1 Überblick: Von der Richtlinie zur Verordnung

1.1 Warum die Änderung?

Aus „Bitte setzt das national um“ wird „Gilt in jedem Mitgliedstaat eins zu eins.“ Das ist kein kleiner Unterschied – das ist ein Paradigmenwechsel.

Früher war es so: Die EU schrieb eine Richtlinie – die Maschinenrichtlinie 2006/42/EG war so eine. Diese Richtlinie sagte: „Hey Mitgliedstaaten, sorgt dafür, dass Maschinen sicher sind. Wie ihr das macht, ist eure Sache.“ Das Ergebnis: Jedes Land interpretierte das ein bisschen anders. Der deutsche Maschinenbauer hatte eine Norm (DIN EN ISO), der Italiener hatte eine andere, der Pole wieder eine. Das funktionierte – aber es war ineffizient und schuf Grauzonen.

Die EU vermittelt ihre bürokratischen Vorgaben hauptsächlich in zwei Darreichungsformen. Einmal gibt es Verordnungen und dann werden noch Richtlinien verabschiedet. Eine EU-Verordnung ist wie ein Gesetz. Sie gilt in allen Ländern der EU gleich. Grundlage für die Interpretation des Verordnungstextes liefern EU-Rat und Parlament gleich großzügig mit. In den sog. Erwägungsgründen (ErwG) steht, was die Verordnungsgeber mit einer Bestimmung beabsichtigen und zum Teil auch, wie sie sich die Umsetzung vorstellen. Abweichende Regelungen, die Grauzonen schaffen könnten, entfallen. Anhang II der Maschinenverordnung (EU) 2023/1230 mit der nicht erschöpfenden Liste der Sicherheitsbauteile entspricht dem „Anhang II“ der deutschen Fassung und dem „II. Melléklet“ der ungarischen Fassung derselben Verordnung. Das ist für einen europäischen Markt praktisch, aber es ist auch starrer.

Warum zieht die EU jetzt an? Weil Maschinen heute nicht mehr die Maschinen von 2006 sind:

Vernetzung: Damals waren Maschinen noch lokal. Sie sprachen über Feldbus miteinander, aber nicht übers Internet. Heute sind sie online und das als Standardfeature.

Digitale Elemente: Firmware-Updates, Cloud-Anbindung, IoT-Sensoren – das war 2006 Zukunftsmusik. Heute ist das Standard. Und jedes digitale Element ist ein potenzieller Angriffsvektor.

KI und Automatisierung: Maschinen treffen heute selbstständig Entscheidungen (Fehlererkennung, Prognosen, adaptive Steuerung). 2006 war das Science-Fiction, da dachten wir höchsten an den steirischen Terminator.

Cyber-Bedrohung: Ransomware, Manipulation, Sabotage – das war in den 1990er-Jahren noch nicht im Fokus. Heute ist das real. Cyberangriffe verursachten 2025 Schäden in Höhe von 289 Mrd. € für die deutsche Wirtschaft und betrafen 87 % der

Unternehmen, vorwiegend KMU. Es gibt Fälle, in denen Maschinen durch Cyberangriffe stillgelegt oder sabotiert wurden.

Die EU-Kommission erkannte: Die alte Maschinenrichtlinie passt nicht mehr. Eine Verordnung mit neuen, klaren Standards war überfällig. **Diese Verordnung heißt EU 2023/1230.** und enthält einen fundamentalen Wandel in der Sicherheitsphilosophie. Ziel ist es nicht mehr nur Menschen und Umwelt vor Schäden durch Maschinen zu schützen, sondern auch die Maschinen selbst vor unbefugtem Zugriff zu schützen.

1.2 Zeitschiene und Übergangsfristen

Der 20. Januar 2027 ist der Stichtag. Aber es ist nicht so, dass alles vorher legal ist und danach illegal wird. Die Realität ist etwas differenzierter.

Das zeitliche Gefüge

Bis 19. Januar 2027: Die alte Maschinenrichtlinie (2006/42/EG) gilt. Einige Teile der neuen Maschinenverordnung EU 2023/1230 gelten bereits. Sie betreffen Marktüberwachung und die sog. notifizierte Stellen. Diese schon in Kraft gesetzten Paragrafen ermöglichen den Mitgliedstaaten die Umsetzung der Maschinenverordnung vorzubereiten. Mehr nicht. Für die Rechtsanwender, also für Maschinenhersteller etc. gilt das Produktregelwerk der Maschinenrichtlinie (2006/42/EG), und zwar bis 19. Januar 2027.

