SOLVETRONIX

Embedded Systems & Legacy-Modernisierung

REGULATORISCHE ANALYSE

Drei EU-Verordnungen treffen Maschinen- und Anlagenhersteller gleichzeitig

CRA · EU AI Act · Maschinenverordnung 2023/1230

Was jedes Unternehmen wissen und tun muss, das Maschinen oder Anlagen auf den EU-Markt bringt | Version 2 — vom Vorstand geprüft

€ 35 Mio. max. Bußgeld EU AI Act (7 % Jahresumsatz)	**€ 15 Mio. max. Bußgeld CRA (2,5 % Jahresumsatz)**	**20.01.2027 Maschinenverordnung vollständig anwendbar**

*Stand: Juni 2026 · Auftraggeber: **Solvetronix** · Optimiert für Website-Publikation*

Das Wichtigste in Kürze

Jede Maschine mit Software ist jetzt ein reguliertes Produkt.
Drei EU-Verordnungen überschneiden sich — mit Fristen zwischen September 2026 und Januar 2027.

Wer heute Maschinen oder industrielle Anlagen für den EU-Markt entwickelt, produziert oder vertreibt, steht vor einem regulatorischen Wendepunkt, den kein Unternehmen ignorieren kann. Drei Verordnungen treten innerhalb von 18 Monaten vollständig in Kraft und treffen den Maschinenbau mit voller Wucht:

1 | Maschinenverordnung (EU) 2023/1230 — ab 20. Januar 2027

Ersetzt die Maschinenrichtlinie 2006/42/EG. KI-Komponenten in sicherheitsrelevanten Funktionen werden zu Hochrisiko-Komponenten. Software-Updates, die Sicherheitsfunktionen verändern, lösen neue CE-Verfahren aus. Jeder OEM mit installiertem Maschinenpark muss prüfen: Hat mein nächstes Update regulatorische Folgen?

2 | EU AI Act (EU) 2024/1689 — Hochrisiko ab 2. August 2026

Wer eine Maschine mit KI-Komponente auf den EU-Markt bringt, ist **Anbieter** (provider) im Sinne des EU AI Act. Für Hochrisiko-KI — einschließlich KI in sicherheitsrelevanten Maschinensteuerungen — gelten 12 eigenständige Pflichten: Risikomanagementsystem, technische Dokumentation, Post-Market-Monitoring, Registrierung in der EU-Datenbank und mehr. Bußgelder bis 35 Mio. € oder 7 % des Jahresumsatzes.

3 | Cyber Resilience Act (EU) 2024/2847 — Meldepflicht ab 11. September 2026

Jedes Gerät mit Firmware, Mikrocontroller oder vernetzter Software ist ein „Produkt mit digitalen Elementen“ nach CRA. Der Hersteller muss Security by Design nachweisen, Schwachstellenmanagement betreiben und aktiv ausgenutzte Schwachstellen innerhalb von 24 Stunden an ENISA melden. Vollständige Anwendung ab 11. Dezember 2027. Bußgelder bis 15 Mio. € oder 2,5 % des Jahresumsatzes.

Kernerkenntnis für Maschinenbauer: Diese drei Verordnungen sind keine parallelen Compliance-Themen, die nacheinander abgearbeitet werden können. Sie sind voneinander abhängig, teilen Dokumentationspflichten und erzeugen gleichzeitige Haftungsrisiken — für das Unternehmen und persönlich für die Geschäftsführung.

Zeitachse: Was wann gilt

Alle drei Verordnungen sind bereits in Kraft — die aktuellen Termine sind operative Pflichten, keine Ankündigungen:

Dez. 2024 CRA in Kraft	Feb. 2025 EU AI Act Art. 5	Jun. 2026 Notified Bodies	2. Aug. 2026 EU AI Act HR	11. Sep. 2026 CRA Meldung	20. Jan. 2027 MVO 2023/1230	11. Dez. 2027 CRA vollständig
Anpassung Entwicklungsprozesse beginnt	Verbotene KI-Praktiken gelten	Notified Bodies verfügbar	Hochrisiko-Pflichten scharf	24h-Meldung bei Schwachstellen	Maschinenverordnung vollständig	CE-Kennzeichnung Cybersecurity

⚠ **Kritisches Datum für Maschinenbauer: 11. September 2026**

In weniger als 90 Tagen tritt die CRA-Meldepflicht in Kraft. Wer kein Schwachstellenmanagement, keine Vulnerability Disclosure Policy und keinen Meldeweg zu ENISA hat, verstößt ab diesem Tag gegen geltendes EU-Recht — für jede Maschine mit Firmware oder eingebetteter Software.

