6(3)-Ausnahme ausgeschlossen

Angaben zur Verarbeitung

Personenbezogene Daten	ja
Rechtsgrundlage	Berechtigtes Interesse (Art. 6 Abs. 1 lit. f)
Besondere Kategorien (Art. 9)	nein
Datenkategorien	Name, Kontaktdaten, Lebenslauf, Zeugnisse, Anschreiben, Angaben zu Qualifikation und Berufserfahrung
Betroffene Personengruppen	Bewerberinnen und Bewerber auf ausgeschriebene Stellen
Empfänger und Dienstleister	Personalabteilung, einstellender Fachbereich, Anbieter des Auswertungsdienstes als Auftragsverarbeiter
Datenstandort und Drittland	Drittland mit Standardvertragsklauseln (SCC)
Speicherdauer / Löschfrist	6 Monate nach Abschluss des Verfahrens
Informationspflichten Art. 13/14	ja
Im Verarbeitungsverzeichnis	ja · VVT-014 Bewerbermanagement

Schwellwertanalyse nach Art. 35 DSGVO

Kriterium	Rechtsgrundlage	Trifft zu	Begründung
-----------	-----------------	-----------	------------

FRISTEN

Die gesetzliche Zeitachse läuft mit

Wann welche Pflicht der EU-KI-Verordnung greift, mit der Rechtsgrundlage je Zeile. Diese Termine gelten unabhängig davon, welche KI-Systeme im Haus laufen.

- Verschobene Fristen sind als verschoben gekennzeichnet, mit altem Datum
- Wo sich Quellen widersprechen, steht „Datum unbestätigt“ — in der Software, nicht in einer Fußnote
- Daneben die eigenen Prüf- und Wiedervorlagetermine je KI-System



TSMONDO KI-Manager

EU-KI-Verordnung & ISO/IEC 42001 · lokal, ohne Cloud

◀

▶

↶

↷

🔍

Alles durchsuchen...

✉

Lizenziert · Muster Maschinenbau GmbH

📁 Übersicht

📁 KI-Projekte

📁 Berichte

📁 Verzeichnisse

📁 Dokumente

📅 Fristen

👤 Zuständige

📊 Regulatorik

🎓 Schulung

📋 Stammdaten

⚙ System

🆘 Hilfe

Gesetzliche Termine der EU-KI-Verordnung

Diese Termine gelten unabhängig von euren KI-Systemen. Berücksichtigt ist die Digital-Omnibus-Verordnung (EU) 2026/1744, die den Geltungsbeginn für Hochrisiko-Systeme verschoben hat. Stand: 29.08.2026. Maßgeblich ist stets der Verordnungstext.

DATUM	WAS GILT	RECHTSGRUNDLAGE	STATUS
1.8.2024	Die KI-Verordnung tritt in Kraft	Art. 113 Abs. 1	gilt
2.2.2025	Verbotene Praktiken und die Pflicht zur KI-Kompetenz gelten	Art. 113 Abs. 3 lit. a (Kapitel I und II)	gilt
2.8.2025	Pflichten für KI-Modelle mit allgemeinem Verwendungszweck, Governance und Sanktionen	Art. 113 Abs. 3 lit. b	gilt
27.7.2026	Die Digital-Omnibus-Verordnung tritt in Kraft und verschiebt den Geltungsbeginn für Hochrisiko-Systeme	Verordnung (EU) 2026/1744	gilt
2.8.2026	Allgemeiner Geltungsbeginn, einschließlich der Transparenzpflichten nach Art. 50	Art. 113 Abs. 2	gilt
2.12.2026	Neue Verbote: nicht einvernehmliche intime Darstellungen und Missbrauchsmaterial Datum unbestätigt	Art. 5 Abs. 1 lit. ba und bb (neu)	steht bevor
2.12.2026	Kennzeichnungspflicht für generative Systeme, die vor dem 02.08.2026 in Verkehr gebracht wurden Datum unbestätigt	Art. 111 Abs. 4 (neu)	steht bevor
2.8.2027	KI-Modelle mit allgemeinem Verwendungszweck aus dem Bestand müssen konform sein	Art. 111 Abs. 3	steht bevor
2.12.2027	Hochrisiko-Systeme nach Anhang III: die Pflichten aus Kapitel III gelten (verschoben vom 02.08.2026)	Art. 113 Abs. 3 lit. c Ziff. i	steht bevor
2.8.2028	Hochrisiko-Systeme nach Anhang I, also KI als Sicherheitsbauteil regulierter Produkte (verschoben vom 02.08.2027)	Art. 113 Abs. 3 lit. c Ziff. ii	steht bevor
2.8.2030	Von Behörden genutzte Hochrisiko-Systeme aus dem Bestand müssen konform sein	Art. 111 Abs. 2	steht bevor

