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 vonstattengeht, 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 Resiliance Act** aufgestellt werden. Maßnahmen zum **Informationssicherheitsmanagament** 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 Körperumrissschablonen
- 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

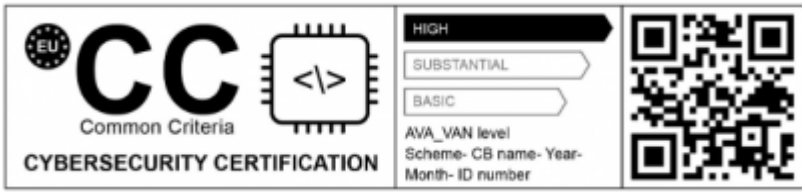
Umsetzung neuer Anforderungen in Bezug auf Cybersicherheit (Sicherheit der Informationstechnik) – Auswahl wichtiger Quellen

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 vorran-gig 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 (AS IC) 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 Privatsphä-re - Evaluationskriterien für IT-Sicherheit (Normenreihe im Entwurf)
- CLC IEC/TR 63074:2025: Maschinensicherheit - Security-Aspekte in Verbindung mit der funktionalen Sicherheit von sicherheitsbezogenen Steuerungssysteme

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, re-moves, 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 Korrumpierung 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 Ver-wendung 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 - LINK
- Management-Blitzlicht zu den wichtigsten Fragen des CRA - LINK

- Flyer: Wie mache ich meine Produkte fit für eine (cyber-)sichere Zukunft - LINK
- Flyer: Wie werden Produkte klassifiziert und welche Arten von Konformitätsnachweisen gibt es - LINK
- Flyer: Drittstellenbewertung – welches Konformitätsbewertungsmodul ist für mein Produkt geeignet - LINK

Weiterhin wurden die folgenden **Technischen Richtlinien des BSI** unter der Nummer TR-03183 - Cyber Resilience Requirements for Manufacturers and Products veröffentlicht:

- Teil 1: General requirements - LINK
- Teil 2: Software Bill of Materials - LINK
- Teil 3: Vulnerability Reports and Notifications - LINK
- Teil H: Cyber Resilience Requirements for Manufacturers and Products - LINK

Umfassende **Informationen zu Standards und bereits heute möglichen Zertifizierungen** (durch das BSI) erhalten Sie HIER sowie mit den folgenden Auflistungen:

- Zertifizierung von Produkten - LINK
- Zertifizierung nach Common Criteria (CC) - LINK
- Informationen und Listen zu aktuellen Zertifikaten (z. B. Betriebssysteme, Netzwerk- und Kommunikationsprodukte, Serveranwendungen, intelligente Messsysteme und sonstige Produkte) - LINK

Normen mit Bezug auf Informationssicherheitsmanagement (Cybersicherheit und Datenschutz)

- prEN ISO/IEC 27000:2025: ... Überblick und Terminologie → NEU: als DIN
- EN ISO/IEC 27001:2023: ... Anforderungen
- EN ISO/IEC 27002:2022: ... Informationssicherheitsmaßnahmen
- ISO/IEC 27003:2017: ... Leitlinie
- ISO/IEC 27004:2016: ... Überwachung, Messung, Analyse und Evaluation
- EN ISO/IEC 27005:2024: ... Leitfaden zur Handhabung von Informationssicherheitsrisiken
- EN ISO/IEC 27006-1:2024: ... Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines
- EN ISO/IEC 27007:2022: ... Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen
- ISO/IEC TS 27008:2019: ... Leitfaden zur Bewertung von Informationssicherheitsmaßnahmen
- ISO/IEC 27010:2015: ... Informationssicherheitsmanagement für sektor- und organisationsübergreifende Kommunikation
- EN ISO/IEC 27011:2020: ... Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen
- ISO/IEC 27013 AMD 1:2024: ... Leitfaden für die integrierte Umsetzung von ISO/IEC 27001 und ISO/IEC 20000-1
- ISO/IEC 27014:2020: ... Governance von Informationssicherheit
- ISO/IEC TR 27016:2014: ... organisationelle Wirtschaftlichkeit
- prEN ISO/IEC 27017:2025: ... Informationssicherheitsmaßnahmen auf der Grundlage von ISO/IEC 27002 für Cloud-Dienste → NEU: als DIN
- EN ISO/IEC 27018:2020: ... Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung

- EN ISO/IEC 27019:2025: … Informationssicherheitsmaßnahmen für die Energieversor-gung
- ISO/IEC 27021 AMD 1:2021: … Anforderungen an die Kompetenz von Sachkundigen für Informationssicherheits-Managementsysteme
- ISO/IEC TS 27022:2021: … Guidance on information security management system processes
- ISO/IEC DIS 27028:2025: … Leitfaden zu den ISO/IEC 27002-Attributen
- ISO/IEC TS 27029:2023: … ergänzendes Dokument zu ISO/IEC 27002
- prEN ISO/IEC 29151:2025: Informationssicherheit, Cybersicherheit und Datenschutz - Maßnahmen und Anleitung für den Schutz personenbezogener Daten → NEU: als DIN

Weiterhin ist vorgesehen, dass in ISO/IEC 27030 bis ISO/IEC 27044 die technischen Gebiete der Informationssi-cherheit abgedeckt werden sollen, z. B. cyber security, intrusion detection und trusted third party authentication.

- ISO/IEC 27031 business continuity
- ISO/IEC 27032 Guidelines for Cybersecurity (herausgegeben im Juli 2012)
- ISO/IEC 27033 Revision von ISO 18028 und umfasst sieben Unterteile:
    - ISO/IEC 27033-1 Guidelines for network security
    - ISO/IEC 27033-2 Guidelines for the design and implementation of network
    - ISO/IEC 27033-3 Reference networking scenarios - Threats, design techniques and control issues (herausgegeben im Dezember 2010)
    - ISO/IEC 27033-4 Securing communications between networks using security gateways - Risks, design techniques and control issues
    - ISO/IEC 27033-5 Securing virtual private networks - Risks, design techniques and control issues
    - ISO/IEC 27033-6 Securing communications across networks using Virtual Private Networks
    - ISO/IEC 27033-7 Guidelines for the design and implementation of network security
- ISO/IEC 27034 Guidelines for application security
- ISO/IEC 27035 Information security incident management

Zertifizierungsnormen zum IT-Servicemanagement

- ISO/IEC 20000 Part 1 – „Service Management System Requirements“
- ISO/IEC 20000 Part 2 – „Code of Practice“
- ISO/IEC 20000 Part 3 – „Guidance on Scope Definition and Applicability of ISO/IEC 20000-1“
- ISO/IEC 20000 Part 4 – „Process Reference Model“
- ISO/IEC 20000 Part 5 – „Exemplar Implementation Plan for ISO/IEC 20000-1“

Ergänzende Normen

- EN ISO/IEC 29147:2020: Informationstechnik - Sicherheitstechniken - Offenlegung von Schwachstellen
- ISO/IEC 29150:2011: Informationstechnik - IT-Sicherheitsverfahren – Signcryption

Geplante Änderung der KI-Verordnung, auch mit Auswirkungen auf die Maschinenverordnung

Zusammenfassung einer Pressemitteilung der Europäischen Kommission zur geplanten Änderungs-Verordnung.

- Verlängerung der Frist für die Umsetzung der Vorschriften für Hochrisiko-KI-Systeme um bis zu 16 Monate
- NEUE TERMINE zur Umsetzung der Anforderungen sind nun:
    - 02.12.2027 für eigenständige KI-Systeme nach Artikel 6 (2) und Anhang III der KI-