---

1 | Maschinenverordnung (EU) 2023/1230

Was sich gegenüber der Maschinenrichtlinie 2006/42/EG ändert

Die Maschinenverordnung 2023/1230 ersetzt die Maschinenrichtlinie 2006/42/EG — das ist kein Update, sondern ein Systemwechsel. Vier zentrale Änderungen für Hersteller:

Maschinenrichtlinie 2006/42/EG (ALT)	Maschinenverordnung 2023/1230 (NEU)
Software kein eigenständiger Regelungsgegenstand	Software explizit Teil der Maschine
KI/ML: keine spezifischen Anforderungen	KI in Sicherheitsfunktionen = Hochrisiko-Komponente
Software-Updates nach CE ungeregelt	Wesentliche Änderung durch Update → neues Konformitätsverfahren
Sicherheitsfunktionen: klassische Elektrik/Mechanik	Einschließlich selbstlernender und adaptiver Systeme
Richtlinie → nationale Umsetzung nötig	Verordnung → direkt anwendbar in allen EU-Mitgliedstaaten

Kritische Frage für jeden OEM: Was ist eine „wesentliche Änderung"?

Art. 2 Abs. 3 MVO 2023/1230 definiert, wann eine Änderung an Maschine oder Software so wesentlich ist, dass ein neues Konformitätsbewertungsverfahren — einschließlich neuer CE-Kennzeichnung — ausgelöst wird:

- **Änderung führt zu neuem Risiko oder erhöht bestehendes Risiko**
- **Sicherheitsziel der ursprünglichen Konformitätsbewertung betroffen**
- **Ursprüngliche Risikobewertung nicht mehr gültig**
- **KI-Komponenten mit Sicherheitsfunktion: jede wesentliche Änderung am Modell oder Trainingsdaten**

Praxisbeispiel: Das OTA-Update, das alles ändert

Ein OEM liefert 3.000 Maschinen in 12 EU-Länder. Das nächste Software-Update optimiert ML-basiertes Sicherheitsmonitoring. Das Update verbessert die Erkennungsrate — und löst damit ein neues Konformitätsbewertungsverfahren aus.

Ohne vorherige Planung wäre das Update nach Art. 7 MVO 2023/1230 bis zum Abschluss der CE-Neubewertung unzulässig. Bei 3.000 installierten Maschinen mit derselben Software: alle betroffen.

KI in Sicherheitsfunktionen: neues Hochrisiko-Profil

Die Maschinenverordnung sieht besondere Anforderungen an Maschinen mit KI-basierten Sicherheitsfunktionen vor. Sie überschneiden sich direkt mit dem EU AI Act Hochrisiko-Profil (Anhang I). Relevante Szenarien in Prozess- und Fertigungsindustrie:

- Adaptives Sicherheitsabschalten auf Basis ML-Anomalieerkennung
- Kollisionserkennung in autonomer Robotik (Chemie-, Pharma-Anlagen)
- KI-gestützte Drucküberwachung und Ventilsteuerung in Prozessanlagen
- Predictive Maintenance mit Eingriff in Sicherheitskreise
- Bildverarbeitungssysteme zur Gefahrenzonenerkennung

Für alle diese Systeme ab 20. Januar 2027: Die technische Dokumentation muss die KI-Komponente explizit beschreiben, das Trainingsverfahren dokumentieren und Systemgrenzen nachweisen (Out-of-Distribution-Verhalten).

---

2 | EU AI Act (EU) 2024/1689

Wer Anbieter ist — und warum das für OEMs entscheidend ist

Der EU AI Act unterscheidet zwei Hauptrollen: Anbieter (provider) und Betreiber (deployer). Für Maschinenbauer ist die Rollenklärung existenziell: In der Regel sind sie Anbieter — nicht Betreiber.

Definition: Anbieter nach Art. 3 EU AI Act

Anbieter ist, wer ein KI-System entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke in Verkehr bringt oder in Betrieb nimmt — auch für den Eigenbedarf.

Für Maschinenbauer bedeutet das: Jede Maschine mit integrierter KI-Komponente, die an Kunden geliefert oder auf den EU-Markt gebracht wird, macht das Unternehmen zum Anbieter des KI-Systems.

