RUBINLAKE



PRODUKTSICHERHEIT

Vernetzte Produkte DACH 2027

Sicherheit ist günstig. Warten kostet Märkte.

RUBINLAKE GmbH

Version 1.2

Inhaltsverzeichnis

Zusammenfassung ... **3**
Zentrale Ergebnisse ... 4
1 Fristen und Geltungsbereich ... **5**
1.1 Vernetzte Geräte in DACH ... 5
1.2 Von der Meldepflicht zur vollen Geltung ... 5
1.3 Geltungsbereich und Ausnahmen ... 7
1.4 Stand der harmonisierten Normen ... 8
1.5 Betroffene Hersteller und Umsetzungsstand ... 9
2 Geräteanforderungen ... **11**
2.1 Vier Gerätearchetypen ... 11
2.2 Acht Gerätefunktionen ... 12
2.3 Eine gemeinsame Sicherheitsbasis ... 14
2.4 Pflichten je Archetyp ... 14
2.5 Wege der Konformitätsbewertung ... 17
3 Kosten je Gerät ... **18**
3.1 Laufende Monatskosten ... 18
3.2 Anteil der CRA-Konformität ... 19
3.3 Data-Act-Kosten auf Unternehmensebene ... 20
3.4 Sicherheitskosten über den Lebenszyklus ... 20
3.5 Flottengröße als wichtigster Kostentreiber ... 21
4 Technologie und Architektur ... **22**
4.1 Connectivity ... 22
4.2 Sicherheitsschicht im Gerät ... 23
4.3 Gerätemanagement und PKI ... 24
4.4 SBOM- und PSIRT-Werkzeuge ... 25
4.5 Datenschnittstellen für den Data Act ... 25
4.6 Pflichten je Schicht ... 26
4.7 Vier Referenzarchitekturen ... 27
5 Schwerpunkt Logistik-Tracking ... **33**
5.1 Tracker- und Tag-Klassen ... 33
5.2 Preis und Laufzeit je Klasse ... 33
5.3 Regulatorische Termine und Tracker-Design ... 35
5.4 Anbieter und Produkte in DACH ... 36
5.5 Bestand und Wachstum bis 2028 ... 36
5.6 Werksausstattung und Nachrüstung ... 37
5.7 Die Nachfrageseite ... 38
6 Schwerpunkt Österreich und Schweiz ... **39**
6.1 Österreich ... 39
6.2 Schweiz ... 41
6.3 Schweizer Hersteller auf dem EU-Markt ... 42
7 Anbieterlandschaft ... **45**
7.1 Marktkonsolidierung 2025-2026 ... 45

7.2 Eingestellte IoT-Dienste als Plattformrisiko ... 47
7.3 Notifizierte Stellen unter dem CRA ... 47
8 Handlungsempfehlungen ... 48
8.1 Geschäftsführung ... 48
8.2 Produkt und Entwicklung ... 49
8.3 Compliance ... 49
8.4 Der Zwölfmonatsplan ... 50
8.5 Förderung der CRA-Umsetzung ... 53
8.6 Fünf Leitfragen ... 53

Anhang ... 55
A Methodik ... 56
A.1 Quellen ... 56
A.2 Messwerte und Annahmen ... 56
A.3 Schätzung der Grundgesamtheit ... 56
B Rechtsgrundlagen ... 61
C Kostenmodell ... 62
C.1 Modellannahmen ... 62
C.2 Erhobene Listenpreise ... 62
C.3 Positionen je Archetyp ... 64
C.4 Konformitätskosten je Produkt ... 65
C.5 Gebühren für die Konformitätsbewertung ... 66
C.6 Sensitivität ... 66
D Anbieterverzeichnis ... 68
D.1 Benötigte Anbieter je Archetyp ... 68
D.2 Gerätemanagement und OTA ... 68
D.3 SBOM, Schwachstellenmanagement und PSIRT ... 69
D.4 Secure Element und PKI ... 70
D.5 IoT-Connectivity ... 72
D.6 IoT-Plattformen ... 72
D.7 Tracker-Anbieter ... 73
D.8 Ingenieurdienstleister ... 74
D.9 Notifizierte Stellen für RED und CRA ... 74
D.10 Listenpreise ... 75
E Förderprogramme ... 77
E.1 Deutschland: Bundesprogramme ... 77
E.2 Deutschland: Landesprogramme ... 78
E.3 Österreich: aws und FFG ... 79
E.4 Schweiz: Innosuisse ... 80
E.5 EU-Ausschreibungen mit CRA-Bezug ... 81
E.6 Überblick ... 81
Über RUBINLAKE ... 86
Haftungsausschluss ... 86
Quellen ... 87

Zusammenfassung

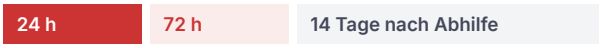
Im Maschinen- und Gerätebau ist heute nicht mehr nur die Fertigung vernetzt, sondern auch das Produkt, das sie verlässt. Fast alle befragten deutschen Hersteller von Produkten mit digitalen Elementen (94 %) bieten bereits Geräte an, die sich nach der Auslieferung aktualisieren lassen. Jedes dieser Geräte verlängert die Verantwortung des Herstellers über das Werkstor hinaus und ist ein möglicher Angriffspunkt. Die Europäische Kommission beziffert die Schäden, die ihr Cyber Resilience Act (CRA) Unternehmen in der EU ersparen könnte, auf 180-290 Mrd. € im Jahr.

Europa antwortet mit fünf Rechtsakten: dem CRA, dem Data Act, der Maschinenverordnung, den Cybersicherheitsregeln der Funkanlagenrichtlinie und der Batterieverordnung. Zwischen August 2025 und Dezember 2027 machen sie Sicherheit, Updates und Datenzugang zur Bedingung für den Marktzugang. Die erste Pflicht gilt bereits. Seit dem 11. September 2026 müssen Hersteller aktiv ausgenutzte Schwachstellen binnen 24 Stunden über die zentrale Meldeplattform der ENISA melden.

Die Hardware der Produkte, die 2027 auf den Markt kommen, muss jetzt feststehen. Doch für den CRA und die Maschinenverordnung steht noch keine harmonisierte Norm im Amtsblatt, und für den CRA ist noch keine notifizierte Stelle benannt. Belastbare Kostenzahlen sind selten, und nur wenige der befragten Hersteller sind vorbereitet. Damit entscheidet nicht mehr der Hersteller, ob Sicherheit ins Produkt gehört, sondern das Gesetz.

FRIST

24 Stunden bis zur Frühwarnung bei aktiv ausgenutzten Schwachstellen



Frühwarnung · Meldung · Abschlussbericht

BEREITSCHAFT

3 % der befragten Hersteller halten sich für voll CRA-konform



NORMEN

0 von 41 beauftragten CRA-Normen stehen im Amtsblatt



KOSTEN

< 0,50 € Sicherheitsaufschlag je Gerät und Monat bei 10.000 Geräten



Dieser Bericht untersucht die Frage, mit welchem Design ein Hersteller die Sicherheit eines vernetzten Produkts über dessen Lebensdauer am günstigsten gewährleistet. Er beantwortet sie für Hersteller mit 100 bis 4.999 Beschäftigten in Deutschland, Österreich und der Schweiz, und zwar an vier typischen Geräten: einem Akkuwerkzeug, einer Maschine mit Gateway, einem steuerbaren Gebäudegerät wie der Wärmepumpe und einem Logistik-Tracker. Unser Kostenmodell bewertet für diese Geräte die Basiskosten für Funk und Cloud und den Sicherheitsaufschlag zu Listenpreisen, im Basisfall für 10.000 Geräte je Produkt über fünf Jahre. Der Sicherheitsaufschlag ist je Gerät gering und bei jedem Produkt etwa gleich hoch. Die Rechnung bestimmen Stückzahl, Funktechnik und Backend, und diese Entscheidungen fallen, bevor die Normen vorliegen.

Zentrale Ergebnisse

F1 Die Pflichten erfassen den Bestand, nicht nur neue Produkte.

86 Mio. M2M-SIM-Profile in deutschen Netzen, +17 % in einem Jahr



Die Meldepflicht des CRA gilt seit dem 11. September 2026 auch für Geräte im Einsatz.

F2 Der Mittelstand ist breit betroffen, und die Vorbereitung hinkt weit hinterher.

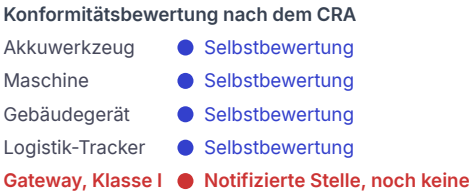
1.750-3.440 Hersteller in DACH, geschätzt



Erst die Hälfte der befragten deutschen Hersteller hat mit der Umsetzung des CRA begonnen.

F3 Ein eigenständig verkauftes Gateway hat noch keinen Weg zur Konformität.

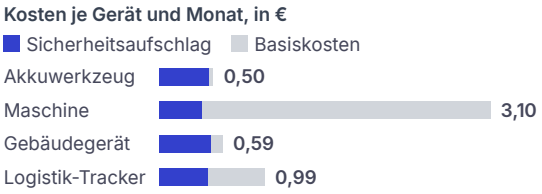
0 bislang notifizierte Stellen unter dem CRA



Ein Gateway der Klasse I braucht eine notifizierte Stelle, solange keine harmonisierte Norm vorliegt.

F4 Nicht die Regulierung macht ein vernetztes Produkt teuer.