Verordnung
    - 02.08.2028 für eingebettete KI-Systeme nach Artikel 6 (1) und Anhang I der KI-Verordnung. Dies sind u. a. Sicherheitsbauteile nach Maschinenverordnung, die KI nutzen.
- Bis spät. zum 02.08.2028 muss die EU-Kommission einen delegierten Rechtsakt unter der Maschinenverordnung erlassen, in dem die einzuhaltenden (relevanten) grundlegenden Sicherheits- und Gesundheitsschutzanforderungen in Bezug auf KI-Systeme bei Maschinen definiert sind.
- Damit soll es bei der vorrangigen Anwendung der sektorspezifischen Rechtsakte (z. B. der Maschinenverordnung) vor der KI-Verordnung bleiben (Vermeidung von Überschneidungen).
- Verschiebung der Anpassung weiterer europäischer Rechtsakte in Bezug auf die KI-Anwendung
- Stärkung und bessere Klärung der Rolle des Büros für Künstliche Intelligenz
- Verpflichtung der Anbieter, KI-Systeme in der EU-Datenbank für Hochrisikosysteme zu registrieren, auch wenn sie der Auffassung sind, dass ihre Systeme nicht als Hochrisikosysteme einzustufen sind.
- Verlängerung der Frist für die Einrichtung von KI-Reallaboren durch die auf nationaler Ebene zuständigen Behörden bis zum 2. August 2027
- Verkürzung der Frist für die Umsetzung von Transparenzlösungen für künstlich erzeugte Inhalte (nämlich von sechs Monaten auf drei Monate); als neue Frist wurde der 2. Dezember 2026 festgesetzt
- nicht einvernehmliche sexuelle und intime Inhalte oder Darstellungen von sexuellem Missbrauch von Kindern mittels KI-Systemen werden NEU als verbotene KI-Praktiken definiert

Den ausführlichen Inhalt der vorgeschlagenen Änderung können Sie HIER abrufen.

KI generell und im Maschinenbau → Umsetzen von Anforderungen – Auswahl wichtiger Normen

- ISO/IEC TS 4213: Information technology — Artificial intelligence — Assessment of machine learning classification performance

→ neuer ENTWURF: ISO/IEC DIS 4213: Information technology — Artificial Intelligence — Performance measurement for AI classification, regression, clustering and recommendation tasks

- (DIN EN) ISO/IEC 5259: Künstliche Intelligenz - Datenqualität für Analytik und maschinelles Lernen (ML)
    - Teil 1: Überblick, Terminologie und Beispiele
    - Teil 2: Datenqualitätsmessgrößen
    - Teil 3: Anforderungen und Leitlinien für das Datenqualitätsmanagement
    - Teil 4: Rahmenwerk für Datenqualitätsprozesse
    - Part 5: Data quality governance framework
    - Part 6: Visualization framework for data quality
- ISO/IEC 5338: Information technology — Artificial intelligence — AI system life cycle processes
- ISO/IEC 5339: Information technology — Artificial intelligence — Guidance for AI applications
- ISO/IEC 5392: Information technology — Artificial intelligence — Reference architecture of knowledge engineering
- DIN ISO/IEC/TR 5469: Künstliche Intelligenz - Funktionale Sicherheit und KI-Systeme
- DIN EN ISO/IEC 8183: Informationstechnologie - Künstliche Intelligenz - Rahmenwerk für den Datenlebenszyklus

- VORNORM DIN CEN/CLC ISO/IEC/TS 12791: Informationstechnik - Künstliche Intelligenz - Behandlung von unerwünschtem Bias bei Klassifizierungs- und Regressionsaufgaben des maschinellen Lernens
- DIN EN ISO/IEC 12792: Informationstechnologie - Künstliche Intelligenz (KI) - Transparenz-Taxonomie von KI-Systemen

- CEN/CLC/TR 18115: Data governance and quality for AI within the European context
- CEN/CLC/TR 18145: Environmentally sustainable Artificial Intelligence
- DIN EN 18228 – ENTWURF: Risikomanagement für Künstliche Intelligenz
- (DIN) EN 18229: Framework für Vertrauenswürdigkeit von Künstlicher Intelligenz
  - Teil 1 – ENTWURF: Protokollierung
  - DRAFT Part 2: Accuracy and robustness
  - Teil 3 (in Planung): Transparenz und menschliche Aufsicht
- DIN EN 18274 - ENTWURF: Kompetenzanforderungen für KI-Ethiker
- DIN EN 18281 – ENTWURF: Künstliche Intelligenz - Bewertungsmethoden für präzise Computer-Vision-Systeme
- DIN EN 18282 – ENTWURF: Künstliche Intelligenz - Cybersicherheitsspezifikationen für KI-Systeme
- EN 18283 – DRAFT: Artificial Intelligence - Concepts, measures and requirements for managing bias in AI systems
- EN 18284 – DRAFT: Quality and governance of datasets in AI
- DIN EN 18286 – ENTWURF: Künstliche Intelligenz - Qualitätsmanagementsystem für EU AI Act Regulierungszwecke