Wann ist Maschinen-KI Hochrisiko? Anhang I × Anhang III

Die Hochrisiko-Klassifikation bestimmt den gesamten Pflichtenumfang. Zwei Wege führen zur Hochrisiko-Einstufung für Maschinenkomponenten:

Weg	Rechtsgrundlage	Praxisbeispiel Maschinenbau
Weg 1	Anhang I: KI in Produkten nach EU-Produktsicherheitsrecht (inkl. MVO 2023/1230)	Jede Maschine mit KI-Sicherheitsfunktion unter MVO — automatisch Hochrisiko
Weg 2	Anhang III Nr. 2: KI zur Steuerung kritischer Infrastruktur	Prozessanlagen mit KI-Steuerung in Chemie, Pharma, Energie

12 Pflichten nach Art. 16 EU AI Act — für jeden OEM

Für Anbieter von Hochrisiko-KI listet Art. 16 EU AI Act alle zwölf Pflichten auf, die vor und nach Markteinführung erfüllt sein müssen. Diese Liste ist die Prüfgrundlage der Marktüberwachungsbehörden:

- 1. Risikomanagementsystem einrichten und aufrechterhalten (Art. 9) — fortlaufender Prozess, kein Projektmilestone
- 1. Daten-Governance sicherstellen (Art. 10) — Trainingsdaten dokumentiert, Bias-Prüfung explizit Pflicht
- 1. Technische Dokumentation erstellen (Art. 11 + Anhang IV) — 10 Jahre aufbewahren
- 1. Protokollierung durch das System sicherstellen (Art. 12)
- 1. Transparenz für Betreiber gewährleisten (Art. 13)
- 1. Menschliche Aufsicht sicherstellen (Art. 14) — einschließlich physischem Not-Aus (Kill-Switch)
- 1. Genauigkeit, Robustheit und Cybersicherheit gewährleisten (Art. 15)
- 1. Qualitätsmanagementsystem einrichten (Art. 17)
- 1. Dokumentation nach Konformitätsbewertung aufbewahren (Art. 18)
- 1. Behörden Informationen bereitstellen (Art. 21)
- 1. Konformitätsbewertung durchführen (Art. 43) — vor Markteinführung
- 1. EU-Konformitätserklärung ausstellen, CE-Kennzeichnung anbringen, in EU-Datenbank registrieren (Art. 47–49)

Bußgelder EU AI Act: drei Stufen

€ 35 Mio. Verbotene KI-Praktiken (Art. 5) oder 7 % Jahresumsatz	**€ 15 Mio. Hochrisiko-Verstöße oder 3 % Jahresumsatz**	**€ 7,5 Mio. Sonstige Verstöße oder 1 % Jahresumsatz**

Rechenbeispiel: Was 3 % für einen mittelgroßen OEM bedeuten

Maschinenbauer mit 80 Mio. € Jahresumsatz, der eine Maschine mit nicht konformer Hochrisiko-KI auf den Markt bringt: 3 % = 2,4 Mio. € mögliches Bußgeld.

Bei 7 % für verbotene Praktiken: 5,6 Mio. €. Das KI-MIG (deutsches Umsetzungsgesetz, Kabinettsbeschluss Feb. 2026) enthält — anders als die DSGVO — keine nationale Bußgeld-Obergrenze.

---

3 | Cyber Resilience Act (EU) 2024/2847

Jede Maschine mit Firmware — „Produkt mit digitalen Elementen“

Der Cyber Resilience Act (CRA) trifft Maschinenbauer dort, wo viele noch nicht geplant haben: nicht das Unternehmen als IT-Betreiber, sondern die Maschine selbst als Produkt.

Definition: Produkt mit digitalen Elementen (Art. 3 CRA)

Jedes Software- oder Hardware-Produkt mit digitalen Elementen, das direkt oder indirekt mit einem Netzwerk oder Gerät verbunden werden kann — einschließlich Firmware, Betriebssysteme für eingebettete Geräte und Fernzugriffslösungen.

Für Maschinenbauer: MCU, PLC, SPS, IPC, Edge-Device, IoT-Gateway, Frequenzumrichter mit Firmware-Update, Steuereinheit mit OPC-UA-Schnittstelle — alles unter die Definition fallend.

Was CRA vom Maschinenhersteller verlangt

Security by Design — Anhang I, Teil I

- Keine bekannten ausnutzbaren Schwachstellen bei Markteinführung
- Secure-by-Default — keine Standardpasswörter, keine offenen Ports ohne Notwendigkeit
- Minimale Angriffsfläche: nur für die Funktion notwendige Schnittstellen
- Schutz vor unbefugtem Zugriff durch Authentifizierung
- Verschlüsselung sensibler Daten und Kommunikation
- Nachweis durch technische Dokumentation — nicht durch Selbsterklärung