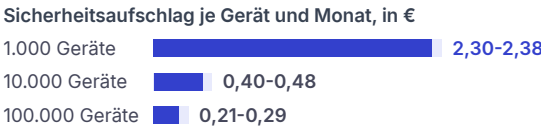
0,50-3,10 € Basiskosten und Sicherheitsaufschlag je Gerät und Monat



Funktechnik und Backend bestimmen die Summe, nicht die Sicherheit.

F5 Die Stückzahl wiegt schwerer als jedes Bauteil.

2,30 € Sicherheitsaufschlag je Gerät und Monat bei 1.000 Geräten



Fixkosten verteilen sich auf alle Geräte. Das Secure Element ist der kleinste Posten.

F6 Tracker brauchen ein neues Batteriekonzept und Mobilfunk ohne 2G.

2028 endet 2G in den deutschen Mobilfunknetzen



Der Nutzer muss die meisten Gerätebatterien ab dem 18. Februar 2027 selbst entnehmen können.

Wer Architektur und Backend jetzt festlegt, verteilt die Kosten der Sicherheit auf seine ganze Flotte. Wer auf die Normen wartet, entwirft unter Termindruck und mit weniger Spielraum. Die Kapitel 1 bis 7 belegen die Ergebnisse, und Kapitel 8 leitet daraus Empfehlungen für die unterschiedlichen Rollen im Unternehmen ab.

1 Fristen und Geltungsbereich

Vernetzte Werkzeuge, Maschinen, Gebäudegeräte und Tracker, die heute entwickelt werden, kommen auf einen Binnenmarkt, dessen Regeln sich bis Dezember 2027 grundlegend ändern. Fünf EU-Rechtsakte erfassen bis dahin jedes dieser Produkte, und die Meldepflicht für Schwachstellen gilt schon seit September 2026, auch für bereits ausgelieferte Geräte. Harmonisierte Normen fehlen noch. Nach unserer Schätzung sind in DACH 1.750 bis 3.440 Hersteller betroffen, und von den befragten Unternehmen sind nur wenige vorbereitet. Das Kapitel nennt die Termine und den Geltungsbereich jedes Rechtsakts und zeigt, wie weit Normung und Hersteller sind.

1.1 Vernetzte Geräte in DACH

Ende 2025 waren in den deutschen Mobilfunknetzen 86,1 Mio. Machine-to-Machine-SIM-Profile (M2M) aktiv, 17 % mehr als ein Jahr zuvor.[78] Das entspricht rund vier Fünfteln der 106,4 Mio. übrigen aktiven SIM-Profile.[78] Österreich kam Ende 2025 auf 27,5 Mio. M2M-SIM-Karten, doppelt so viele wie die 13,8 Mio. übrigen genutzten SIM-Karten und mehr als dreimal so viele wie Ende 2021 (8,4 Mio.). Ein Teil davon steckt in Geräten im Ausland.[337, 338] In der Schweiz stieg die Zahl der M2M-Abonnemente 2024 um 14,3 % auf 5,2 Mio., die der Mobilfunkabonnemente insgesamt nur um 2,5 %.[48]

Diese Zahlen erfassen nur Geräte im Mobilfunknetz. Werkzeuge und Gebäudegeräte, die über BLE oder WLAN kommunizieren, kommen hinzu. Weltweit zählt Ericsson Ende 2025 22,3 Mrd. Verbindungen im Internet der Dinge (IoT), davon 4,5 Mrd. oder rund ein Fünftel über Mobilfunk.[134] Ericsson erwartet bis 2031 mehr als eine Verdopplung auf 47,1 Mrd.[134]

1.2 Von der Meldepflicht zur vollen Geltung

Die Meldepflicht des Cyber Resilience Act (CRA) für Schwachstellen gilt seit dem 11. September 2026, die Maschinenverordnung ab dem 20. Januar 2027 und der vollständige CRA ab dem 11. Dezember 2027.[167, 168, 171] Fünf Rechtsakte geben den Takt vor: der CRA,[171] der Data Act,[170] die Maschinenverordnung,[168] die delegierte Verordnung zur Cybersicherheit unter der Funkanlagenrichtlinie (RED)[141] und die Batterieverordnung mit dem Batteriepass.[169] Alle fünf sind Verordnungen. Sie gelten in Deutschland und Österreich unmittelbar, ohne nationale Umsetzung, und für Produkte aus der Schweiz, sobald diese in der EU in Verkehr gebracht werden. Drei der sechs Fristen sind bereits erreicht, und der volle CRA kommt als letzter (Abbildung 1). Ein Produkt muss alle fünf Rechtsakte zugleich erfüllen, wenn seine Entwicklung jetzt beginnt und es 2028 ausgeliefert wird.

Eine Berichtigung hat den Geltungsbeginn der Maschinenverordnung vom ursprünglich vorgesehenen 14. Januar verschoben.[167] Die delegierte RED-Verordnung gilt nach einer Änderung seit dem 1. August 2025, ein Jahr später als ursprünglich beschlossen.[145] Fünf der acht Stichtage sind verstrichen, der volle CRA kommt zuletzt (Tabelle 1).

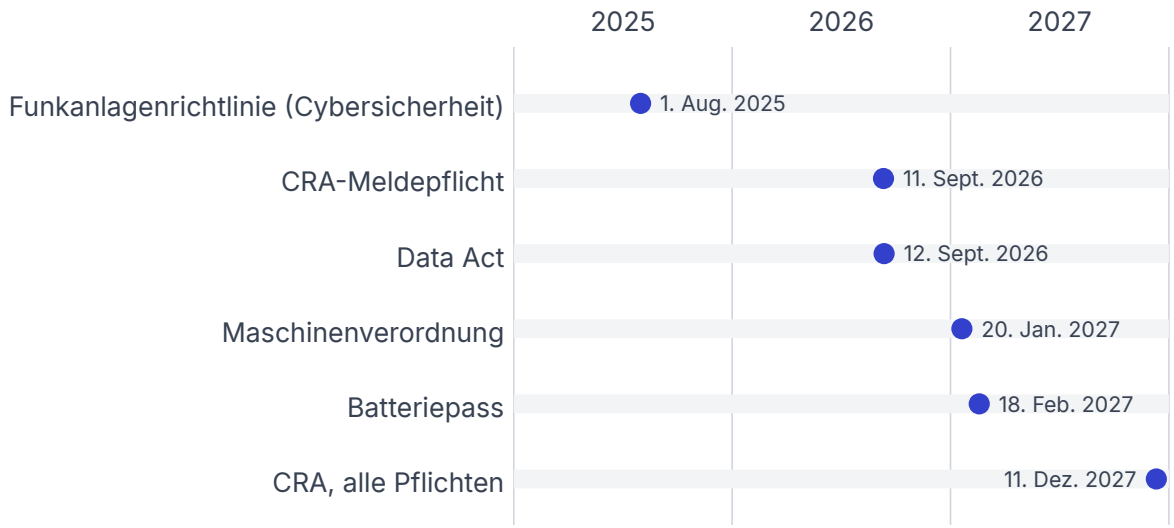


Abbildung 1: **Geltungsbeginn der EU-Rechtsakte**

DATUM	RECHTSAKT	GELTENDE PFLICHTEN	BETROFFENE PRODUKTE
1. Aug. 2025	Delegierte VO (EU) 2022/30 zur RED	Grundlegende Anforderungen an Netzschutz, Datenschutz und Betrugsschutz	Funkanlagen, die ab diesem Tag in Verkehr gebracht werden
12. Sept. 2025	Data Act	Allgemeine Geltung: vorvertragliche Information, Zugangsrechte von Nutzern und Dritten, Vertragsregeln	Vernetzte Produkte und verbundene Dienste in der EU
11. Juni 2026	CRA	Regeln für die Notifizierung von Konformitätsbewertungsstellen	Notifizierte Stellen und Behörden
11. Sept. 2026	CRA	Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Vorfälle	Alle Produkte mit digitalen Elementen am Markt, auch solche, die vor 2027 in Verkehr gebracht wurden
12. Sept. 2026	Data Act	Datenzugang ab Werk	Vernetzte Produkte, die nach diesem Tag in Verkehr gebracht werden
20. Jan. 2027	Maschinenverordnung	Volle Geltung; Maschinenrichtlinie 2006/42/EG aufgehoben	Maschinen und dazugehörige Produkte, die ab diesem Tag in Verkehr gebracht werden
18. Feb. 2027	Batterieverordnung	Batteriepass, QR-Code auf allen Batterien, Entnehmbarkeit von Gerätebatterien durch Endnutzer	Batterien und Produkte mit Batterien, die ab diesem Tag in Verkehr gebracht werden
11. Dez. 2027	CRA	Grundlegende Anforderungen, Konformitätsbewertung, CE-Kennzeichnung	Produkte mit digitalen Elementen, die ab diesem Tag in Verkehr gebracht werden

Tabelle 1: **Stichtage und betroffene Produkte**
Quellen: [141, 145, 167, 168, 169, 170, 171].

11. September 2026, CRA-Meldepflichten. Artikel 14 gilt 15 Monate vor dem Rest der Verordnung.[171] Für eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Vorfall sind binnen 24 Stunden eine Frühwarnung und binnen 72 Stunden eine Meldung fällig.[171] Beide laufen

über die einheitliche Meldeplattform der ENISA, die seit dem 11. September 2026 in Betrieb ist.[133, 156] Der Abschlussbericht ist spätestens 14 Tage nach Verfügbarkeit einer Korrektur oder Abhilfemaßnahme fällig, bei einem schwerwiegenden Vorfall einen Monat nach der Meldung.[171] Die Meldung geht an das als Koordinator benannte CSIRT des Mitgliedstaats der Hauptniederlassung, und die ENISA erhält sie zugleich.[171] Betroffene Nutzer sind zu informieren, gegebenenfalls in einem strukturierten, maschinenlesbaren Format.[171] Verwalter von Open-Source-Software melden erst ab dem 11. Dezember 2027.[156]

Die Meldepflicht erfasst auch Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden.[171] Für ein 2023 verkauftes Werkzeug, das noch im Einsatz ist, gilt sie schon heute.

