

	integrated safety & compliance Ausgewählte Informationsquellen zur Umsetzung aktueller Anforderungen aufgrund des Einsatzes moderner Technologien	
Startseite Informationsseite	Diese Anwendung richtet sich ausschließlich an Unternehmen (gewerblicher Kontext). Die Inhalte werden fortlaufend angepasst.	
...	Impressum & Rechtliches	Datenschutz

Alle hier gegebenen Informationen wurden sorgfältig und nach bestem Wissen zusammengestellt und dienen Ihrer Information. Dennoch müssen die Angaben unverbindlich bleiben. Einzig und allein die verantwortlichen Wirtschaftsakteure tragen die Verantwortung für die Umsetzung relevanter Rechtsakte anhand der verbindlichen Texte der europäischen Gesetzgebung. Sollten Sie Fehler in der nachfolgenden Aufstellung festgestellt haben, bin ich Ihnen für einen Hinweis dankbar.

Achten Sie auch unbedingt auf den oben angegebenen Stand der Veröffentlichung. Da es sich bei den hier mitgegebenen Informationen z. T. noch um Entwürfe von Dokumenten handelt und die technische Entwicklung sehr dynamisch vorstättengeht, ist bei einer späteren Nutzung unbedingt vorher zu prüfen, inwieweit dort ge-nannte Inhalte noch stimmen.

Gern nehme ich auch Ihre Hinweise zur Ergänzung und Aktualisierung der Inhalte entgegen.

Für Beratungen im Zusammenhang mit zu den erfüllenden Rechtsvorschriften, wenn ein Produkt auf dem Markt bereitgestellt wird, im Allgemeinen und bei der Ausführung von EU-Konformitätsverfahren und Risikobeurteilungen im Speziellen, stehe ich Ihnen gern zur Verfügung: bialek@bialek-ing.de

Ingenieurbüro Jürgen Bialek

Beratender Ingenieur ~ Sachverständiger ~ Internat. Schweißfachingenieur

Certified Product Compliance Officer (EN ISO/IEC 17024)

Halsbrücker Str. 34, 09599 Freiberg (Sachs)

www.bialek-ing.de

Grundlagen

Der Einsatz moderner Steuerungen und neuer **Informations- und Kommunikationstechnologien** bei der Entwicklung moderner Produkte, z. B. von Maschinen verschafft den Herstellern entscheidende Wettbewerbsvorteile führt aber auch dazu, dass ebenso neuartige Risiken, die mit dem Einsatz dieser Technologien in Verbindung stehen, beherrschbar bleiben müssen.

Mit einer ganzen Reihe von Grundlagen-Rechtsakten definiert der Gesetzgeber (Europäische Union, ggf. mit nationalen Umsetzungen) Basis-Anforderungen - siehe z. B. hier:

https://wiki.product-compliance.net/doku.php?id=zusatzinformationen:lex_hn:p04:p04

Darüber hinaus gibt es konkretisierte Anforderungen, die z. B. mit der sogen. **KI-Verordnung** oder dem **Cyber Resilience Act** aufgestellt werden. Maßnahmen zum

Informationssicherheitsmanagement sind in den Blick zu nehmen.

Schließlich gibt es bereits heute detaillierte und zugeschnittene Anforderungen für eine ganze Reihe von Produktgruppen, wie z. B. die Funkanlagen oder die Maschinen, sofern sie mit sol-chen Technologien ausgestattet werden. Für weitere Produktgruppen stehen diese Aspekte ebenfalls an (z. B. Spielzeug).

Zur notwendigen und geregelten Weitergabe von Informationen von den Herstellern an die Verwender von Produkten wird in zunehmendem Maße auf Digitalisierung gesetzt. So sind der **Digitale Produktpass (DPP)** und vergleichbare Informationsinhalte die Basis dieser Anforderungen.