Schwachstellenmanagement — Anhang I, Teil II

- Systematische Erfassung und Behebung von Schwachstellen über den gesamten Produktlebenszyklus
- Bereitstellung von Sicherheitsupdates mindestens 5 Jahre oder für die erwartete Nutzungsdauer
- Koordiniertes Vulnerability Disclosure Policy-Verfahren — muss bis 11.09.2026 definiert sein
- Dokumentation aller identifizierten Schwachstellen und ergriffener Maßnahmen

24-Stunden-Uhr: neue Meldepflicht ab 11. September 2026

Frist	Meldung	An wen	Was übermittelt wird
24 Stunden	Erstmeldung (Early Warning)	ENISA + cert.at / GovCERT Austria (operativer AT-Kontakt)	Hinweis auf aktiv ausgenutzte Schwachstelle
72 Stunden	Ergänzende Meldung	ENISA + cert.at / GovCERT Austria	Schweregrad, erste Ursachenanalyse
14 Tage nach Update	Abschlussbericht	ENISA + cert.at / GovCERT Austria	Vollständige Analyse, Maßnahmen, bereitgestellter Fix

Dramatische Folge für Legacy-Produkte im Feldeinsatz

CRA gilt für Produkte, die erstmals nach dem 11. Dezember 2027 auf den Markt gebracht werden. Aber: Die Meldepflicht für aktiv ausgenutzte Schwachstellen gilt ab 11. September 2026 — auch für Schwachstellen in bereits ausgelieferten Geräten.

Ein OEM mit 15-jährigem Maschinenpark, der eine kritische Firmware-Schwachstelle entdeckt, muss ab September 2026 melden. Ohne Schwachstellenmanagement, Meldeprozess und CSIRT-Kontakte: Verstoß ab dem ersten bekannten Vorfall.

Bußgelder CRA: drei Stufen

€ 15 Mio. Verstoß Anhang I oder 2,5 % Jahresumsatz	€ 10 Mio. Sonstige Verstöße oder 2 % Jahresumsatz	€ 5 Mio. Falschangaben oder 1 % Jahresumsatz

---

Kumulativer Effekt: Was OEMs mehrfach trifft

Vier Regelungsebenen sind keine isolierten „Silos“. Sie teilen Dokumentationspflichten, betreffen dieselben technischen Systeme und können durch denselben Vorfall ausgelöst werden:

Pflicht / Ereignis	MVO 2023/1230	EU AI Act	CRA	DSGVO / DSG 2018
Techn. Dokumentation	Anhang IV MVO	Art. 11 + Anhang IV	Art. 13 + Anhang V	Verarbeitungsverzeichnis Art. 30
KI-Sicherheitsfunktion	ESA-Anforderungen	Hochrisiko Art. 16	Security by Design	DSFA Art. 35 DSGVO
Software-/Firmware-Update	Wesentliche Änderung prüfen	Post-Market-Monitoring	Schwachstellenmanagement + OTA	Ggf. neue Rechtsgrundlage
CE-Kennzeichnung	CE nach MVO	CE für KI-Komponente	CE + Cybersecurity 2027	Nicht anwendbar
Vorfall/Schwachstelle	Rückruf/Korrektur	Marktüberwachung melden	24h cert.at + ENISA	72h DSB Wien Art. 33
Management-Haftung	Produkthaftung	Bußgeld bis 35 Mio.	Bußgeld bis 15 Mio.	Bußgeld bis 20 Mio.

Worst Case: ein Software-Vorfall, vier Behörden, vier Fristensysteme

ML-Sicherheitsmonitoring in einer Prozessanlage entdeckt eine aktiv ausgenutzte Schwachstelle. Das Bildverarbeitungssystem erfasst dabei Bewegungen von Mitarbeitern.

→ CRA: Meldung an cert.at / GovCERT Austria innerhalb von 24 Stunden
→ EU AI Act Art. 73: Meldung an nationale Marktüberwachung innerhalb von 2 Werktagen
→ DSGVO Art. 33 / DSG 2018: Meldung an DSB Wien innerhalb von 72 Stunden (bei personenbezogenen Daten)
→ NISG 2026: Meldung als kritische Infrastruktur innerhalb von 24 Stunden (ab 01.10.2026)

Vier Behörden, vier Meldeformate, vier Fristensysteme — gleichzeitig. Ohne vorbereitetes Incident-Response-Playbook kann kein Unternehmen handeln.

---

4 | DSGVO / DSG 2018 — wenn Maschinen personenbezogene Daten verarbeiten

Maschinen und Anlagen erfassen zunehmend Daten, die sich direkt oder indirekt auf Personen beziehen — Mitarbeiter, Bediener, Besucher. Neben den drei Produktverordnungen entsteht ein viertes Regelungsfeld: DSGVO (EU) 2016/679 und das österreichische Datenschutzgesetz (DSG 2018).