Ab 20. Januar 2027: Die neue Verordnung ist vollständig anwendbar. Nur noch Maschinen, die nach der neuen Verordnung konform sind, dürfen neu auf den Markt. Die Maschinenrichtlinie gilt nicht mehr.

Bestandsschutz bis 2029: Maschinen, die vor 2027 nach der Maschinenrichtlinie eine CE-Kennzeichnung erhalten haben, dürfen weiterlaufen und instandgehalten werden. Aber: Reparaturen und Instandhaltung müssen auch weiterhin sicher erfolgen. Wenn dich ein Betreiber fragt, „darf ich meine alte Maschine noch nutzen?“, lautet die Antwort: Ja, aber nur mit angemessenem Wartungsstandard. Einen festen „Bestandsschutz bis 2029“ nennt die Verordnung nicht. Ein Grund dafür ist, dass die Maschinenverordnung EU 2023/1230 (MVO) wie auch die Maschinenrichtlinie 2006/42/EG sich in erster Linie an Maschinenhersteller richten und nur indirekt die Betreiber von Maschinen betreffen (mehr dazu siehe unten; für den sicheren Betrieb sind die Betriebssicherheitsverordnung (BetrSichV) bzw. die Technischen Regeln wie die TRBS 1115-1 zuständig, siehe dazu auch unten das Kapitel zur Compliance). Kurz gesagt: Maschinen, die vor dem 20. Januar 2027 in Verkehr gebracht oder in Betrieb genommen wurden, dürfen grundsätzlich weiter betrieben werden; eine wesentliche Veränderung kann aber neue Herstellerpflichten auslösen.

Die Falle für Hersteller: Viele Hersteller denken: „Okay, ich habe noch Zeit. Ich kümmere mich Ende 2026." Das ist ein Fehler. Hier ist warum:

Entwicklung, Testing und Dokumentation brauchen Zeit. Wenn du im Herbst 2026 anfängst, bist du Anfang 2027 noch nicht fertig.

Deine Kunden (Betreiber) wollen nicht die letzte Maschine vor dem Stichtag, weil sie befürchten, dass spätere Umbauten wahrscheinlich nach neuem Recht bewertet werden. Das ist für sie strategisch riskant.

Außerdem müssen deine Kunden – die Betreiber von Maschinen – vielleicht schon bald selbst die Konformität bei Umrüstungen erklären?

Konkurrenten, die 2025 anfangen, sind 2027 schneller am Markt – und verkaufen vor dir.

Die Rechtslage für Betreiber: Altmaschinen dürfen weiter betrieben werden. Aber „betreiben" heißt nicht „beliebig herumbasteln". Wer ein großes Retrofit macht (z. B. Steuerung tauscht), wird zum Hersteller – und muss dann die neue Verordnung erfüllen. Das ist ein rechtliches Risiko, das viele Betreiber unterschätzen.

Kurz: Wer die Übergangsfrist zum Aussitzen nutzt, plant sein eigenes Lieferverbot.

1.3 Wer ist betroffen?

Die einfache Antwort: Fast jeder, der mit Maschinen zu tun hat.

Für die Praxis sind drei Begriffe entscheidend: „Bereitstellung auf dem Markt" (jede Abgabe eines Produkts im EU-Markt), „Inverkehrbringen" (erstmalige Bereitstellung auf dem Markt) und „Inbetriebnahme" (erstmalige bestimmungsgemäße Verwendung). Diese Begriffe entscheiden, welches Recht wann greift – und wer welche Rolle/Haftung hat.

Hersteller – das ist klar. Wenn du eine Maschine designst und auf den Markt bringst, musst du die Maschinenverordnung erfüllen.

Importeure und Händler – auch betroffen. Wenn du eine Maschine importierst und weiterverkaufst, haftest du mit dafür, dass sie den europäischen Vorschriften entspricht. Du kannst dich nicht einfach auf den Hersteller ausreden. Ein Nicht-EU-Hersteller braucht einen Bevollmächtigten (Authorised Representative). Also können Nicht-EU Hersteller einen Bevollmächtigten in der EU schriftlich mandatieren. Der Bevollmächtigte übernimmt klar definierte Aufgaben (z. B. Dokumente bereithalten, Behördenkontakt) – die Gesamtverantwortung des Herstellers bleibt aber bestehen. Der Bevollmächtigte ist sozusagen der juristische Ansprechpartner.