12. September 2025 und 12. September 2026, Data Act. Der Datenzugang ab Werk gilt nur für Produkte, die nach dem 12. September 2026 in Verkehr gebracht werden.[170] Die Rechte des Nutzers, Daten zu erhalten und an Dritte weitergeben zu lassen, gelten dagegen seit dem 12. September 2025, ohne Stichtag für das Inverkehrbringen. Sie erfassen damit auch den Bestand.[170]

11. Juni 2026, notifizierte Stellen unter dem CRA. Seit dem 11. Juni 2026 können die Mitgliedstaaten Konformitätsbewertungsstellen unter dem CRA notifizieren.[171] Bisher ist unter dem CRA keine Stelle notifiziert.[161] Deutschland hat das BSI als notifizierende Behörde gemeldet, Österreich noch keine.[161]

20. Januar 2027, Maschinenverordnung. An diesem Tag ersetzt die Maschinenverordnung die Maschinenrichtlinie 2006/42/EG.[167, 168] Maschinen, die zuvor richtlinienkonform in Verkehr gebracht wurden, dürfen danach weiter bereitgestellt werden.[168] Die grundlegenden Anforderungen an den Schutz gegen Korrumpierung und an die Sicherheit und Zuverlässigkeit von Steuerungen sind für vernetzte Maschinen neu.[168]

18. Februar 2027, Batterien. Batterien für leichte Verkehrsmittel (LV-Batterien), Industriebatterien über 2 kWh und Traktionsbatterien für Elektrofahrzeuge, die ab diesem Tag in Verkehr gebracht werden, brauchen einen Batteriepass mit Daten zur einzelnen Batterie, einschließlich Daten aus ihrer Nutzung.[169] Alle Batterien brauchen einen QR-Code, und Produkte mit Gerätebatterien müssen so gebaut sein, dass Endnutzer die Batterie entnehmen und ersetzen können.[169]

1.3 Geltungsbereich und Ausnahmen

Keine der Ausnahmen nimmt ein typisches Werkzeug, eine Maschine, ein Gebäudegerät oder einen Tracker aus dem Anwendungsbereich. Der CRA klammert Medizinprodukte, Fahrzeuge, Luftfahrt, Schiffsausrüstung und Verteidigung aus.[171] Die Unterschiede zwischen den Produkten stecken im Detail der einzelnen Rechtsakte.

CRA. Der CRA erfasst Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netz einschließt.[171] Abgesehen von der Meldepflicht fallen Bestandsprodukte nur dann unter den CRA, wenn sie nach Beginn seiner vollen Geltung wesentlich verändert werden.[171] EU-Baumusterprüfbescheinigungen, die nach anderen Harmonisierungsrechtsvorschriften der Union für Cybersicherheitsanforderungen ausgestellt wurden, bleiben bis zum 11. Juni 2028 gültig.[171]

Delegierte RED-Verordnung. Jede internetfähige Funkanlage muss seit dem 1. August 2025 das Netz schützen.[141] Sie muss auch personenbezogene Daten, Verkehrs- und Standortdaten schützen, wenn sie solche verarbeitet.[141] Der Rechtsakt schließt die Kommunikation „über andere Geräte“ ein. Deshalb fällt auch ein Bluetooth-Werkzeug darunter, das die Cloud über eine Smartphone-App erreicht.[141] Medizin- und IVD-Produkte sind von allen Anforderungen ausgenommen, Produkte

unter dem Luftfahrt-, dem Fahrzeug-Typgenehmigungs- und dem Mautrecht nur vom Datenschutz und vom Betrugsschutz, nicht vom Netzschutz.[141] Die delegierte Verordnung 2026/339 hebt den Rechtsakt mit Wirkung zum Beginn der vollen Geltung des CRA auf.[154] Von da an unterliegen Funkprodukte nur noch einem Cybersicherheitsregime, dem CRA, statt zweien.[154] Die Marktüberwachung prüft Funkanlagen, die bis zum 10. Dezember 2027 in Verkehr gebracht werden, weiterhin anhand der Anforderungen der delegierten Verordnung.[154]

Data Act. Ein vernetztes Produkt ist ein Gegenstand, der „Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt", diese übermitteln kann und „dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei als des Nutzers ist".[170] Die Zugangspflichten des Kapitels II gelten nicht für Kleinst- und Kleinunternehmen ohne große Partner- oder verbundene Unternehmen. Für mittlere Unternehmen greifen sie erst ein Jahr, nachdem diese zum mittleren Unternehmen geworden sind, oder ein Jahr nach dem Inverkehrbringen eines Produkts.[170] Ein kleines Unternehmen beschäftigt weniger als 50 Personen, ein mittleres weniger als 250.[138] Hersteller ab 100 Beschäftigten gewinnen damit höchstens ein Jahr Aufschub je Produkt.[170] Der Digital-Omnibus-Vorschlag der Kommission vom 19. November 2025 würde den Data Act ändern. Zum Zeitpunkt der Veröffentlichung befindet er sich in erster Lesung und ist noch nicht angenommen.[153, 174] Maßgeblich bleibt damit der geltende Text.

Maschinenverordnung. Akkuwerkzeuge und stationäre Maschinen fallen unter die Definition der Maschine: eine Gesamtheit mit einem anderen Antriebssystem als menschlicher oder tierischer Kraft und mindestens einem beweglichen Teil.[168] Eine Prüfung durch Dritte ist für sechs Kategorien Pflicht, darunter Sicherheitsbauteile und eingebettete Systeme mit selbstentwickelndem Verhalten, die maschinelles Lernen für Sicherheitsfunktionen nutzen.[168] Haushaltsgeräte für den häuslichen Gebrauch, Audio-, Video- und IT-Geräte, Büromaschinen und Niederspannungsschaltgeräte sind ausgenommen, soweit sie unter die Niederspannungsrichtlinie oder die RED fallen.[168]

Batterieverordnung. Eine Gerätebatterie ist gekapselt, wiegt höchstens 5 kg und ist „nicht speziell für industrielle Zwecke ausgelegt".[169] Jede Batterie über 5 kg, die keine Traktions-, LV- oder Starterbatterie ist, ist eine Industriebatterie.[169] Typische Werkzeugakkus und Trackerzellen sind daher Gerätebatterien und brauchen keinen Pass. Ein stationärer Heimspeicher ist dagegen eine Industriebatterie und braucht bei mehr als 2 kWh einen Pass.

1.4 Stand der harmonisierten Normen

Von den fünf Rechtsakten hat nur die RED harmonisierte Normen im Amtsblatt, für den CRA und die Maschinenverordnung ist noch keine veröffentlicht (Tabelle 2).[136, 148, 151, 159] Der Normungsauftrag zum CRA verlangt 41 Normen, die ersten zum 30. August 2026.[147] Seit August 2026 sind 17 vertikale CRA-Normentwürfe des ETSI in der öffentlichen Umfrage.[136] Die Umfrage endet je nach Produktkategorie zwischen Mitte September und Mitte November 2026.[136]

RECHTSAKT	STAND	RECHTSSTATUS
RED 2022/30	EN 18031-1, −2 und −3:2024 am 30. Jan. 2025 im Amtsblatt veröffentlicht, mit Einschränkungen (keine Konformitätsvermutung, wenn Nutzer Passwörter überspringen können; bei −2 Kindersicherung; bei −3 Abschnitt 6.3.2.4)	Amtlich
CRA	Normungsauftrag M/606 (C(2025) 618 vom 3. Feb. 2025): 41 Normen. Ursprüngliche Fristen: 2 horizontale Kernnormen 30. Aug. 2026, 26 vertikale Normen 30. Okt. 2026, 13 weitere horizontale Normen 30. Okt. 2027	Amtlicher Auftrag

RECHTSAKT	STAND	RECHTSSTATUS
CRA	ETSI: 17 vertikale Entwürfe seit 13. Aug. 2026 in öffentlicher Umfrage; horizontale Normen von CEN/CENELEC bis Ende 2026 geplant	Entwurf
Maschinenverordnung	Keine Normenliste unter der Verordnung 2023/1230 veröffentlicht; die Kommission erwartet die erste Liste vor Ende 2026	Entwurf
Maschinenrichtlinie	Liste aktualisiert durch Durchführungsbeschluss 2026/2015 vom 4. Sept. 2026; aufgehoben mit Wirkung zum 20. Jan. 2027	Amtlich, auslaufend
Leitfaden	BSI TR-03183 Teile 1, 2, 3 und H: unverbindlich, keine Konformitätsvermutung	Leitfaden

Tabelle 2: **Harmonisierte Normen je Rechtsakt**
Quellen: [54, 82, 136, 147, 148, 151, 155, 159].

KRITISCH
Noch keine Konformitätsvermutung für den CRA
Mit der Maschinenrichtlinie entfällt am 20. Januar 2027 auch ihre Normenliste, und eine Nachfolgeliste unter der Maschinenverordnung oder dem CRA gibt es noch nicht. Neue Maschinen kommen dann ohne Konformitätsvermutung aus harmonisierten Normen auf den Markt, bis die erste Liste erscheint.