Wann Maschinendaten personenbezogen werden

Die Grenze ist oft unklar — für die österreichische Datenschutzbehörde in Wien (DSB) rechtlich eindeutig:

Bildverarbeitungssysteme (Kollisionserkennung, Qualitätskontrolle)	**Erfassen Bilder oder Bewegungsmuster von Personen → personenbezogene Daten; bei biometrischen Merkmalen: Art. 9 DSGVO (besondere Kategorien)**
ML-Performance-Monitoring von Maschinenbedienern	**Taktzeiten, Fehlerquoten, Eingriffsmuster je Mitarbeiter → Art. 22 DSGVO (automatisierte Einzelentscheidung mit erheblicher Auswirkung)**
Näherungssensoren in kollaborativer Robotik (Cobots)	**Erfassung von Aufenthaltsort und Bewegung → personenbezogene Daten; ggf. biometrische Ortung**

Sprachsteuerung und NLP-Schnittstellen	Stimmaufnahmen = biometrische Daten nach Art. 9 DSGVO — auch bei rein technischer Nutzung ohne Identifikationsabsicht

Drei relevante DSGVO-Artikel für Maschinenhersteller

- **Art. 6 DSGVO — Rechtsgrundlage:** Jede Verarbeitung personenbezogener Daten durch die Maschine erfordert eine dokumentierte Rechtsgrundlage (Einwilligung, berechtigtes Interesse, Vertragserfüllung). Der OEM muss den Endkunden informieren.
- **Art. 22 DSGVO — automatisierte Einzelentscheidungen:** ML-Prozesse mit erheblicher Auswirkung auf Personen (Leistungsbewertung, sicherheitsrelevantes Abschalten mit Personenbezug) sind anzeigepflichtig und müssen manuelle Übersteuerung ermöglichen.
- **Art. 35 DSGVO — Datenschutz-Folgenabschätzung (DSFA):** Bei hohem Risiko für Rechte und Freiheiten (biometrische Erfassung, systematische Überwachung) vor Inbetriebnahme DSFA durchführen. Für österreichische Unternehmen: zuständig ist DSB Wien (www.dsb.gv.at).

Doppelter Meldepfad CRA/DSGVO: zwei Uhren gleichzeitig

Wenn ein CRA-relevanter Sicherheitsvorfall an einer Maschine gleichzeitig personenbezogene Daten betrifft — typisch bei Bildverarbeitung, Bediener-Monitoring und Cobot-Näherungssensoren — gelten zwei vollständig getrennte Meldepflichten:

	CRA-Meldepfad	DSGVO-Meldepfad
Rechtsgrundlage	CRA Art. 14	DSGVO Art. 33 / DSG 2018
Frist (Erstmeldung)	24 Stunden	72 Stunden
An wen (Österreich)	cert.at / GovCERT Austria + ENISA	DSB Wien (www.dsb.gv.at)
Was gemeldet wird	Aktiv ausgenutzte Schwachstelle im Produkt	Verletzung des Schutzes personenbezogener Daten
Folgemeldung	Ergänzung 72h + Abschlussbericht 14d	Art. 34: Betroffene informieren bei hohem Risiko

Österreich-Spezifik: DSG 2018 und DSB Wien

Das österreichische Datenschutzgesetz (DSG 2018, BGBl. I Nr. 165/1999 idgF BGBl. I Nr. 74/2023) konkretisiert die DSGVO für Österreich. Für Maschinenbauer und österreichische Endkunden:

- **Zuständige Aufsichtsbehörde:** Datenschutzbehörde Wien (DSB Wien), Wickenburggasse 8, 1080 Wien | www.dsb.gv.at | dsb@dsb.gv.at
- **Bußgelder:** bis 20 Mio. € oder 4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist)
- **Schnittstelle ASchG:** ArbeitnehmerInnenschutzgesetz bei Mensch-Maschine-Kollaboration mit KI (Cobots, autonome Intralogistik) — Gefährdungsbeurteilung mit KI-spezifischen Risiken

---

5 | ArbVG §§ 96/96a — österreichische Day-1-Blocking-Condition

⛔ Für österreichische Endkunden (Arbeitgeber/Betreiber): kein Go-Live ohne Betriebsvereinbarung

Die am häufigsten übersehene Pflicht bei Maschinen mit Personendatenerfassung in österreichischen Betrieben. Sie liegt beim Endkunden — aber ein verantwortungsvoller OEM weist Kunden explizit darauf hin.