- ISO/IEC TR 20226: Information technology — Artificial intelligence — Environmental sustainability aspects of AI systems
- ISO/IEC CD TS 22440: Artificial intelligence — Functional safety and AI systems
  - DRAFT Part 1: Requirements
  - DRAFT Part 2: Guidance
  - DRAFT Part 3: Examples of application

- DIN EN ISO/IEC 22989: Informationstechnik - Künstliche Intelligenz - Konzepte und Terminologie der künstlichen Intelligenz ENTWURF für Amendment 1 (2025-09)
- DIN EN ISO/IEC 23053: Framework für Systeme der künstlichen Intelligenz (KI) basierend auf maschinellem Lernen (ML) ENTWURF für Amendment 1 (2025-09)
- DRAFT ISO/IEC CD 23282: Artificial Intelligence — Evaluation methods for accurate natural language processing systems

- DIN EN ISO/IEC 23894: Informationstechnik - Künstliche Intelligenz - Leitlinien für Risikomanagement

- ISO/IEC TR 24027: Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
- ISO/IEC TR 24028: Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC TR 24029-1: Artificial Intelligence (AI) — Assessment of the robustness of neural networks – Part 1: Overview
- ISO/IEC 24029-2: Artificial intelligence (AI) — Assessment of the robustness of neural networks – Part 2: Methodology for the use of formal methods
- DRAFT ISO/IEC DIS 24029-3: Artificial intelligence (AI) — Assessment of the robustness of neural networks – Part 3: Methodology for the use of statistical methods

- ISO/IEC TR 24368: Information technology — Artificial intelligence — Overview of ethical and

societal concerns
- ISO/IEC TR 24372: Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems
- DIN EN ISO/IEC 24970 – ENTWURF: Künstliche Intelligenz - KI-System-Protokollierung
- DIN EN ISO/IEC 25059 – ENTWURF: Software-Engineering - Systeme und Software Qualitätsanforderungen und Bewertung (SQuaRE) - Qualitätsmodell für KI-Systeme
- DRAFT ISO/IEC FDIS 27090 Cybersecurity — Artificial Intelligence — Addressing security threats and compromises to artificial intelligence systems
- ISO/IEC TR 29119-11: Software and systems engineering — Software testing – Part 11: Guidelines on the testing of AI-based systems

Siehe auch weitere Teile der Normenreihe ISO/IEC 29119 zum Thema Software and systems engineering — Software testing

- DIN SPEC 32792: Semantische Daten-Annotationen zur Unterstützung KI-gestützter Datenverarbeitung
- ISO/IEC 38507: Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
- DIN ISO/IEC 42001 - ENTWURF: Informationstechnik - Künstliche Intelligenz – Managementsystem
- DRAFT ISO/IEC 42002: Vocabulary and Definitions for AI Governance
- ISO/IEC 42005: Information technology — Artificial intelligence (AI) — AI system impact assessment
- ISO/IEC 42006: Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems
- DRAFT ISO/IEC DIS 42007: Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems
- DIN SPEC 91491: KI-generierte Datenschemas zur Integration und Konsolidierung heterogener Datenquellen
- DIN SPEC 92001: Künstliche Intelligenz - Life Cycle Prozesse und Qualitätsanforderungen
    - Teil 1: Qualitäts-Meta-Modell
    - Teil 2: Robustheit
    - Teil 3: Erklärbarkeit
- VORNORM DIN/TS 92004: Künstliche Intelligenz - Qualitätsanforderungen und -prozesse - Risikoidentifikation und -analyse für KI-Systeme im gesamten Lebenszyklus
- DIN SPEC 92005: Künstliche Intelligenz - Quantifizierung von Unsicherheiten im Maschinellen Lernen
- DIN SPEC 92006: Künstliche Intelligenz - Anforderungen an KI-Prüfwerkzeuge
- DIN SPEC 92007: Künstliche Intelligenz - Referenzdatensätze - Allgemeine Anforderungen an Testdatensätze

