

Aktuelles zu CE-Produktvorschriften

Heinz Kogler,
Wirtschaftskammer Österreich/Enterprise Europe Network



Business Support on Your Doorstep



WIRTSCHAFTSKAMMER ÖSTERREICH

Aktueller Stand von neuen EU-Vorschriften

- EU-Maschinenverordnung
- Digitalisierung von Produktinformationen und Konformität
- Cyber Resilience Act: Cybersicherheit für digitale Produkte
- Safety vs. Security
- EU-Verordnung 2024/1689 über Künstliche Intelligenz (AI act)
- EU-Batterienverordnung

Maschinenverordnung (EU) 2023/1230

Regelt die **Sicherheits- und Gesundheitsanforderungen**, die bei Konstruktion und Bau von Maschinen und verwandten Produkten berücksichtigt werden müssen.

Sicherheit und Gesundheit von Personen und ggf. von Haustieren und Sachen sowie ggf. der Umwelt im Fokus

Keine Übergangsfrist: bis 19.01.2027 sind Maschinen nach der derzeit geltenden Maschinenrichtlinie 2006/42/EG in Verkehr zu bringen. **Ab 20. Januar 2027** muss hierfür die Maschinenverordnung (EU) 2023/1230 angewendet werden.



WIRTSCHAFTSKAMMER ÖSTERREICH

EU Maschinenverordnung 2023/1230/EU

Wesentliche Änderungen:

- Grundlegende Sicherheits- und Gesundheitsschutzanforderungen: künftig im Anhang III (statt MRL Anhang I)
- Gefährliche Maschinen in Anhang I (vgl. Anhang IV in MRL)
- Bestimmte Maschinen sind nur mit Einbeziehung einer „Benannten Stelle“ konformitätszubewerten (insbes.: abnehmbare Gelenkwellen, Fahrzeug-Hebebühnen, Sicherheitsbauteile mit maschinellem Lernen/KI)
- Sägen, Fräsen Spritzgussmaschinen u.Ä. sind wie bisher entweder durch die Anwendung harmonisierter Normen oder mit Benannter Stelle konformitätszubewerten.
- Spezifische Anforderungen an Cybersecurity
- Steuerungssoftware einer Maschine : Jede Steuerungslogik muss dokumentiert, nachvollziehbar und überprüfbar sein

Digitalisierung von Dokumentation/Instructions

Die EU-Maschinenverordnung erlaubt die Einführung digitaler Konformitätserklärungen und Betriebs- und Montageanleitungen.

Für B2B-Maschinen sind auch digitale Betriebsanleitungen zulässig.

Für nicht professionelle Nutzer (Konsumenten) sind weiterhin mindestens die Sicherheitsinformationen in Papierform zur Verfügung stellen.

Omnibus IV: Digitale Gebrauchsanweisungen; gemeinsame Spezifikationen

Digitale Gebrauchsanweisungen

Hersteller können Gebrauchsanweisungen digital bereitstellen, was Papier spart und den Zugang erleichtert.

Bei ernsthaften Risiken müssen Sicherheitsinformationen stets auch in Papierform verfügbar sein, um den Verbraucherschutz zu garantieren.

Gemeinsame (technische) Spezifikationen

Alternative Lösung zum Nachweis der Produktsicherheit bei "Normungsversagen", falls für risikoreiche Produkte keine harmonisierten Normen zustandekommen

Umsetzungsfrist: 24 Monate nach Annahme in Brüssel



WIRTSCHAFTSKAMMER ÖSTERREICH

Maschinenverordnung-Änderungen:

- ‘digital contact’ means any up-to-date and freely accessible online communication channel such as email addresses through which economic operators can be contacted without the need to register or to download or use additional applications specific to the economic operator;’
- manufacturers shall draw up the EU declaration of conformity, in digital format, in accordance with Article 21 and affix the CE marking
- ‘Manufacturers shall ensure that the machinery or related product is accompanied by the internet address or machine-readable code through which the EU declaration of conformity set out in Part A of Annex V can be directly accessed
- ‘Manufacturers shall, further to a reasoned request from a competent national authority, provide that authority, in digital format, with all the information and documentation necessary to demonstrate the conformity of the machinery

Änderungen von CE-Richtlinien (EMC, LVD, RohS...)