Produkte der Klasse I des CRA dürfen sich nur selbst bewerten, wenn sie harmonisierte Normen, gemeinsame Spezifikationen oder ein europäisches Zertifizierungsschema vollständig anwenden.[171] Ohne sie brauchen sie eine notifizierte Stelle, die es unter dem CRA noch nicht gibt. Diese Produkte trifft die Lücke am härtesten.

1.5 Betroffene Hersteller und Umsetzungsstand

Von den 4.410 Herstellern mit 100 bis 4.999 Beschäftigten in DACH stellen nach unserer Schätzung 1.750 bis 3.440 vernetzte Produkte her, mehr als vier Fünftel davon in Deutschland (Abbildung 2).[37, 56, 175, 190, 367] Die Vorbereitung auf den CRA hinkt hinterher. Lediglich 3 % der befragten deutschen Industrieunternehmen halten sich für vollständig konform.[330]

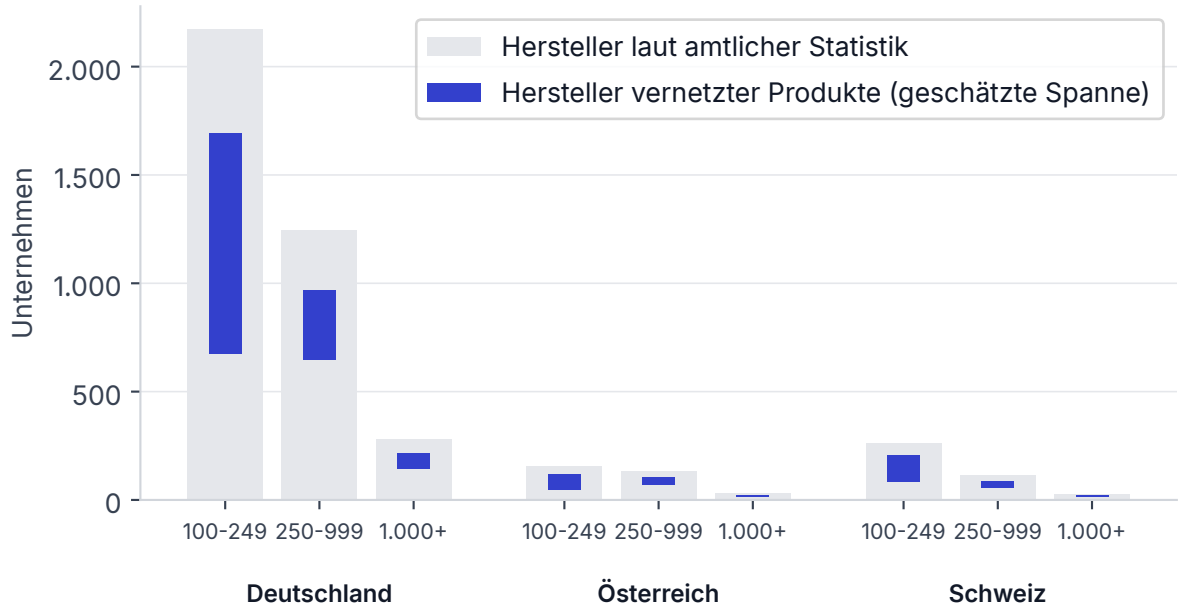


Abbildung 2: **Hersteller nach Land und Größenklasse**
Anmerkung: Schweiz 2024, sonst 2023. Quellen: [37, 56, 175, 190, 367].

Die Grundgesamtheit ist klein und konzentriert. In Deutschland stellen die 3.692 Unternehmen mit 100 und mehr Beschäftigten in Elektronik, Elektrotechnik, Maschinenbau und Medizintechnik (WZ 26, 27, 28 und 32.5) rund ein Drittel der 11.359 rechtlichen Einheiten dieser Zweige mit 20 und mehr Beschäftigten. Sie beschäftigen aber 1,77 Mio. der 2,11 Mio. tätigen Personen, also 84 %.[367] Die Größenklasse 100-249 stellt die meisten Unternehmen, hat aber den kleinsten Anteil an Herstellern vernetzter Produkte. Dort ist unsere Schätzung am unsichersten, mit einer Spanne von 673 bis 1.692 deutschen Herstellern vernetzter Produkte (Kapitel A.3).[37, 190, 367]

- **Vernetzte Funktionen sind bei größeren Unternehmen Standard.** Die große Mehrheit der 100 befragten deutschen Industrieunternehmen, die Produkte mit digitalen Elementen herstellen (94 %), bietet bereits updatefähige Produkte an.[331] Von 555 befragten Industrieunternehmen ab 100 Beschäftigten setzen 45 % IoT-Plattformen ein, weitere 33 % planen dies.[37]
- **Die Umsetzung hängt von der Unternehmensgröße ab.** Die Hälfte der befragten Unternehmen setzt den CRA bereits aktiv um, unter denen mit 500 und mehr Beschäftigten 59 %, unter den kleineren 37 %. Ebenso viele haben keine eigene externe Meldestelle für Schwachstellen, obwohl die Meldepflicht bereits gilt.[330, 331]
- **Software-Stücklisten fehlen meist.** Von 200 befragten deutschen Industrieunternehmen haben 18 % eine Software-Stückliste (SBOM) für alle betroffenen Produkte, 39 % haben ihre Software zumindest teilweise erfasst, und 24 % haben nichts unternommen.[307] Nur 46 % kennen den CRA.[307]
- **In der Breite der Wirtschaft ist der CRA kaum bekannt.** Von 1.003 befragten deutschen Unternehmen mit 10 und mehr Beschäftigten wissen 29 %, was der CRA für sie bedeutet.[36] Mehr als ein Viertel (28 %) hat noch nie von ihm gehört.[36]

KURZ GESAGT

Die Regulierung vernetzter Produkte ist kein Projekt für Dezember 2027, sondern verlangt schon heute einen Meldeprozess für verkaufte Geräte. Die Designentscheidungen für Produkte, die jetzt in die Entwicklung gehen, fallen ohne Normen als Leitplanke. Das nächste Kapitel zeigt, was die fünf Rechtsakte vom Gerät selbst verlangen.

2 Geräteanforderungen

Vertrauensanker und Geräteidentität lassen sich nach der Auslieferung nicht nachrüsten. Deshalb müssen die Sicherheitsfunktionen eines vernetzten Geräts bereits vor dem Design-Freeze feststehen. Aus den fünf Rechtsakten ergeben sich acht solcher Gerätefunktionen, und der Cyber Resilience Act (CRA) verlangt alle acht. Alle vier Beispielgeräte, vom Akkuwerkzeug bis zum Logistik-Tracker, fallen in die Standardklasse des CRA und dürfen ihre Konformität selbst bewerten. Nur ein eigenständig verkauftes Gateway kann als Router oder Firewall zu den wichtigen Produkten zählen und braucht dann eine notifizierte Stelle, die es unter dem CRA noch nicht gibt. Das Kapitel stellt diese vier Archetypen vor, leitet die Funktionen aus den Rechtstexten ab und zeigt, wo die Einstufung von einer Designentscheidung abhängt.

2.1 Vier Gerätearchetypen

Wir untersuchen Pflichten, Kosten und Architektur an vier Gerätearchetypen. Ein Archetyp ist ein typisches Gerät, das für eine ganze Produktgruppe steht und deren übliche Kombination aus Funktechnik, Weg in die Cloud und geltenden Rechtsakten mitbringt. Die vier Archetypen sind ein Akkuwerkzeug mit BLE-Tracker, eine Maschine mit Gateway, ein Gebäudegerät nach § 14a EnWG und ein Logistik-Tracker für Assets, Container und Anhänger.

1. Akkuwerkzeug mit BLE-Tracker. Ein Akkubohrschrauber, Schlagschrauber, Winkelschleifer oder eine Akkusäge mit wechselbarem Akkupack und Bluetooth-Low-Energy-Funk (BLE). Der Funk dient der Konfiguration und Diagnose per Smartphone-App, und der Besitzer kann das Werkzeug darüber orten. Die App leitet Daten an die Cloud des Herstellers weiter. Das Werkzeug ist eine Maschine im Sinne der Maschinenverordnung, eine angetriebene Gesamtheit mit beweglichen Teilen.[168] Der Akkupack ist eine Gerätebatterie, wenn er gekapselt ist, höchstens 5 kg wiegt und nicht speziell für industrielle Zwecke ausgelegt ist.[169]

2. Maschine mit Gateway. Eine stationäre Maschine (Werkzeug-, Verpackungs-, Prozess- oder Handhabungsmaschine), deren Steuerung über ein Edge-Gateway mit dem Netz des Betreibers oder einem Cloud-Dienst verbunden ist, per Ethernet, WLAN oder Mobilfunkmodem. Das Gateway kann in die Maschine eingebaut und mit ihr in Verkehr gebracht oder als Nachrüstprodukt separat verkauft werden. Davon hängt seine CRA-Klasse ab.

3. Gebäudegerät nach § 14a EnWG. Eine Wärmepumpe, Wallbox, Klimaanlage oder ein stationärer Batteriespeicher, den der Verteilnetzbetreiber nach § 14a Energiewirtschaftsgesetz drosseln darf.[61] Die Festlegung BK6-22-300 der Bundesnetzagentur vom 27. November 2023 regelt diese netzorientierte Steuerung seit dem 1. Januar 2024.[74] Ein gedrosseltes Gerät muss bei Direktansteuerung weiterhin mindestens 4,2 kW beziehen können.[74] Das Gerät empfängt ein Steuersignal und kann Energiedaten melden. Manche Modelle verbinden sich zusätzlich per WLAN oder Ethernet mit einer App.