Das Arbeitsverfassungsgesetz (ArbVG) verpflichtet österreichische Arbeitgeber (Maschinenbetreiber), bestimmte Systeme vor Inbetriebnahme mit dem Betriebsrat zu vereinbaren. Ohne Vereinbarung ist der Einsatz rechtswidrig — unabhängig von CE-Kennzeichnung, EU AI Act-Compliance oder CRA-Zertifizierung.

§ 96 Abs. 1 Z 7 ArbVG — Betriebsvereinbarungspflicht

Die Einführung von Systemen zur Kontrolle von Verhalten oder Leistung von Arbeitnehmern erfordert eine Betriebsvereinbarung — in Form einer schriftlichen Kollektivvereinbarung. Ohne diese Vereinbarung darf das System nicht eingesetzt werden. Der Betriebsrat hat faktisches Vetorecht.

Betroffene Maschinensysteme:

- Alle Bildverarbeitungssysteme (Kameras, 3D-Sensoren) mit Erfassung von Mitarbeitern im Arbeitsbereich
- ML-Performance-Monitoring (Taktzeiten, Fehlerquoten je Bediener)
- Näherungssensoren in kollaborativer Robotik mit Speicherung von Personenanwesenheit
- Zugangskontrollsysteme mit biometrischer Komponente
- KI-Assistenten mit individueller Leistungsbewertung

§ 96a ArbVG — Mitbestimmung bei Datenverarbeitungssystemen

Systeme zur automatisierten Erfassung, Verarbeitung und Übermittlung von Daten über Arbeitnehmer müssen mit dem Betriebsrat besprochen werden. Bei fehlender Einigung kann ein Einigungsstelle-Verfahren (§ 96a Abs. 3 ArbVG) angerufen werden. Bis zur Entscheidung — kein produktiver Einsatz.

Praxisempfehlung für OEM: Was in technische Dokumentation und Betriebsanleitung gehört

Österreichische OEM und OEM mit österreichischen Kunden sollten explizit in technischer Dokumentation und Betriebsanleitung aufnehmen:

1. Welche personenbezogenen Daten das System erfasst, verarbeitet oder speichert
2. Ob und wie Mitarbeiter systematisch beobachtet, gemessen oder bewertet werden
3. Hinweis, dass vor Inbetriebnahme in österreichischen Betrieben ArbVG §§ 96/96a zu prüfen sind
4. Hinweis auf ASchG-Gefährdungsbeurteilung bei Mensch-Maschine-Kollaboration

Dieser Hinweis schützt den OEM vor Haftungsrisiken und positioniert ihn als verantwortungsvollen Anbieter gegenüber HR-Abteilungen und Betriebsräten.

---

6 | Technische Normen: Bewertungsgrundlage

Regulatorische Pflichten nach MVO 2023/1230, EU AI Act und CRA lassen sich ohne technische Normen nicht operationalisieren. Für Maschinenbauer sind zentral:

Norm	Inhalt	Relevanz MVO / EU AI Act / CRA
EN ISO 13849-1:2023	Funktionale Sicherheit Maschinensteuerungen — Performance Level (PL a–e)	MVO: Risikobewertung Sicherheitsfunktionen; EU AI Act: KI in PLr-relevanten Funktionen
IEC 62061:2021	Funktionale Sicherheit Maschinen — SIL 1–3	MVO: Alternative zu ISO 13849 für elektrische Sicherheitssysteme
IEC 61508:2010	Funktionale Sicherheit E/E/PE-Systeme	Basis für IEC 62061 und IEC 62443; relevant für adaptives KI in Sicherheitssteuerungen
IEC 62443-4-2:2019	OT/ICS-Sicherheitsanforderungen (Security Level SL-C 1–4)	CRA: Security by Design für SPS, IPC, Safety Controller, Industriegateways
IEC 62443-2-4:2015	Sicherheitsprogramm für IACS-Dienstleister	Relevant für Solvetronix als Dienstleister für Embedded-Modernisierung
ISO/IEC 42001:2023	KI-Managementsystem-Norm (AIMS) — international zertifizierbar	EU AI Act: Strukturrahmen für Art. 9 Risikomanagement + Art. 17 QMS; ~70–80 % AI Act-Abdeckung
OWASP Embedded Top 10	Sicherheitsanforderungen für Embedded Systems und Firmware	CRA: Basis für Firmware-Security-Audit; ergänzt IEC 62443 auf MCU/SoC-Ebene

Kritischer Hinweis: Fehlende harmonisierte Normen nach Art. 40 EU AI Act

Art. 40 EU AI Act erlaubt Konformitätsvermutung durch harmonisierte Normen. Für KI in Maschinen (Anhang I × MVO 2023/1230) existieren solche Normen **Stand Juni 2026 NICHT**.