- ‘Manufacturers shall indicate, on the apparatus, their name, registered trade name or registered trademark as well as their postal address and digital contact or, where that is not possible, on its packaging or in a document accompanying the apparatus. The postal address and digital contact shall indicate a single point through which the manufacturer can be contacted.
- Manufacturers shall ensure that the apparatus is accompanied by instructions and information, in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned. The instructions and information may be provided in electronic form. In the case of apparatus intended for consumers or that can, under reasonably foreseeable conditions, be used by consumers, even if not intended for them, the manufacturer shall provide, in paper format, or mark on the apparatus, the information (instructions, manual). Such information shall be easily visible and legible for consumers.

Sicherheitsbauteile mit KI-Funktion

- Sind Hochrisiko-KI- Systeme laut EU- KI-Verordnung (Annex I)
- Durch die Klarstellungen bzw. Vereinfachungen durch den sog. AI-Omnibus werden parallele Pflichten aus beiden Verordnungen weitgehend vermieden.
- Vorrangig gelten die sektorspezifischen Anforderungen der Maschinen-Verordnung. Die materiellen Anforderungen an KI-gestützte Maschinen werden künftig sektorspezifisch in der Maschinen-Verordnung geregelt.
- Die Europäische Kommission soll die Anforderungen an KI im Maschinenbereich durch **delegierte Rechtsakte** zu Anhang III der Maschinen-Verordnung konkretisieren.
- Risikomanagement, Datenqualität, technische Dokumentation, Aufzeichnungspflichten, Transparenz, menschliche Aufsicht, Genauigkeit, Robustheit und Cybersicherheit. Die sektorspezifischen Vorgaben gelten **ab dem 2. August 2028**.

Cyber Resilience Act: Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

Sicherheitsziele der Verordnung

Die Verordnung soll sicherstellen, dass digitale Produkte weniger Schwachstellen aufweisen und die Hersteller für Cybersicherheit haften. Gilt für Produkte mit digitalen Elementen (auch Software), die eine Datenverbindung zu Geräten oder Netzwerken haben, während des gesamten Lebenszyklus

Anwendungsbereich der Verordnung

Seit 11. September 2026: Meldepflicht bei aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen

Ab 11.12.2027: alle Anforderungen gelten, inkl. CE-Kennzeichnung

Betroffene Akteure

Die Verordnung betrifft Hersteller, Händler und Einführer von digitalen Produkten



WIRTSCHAFTSKAMMER ÖSTERREICH

Klassifizierung der Produkte und betroffene Gruppen

Produktklassifikationen

Produkte werden in Standard, „wichtig Klasse I“ und „wichtig Klasse II“ sowie „kritisch“ eingeteilt

Standard-Produkte

Rund 90 Prozent der Produkte sind nicht kritisch, z.B. Smartphones, Festplatten, Monitore, Lautsprecher, PC-Spiele mit digitalen Komponenten

Wichtige Produkte Klasse 1: z.B. Passwortmanager, Sprachassistenten im Smarthome, Spielzeug mit Internetverbindung

Wichtige Produkte Klasse 2: z.B. Firewalls, manipulationssichere Mikroprozessoren

Kritische Produkte:

z.B. Hardwaregeräte mit Sicherheitsboxen, Smartcards einschließlich Secure Elements

Cyber Resilience Act/Konformitätsbewertung und Verfahren

Produktklassifizierung und Anforderungen

Wichtige und kritische Produkte unterliegen strengeren Konformitätsverfahren als Standardprodukte (letztere: Selbstbewertung). Hersteller können außerdem Klasse 1 Produkte selbst bewerten, falls harmonisierte Normen vorliegen.

Modul A: Interne Fertigungskontrolle

Hersteller bewerten selbst die Konformität ihrer Produkte durch interne Fertigungskontrollen ohne externe Prüfstellen.

Modul B und C: Baumusterprüfung

Notifizierte Stellen prüfen die Produktkonformität mittels Baumusterprüfung, gefolgt von interner Fertigungskontrolle durch den Hersteller.

Modul H: Umfassende Qualitätssicherung

Umfassende Qualitätssicherungsverfahren werden von notifizierten Stellen bewertet, um Herstellungsprozesse und Produktqualität sicherzustellen.



WIRTSCHAFTSKAMMER ÖSTERREICH

Sicherheit: Safety vs. Security

Ziel der EU-Maschinen-VO:

... die Sicherheit und Gesundheit von Personen, insbesondere von Arbeitnehmern und Verbrauchern, und gegebenenfalls von Haustieren und Sachen sowie, die Umwelt zu schützen.