Betreiber – auch betroffen, aber subtiler. Solange du die Maschine wie vorgesehen verwendest, ist die Haftung für ein fehlerhaftes Produkt das Problem des Herstellers und Fehler – Konstruktionsfehler – liegen dann vor, wenn die Maschine nicht die Sicherheit bietet, die man unter Berücksichtigung aller Umstände (insbesondere Gebrauchsanleitung, Vernunft, Zweck) erwarten kann. Aber sobald du etwas Wesentliches veränderst (Retrofit, große Modifikation), wirst du selbst zum Hersteller. Und dann schuldest du die gleiche Konformität, d. h., du haftest dafür, dass die Maschine die Sicherheit bietet, die man unter Berücksichtigung aller Umstände erwarten kann.

Die gefährdetste Gruppe: „Heimliche Hersteller“ – das sind Betreiber, die ihre alte Maschine „smartmachen“ wollen. Ein bisschen IoT-Sensor hier, ein bisschen Cloud-Anbindung da, vielleicht noch ein KI-Modul für Fehlervorhersage. Das klingt modern – aber rechtlich kann das der Punkt sein, wo die Maschine als „wesentlich verändert“ gilt und der Betreiber Hersteller wird. Mit allen Konsequenzen.

Service-Dienstleister und Integratoren – auch betroffen. Wenn du eine alte Maschine erweiterst oder wenn du Software installierst, die Sicherheitsfunktionen beeinflusst, kannst du auch zum Hersteller werden.

Die unbequeme Wahrheit: Es reicht nicht, sich selbst als Betreiber zu definieren und zu hoffen, dass der Hersteller schon alles richtig macht. Wenn etwas schiefgeht, kann die Behörde – oder schlimmer: ein Anwalt im Schadensfall – dich auch als Hersteller reklassifizieren, wenn du genug an der Maschine gemacht hast.

2 Neue Anforderungen im Detail

2.1 Grundlegende Sicherheits- und Gesundheitsschutzanforderungen (Anhang III)

Das bekannte Fundament der Maschinensicherheit bleibt erhalten. Anhang III der neuen Verordnung nennt die gleichen grundlegenden Anforderungen wie die alte:

Mechanische Sicherheit: keine scharfen Kanten, keine Quetschstellen, keine fehlende Schutzeinrichtung und keine herabfallenden Teile. Das sind altbekannte Anforderungen – und sie gelten weiterhin.

Elektrische Sicherheit: Schutz vor Stromschlag, Brandschutz, Isolationen, Erdungen, Schutz vor elektrostatischer Aufladung. Auch das ist nicht neu – aber auch nicht weniger wichtig.

Funktionale Sicherheit: Not-Halt, Schutzfunktionen, sichere Stillsetzung, Prüfbarkeit etc. Das fällt auch in die Klassikerkategorie.

Aber: Neu hinzu kommt eine ganze Dimension, nämlich die digitalen Baustellen.

Die digitalen Baustellen

Software und Firmware: Die Maschine läuft heute auf Code. Dieser Code muss sicher sein. Das heißt: Schwachstellenanalyse, Update-Mechanismus, Schutz vor Manipulation.

Vernetzung: Die Maschine spricht mit der Außenwelt, aber auch mit anderen Maschinen. Das Netzwerk ist ein Vektor. Es muss geschützt sein – nicht so geschützt wie das Internetbanking (das ist nicht praktisch), aber angemessen.

Datenschnittstellen: Externe Systeme greifen auf die Maschine zu – Service-Dienstleister übers VPN, Betreiber über Web-Interface, Integrationen ins MES. Jeder Zugriffsweg ist ein potenzielles Risiko.

Das zentrale Netzwerk: Die Maschine muss sicher vernetzt laufen. Das ist eine Grundanforderung geworden.

Praktisch heißt das: Deine CE-Checkliste wird länger. Früher fragtest du: „Funktioniert die Schutztür?“ Jetzt fragst du auch: „Kann ein Hacker die Schutztürlogik manipulieren? Wenn ja: Wie schütze ich meine Maschine dagegen?“

2.2 Cybersicherheit als Schutzanforderung

Die Cyber-Anforderungen stehen im Anhang III der MVO – insbesondere unter Punkt 1.1.9 (Schutz gegen Manipulation/Korruption, inkl. Nachweis von Eingriffen in Hardware/Software) und 1.2.1 (Sicherheit und Zuverlässigkeit von Steuerungen, inkl. Schutz gegen böswillige Angriffe).