4. Logistik-Tracker für Assets, Container und Anhänger. Ein batteriebetriebenes, gekapseltes Gerät mit Satellitenortung (GNSS), Mobilfunk (LTE-M, NB-IoT oder 2G/4G) und oft Bluetooth, montiert an Geräten, Containern oder Anhängern. Es meldet Position und Sensordaten wie Temperatur, Erschütterung oder Türstatus an eine Plattform des Flotten- oder Asset-Eigentümers. Es ist keine Maschine und wird von einer kleinen Gerätebatterie versorgt.

2.2 Acht Gerätefunktionen

Keiner der fünf Rechtsakte schreibt ein Bauteil vor oder verwendet das Wort „Secure Boot“. Sie beschreiben Ziele, die ein Entwicklungsteam in acht Funktionen umsetzen muss. Der CRA verlangt alle acht, die Maschinenverordnung sechs (Abbildung 3).[168, 171] Firmware-Integrität, Authentifizierung und Update-Mechanismus bestimmen die Hardware. SBOM, Schwachstellenmanagement und Protokollierung sind ebenso Prozess wie Technik. Datenexport und Produktidentifikation betreffen Daten, die das Gerät verlassen.

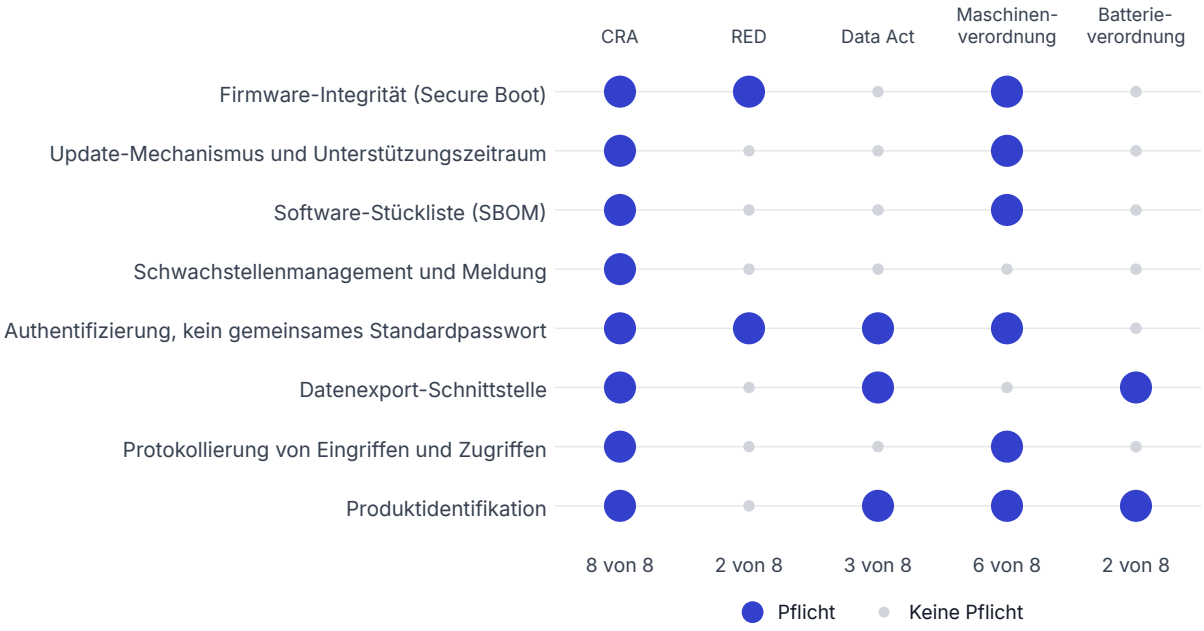


Abbildung 3: Gerätefunktionen je Rechtsakt
Anmerkung: Artikel und Anhangsnummern je Rechtsakt in Tabelle 22. Quellen: [141, 148, 168, 169, 170, 171].

Firmware-Integrität. Der CRA verlangt, gespeicherte, übermittelte und verarbeitete Daten, Befehle, Programme und die Konfiguration gegen nicht autorisierte Manipulation zu schützen, Korrumpierungen zu melden und die Folgen von Angriffen einzudämmen.[171] Die Maschinenverordnung verlangt, dass Software und Daten, die für die Einhaltung der Sicherheitsanforderungen kritisch sind, „als solche identifiziert“ und „angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt“ werden.[168] Beide Texte lassen den Mechanismus offen. Der Begriff Secure Boot erscheint nur in der Durchführungsverordnung 2025/2392, und zwar bei Mikrocontrollern und Mikroprozessoren, deren Sicherheitsfunktionen „andere Produkte … wie eine sichere Bootkette“ schützen.[149] Die übliche technische Lösung ist eine verifizierte Bootkette mit einem Vertrauensanker in der Hardware.

Update-Mechanismus und Unterstützungszeitraum. Schwachstellen müssen sich über Sicherheitsupdates beheben lassen, standardmäßig automatisch, mit Opt-out und Aufschubmöglichkeit.[171] Der Hersteller verteilt Updates sicher, unverzüglich und kostenlos und, wo technisch machbar, getrennt von Funktionsupdates.[171] Der Unterstützungszeitraum muss die erwartete Nutzungsdauer abbilden und mindestens fünf Jahre betragen, es sei denn, das Produkt wird voraussichtlich kürzer genutzt.[171] Jedes Sicherheitsupdate bleibt nach seiner Veröffentlichung mindestens zehn Jahre oder für den Rest des Unterstützungszeitraums verfügbar, je nachdem, was länger ist.[171] Das Ende des Unterstützungszeitraums ist dem Nutzer anzugeben.[171] Der Hersteller einer Maschine, die fünfzehn Jahre im Einsatz ist, richtet den Support deshalb an der erwarteten Nutzungsdauer aus, nicht an der Mindestfrist von fünf Jahren.

Software-Stückliste (SBOM). Hersteller müssen eine SBOM „in einem gängigen und maschinenlesbaren Format“ erstellen, die „zumindest die obersten Abhängigkeiten“ abdeckt.[171] Die Kommission kann Format und Elemente per Durchführungsrechtsakt festlegen.[171] Bis dahin macht die Technische Richtlinie TR-03183 Teil 2 (Version 2.1.0) des Bundesamts für Sicherheit in der Informationstechnik (BSI) formale und technische Vorgaben für die SBOM, unverbindlich und ohne Konformitätsvermutung.[54] Die Maschinenverordnung verlangt zusätzlich ein eigenes Software-Inventar. Die Maschine muss die für den sicheren Betrieb nötige Software identifizieren und diese Information „jederzeit in leicht zugänglicher Form“ bereitstellen können.[168]

Schwachstellenmanagement und Meldung. Nur der CRA verlangt diese Funktion. Er fordert unverzügliche Behebung, regelmäßige Sicherheitstests, die Veröffentlichung behobener Schwachstellen, eine Richtlinie zur koordinierten Offenlegung und eine Kontaktadresse für Meldungen.[171] Die Nutzerinformationen müssen eine zentrale Anlaufstelle nennen.[171] Seit dem 11. September 2026 gilt zudem die Meldekette nach Artikel 14.[171] BSI TR-03183 Teil 3 behandelt den Umgang mit eingehenden Schwachstellenmeldungen, ebenfalls unverbindlich.[54]

Authentifizierung. Vier der fünf Rechtsakte verlangen eine Authentifizierung. Der CRA fordert eine sichere Standardkonfiguration und Schutz vor unbefugtem Zugriff.[171] Unter der RED begründet keiner der drei Teile der EN 18031 eine Konformitätsvermutung, wenn „bei Anwendung der Abschnitte 6.2.5.1 und 6.2.5.2 der Nutzer kein Passwort festlegen und verwenden muss“.[148] Ein Einrichtungsablauf, bei dem der Nutzer das Passwort überspringen kann, fällt also aus der Norm heraus. Data Act und Maschinenverordnung setzen ebenfalls einen geschützten Zugang voraus.[168, 170]

Datenexport-Schnittstelle. Der Data Act verlangt den Datenzugang ab Werk für alle Produkte, die nach dem 12. September 2026 in Verkehr gebracht werden.[170] Produktdaten und Daten verbundener Dienste müssen samt der zur Auslegung nötigen Metadaten für den Nutzer „standardmäßig einfach, sicher, unentgeltlich, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt“ zugänglich sein.[170] Vor dem Kauf nennt der Verkäufer Art, Format und geschätztes Volumen der Daten, ob das Produkt kontinuierlich und in Echtzeit Daten erzeugt, wo es Daten speichert und wie der Nutzer darauf zugreift.[170] Der Dateninhaber stellt die ohne Weiteres verfügbaren Daten bereit, wenn der Nutzer nicht direkt am Gerät zugreifen kann, soweit relevant und technisch durchführbar „kontinuierlich und in Echtzeit“.[170] Auf Verlangen des Nutzers gibt er sie an Dritte weiter.[170] Übliche Umsetzungen sind ein Bluetooth-Dienst, ein OPC-UA- oder Modbus-Endpunkt oder eine authentifizierte Cloud-API, jeweils mit einem Datenkatalog, der zur vorvertraglichen Information passt. Das Gerät muss den Übertragungsweg nach dem CRA absichern.[171] Die Batterieverordnung verlangt für Batterien in ihrem Anwendungsbereich einen Pass, der Modelldaten mit Daten zur einzelnen Batterie verbindet, einschließlich Daten, die sich „aus der Nutzung dieser Batterie ergeben“.[169] Die Verbindung vom Gerät zum Backend des Batteriepasses fällt damit selbst unter die Pflicht, wenn allein das Batteriemanagementsystem die Nutzungsdaten liefert.