Hier nachstehend finden Sie jeweils einen Link zum ISO-Komitee JTC1/SC 42 mit einer:

- aktuellen Liste veröffentlichter ISO-Normen
- aktuellen Liste der Normungsprojekte

Verfolgen Sie aktuelle Entwicklungen auch in einem Podcast von Arno Schimmelpfennig für DIN ANP

zum Thema „KI-Ethik-News„

Landscape Analysis Reports der Organisation StandICT.eu

- Landscape of Artificial Intelligence Standards - LINK
- Landscape of Trusted Information Standards - LINK

Umsetzung neuer Anforderungen zur Sicherheit von Maschinensteuerungen – Auswahl wichtiger Quellen

Aktualisierte Normung

- Normenreihe EN ISO 13849: Sicherheitsbezogene Teile von Steuerungen (Teil 1 NEU; Teil 2 liegt als NEUER Entwurf vor)
- Norm EN 62061: Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (NEU)
- Norm DIN CLC IEC/TS 63394: Sicherheit von Maschinen - Leitlinien zur funktionalen Sicherheit sicherheitsbezogener Steuerungssysteme (NEU)
- laufende Aktualisierung von harmonisierten Typ-B-Normen zu Sicherheitsbauteilen
- Funktionale Sicherheit bestimmter Maschinengruppen, z. B.:
    - Erdbaumaschinen
    - Traktoren und Maschinen für die Land- und Forstwirtschaft
    - Geländegängige Stapler
- Entsprechende Abschnitte der harmonisierten Typ-C-Normen für Maschinen zu Sicherheitssteuerungen
- umfassende Reihen technischer Regeln beim VDI zu funktionaler Sicherheit

Einsatz sicherer Bussysteme

EN IEC 61784-3:2022-02 „Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile
Prüfgrundsatz von DGUV Test (Prüf- und Zertifizierungsstelle Elektrotechnik) GS-ET-26 Grundsätze für die Prüfung von „Bussystemen für die Übertragung sicherheitsbezogener Nachrichten“

hier weiterhin mit IFA Report 2/2017:
„Funktionale Sicherheit von Maschinensteuerungen“ → Kapitel 6.2.18 und 8.2.16

Informationssicherheit (nicht nur) von Maschinen

Ziel: sicherer Betrieb vernetzter Komponenten
Maschinenverordnung rückt dies in Anhang III, Abschnitt 1.1.2. stärker in den Fokus
Validierung von Software (vgl. EN ISO 13849 und IEC 61508) hilft, dieses Ziel zu erreichen
Betrifft alle Lebensphasen, z. B. auch inkl. Entsorgung
→ **IEC 62443** - ganzheitlicher Ansatz zur Informationssicherheit über den kompletten Lebenszyklus von Industriekomponenten oder Systemen
→ derzeit 17 Teile erschienen oder in Bearbeitung / in Planung
→ mehr als 2000 Seiten nach Fertigstellung

→ Gliederung in sechs Themenschwerpunkte mit dem Stand, wie hier nachfolgend gezeigt:

Dokumente in grüner Schrift werden derzeit noch erarbeitet. Dokumente in schwarzer Schrift sind durch IEC veröffentlicht. **Dokumente in halbfetter Schrift sind als deutsche Norm (DIN) veröffentlicht.**	
Schwerpunkt 1: Allgemeine Grundlagen	IEC/TS 62443-1-1 Concepts and models IEC 62443-1-2 Master glossary of terms and abbreviations IEC 62443-1-3 System security conformance metrics IEC 62443-1-4 IACS security lifecycle and use-cases IEC/TS 62443-1-5 Scheme for IEC 62443 security profiles
Schwerpunkt 2: Sicherheitsanforderungen für Betreiber und Dienstleister	**IEC 62443-2-1 Security program requirements for IACS asset owners** IEC 62443-2-2 Security Protection Rating IEC/TR 62443-2-3 Patch management in the IACS environment **IEC 62443-2-4 Security program requirements for IACS service providers**
Schwerpunkt 3: Sicherheitsanforderungen an Automatisierungssysteme	IEC/TR 62443-3-1 Security technologies for IAC **IEC 62443-3-2 Security risk assessment and system design** **IEC 62443-3-3 System security requirements and security levels**
Schwerpunkt 4: Sicherheitsanforderungen an Automatisierungskomponenten	**IEC 62443-4-1 Secure product development lifecycle requirements** **IEC 62443-4-2 Technical security requirements for IACS components**
Schwerpunkt 5: Profile	in Bearbeitung
Schwerpunkt 6: Evaluationsmethodik	IEC/TS 62443-6-1 Security evaluation methodology for IEC 62443 - Part 2-4: Security program requirements for IACS service providers IEC/TS 62443-6-2 Security evaluation methodology for IEC 62443 - Part 4-2: Technical security requirements for IACS components