Für die konkrete Umsetzung gibt es bereits erste Normen, Spezifikationen und weitere Hilfestellungen. Weitere Inhalte liegen als Entwürfe vor oder müssen noch erarbeitet werden. Insgesamt ist jedoch von einer äußerst dynamischen Entwicklung auszugehen, bei der neue Dokumente und Informationen in recht kurzer „Schlagzahl“ veröffentlicht werden.

Deshalb soll hier, auch in Ergänzung einschlägiger Veröffentlichungen oder Seminarskripte eine Auflistung ausgewählter Maßnahmen zur Umsetzung bestehender und zukünftiger Anforderungen veröffentlicht und gepflegt werden.

Umsetzen neuer Anforderungen an die Ergonomie (Maschinen und andere technische Produkte) - Auswahl wichtiger Quellen

Grundsätze

- EN ISO 12100: Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung
 - hier speziell in dem Kapitel „Beachten ergonomischer Grundsätze“

!!! Die Norm wird derzeit umfassend überarbeitet !!!

- ISO/TR 22100-3: Implementierung ergonomischer Grundsätze in Sicherheitsnormen
- Normenreihe EN 614: Sicherheit von Maschinen – Ergonomische Gestaltungsgrundsätze, im Einzelnen mit:
 - Allgemeinen Leitsätzen ergonomischer Maschinengestaltung
 - Wechselwirkungen zwischen der Gestaltung von Maschinen und den Arbeitsaufgaben
 - Ergonomischen Grundsätzen für die Gestaltung mobiler Maschinen

!!! Teil 1 der Normenreihe wird derzeit umfassend überarbeitet !!!

Aspekte psychischer Arbeitsbelastung

- EN ISO 6385: Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen
- Normenreihe EN ISO 10075: Ergonomische Grundlagen bezüglich psychischer Arbeitsbelastung, im Einzelnen mit:
 - Allgemeinen Aspekten
 - Gestaltungsgrundsätzen
 - Verfahren zur Messung und Erfassung psychischer Arbeitsbelastungen

!!! Die gesamte Normenreihe wird derzeit umfassend überarbeitet !!!

Umsetzen neuer Anforderungen zur Mensch-System-Interaktion (z. B. Maschinen, Geräte etc.)

Maschinen- oder Produktentwicklung auf der Grundlage von Nutzungskonzepten

- Normenreihe EN 16710: Verfahren der Ergonomie, im Einzelnen mit:
 - Methode zum Verständnis wie Endnutzer ihre Arbeit mit Maschinen durchführen
 - Methode für die Arbeitsanalyse zur Unterstützung von Entwicklung und Design

!!! Teil 2 der Normenreihe wird derzeit umfassend überarbeitet !!!

- EN ISO 14738: Anthropometrische Anforderungen an die Gestaltung von Arbeitsplätzen für Industrie und Dienstleistungen
- DGUV-Information 209-068 und 209-069: Ergonomische Maschinengestaltung

Zugänge und Einstellbarkeit

- Normenreihe DIN 33402/ Normenreihe EN 547 / Normenreihe EN ISO 7250: Körpermaße des Menschen
- Normenreihe DIN 33411: Körperkräfte des Menschen / Normenreihe EN 1005: Menschliche körperliche Leistung
- DIN/TS 35444: Verfahren zur Messung von technisch notwendigen manuellen Betätigungskräften
- EN 13861: Leitfaden für die Anwendung von Ergonomie-Normen bei der Gestaltung von Maschinen
- Normenreihe EN ISO 15536: Computer-Manikins und Körperumrisschablonen
- harmonisierte Europäische Typ-C-Normen oder vergleichbare Systemanforderungen, z. B. für:
 - Erdbaumaschinen, Straßenbaufahrzeuge
 - Leitzentralen, etc.