Folge: Selbst korrekt durchgeführte Konformitätsbewertung nach Anhang VI EU AI Act (Selbstbewertung) ohne Normenreferenz schafft in der Aufsichtspraxis keine belastbare Rechtswirkung. OEM mit verpflichtender Drittparteibewertung nach MVO (Anhänge IX, X) müssen davon ausgehen, dass Notified Bodies diese auch für die KI-Komponente anwenden.

ISO/IEC 42001 kann als Strukturrahmen dienen, ersetzt aber keine EU AI Act-Konformitätsbewertung.

CRA Anhang II: Nicht alle Produkte gleich — Klassifikation entscheidet

CRA unterscheidet drei Produktkategorien mit unterschiedlichen Konformitätspfaden:

Kategorie	Anforderung	Typische Maschinenbau-Produkte
Standardprodukte	Selbstbewertung (Anhang IX) — ohne Notified Body	Einfache Sensoren, Standard-IoT-Geräte, Firmware ohne Sicherheitsfunktion
Wichtige Produkte Klasse I (Anhang II)	Selbstbewertung ODER freiwillige Drittparteizertifizierung; ohne harmonisierte Norm: Drittpartei Pflicht	Industrielle Firewalls, Standard-SPS, Industrierouter
Wichtige Produkte Klasse II (Anhang II)	Verpflichtende Bewertung durch akkreditierten Dritten	Safety Controller, Industriegateways mit Remote Access, SPS in kritischer Infrastruktur

SBOM — Software Bill of Materials: neue Pflicht ab 2027

Art. 13 CRA verpflichtet Hersteller von Produkten mit digitalen Elementen, eine SBOM zu erstellen und zu pführen — maschinenlesbares Verzeichnis aller Softwarekomponenten, Bibliotheken und Abhängigkeiten.

- **Format:** maschinenlesbar, bevorzugt CycloneDX oder SPDX — kein PDF-Listenformat
- **Inhalt:** alle Softwarekomponenten inkl. Open-Source-Bibliotheken, Versionsnummern, bekannte Schwachstellen (CVE-Referenzen)
- **Zweck:** Schwachstellen-Scanning ohne vollständigen Quellcodezugang; Basis für koordiniertes Disclosure
- **Praxisrelevanz:** Bei Legacy-Systemen mit undokumentierter Software-History ist SBOM-Erstellung oft der aufwendigste CRA-Schritt — ggf. Reverse Engineering der Abhängigkeiten nötig

GPAI in industriellen Anwendungen — unterschätzter Sonderfall

Neben spezialisierten KI-Modellen für Qualitätskontrolle oder Steuerung werden zunehmend GPAI-Modelle (General Purpose AI, Art. 51–56 EU AI Act) eingebettet — für natürlichsprachliche Maschinensteuerung, multimodale Qualitätsprüfung oder LLM-Wartungsassistenten.

GPAI in Maschinen: Art. 51 ff. EU AI Act — eigener Pflichtenkatalog

GPT-basierte Maschinensteuerung, CLIP/Vision-Language-Modelle für Qualitätskontrolle oder eingebettete Foundation Models unterliegen Art. 51 ff. EU AI Act — zusätzlich zu Hochrisiko-Anforderungen:

→ Art. 53: technische Dokumentation nach Anhang XI, Copyright-Strategie, Trainingsdaten-Zusammenfassung
→ Art. 55: bei systemischem Risiko (Training > 10^{25} FLOPs): Red Teaming, Systemrisiko-Bewertung, Vorfallmeldung an EU AI Office
→ GPAI Code of Practice (10. Juli 2025): verbindlicher Compliance-Rahmen für Anbieter eingebetteter Foundation Models

Praxisfrage für OEM: Integriere ich ein GPAI-Modell als Komponente in meine Maschine oder entwickle ich ein zweckgebundenes Modell? Die Antwort bestimmt, ob Art. 51 ff. zusätzlich zu Art. 16 gilt.

Was Solvetronix für Maschinenbauer und OEM leistet

Solvetronix verbindet tiefe Embedded-Expertise mit regulatorischem Verständnis — und hilft Maschinenbauern und Anlagenherstellern, drei Verordnungen nicht als Bürokratie, sondern als lösbare technische Aufgabe zu sehen.