Landscape Analysis Reports der Organisation StandICT.eu

- 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
- Landscape of Digital Twins
- Guidance for the Integration of Digital Twins in Data Spaces
- Landscape of Edge Computing Standards

Grundlagen zum Digitalen Produktpass (DPP)

Ziel ist die Umsetzung einer weitgehenden Kreislaufwirtschaft in der EU und Ablösung des „line-aren Modells“ von nehmen, herstellen, verwenden, entsorgen mit folgenden Aspekten (vgl. z. B. HIER):

- Verringerung des Drucks auf die natürlichen Ressourcen
- Eindämmung des Verlusts der biologischen Vielfalt
- Erreichung der Klimaneutralität bis 2050
- Aufbau eines widerstandsfähigeren und wettbewerbsfähigeren Europas
- auch: Deal für eine saubere Industrie

Bis Ende 2026 soll ein **Circular Economy Act** in der EU verabschiedet werden: vgl. z. B. HIER

Bereits heute gibt es entscheidende regulatorische Säulen zur Umsetzung avisierter Ziele:

- **Ecodesign für Sustainable Products Regulation (ESPR)**, gemeinsam mit dem Ecodesign for Sustainable Products and Energy Labelling Working Plan 2025-2030
- **Packaging and Packaging Waste Regulation (PPWR)**
- **Critical Raw Materials Act (CRMA)**