Signalisierung und Bedienelemente

- EN ISO 7731: Gefahrensignale für öffentliche Bereiche und Arbeitsstätten - Akustische Gefahrensignale
- EN ISO 24500 ff.: Zugängliche Gestaltung (Signale, Sprachführung, etc.)
- EN 842: Optische Gefahrensignale - Allgemeine Anforderungen, Gestaltung und Prüfung
- Normenreihe EN 894: Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen
- EN 981: System akustischer und optischer Gefahrensignale und Informationssignale
- Normenreihe EN 61310: Anzeigen, Kennzeichen und Bedienen

Generelles und Interaktion

- Normenreihe DIN 33411: Körperkräfte des Menschen / Normenreihe EN 1005: Menschliche körperliche Leistung
- DIN/TS 35444: Verfahren zur Messung von technisch notwendigen manuellen Betätigungskräften
- EN 13861: Leitfaden für die Anwendung von Ergonomie-Normen bei der Gestaltung von Maschinen
- neuer Normenentwurf EN 17161: „Design für Alle“-Ansatz - Management der Barrierefreiheit von Produkten und Dienstleistungen
- EN 60447: Grund- und Sicherheitsregeln für die Mensch-Maschine-Schnittstelle, Kennzeichnung – Bedienungsgrundsätze
- neuer Normenentwurf EN IEC 62508: Leitlinien zu den menschlichen Aspekten der Zuverlässigkeit
- EN IEC 63303: Mensch-Maschine-Schnittstellen für Prozessautomatisierungssysteme
- EN 301549: Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen
- Normenreihe EN ISO 9241: (bisher unter dem Titel: Ergonomische Anforderungen für Bürotätigkeiten) Titel neuer Normenteile: Ergonomie der Mensch-System-Interaktion mit

folgenden beispielhaften Inhalten:

Gebrauchstauglichkeit: Begriffe und Konzept (Teil 11)	Interaktionsprinzipien (110)
Grundsätze der Informationsdarstellung (112)	Empfehlungen für die Gestaltung von konzeptuellem Design, Benutzer-System-Interaktion, Benutzungsschnittstellen und Navigation (115)
Empfehlungen zur visuellen Informationsdarstellung (125)	Empfehlungen zur auditiven Informationsdarstellung (126)
Leitlinien für die Individualisierung von Software (129)	Formulardialoge (143)
Leitlinien zur Gestaltung von Benutzungsschnittstellen für das World Wide Web (151)	Sprachdialogsysteme (154)
Leitfaden zu visuellen User-Interface-Elementen (161)	Leitlinien für die Barrierefreiheit von Software (171)
Menschzentrierte Gestaltung interaktiver System (210)	Prozesse zur Ermöglichung, Durchführung und Bewertung menschzentrierter Gestaltung für interaktive Systeme in Hersteller- und Betreiberorganisationen (220)
Einführung in die Anforderungen an elektronische optische Anzeigen (300)	Terminologie für elektronische optische Anzeigen (302)
Anforderungen an elektronische optische Anzeigen (303)	Rahmen und Anleitung zur Gestensteuerung (960)

Landscape Analysis Reports der Organisation StandICT.eu

LINK

- Report of TWG IoT & Edge: [Landscape of Internet of Things | V.2](#)
- [Landscape of Internet of Things \(IoT\) Standards](#)
- [IoT Standardisation Gaps](#)
- [Landscape of Robotics Standards](#)

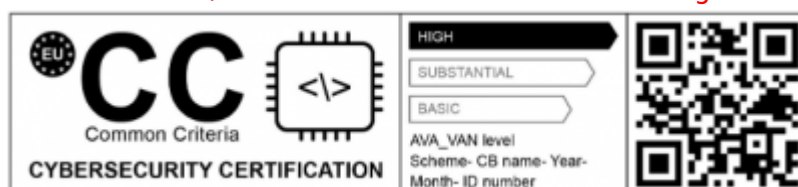
Umsetzung neuer Anforderungen in Bezug auf Cybersicherheit (Sicherheit der Informationstechnik) - Auswahl wichtiger Quellen

Allgemeines

Das Erfüllen der Anforderungen z. B. von Anhang III Nr. 1.1.9 der Maschinenverordnung (EU) 2023/1230 und damit Sicherheit gegen Korrumpierung installierter Systeme kann vorrangig erreicht werden durch:

- Einsatz (zugekaufter) zertifizierter Systeme (Hardware/ Software) nach der Verordnung (EU) 2019/881 („Cybersicherheits-Grundverordnung“) und der Verordnung (EU) 2024/482 in Bezug auf die gemeinsamen Kriterien der europäischen Cybersicherheitszertifizierung (EUCC)
- Entwicklung eigener Systeme, die diesen Anforderungen entsprechen

Der Einsatz solcher zertifizierter Systeme löst zudem die Konformitätsvermutung in Bezug auf Anhang III Nr. 1.1.9 und/oder 1.2.1 der Maschinenverordnung aus!



Basis der Zertifizierung sind die Anforderungen der Normenreihe EN ISO/IEC 15408 und der Norm EN ISO/IEC 18045 (auch mit neuen Normenentwürfen).

Gleiches trifft sinngemäß auf konforme (zertifizierte) Systeme nach den Verordnungen (EU) 2024/2847 („Cyber Resilience Act“) und (EU) 2024/1689 („KI-Verordnung“) zu.

Sind Sie bzw. sind Ihre Systeme von der KI-Verordnung betroffen?



Prüfen Sie es [HIER](#)

Erste normative Ansätze - Grundlagen

- EN ISO 12100: Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung

!!! Die Norm wird derzeit umfassend überarbeitet !!!

- neue Anforderungen speziell in dem Kapitel „Konstruktion von Steuerungen“

EN 40000er Reihe

- prEN 40000-1-1:2025: Cybersicherheitsanforderungen für Produkte mit digitalen Bestandteilen – Vokabular → **NEU: als DIN**
- prEN 40000-1-2:2025: ... Teil 1-2: Grundsätze für die Cyberresilienz → **NEU: als DIN**
- prEN 40000-1-3:2025: ... Teil 1-3: Umgang mit Schwachstellen → **NEU: als DIN**
- prEN 40000-1-4: ... Teil 1-4: Generic security requirements
- prEN 40000-1-5: ... Teil 1-5: Threats and security objectives
- prEN 40000-10:2026: ... Teil 10: Produkte mit digitalen Elementen, die in Identitätsmanagementsystemen und Software und Hardware für die Verwaltung des privilegierten Zugangs verwendet werden, einschließlich Authentifizierungs- und Zugangskontrollleser, einschließlich biometrischer Leser → **NEU: als DIN**
- prEN 40000-11:2026: ... Teil 11: Hardware-Geräte mit Sicherheitsboxen, die eine physische Hardware-Umhüllung enthalten und für die Bereitstellung von Sicherheitsfunktionen, wie sichere Speicherung und kryptografische Operationen in einer offenen Umgebung ausgelegt sind → **NEU: als DIN**

EN 507xx Reihe

- prEN 50742:2025: Sicherheit von Maschinen - Schutz vor Korruption → **NEU: als DIN**
- prEN 50764: Cybersecurity requirements for platforms of smartcards and similar devices including secure elements
- prEN 50765: Cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities
- prEN 50766: Cybersecurity requirements for tamper-resistant microprocessors and microcontrollers
- prEN 50767: Cybersecurity requirements for application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities

Security for Operational Technologies (based on EN IEC 62443)

- prEN 50770-1: ... Security Profile for firewalls and intrusion detection and prevention systems
- prEN 50770-2: ... Security Profile for network management systems
- prEN 50770-3: ... Security Profile for physical and virtual network interfaces
- prEN 50770-4: ... Security Profile for products with digital elements with the function of virtual private network (VPN)
- prEN 50770-5: ... Security Profile for routers, modems intended for the connection to the internet, and switches
- prEN 50770-6: ... Security Profile for security information and event management (SIEM) systems

Sonstige

- EN ISO/IEC 15408: Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit (Normenreihe im Entwurf)
- CLC IEC/TR 63074:2025: Maschinensicherheit - Security-Aspekte in Verbindung mit der funktionalen Sicherheit von sicherheitsbezogenen Steuerungssystemen