Protokollierung. Der CRA verlangt, relevante interne Aktivitäten einschließlich Zugriffen auf oder Änderungen an Daten, Diensten und Funktionen aufzuzeichnen und zu überwachen, mit Opt-out für den Nutzer, und mögliche unbefugte Zugriffe zu melden.[171] Die Maschinenverordnung geht am weitesten. Die Maschine muss „Nachweise über einen rechtmäßigen oder unrechtmäßigen Eingriff“ in sicherheitsrelevante Hardware, in die Software und in ihre Konfiguration sammeln.[168] Ihre Steuerung führt ein Protokoll der Eingriffsdaten und der nach dem Inverkehrbringen aufgespielten Versionen der Sicherheitssoftware, „für fünf Jahre nach dem Aufspielen“, zur Vorlage auf begründetes Verlangen einer nationalen Behörde.[168] Steuerungen mit selbstentwickelndem Verhalten bewahren zudem Daten zu sicherheitsrelevanten Entscheidungen ein Jahr auf.[168]

Produktidentifikation. Produkt oder Software müssen sich nach vier der fünf Rechtsakte eindeutig identifizieren lassen: nach dem CRA in den Nutzerinformationen,[171] nach dem Data Act in der vorvertraglichen Information,[170] nach der Maschinenverordnung für die sicherheitsrelevante Software[168] und nach der Batterieverordnung über den QR-Code, den ab dem 18. Februar 2027 jede Batterie trägt, und bei Industriebatterien über 2 kWh zusätzlich über den Batteriepass.[169]

2.3 Eine gemeinsame Sicherheitsbasis

Vier der fünf Rechtsakte verlangen im Kern dieselben wenigen Gerätefähigkeiten, und der CRA hält das selbst fest. Seine grundlegenden Anforderungen „umfassen alle Elemente“ der Cybersicherheitsanforderungen der RED.[171] Der CRA kann nach eigener Aussage auch die Einhaltung der Cybersicherheitsanforderungen der Maschinenverordnung erleichtern, sofern der Hersteller die Überschneidung über harmonisierte Normen und eine Risikobeurteilung nachweist, die diese Risiken erfasst.[171] Der Data Act, oft als Gegenspieler der Sicherheit verstanden, verlangt, dass der Zugang „sicher“ erfolgt, und erlaubt dem Dateninhaber, eine Weitergabe zu beschränken, die die Sicherheit des Produkts untergraben könnte.[170] Sechs Fähigkeiten bilden diese gemeinsame Basis (Tabelle 3).

FÄHIGKEIT	ERFÜLLT ANFORDERUNGEN VON	ZWECK
Hardware-Vertrauensanker und verifizierter Bootvorgang	CRA, RED, Maschinenverordnung	Schützt Firmware und Sicherheitssoftware gegen Manipulation
Eindeutige Geräteidentität, kein gemeinsames Standardpasswort	CRA, RED, Data Act	Voraussetzung für authentifizierten Datenexport und für die RED-Norm EN 18031
Signierte Over-the-Air-Updates mit Rollback-Schutz	CRA, Maschinenverordnung	Sicherheitsupdates mindestens fünf Jahre lang, jedes zehn Jahre abrufbar
Manipulationssicheres Ereignisprotokoll mit Versionsverlauf der Software	CRA, Maschinenverordnung	Maschinen müssen Eingriffe nachweisen und Sicherheitssoftware fünf Jahre protokollieren
Authentifizierter, dokumentierter Datenexport, lokal oder über die Cloud	Data Act, CRA	Nutzt dasselbe Identitäts- und Zugriffsmodell wie der Servicekanal
SBOM je Firmware-Release, Eingang für Schwachstellenmeldungen, festgelegter Meldeablauf	CRA	Seit dem 11. Sept. 2026 Pflicht, auch für Produkte im Einsatz

Tabelle 3: **Gerätefähigkeiten der gemeinsamen Sicherheitsbasis**

Ein Produkt mit gemeinsamem Standardpasswort und unsignierter Firmware fällt deshalb bei vier Rechtsakten zugleich durch. Auch ein einfacher Logistik-Tracker braucht diese Basis. Sein Nutzer, meist der Flottenbetreiber, hat nach dem Data Act ein Recht auf die Positions- und Sensordaten.[170] Die Tracker im Einsatz sind zudem genau der Bestand, für den die Meldepflicht des CRA bereits gilt.[171] Ein Gerät ohne eindeutige Zugangsdaten, signierte Updates und SBOM lässt sich weder patchen, noch kann der Hersteller eine Schwachstelle darin binnen 24 Stunden melden.

2.4 Pflichten je Archetyp

Jeder Archetyp fällt unter den CRA und den Data Act, und jeder hat eine Pflicht, die leicht übersehen wird (Tabelle 4).[170, 171] Mehrere Einstufungen hängen vom Design ab oder von einer Auslegungsfrage, die die Rechtstexte offenlassen. Der Hersteller muss seine Einstufung in diesen Fällen ausdrücklich dokumentieren.

RECHTSAKT UND ANFORDERUNG	AKKUWERKZEUG	MASCHINE	GEBÄUDEGERÄT	LOGISTIK-TRACKER
CRA: Anwendungsbereich, Meldung ab 11. Sept. 2026, vollständig ab 11. Dez. 2027	Ja	Ja, Maschine und Gateway	Ja	Ja
CRA: Klasse	Standard, das Bluetooth-Modul hebt die Klasse nicht an	Maschine: Standard. Gateway, eigenständig verkauft: bedingt Klasse I (Router) oder Klasse II (Firewall)	Standard, kein Smart-Home-Sicherheitsprodukt	Standard, kein Wearable
CRA: Konformitätsbewertung	Modul A	Maschine: Modul A. Gateway Klasse I: Modul A nur bei vollständig angewandten harmonisierten Normen, sonst B+C oder H. Klasse II: B+C, H oder EUCC	Modul A	Modul A
CRA: Unterstützungszeitraum	≥ 5 Jahre oder erwartete Nutzungsdauer	Erwartete Nutzungsdauer der Maschine, wenn länger als 5 Jahre	≥ 5 Jahre oder erwartete Nutzungsdauer	≥ 5 Jahre oder erwartete Nutzungsdauer
RED (VO 2022/30), Art. 3 Abs. 3 lit. d	Ja, auch bei Verbindung über die App	Bedingt: Gateway oder Steuerung mit Funk	Bedingt: Modelle mit WLAN oder Mobilfunk	Ja
RED (VO 2022/30), Art. 3 Abs. 3 lit. e	Ja, wenn Standort- oder Nutzerdaten verarbeitet werden	Bedingt: personenbezogene Daten auf HMI oder Gateway	Bedingt: personenbezogene Daten, z. B. Verbrauchsprofile	Ja: Standortdaten
Data Act, Art. 3 Abs. 1: Datenzugang ab Werk	Ja: Nutzungs-, Akku- und Standortdaten	Ja: Betriebsdaten der Maschine	Ja: Betriebs- und Energiedaten	Ja: Positions- und Sensordaten
Maschinenverordnung, Anhang III 1.1.9 / 1.2.1	Ja	Ja, Anhang I Teil A nur bei ML-basierten Sicherheitsfunktionen	Bedingt: Ausnahme für Haushaltsgeräte prüfen	Nein
Batterieverordnung: Batteriepass (Art. 77)	Nein, solange der Pack eine Gerätebatterie ist	Nur bei eingebauter Industriebatterie > 2 kWh	Speicher > 2 kWh: ja	Nein: Gerätebatterie
Batterieverordnung: QR-Code (Art. 13 Abs. 6)	Ja	Wenn Batterien eingebaut sind	Ja, für den Speicher	Ja
Batterieverordnung: Entnehmbarkeit durch Endnutzer (Art. 11)	Ja, Akkupacks sind bauartbedingt wechselbar	-	-	Ja, Ausnahme nur, wenn für die Sicherheit nötig

Tabelle 4: Anforderungen der fünf Rechtsakte je Archetyp
Anmerkung: Unsere Einstufung für das typische Design, „Bedingt“ dort, wo das Design oder eine offene Auslegung entscheidet. Quellen: [141, 149, 168, 169, 170, 171].

Akkuwerkzeug. Drei Regelwerke treffen in einem Gehäuse aufeinander. Als Maschine fällt das Werkzeug ab dem 20. Januar 2027 unter die Cybersicherheitsanforderungen der

Maschinenverordnung. Der App-Kanal darf keine Gefährdung verursachen, wenn er sicherheitsrelevante Parameter wie Drehzahl, Drehmoment oder Rückschlagerkennung ändern kann, und die Sicherheitsfirmware muss geschützt und identifizierbar sein.[168] Der BLE-Funk bringt die RED ins Spiel. Ein Werkzeug, das das Internet nur über das Smartphone des Nutzers erreicht, ist eine internetfähige Funkanlage, weil der Text die Kommunikation über andere Geräte einschließt.[141] Mit Standort- oder Nutzerdaten kommt die Datenschutzanforderung hinzu.[141] Das eingebaute Bluetooth-Modul ist selbst eine Netzschnittstelle der Klasse I, hebt die CRA-Klasse des Werkzeugs aber nicht an.[149, 171] Der Datenzugang ab Werk nach dem Data Act umfasst Nutzungs-, Akku- und Standortdaten.[170] Der Akkupack bekommt einen QR-Code, aber keinen Pass, solange er eine Gerätebatterie ist.[169] Ein Akkupack, der nur für den gewerblichen oder industriellen Einsatz vermarktet wird, kann dagegen als Industriebatterie gelten. Seine Einstufung ist deshalb ausdrücklich zu dokumentieren.