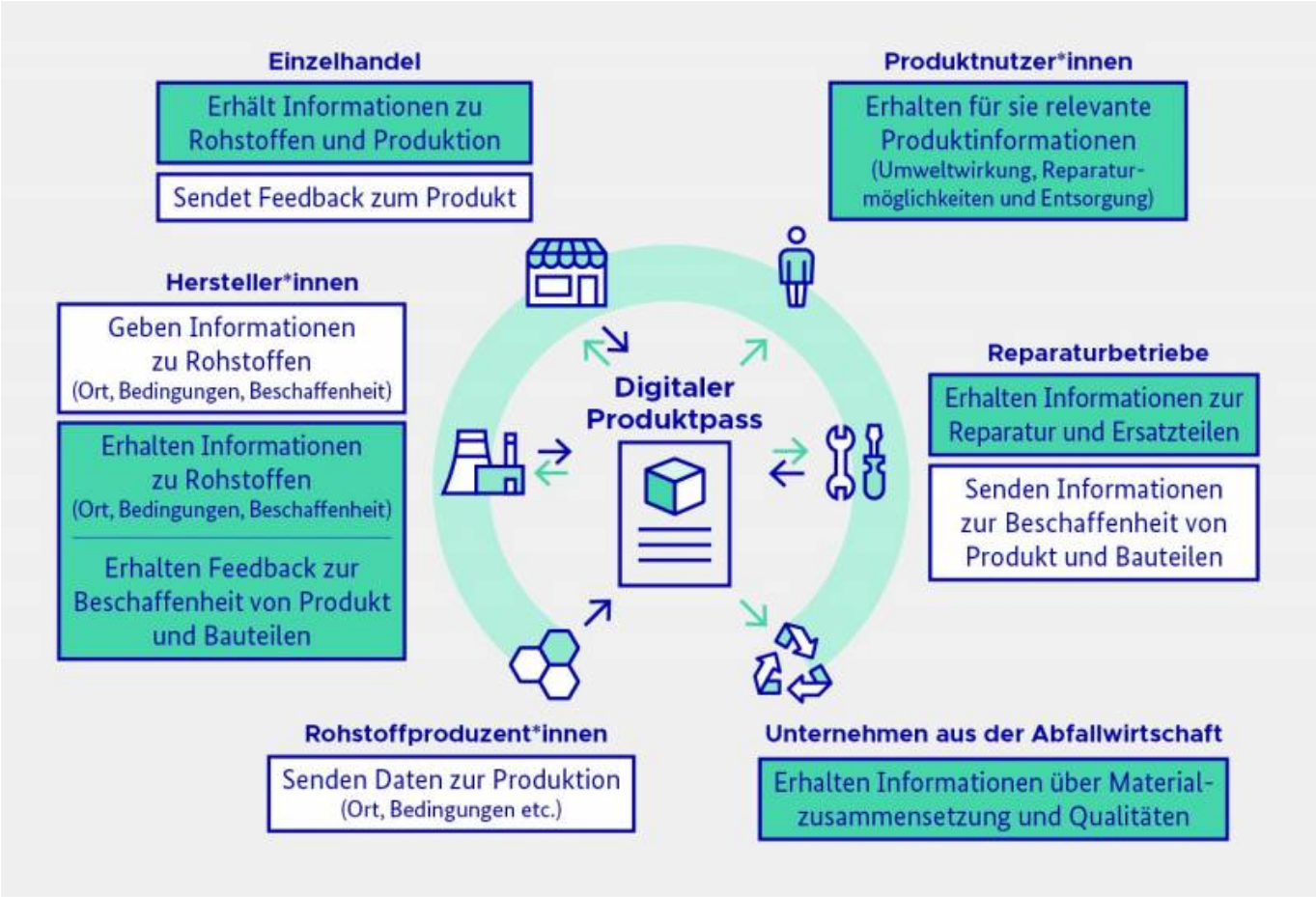
und in Ergänzung mit den sogen.

- Clean Industrial Deal
- Competitiveness Compass

Die Ecodesign für Sustainable Products Regulation (ESPR) oder in der deutschen Übersetzung die **Ökodesign-Verordnung** gilt im Prinzip für ALLE PRODUKTE. *Definition (Artikel 2 Nr. 1 der VO): „… alle physischen Waren, die in Verkehr gebracht oder in Betrieb genommen werden; […]“*
Aber: Die Verordnung (EU) 2024/1781 ist eine Rahmenrechtsvorschrift. Detaillierte Anforderungen zu einzelnen Produktgruppen werden erst in jeweils zu erlassenden delegierten Verordnungen (=direkte Gesetzeskraft) gestellt. Die Ökodesign-Verordnung hat einen weitreichenden Scope:

1. Festlegen eines Rahmens von Ökodesign-Anforderungen mit dem Ziel:
    - nachhaltige Produkte in den Verkehr zu bringen oder in Betrieb zu nehmen,
    - Verringerung des CO2-Fußabdrucks von Produkten,
    - Verringerung des Umweltfußabdrucks von Produkten über den gesamten Lebenszyklus hinweg.
2. Einführung eines digitalen Produktpasses
3. Festlegen verbindlicher Anforderungen an umweltorientierter Vergabe öffentlicher Auf-träge
4. Verhindern des Vernichtens (bestimmter) Verbraucherprodukte

Die Einführung eines Digitalen Produktpasses unter ESPR ist sicher nicht der Hauptinhalt der Ökodesign-Verordnung, aber wahrscheinlich der Teil, der von Produktherstellern und anderen Verantwortlichen beim Bereitstellen von Produkten auf dem Markt die größten administrativen und dokumentarischen Anstrengungen erfordert.
Die ausführliche Darstellung von der Website des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit auf der folgenden Seite zeigt den Ansatz des DPP.



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

Permanent link:
https://product-compliance.net/doku.php?id=zusatzinformationen:anforderungen_umsetzen&rev=1783943979

Last update: **2026/07/13 13:59**