(englisch: health and *safety* requirements)

Cybersicherheit (*IBM-Definition*): Menschen, Systeme und Daten durch den Einsatz verschiedener Technologien vor Cyberangriffen zu schützen.

- (englisch: *cybersecurity*)

Zu Cybersicherheitsbedrohungen gehören Ransomware und Malware, Phishing-Betrug, Datendiebstahl und Angriffe, die durch künstliche Intelligenz (KI) unterstützt werden.

Unternehmenssicherheit

- NIS 2 Netz- und Informationssystemsicherheit
- Ziel: Aufbau von Cybersicherheitskapazitäten, Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren (Utilities, Grundversorgung...) verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen

DORA Digital Operational Resilience Act

Für Finanzunternehmen:

- Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);
- Meldung schwerwiegender IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen an die zuständigen Behörden;
- Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle an die zuständigen Behörden;

Netz- und Informationssystemsicherheit NIS 2

Sektoren mit hoher Kritikalität:

Anlage 1

Betroffen sind **große und mittlere Unternehmen** aus folgenden Sektoren

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

Sonstige kritische Sektoren:

Anlage 2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie
- Lebensmittel (Produktion, Verarbeitung und Vertrieb)
- verarbeitendes/herstellendes Gewerbe
- Anbieter digitaler Dienste
- Forschungseinrichtungen

EU Verordnung 2024/1689 über Künstliche Intelligenz (AI act)

CE-Kennzeichnung für Anwendungen mit hohem Risiko für die Sicherheit von Personen oder deren Grundrechte (1)

- Ist seit dem **2.8.2026** für folgende Themen anzuwenden:
- Bestimmte kritische Infrastrukturen, z.B. Straßenverkehr sowie die Versorgung mit Wasser, Gas, Heizung und Strom;
- Bildung und berufliche Ausbildung, z.B. zur Bewertung von Lernergebnissen und zur Steuerung des Lernprozesses;
- Beschäftigung, Arbeitsmanagement und Zugang zur Selbstständigkeit, z.B. zur Schaltung gezielter Stellenanzeigen, zur Analyse und Filterung von Bewerbungen sowie zur Bewertung von Kandidaten;

EU Verordnung 2024/1689 über Künstliche Intelligenz (AI act)

CE-Kennzeichnung für Anwendungen mit hohem Risiko (2)

- Zugang zu wesentlichen privaten und öffentlichen Dienstleistungen und Leistungen (z.B. Gesundheitswesen), Bonitätsbewertung natürlicher Personen sowie Risikobewertung und Preisgestaltung im Zusammenhang mit Lebens- und Krankenversicherungen;
- Bestimmte Systeme in den Bereichen Strafverfolgung, Grenzkontrolle, Justizverwaltung und demokratische Prozesse;
- Biometrische Identifikation

In diesen Fällen ist verpflichtend:

- Anwendung Harmonisierter Normen
- und/oder Beauftragung einer Benannten Stelle



**CE-Kennzeichnung
erforderlich!**

EU Batterienverordnung 2023/1542

Gilt grundsätzlich für alle Batteriekategorien (von Knopfzelle bis Fahrzeug- und Industriebatterie)

- Hersteller müssen seit dem 18. August 2024 vor dem Inverkehrbringen oder der Inbetriebnahme die **CE-Kennzeichnung an Batterien** anbringen.
- CE-Kennzeichnung zeigt Einhaltung der EU-Anforderungen an Sicherheit, Gesundheitsschutz und Umweltschutz an.
- Hersteller (dh. nationaler Inverkehrbringer, inbes. auch Händler) muss im Herstellerregister eingetragen sein

Digitaler Batterie Pass:

- ab dem 18. Februar 2027 verpflichtend
- Gilt für Industrie- und E-Antriebsbatterien
- Inhalt: Bereitstellung umfangreicher Daten, z.B. CO₂-Bilanzen, Rohstoffherkunft, chemische Zusammensetzung und Recyclingfähigkeit



Business Support on Your Doorstep



Fragen?

Mag. Heinz Kogler
Enterprise Europe Network in der
Wirtschaftskammer Österreich

een@wko.at
www.wko.at/een
Tel 05 90 900 4206