Praktisch verlangen diese Punkte u. a.:

1. sicherheitskritische Software/Daten eindeutig kennzeichnen,
2. Schutz gegen unbeabsichtigte und absichtliche Manipulation (z. B. Signaturen, Integritätsprüfungen, Rechtekonzept),
3. Nachweis/Logging von Eingriffen und Softwareänderungen,
4. Steuerungen so auslegen, dass sie auch „malicious attempts" mitdenken, wenn diese vernünftigerweise vorhersehbar sind (z. B. Remote-Zugriff, Service-VPN, Netzwerksegmente).

Bonus-Punkt für Hersteller: Wenn du Cyber-Schutzmechanismen nach einem EU-Cybersicherheits-Zertifizierungsschema (Cybersecurity Act, EU 2019/881) zertifizieren lässt und das Zertifikat die relevanten Punkte abdeckt, kann das eine Vermutungswirkung für die Anforderungen aus Anhang III (u. a. 1.1.9 und 1.2.1) der MVO unterstützen.

Das bedeutet, im Problemfall muss man dir nachweisen, dass du etwas falsch gemacht hast. Das ist eine im Streitfall sehr günstigen Ausgangspositionen, vorausgesetzt du hast nicht extremen Blödsinn gemacht.

Das EU-Parlament und der Rat sagen in der neuen Verordnung: Sicherheitsfunktionen dürfen durch Cyber-Ereignisse nicht beeinträchtigt werden.

Was das konkret heißt

Ein Hacker darf deine Schutztür nicht aushebeln können. Das ist eine konkrete Anforderung. Wenn jemand von außen, übers Netzwerk oder physisch, die Logik so manipulieren kann, dass die Schutztür nicht mehr blockiert, dann erfüllt deine Maschine nicht die Anforderung der EU-Maschinenverordnung.

Beispiele, die damit nicht mehr okay sind

Der Service-Dienstleister connectet mit Standard-Passwort und ändert die Schutztürlogik ab.

Die Parametrierung der Sicherheits-SPS hat keine Integritätsprüfung – wer die Parameter ändert, kann die sichere Geschwindigkeit auf „beliebig schnell" setzen.

Die Firmware wird regelmäßig aktualisiert, aber nach dem Update wird nicht geprüft, ob die Sicherheitsfunktionen noch funktionieren.

Das Netzwerk, auf dem Sicherheitssignale laufen, ist nicht getrennt vom Office-Netzwerk – wenn ein Office-Laptop gehackt wird, kann der Hacker auch die Sicherheitssignale sehen und manipulieren.

Das ist nicht kompliziert, aber es ist neu im Fokus.

Früher konnte man sagen: „Na ja, der Schaltschrank ist abgeschlossen, also ist das sicher." Heute ist die Antwort: „Ja, aber der Schaltschrank ist auch übers Netzwerk erreichbar. Also: Wie schützt du das Netzwerk?"

Die gute Nachricht: Die Anforderung ist klar. Du brauchst ein Schutzkonzept. Du brauchst regelmäßige Prüfungen. Du brauchst Dokumentation. Das ist nicht neu – das sind die gleichen Anforderungen wie für traditionelle Sicherheitsfunktionen. Nur dass die Cyber-Komponente jetzt mit einberechnet ist.

2.3 KI-Sicherheitskomponenten

KI in Maschinen ist Realität. Fehlererkennung, Prognosen, adaptive Steuerung, autonome Entscheidungen – das läuft heute in modernen Maschinen.

Die Verordnung stellt sich der Frage: Was passiert, wenn KI eine Sicherheitsfunktion beeinflusst?

Antwort: Dann wird die KI selbst zur sicherheitsrelevanten Komponente.

Das ist wichtig

Nicht jede KI ist kritisch. Ein KI-Modul, das die Taktzeit optimiert, ist an sich nicht sicherheitskritisch – wenn es fehlschlägt, wird die Maschine langsamer, aber nicht unsicher. Aber ein KI-Modul, das entscheidet, ob eine Person im Arbeitsbereich ist oder nicht (zur Aktivierung von Sicherheitsfunktionen), ist sicherheitskritisch.

