Inhalt

Vorwort 9

Teil I: Die neue Maschinenverordnung (EU) 2023/1230 – Was ändert sich ab 20. Januar 2027? 13

1 Überblick: Von der Richtlinie zur Verordnung 15
1.1 Warum die Änderung? 15
1.2 Zeitschiene und Übergangsfristen. 16
1.3 Wer ist betroffen? 17

2 Neue Anforderungen im Detail 19
2.1 Grundlegende Sicherheits- und Gesundheitsschutzanforderungen (Anhang III) 19
2.2 Cybersicherheit als Schutzanforderung 20
2.3 KI-Sicherheitskomponenten 21
2.4 Digitale Produktpässe und Rückverfolgbarkeit 22

3 CE-Kennzeichnung unter neuer Maschinenverordnung 25
3.1 Konformitätsbewertungsverfahren (Artikel 25) 25
3.2 Technische Dokumentation: Was muss neu rein?. 29
3.3 EU-Konformitätserklärung (Artikel 21) 33

4 Die „Retrofit-Falle“: Wesentliche Veränderung (Artikel 3 Nr. 16 MVO) 37
4.1 Wann wird der Betreiber zum Hersteller?. 38
4.2 Rechtsfolgen einer wesentlichen Veränderung 51
4.3 Checkliste: Ist meine Änderung eine wesentliche Veränderung? 52

5 KI in Maschinen: Was Hersteller wissen müssen 57
5.1 Hochrisiko-KI vs. Standard-KI. 57
5.2 Anforderungen an Hochrisiko-KI. 57
5.3 Schnittstelle zur KI-Verordnung 58

Teil II: Cyber-Gefährdungsbeurteilung für Maschinen – Der technische Kern 63

6 Warum Cyber zur Safety-Frage wird 65
6.1 Der elektrotechnische Kern. 65
6.2 TRBS 1115 Teil 1: Cybersicherheit für MSR-Einrichtungen 66
6.3 Die Brücke: CRA + MRL + TRBS = neue Gefährdungsbeurteilung . . 67

7 Vorgehensmodell in 7 Schritten (praxistauglich) 69
7.1 Schritt 1: Safety-Funktionsliste erstellen (elektrotechnisch, nicht abstrakt) 69
7.2 Schritt 2: Digitale Einflüsse markieren („digitaler Schatten" jeder Safety-Funktion) 70
7.3 Schritt 3: Cyber-Szenarien als Safety-Versagen formulieren 71
7.4 Schritt 4: Exposition bewerten (elektrotechnisch greifbar) 72
7.5 Schritt 5: Maßnahmen definieren (zuerst Schutzfunktion, dann Komfort) 72
7.6 Schritt 6: Wirksamkeit prüfen und Änderungen beherrschen. 73
7.7 Schritt 7: Evidence Pack für CE zusammenstellen. 74

8 Technische Maßnahmen konkret. 75
8.1 Netzwerksegmentierung (Safety-Zonen) 75
8.2 Zugriffskontrolle (physisch + digital). 76
8.3 Firmware-Integrität & Update-Management 76
8.4 Fernwartung: Wie absichern? 78
8.5 Logging & Monitoring für Sicherheits-SPS/Antriebe 79

9 Prüfung & Dokumentation 81
9.1 Prüfung vor Inbetriebnahme (§ 15 BetrSichV). 81
9.2 Wiederkehrende Prüfung (§ 16 BetrSichV) 87
9.3 Cyber-Aspekte in Prüfprotokollen 87
9.4 Was muss in der technischen Dokumentation stehen? 87

Teil III: Fallbeispiele & Praxisanwendung. 89

10 Fall 1: CNC-Fräsmaschine mit Remote-Service 91
10.1 Ausgangslage 91
10.2 Cyber-Szenario (als Safety-Versagen) 91
10.3 Maßnahmenpaket (elektrotechnisch) 92
10.4 Konformitäts-Check-Fragen 2027 (CNC) 93

11 Fall 2: Verpackungsmaschine mit Formatwechsel 95
11.1 Ausgangslage 95
11.2 Cyber-Szenario 95
11.3 Maßnahmenpaket 96
11.4 Konformitäts-Check-Fragen 2027 (Verpackung) 102

12 Fall 3: Robotikzelle (Safety over Bus + externe Integrationen) . . 103
12.1 Ausgangslage 103
12.2 Cyber-Szenario 103
12.3 Maßnahmenpaket 104
12.4 Konformitäts-Check-Fragen 2027 (Robotikzelle) 110

Teil IV: Compliance-Essentials (kompakt) 113

13 CRA-Überblick: Was Maschinenhersteller 2026 wissen müssen 115
13.1 Geltungsbereich: „Digitale Elemente“ – betrifft meine Maschine? . . 115
13.2 Meldepflichten ab 11. September 2026 nach CRA. 117
13.3 CE-Kennzeichnung: CRA-Anforderungen parallel zu MRL/MVO . . 118
13.4 Schnellcheck: Bin ich CRA-pflichtig? 119

14 Haftung kompakt: Wer haftet wofür? 121
14.1 Hersteller vs. Betreiber bei wesentlicher Veränderung. 121
14.2 Produkthaftung bei Cyber-Vorfällen. 122
14.3 Organisationsverschulden: Was muss ich nachweisen? 123

15 Lieferantensteuerung & Einkauf. 125
15.1 Was muss ich von Komponentenherstellern verlangen?. 125
15.2 Firmware-Updates: Wer ist verantwortlich?. 126
15.3 Vertragsklauseln für Cyber-Absicherung 126

Teil V: Werkzeuge & Checklisten 129

16 Checklisten. 131
16.1 MRL-Konformitäts-Check 2027. 131
16.2 Cyber-Gefährdungsbeurteilung pro Safety-Funktion (Musterformular). 134
16.3 Remote-Service-Absicherung. 137

17 Mustervorlagen 139
17.1 Struktur „Technische Dokumentation mit Cyber-Kapitel“ 139
17.2 Prüfprotokoll Cyber-Aspekte (Anlage zu § 15/16 BetrSichV) 140
17.3 Freigabeprozess für Software-Updates an sicherheitsrelevanten MSR 144