Siehe auch zusätzliche Informationen zur Normenreihe EN IEC 62443 hier unten im Abschnitt Umsetzung neuer Anforderungen zur Sicherheit von Maschinensteuerungen

Cybersecurity-Anforderungen für Funkanwendungen - ETSI EN 304 6xx Reihe

- prEN 304 617: Essential cybersecurity requirements for browsers
- prEN 304 618: Essential cybersecurity requirements for password managers
- prEN 304 619: Essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software
- prEN 304 620: Essential cybersecurity requirements for Virtual Private Networks (VPNs)
- prEN 304 621: Essential cybersecurity requirements for Network Management systems
- prEN 304 622: Essential cybersecurity requirements for Security information and event management (SIEM) systems
- prEN 304 623: Essential cybersecurity requirements for boot managers
- prEN 304 624: Essential cybersecurity requirements for Public key infrastructure and digital certificate issuance software
- prEN 304 625: Essential cybersecurity requirements for physical and virtual network interfaces
- prEN 304 626: Essential cybersecurity requirements for operating systems
- prEN 304 627: Essential cybersecurity requirements for routers, modems intended for the

connection to the internet, and switches

- prEN 304 631: Essential cybersecurity requirements for smart home general purpose virtual assistants
- prEN 304 632: Essential cybersecurity requirements for smart home products with security functionalities; including smart door locks, security cameras, baby monitoring systems and alarm systems
- prEN 304 633: Essential cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features
- prEN 304 634: Essential cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring purpose and for personal wearable products that are intended for the use by and for children
- prEN 304 635: Essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
- prEN 304 636: Essential cybersecurity requirements for firewalls, intrusion detection and/or prevention systems
- prEN 304 642: Cybersecurity Requirements for Network Functions of Telecommunications Systems

Normungsauftrag der Europäischen Kommission

[LINK](#)

Der Normungsauftrag der Europäischen Kommission umfasst insgesamt 41 Einzelpositionen, die bis zum 30.10.2026 bzw. 30.10.2027 von den Normungsgremien zu erarbeiten sind.

Maschinen und Cybersicherheit und das BSI

Neben den bereits spätestens ab dem 20.01.2027 umzusetzenden Anforderungen der Maschinenverordnung zum Schutz gegen Korruption und zur besonderen Sicherheit von Steuerungen (Cybersicherheit im weitesten Sinne) ist ab dem 11.12.2027 zusätzlich die [Verordnung \(EU\) 2024/2847 \(„Cyber Resilience Act“\)](#) anzuwenden.

In dieser Rechtsverordnung geht es um auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt (Art. 2, Abs. 1 der VO (EU) 2024/2847). Ausnahmen vom Anwendungsbereich oder spezielle Einschränkungen werden mit den weiteren Absätzen des Artikels 2 beschrieben.

Bereits zu einem früheren Zeitpunkt (11.09.2026) greift die Meldepflicht von Herstellern betroffener Systeme in Bezug auf jede ausgenutzte Schwachstelle, die in einem Produkt mit digitalen Elementen enthalten sind.

Ergänzende Informationen finden Sie auf der Homepage der Europäischen Kommission [**Cyber Resilience Act - Implementation**](#)

Für eine erste Positionierung finden Sie u. a. auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umfassende Informationen, z. B.: • Übersicht zum Cyber Resilience Act • Management-Blitzlicht zu den wichtigsten Fragen des CRA • Flyer: Wie mache ich meine Produkte fit für eine (cyber-)sichere Zukunft • Flyer: Wie werden Produkte klassifiziert und welche Arten von Konformitätsnachweisen gibt es • Flyer: Drittstellenbewertung – welches Konformitätsbewertungsmodul ist für mein Produkt geeignet

From:
<https://www.product-compliance.net/> - **Product Compliance**

Permanent link:
https://www.product-compliance.net/doku.php?id=zusatzinformationen:anforderungen_umsetzen&rev=1783937396

Last update: **2026/07/13 12:09**