Maschine mit Gateway. Die Maschine selbst ist ein CRA-Produkt der Standardklasse, weil die Kernfunktion einer Werkzeugmaschine keiner Kategorie wichtiger oder kritischer Produkte entspricht.[171] Beim Gateway wird die Einstufung heikel. Ein eigenständig in Verkehr gebrachtes Gateway, dessen Kernfunktion die Weiterleitung von Datenverkehr zwischen Anlagennetz und Internet ist, entspricht der Beschreibung eines Routers und ist dann ein Produkt der Klasse I.[149] Ein Gateway, das nur als fester Bestandteil der Maschine verkauft wird, wird mit der Maschine bewertet, die in der Standardklasse bleibt. Dieselbe Hardware braucht zwei Einstufungen, wenn sie auf beiden Wegen verkauft wird. Ein Gateway, dessen beworbene Kernfunktion der Schutz des Anlagennetzes durch Überwachung und Beschränkung des Datenverkehrs ist, entspricht dagegen der Beschreibung einer Firewall. Es gehört zur Klasse II und braucht zwingend eine notifizierte Stelle oder eine Zertifizierung.[149] Ein routendes Gateway, das lediglich Firewall-Regeln mitbringt, bleibt nach unserer Lesart ein Router. Für den Bestand langlebiger Maschinen zählt das Zugangsrecht nach Artikel 4 des Data Act mehr als der Datenzugang ab Werk, der nur neu in Verkehr gebrachte Maschinen erfasst.[170] Die Maschine braucht eine notifizierte Stelle nach der Maschinenverordnung nur, wenn sie selbstentwickelnde, auf maschinellem Lernen beruhende Sicherheitsfunktionen enthält.[168]

Gebäudegerät. Eine Wärmepumpe oder Wallbox ist kein Smart-Home-Produkt mit Sicherheitsfunktionen, das die physische Sicherheit von Verbrauchern schützt, und bleibt daher im CRA in der Standardklasse.[149, 171] Ein Heim-Energiemanager, der zwischen Heimnetz und Internet routet, kann dagegen selbst ein Router sein. Ein Smart-Meter-Gateway im Steuerpfad nach § 14a ist ein kritisches Produkt.[171] Es gehört aber dem Messstellenbetreiber, nicht dem Gerätehersteller, und ändert die Klasse des Geräts nicht.[171] Der Hersteller muss zudem einstufen und dokumentieren, ob eine Haushaltswärmepumpe unter die Maschinenverordnung fällt oder unter deren Ausnahme für Haushaltsgeräte.[168] Ein stationärer Speicher über 5 kg gilt als Industriebatterie und braucht bei mehr als 2 kWh einen Pass.[169] Deshalb trifft der Batteriepass diesen Archetyp am stärksten.

Logistik-Tracker. Der Tracker ist ein CRA-Produkt der Standardklasse und eine internetfähige Funkanlage, die Standortdaten verarbeitet. Es gelten also beide RED-Buchstaben und damit EN 18031-1 und −2.[141, 148] Er ist kein Wearable der Klasse I, weil er an Waren montiert und nicht am Körper getragen wird.[149] Nach Lesart der Kommission umfasst diese Klasse Produkte, die Gesundheitsdaten erfassen.[149] Ein am Körper getragener Tracker, der nur die Position meldet, fällt nicht darunter. Ein Personen-Notsignalgerät mit Sturzerkennung ist im Einzelfall zu prüfen. Der Tracker bleibt ein vernetztes Produkt im Sinne des Data Act, weil er Daten im Namen seines Nutzers überträgt, nicht im Namen Dritter.[170] Die am wenigsten beachtete Pflicht steht in der Batterieverordnung. Ab dem 18. Februar 2027 muss eine Gerätebatterie in einem Produkt mit handelsüblichem Werkzeug „vom Endnutzer leicht entnommen und ersetzt werden“ können, und

eine Anleitung dazu muss online verfügbar sein.[169] Ein vergossener, verklebter oder verschweißter Tracker erfüllt das nicht. Die Ausnahme für Geräte, die überwiegend in nasser Umgebung eingesetzt werden, gilt nur, wenn sie für die Sicherheit nötig ist.[169] Ein IP67-Tracker am Anhänger fällt deshalb nur mit dieser Begründung darunter. Ohne sie muss sich das Batteriefach mit handelsüblichem Werkzeug öffnen lassen.

2.5 Wege der Konformitätsbewertung

Der CRA stuft ein Produkt nach seiner Kernfunktion ein, nicht nach den Komponenten, die es enthält. Ein Produkt, dessen Kernfunktion einer Kategorie in Anhang III entspricht, ist wichtig (Klasse I oder II), eines nach Anhang IV kritisch, alles andere gehört zur Standardklasse.[171] Die Durchführungsverordnung 2025/2392 beschreibt seit dem 21. Dezember 2025 jede Kategorie. Sie bestätigt, dass das Produkt „als Ganzes“ entscheidet. Eine Komponente mit der Kernfunktion eines wichtigen Produkts macht das Produkt, in das sie eingebaut ist, nicht schon dadurch wichtig.[149] Ein Produkt, das die Funktionen einer Kategorie ausführen kann, fällt nicht unter diese Kategorie, wenn seine Kernfunktion eine andere ist, so wie ein Smartphone kein Betriebssystem ist.[149] Nur Produkte der Standardklasse dürfen sich stets selbst bewerten, Produkte der übrigen Klassen nur unter Bedingungen oder gar nicht (Tabelle 5).[171]

KLASSE	RELEVANTE ANHANGSEINTRÄGE	KONFORMITÄTSBEWERTUNG
Standard	Alles, was nicht in Anhang III oder IV steht, darunter Werkzeuge, Maschinen, Wärmepumpen, Wallboxen und Tracker	Modul A (interne Kontrolle); B+C, H oder Zertifizierungsschema freiwillig
Wichtig, Klasse I	III-I.8 Bootmanager; III-I.10 physische und virtuelle Netzschnittstellen (inkl. Bluetooth-, WLAN-, Ethernet-, Feldbusadapter); III-I.11 Betriebssysteme (inkl. Echtzeit-Betriebssysteme); III-I.12 Router, Modems für die Internetverbindung (inkl. Mobilfunkmodems), Switches; III-I.14 Mikrocontroller mit Sicherheitsfunktionen; III-I.17 Smart-Home-Produkte mit Sicherheitsfunktionen	Modul A nur bei vollständiger Anwendung harmonisierter Normen, gemeinsamer Spezifikationen oder eines europäischen Zertifizierungsschemas der Stufe „substanziell“; sonst B+C oder H mit notifizierter Stelle
Wichtig, Klasse II	III-II.2 Firewalls, Angriffserkennungs- und -abwehrsysteme; III-II.4 manipulationssichere Mikrocontroller (AVA_VAN 2 oder 3)	B+C, H oder europäisches Zertifizierungsschema der Stufe „substanziell“
Kritisch	IV.2 Smart-Meter-Gateways und andere Geräte für fortgeschrittene Sicherheitszwecke; IV.3 Chipkarten und ähnliche Geräte einschließlich Secure Elements	Europäisches Zertifikat, wo ein delegierter Rechtsakt nach Art. 8 Abs. 1 es verlangt; sonst die Verfahren der Klasse II

Tabelle 5: CRA-Produktklassen und Konformitätsbewertung
Quellen: [149, 171].

In den Komponenten der vier Archetypen stecken viele wichtige und kritische Produkte: das Bluetooth- oder Mobilfunkmodul, das Echtzeit-Betriebssystem und der Mikrocontroller mit Secure Boot in Klasse I, das Secure Element als kritisches Produkt. Ihre Hersteller brauchen dafür eine eigene Konformitätsbewertung. Werkzeug, Maschine, Wärmepumpe und Tracker bleiben trotzdem in der Standardklasse.[149, 171] Der Kauf CRA-konformer Komponenten spart also Arbeit, ersetzt aber nicht die eigene Bewertung des ganzen Produkts.

Die Einstufung eines Gateways fällt am teuersten aus. Ein Gateway der Klasse I kann sich nicht selbst bewerten und braucht eine notifizierte Stelle, solange keine harmonisierte CRA-Norm im Amtsblatt steht.[171] Unter dem CRA ist noch keine Stelle notifiziert.[161] Der Normungsauftrag M/606 der Kommission sieht die Normen für Router, Modems und Switches und für Firewalls, ausdrücklich

auch für solche im industriellen Einsatz, bis zum 30. Oktober 2026 vor.[147] Die Veröffentlichung im Amtsblatt folgt erst danach. BSI TR-03183 Teil H beschreibt, wie ein Hersteller ein ISO/IEC-27001-konformes Managementsystem für die Bewertung nach Modul H nutzen kann.[54] Für ein Gateway mit Markteinführung 2028 ist die notifizierte Stelle damit der Planungsfall. Eine bis dahin im Amtsblatt veröffentlichte Norm wäre ein Gewinn, aber keine Planungsgrundlage.

KURZ GESAGT

Für die meisten Hersteller ist die Konformität damit eine Aufgabe der Entwicklung, nicht der Zulassung. Nur der eigenständige Verkauf eines Gateways macht sie von Normen und notifizierten Stellen abhängig, die noch fehlen. Das nächste Kapitel zeigt, was die acht Funktionen je Gerät und Monat kosten.