Für sicherheitskritische KI brauchst du:

Transparenz: Du und der Betreiber müssen wissen, dass KI im Einsatz ist. Nicht versteckt – transparent.

Nachvollziehbarkeit: Die KI trifft eine Entscheidung (z. B. „Diese Vibration ist normal"). Ein Mensch muss nachvollziehen können, warum die KI diese Entscheidung traf. Das nennt man Explainability.

Menschliche Überwachung: Der Mensch darf sich nicht vollständig auf die KI verlassen. Es muss einen Mechanismus geben, um die KI zu überschreiben oder zu korrigieren. Es darf keine „vollautomatische" KI eingesetzt werden.

Logging: Alle Ereignisse, Eingaben, Ausgaben und Systemstatusmeldungen des verwendeten KI-Systems werden protokolliert. Im Ernstfall (Unfall, Audit) kannst du nachvollziehen: Was hat die KI entschieden? Wann? Basierend auf welchen Eingaben? Das nennt man neudeutsch Traceability.

Das größte Missverständnis: Viele denken: „KI ist ja Lernsystem, also kann ich nicht vorhersagen, was es tut." Falsch. Für sicherheitskritische Anwendungen musst du das vorhersagen können. Die KI muss entsprechend programmiert sein. Du musst goal drifts etc. verhindern können oder du darfst KI gar nicht einsetzen.

Die Botschaft: KI darf nicht zum Bauchgefühl im Schaltschrank werden. Sie darf nicht die Verantwortung ersetzen. Sie muss transparent sein, überwacht werden, und sie darf nicht die letztendliche Entscheidungsquelle für Sicherheit sein.

2.4 Digitale Produktpässe und Rückverfolgbarkeit

Der Begriff „Produktpass" ist in der Maschinenverordnung so nicht als Pflichtbegriff verankert. Was klar geregelt ist: digitale Bereitstellung von Betriebsanleitung/Erklärung, Nachweisbarkeit von Softwareständen sowie Schutz/Protokollierung von Eingriffen in sicherheitsrelevante Hard-/Software. Ggf. den Abschnitt eher als „digitale Anleitung/DoC + Software-Traceability" rahmen. Aber heute benennen wir das mal der Einfachheit halber als Produktpass.

Die Maschine bekommt also ihren digitalen „Steckbrief". Das ist nicht neu (Seriennummern gibt es schon lange), aber es wird viel strukturierter und digitaler.

Das muss dokumentiert werden

Softwarestand: Welche Firmware-Version läuft auf welcher Komponente? Und für jede Version: Wann wurde sie eingespielt? Wer hat das gemacht? War das Update signiert? Außerdem den Quellcode der sicherheitsrelevanten Software.

Änderungshistorie: Jede Änderung wird protokolliert. Nicht nur Software-Updates, auch Hardware-Austausch, Parametrierungen, Rekonfigurationen.

Sicherheitsrelevante Informationen: Die Programmierlogik der Schaltung, bekannte Schwachstellen, Patches, Workarounds. Wird der sicherheitsrelevante Betrieb durch Sensordaten gesteuert, sind ggf. die allgemeinen Merkmale, Fähigkeiten und Einschränkungen des verwendeten Systems sowie der Daten und der Entwicklungs-, Test- und Validierungsverfahren zu beschreiben. Das muss für die Maschine auffindbar sein.

QR-Code oder digitale Schnittstelle: Die Maschine selbst (oder eine zentrale Plattform) liefert diese Informationen auf Abruf. Behörde kommt, scannt einen Code, hat alle Infos, die sie berechtigterweise angefragt hat.

Warum das wichtig ist

Szenario: Eine Schwachstelle wird entdeckt. Du musst schnell wissen, welche Maschinen betroffen sind. Ohne Rückverfolgbarkeit: Du fragst deine Kunden, fragst deine Distributoren, fragst deine Service-Partner. Das dauert Wochen. Mit Rückverfolgbarkeit: Du hast eine zentrale Datenbank, siehst sofort, wo deine Maschinen sind und wo welche Versionen laufen.

Praktisch umsetzbar

Das ist nicht kompliziert. Es ist eine Struktur. Eine Datenbank (Excel reicht zum Start). Ein Prozess: Bei jedem Update wird dokumentiert. Bei jedem Patch wird verwaltet.

Aber: Wer das nicht tut und später eine Schwachstelle hat, kann schlecht nachvollziehen, welche Maschinen betroffen sind und hat ein Haftungsrisiko.