FRISTEN · GESETZLICHE TERMINE

Aufgaben hängen an Personen, nicht an Abteilungen

- Drei Ansichten: nach Person, als Kanban-Board, als Auslastung
- Jede Zeile nennt Rechtsgrundlage und KI-System
- Übergabe an die Beteiligten als CSV, Kalendereintrag, Mail oder PDF



Was den laufenden Betrieb trägt

Register für offene Punkte

Was auffällt, wird als Punkt erfasst statt als Notiz: Beschreibung, Ursache, Verantwortlicher, Termin, Status. Die Liste ist die Grundlage für den nächsten Bericht an die Geschäftsführung.

NICHTKONFORMITÄT

Schulung mit Namensliste

Acht Module zu Grundlagen, Kompetenzpflicht, Risikoklassen, Verboten, Transparenz, menschlicher Aufsicht, Datenschutz und Arbeitsalltag. Wer teilgenommen hat, steht namentlich im Schulungsnachweis.

ART. 4 · KI-KOMPETENZ

Berichte für die Geschäftsführung

Ein Bericht auf zwei Seiten: wie viele KI-Systeme laufen, wie sie eingestuft sind, welche Risiken offen sind, was ansteht. Dazu der Konformitätsbericht je System und ein Dossier über alles.

BERICHTE

Auf dem eigenen Rechner, ohne Konto

Lokal statt Cloud

Ein Programm für Windows, portabel, ohne Installation und ohne Administratorrechte. Es gibt kein Benutzerkonto, keine Anmeldung und keinen Server, der die Daten sieht.

WINDOWS · PORTABEL

Auf der eigenen Platte

Die Daten liegen in einer Datei auf dem eigenen Rechner oder in einem gemeinsamen Ordner. Auf Wunsch verschlüsselt die Anwendung sie mit AES-256; das schalten Sie mit einem Master-Passwort ein. Kein Auftragsverarbeitungsvertrag, kein Drittlandtransfer, keine Datenschutzfrage zum Werkzeug selbst.

VERSCHLÜSSELUNG ZUSCHALTBAR

Signiert und geprüft

Das Programm ist mit einem Zertifikat signiert; Windows meldet keinen unbekannten Herausgeber. Sicherung und Rücksicherung des Datenbestands sind eingebaut.

CODESIGNATUR

PREISE

Eine Lizenz für das ganze Unternehmen, gestaffelt nach Größe

BESCHÄFTIGTE IM UNTERNEHMEN	MONATLICH	JÄHRLICH
bis 49	49 € netto	499 € netto
50 bis 249	99 € netto	999 € netto
250 bis 999	199 € netto	1.990 € netto
1.000 bis 4.999	299 € netto	2.990 € netto
ab 5.000	auf Anfrage	auf Anfrage

Der Preis gilt je Unternehmen, nicht je Arbeitsplatz und nicht je KI-System — die Zahl der Nutzer ist nicht begrenzt. Eine GmbH & Co. KG zählt als ein Unternehmen; Tochter- und Schwestergesellschaften brauchen je eine eigene Lizenz. Vorab 21 Tage testen, voller Umfang, ohne Zahlungsdaten.



TSMONDO

KI-MANAGER · TSMONDO.DE