Leistungen im Kontext der drei Verordnungen

CRA	EU AI Act	MVO 2023/1230
Firmware-Security-Audit nach OWASP Embedded Top 10	KI-Komponenten-Review: Risikoklassifikation Anhang I / III	Analyse wesentlicher Änderungen bei Software-Updates
Security-by-Design-Beratung für neue und Bestandsprodukte	Technische Dokumentation KI-Komponente (Art. 11)	Konformitätspfadanalyse für ML-Sicherheitsfunktionen
Vulnerability Disclosure Policy erstellen	Post-Market-Monitoring-Konzept für KI-Systeme	Risikobewertungs-Update für KI-erweiterte Maschinen
OTA-Update-Architektur (sichere Firmware-Rollouts)	Menschliche Aufsicht / Kill-Switch (Art. 14)	Legacy-Steuerungen CRA/MVO-konform bringen
Meldeprozess für 24h-CSIRT-Berichte aufbauen	Bias-Analyse Trainingsdaten (Art. 10)	Retrofit statt Ersatz — Dokumentation inklusive

Unser Einstiegsformat: Regulatory Readiness Check

Regulatory Readiness Check — in einem Tag

Für jeden Maschinenbauer, der wissen will, wo er heute steht:

1. **Produktinventur:** Welche Geräte/Maschinen fallen unter CRA, EU AI Act, MVO 2023/1230?
2. **Gap-Analyse:** Welche der drei Pflichtenprogramme erfüllt, welche nicht?
3. **Prioritätenmatrix:** Was muss bis September 2026 stehen — was kann bis Dezember 2027 warten?
4. **Maßnahmenplan:** Konkrete nächste Schritte mit Aufwandsschätzung

Ergebnis: Strukturiertes Dokument als Grundlage für interne Entscheidungen und Behördenanfragen.

Warum „modernisieren statt ersetzen“ jetzt regulatorisch sinnvoll ist

Solvetronix spezialisiert sich auf Legacy-Modernisierung — genau der regulatorische Ansatz, der für Maschinenbauer Sinn ergibt:

- CRA verlangt Security by Design — erreichbar durch Firmware-Härtung und Retrofit ohne neue Hardware
- MVO 2023/1230 erfordert keinen Ersatz bei Software-Updates — wenn die Änderung nicht wesentlich ist, bleibt bestehende CE gültig

- EU AI Act Art. 43 Abs. 1: Für Maschinen unter MVO 2023/1230 (Anhang I) folgt der KI-Konformitätspfad dem Produktsicherheitsrecht — wo MVO Drittparteibewertung vorschreibt, gilt das auch für die KI-Komponente
- EOL-Komponenten + neue Compliance-Anforderungen: Firmware-Redesign oft günstiger als Maschinenersatz

---

Quellenverweise

Alle regulatorischen Angaben basieren auf folgenden offiziellen Quellen (Stand Juni 2026):

- Verordnung (EU) 2023/1230 über Maschinen — Amtsblatt der EU, 29.06.2023
- Verordnung (EU) 2024/1689 (EU AI Act) — Amtsblatt der EU, 12.07.2024
- Verordnung (EU) 2024/2847 (Cyber Resilience Act) — Amtsblatt der EU, 20.11.2024
- Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO); österreichisches Datenschutzgesetz (DSG 2018) — BGBl. I Nr. 165/1999 idgF BGBl. I Nr. 74/2023
- NISG 2026 — Netz- und Informationssystemsicherheitsgesetz 2026 (BGBl. I Nr. 94/2025)
- IEC 62443 (Industrial Automation and Control Systems Security), EN ISO 13849-1 (Funktionale Sicherheit), IEC 61508 (Safety Integrity Levels)
- ISO/IEC 42001:2023 (AI Management System Standard)
- EU AI Act Compliance Checker — artificialintelligenceact.eu
- Fraunhofer IESE, TÜV Rheinland — Leitfäden zur Umsetzung MVO 2023/1230 und EU AI Act (2025/2026)

Hinweis DORA: DORA (Verordnung EU 2022/2554) gilt für Finanzinstitute, nicht für Maschinenbauer. Relevanter Sonderfall: OEM als IKT-Dienstleister für Finanzinstitute (Geldautomaten, Zahlungsterminals, Rechenzentrumsinfrastruktur) — dann gilt DORA Art. 28 (IKT-Drittparteien-Risikomanagement). Für Standard-Maschinenbauer ohne Finanzsektor-Bezug entstehen keine DORA-Pflichten.

Hinweis: Dieses Dokument dient der Information und ersetzt keine Rechtsberatung. Regulatorische Bewertungen im Einzelfall sollten mit qualifizierten Rechts- und Compliance-Experten abgestimmt werden.