3 Kosten je Gerät

Ein Hersteller vernetzter Produkte bezahlt Funk, Cloud und Sicherheit Monat für Monat, solange seine Geräte im Einsatz sind, und muss diese Kosten in seine Preise einkalkulieren. Im Basisfall kostet die Connectivity- und Sicherheitsschicht 0,50-3,10 € je Gerät und Monat, das Trägerprodukt nicht enthalten. Auf die Sicherheit entfallen davon bei jedem Archetyp 0,40-0,48 €, und nur die Flottengröße verändert diesen Betrag nennenswert. Das Kapitel gibt einen detaillierten Einblick in Basiskosten und Sicherheitsaufschlag, ordnet die Kosten des Cyber Resilience Act (CRA) und des Data Act ein und zeigt, wie Flottengröße, Funktechnik und Produktklasse den Aufschlag verändern.

3.1 Laufende Monatskosten

Für diesen Bericht haben wir ein eigenes Kostenmodell aufgebaut. Es rechnet vier Archetypen durch: ein Akkuwerkzeug mit BLE-Tracker, eine Maschine mit Mobilfunk-Gateway, ein Gebäudegerät nach § 14a EnWG und einen Logistik-Tracker. Das Modell erfasst die Connectivity- und Sicherheitsschicht vom Funkchip bis zur Konformitätsbewertung zu veröffentlichten Listenpreisen, nicht aber Motor, Akku, Gehäuse und Hauptsteuerung des Trägerprodukts. Einmalkosten je Gerät wie Chips, SIM-Pakete und Zertifikate verteilen wir auf 60 Monate. Einmalkosten je Produkt wie sichere Entwicklung, Dokumentation und Konformitätsbewertung legen wir auf alle Geräte der Flotte und auf 60 Monate um, Monatsgebühren auf Flottenebene, etwa für eine Zertifizierungsstelle (CA) oder ein Tool-Abonnement, auf alle Geräte der Flotte. Im Basisfall rechnen wir mit 10.000 Einheiten über fünf Jahre (Positionen, Annahmen und Sensitivität in Anhang C).

Nach unserem Modell kostet ein konformes Akkuwerkzeug im Basisfall 0,50 € im Monat, die Maschine 3,10 €. Das Gebäudegerät liegt mit 0,59 € und der Logistik-Tracker mit 0,99 € dazwischen. Mobilfunktarif und dauerhafter Cloud-Verkehr machen bei der Maschine zusammen fast vier Fünftel der Summe aus (2,44 von 3,10 €). Die Funktechnik entscheidet also über die Gesamtkosten (Abbildung 4).

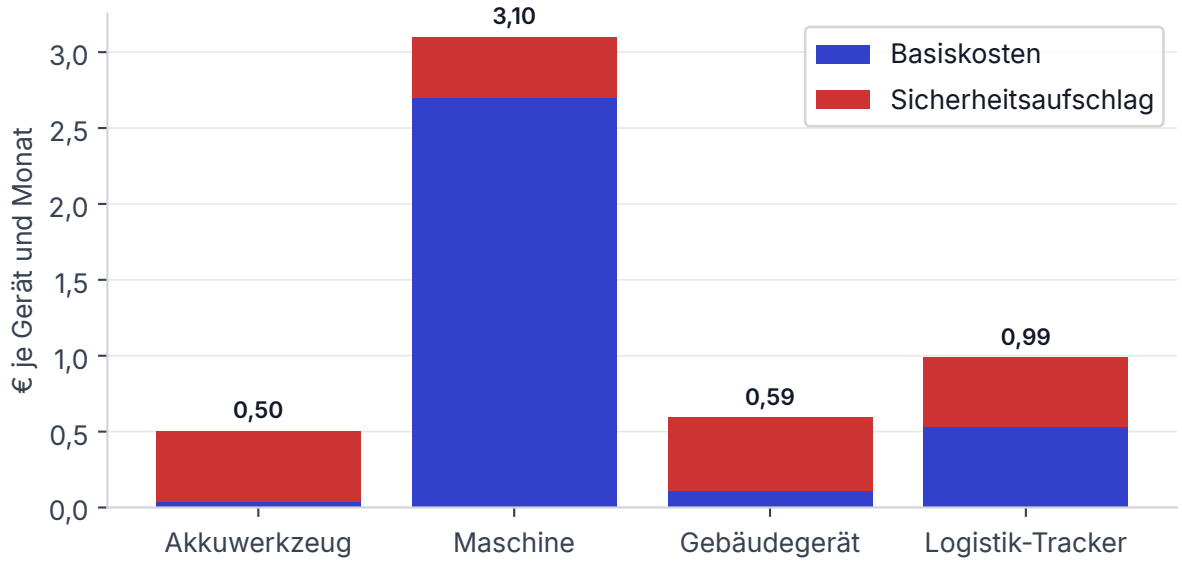


Abbildung 4: Kosten je Gerät und Monat nach Archetyp
Quelle: RUBINLAKE-Kostenmodell.

Der Sicherheitsaufschlag ist dagegen bei allen Archetypen nahezu gleich hoch, 0,40-0,48 € je Gerät und Monat. Er umfasst Secure Element, Public-Key-Infrastruktur (PKI), signierte Over-the-Air-Updates (OTA), Software-Stückliste (SBOM) und Werkzeuge für das Schwachstellenmanagement, sichere Entwicklung, Dokumentation und Konformitätsbewertung. Der Aufschlag schwankt kaum. Sein Anteil an den Gesamtkosten hängt deshalb von den Basiskosten ab. Bei der Maschine macht er 13 % der Monatskosten aus, beim Akkuwerkzeug 93 % (Tabelle 6). Bei Geräten ohne SIM kostet die Konformität mehr als die Connectivity; bei Geräten mit SIM wiegt der Tarif schwerer als das Gesetz.

ARCHETYP	BASISKOSTEN (€/MONAT)	SICHERHEITS-AUFSCHLAG (€/MONAT)	SUMME (€/MONAT)	AUFSCHLAG ÜBER 5 JAHRE JE EINHEIT (€)	ANTEIL DES AUFSCHLAGS (%)
Akkuwerkzeug mit BLE-Tracker	0,04	0,47	0,50	28,06	93
Maschine mit Gateway	2,70	0,40	3,10	24,09	13
Gebäudegerät nach § 14a EnWG	0,11	0,48	0,59	28,92	81
Logistik-Tracker	0,53	0,46	0,99	27,49	46

Tabelle 6: Basiskosten und Sicherheitsaufschlag je Archetyp
Anmerkung: Rundungsdifferenzen möglich. Quelle: RUBINLAKE-Kostenmodell.

3.2 Anteil der CRA-Konformität

In unserem Modell beträgt der Kostenblock für die CRA-Konformität je Produkt im Basisfall 0,175 € je Gerät und Monat, rund zwei Fünftel des Aufschlags (36-44 %). Wir übernehmen dafür die Schätzungen der Kommission je Produkt, die einzigen veröffentlichten Werte dieser Art. Bei durchschnittlichen Entwicklungskosten von 140.000 € veranschlagt die Kommission für sichere Entwicklung zusätzlich 30,5 % (42.700 €), für Dokumentation und Meldungen 9 % (12.600 €) und

für die Selbstbewertung 18.400 €.[144] Für eine Bewertung durch Dritte setzt sie 25.000 € an, für wiederkehrende Prüfungen 3.000-5.000 € je Produkt.[144]

Wir haben diesen Kostenblock bewusst vorsichtig gerechnet und setzen alle Werte voll an, als hätte der Hersteller heute noch keine umfassenden Sicherheitsmaßnahmen. Die Kommission selbst rechnet jedoch etwa die Hälfte des Aufwands für sichere Entwicklung dem üblichen Geschäftsbetrieb zu. Ihren eigenen Wert für die Dokumentation bezeichnet sie als nicht überprüft und vermutlich zu hoch.[144]

EU-weit erwartet die Kommission Konformitätskosten von bis zu rund 29 Mrd. €. Dem stehen jährlich 180-290 Mrd. € an vermiedenen Schäden durch Sicherheitsvorfälle in Unternehmen gegenüber, hochgerechnet aus der Schadensschätzung des Bitkom für Deutschland.[142, 144] Der Regierungsentwurf des deutschen Durchführungsgesetzes weist keinen eigenen Erfüllungsaufwand für die Wirtschaft aus.[100]

Die Gebühren notifizierter Stellen sind der am wenigsten transparente Kostenposten. Nur wenige Stellen veröffentlichen ihre Preise. Serma bietet eine EU-Baumusterprüfung nach der Funkanlagenrichtlinie (RED) durch das LCIE (notifizierte Stelle 0081) ab 3.900 € an.[359] Für die RED schätzt die Kommission die Prüfung durch Dritte je Modell auf 5.000-15.000 € bei einfachen Produkten und auf 50.000 € oder mehr bei stark softwareabhängigen Geräten.[140]

3.3 Data-Act-Kosten auf Unternehmensebene

Der Data Act verursacht Kosten je Unternehmen, nicht je Gerät. Die Kommission beziffert die Kosten für den Zugang zu Produktdaten auf höchstens 300.000 € im Jahr je kleinem oder mittlerem Unternehmen (KMU) und 1 Mio. € je Großunternehmen.[143] Für den gesamten IoT-Markt schätzt sie 410 Mio. € einmalig und 88 Mio. € im Jahr. Kosten je Produkt nennt sie nicht.[143]

Die Obergrenze kann den gesamten Sicherheitsaufschlag übersteigen, wenn ein Unternehmen sie auf seine Flotte umlegt. Für ein KMU an der Obergrenze von 300.000 € ergäben sich bei 10.000 Einheiten 2,50 € je Gerät und Monat. Für ein Großunternehmen, das 1 Mio. € auf 100.000 Geräte verteilt, wären es 0,83 €.[143] Die Kosten je Gerät dürften nur einen Bruchteil dieser Werte ausmachen, wenn ein Produkt seine Daten bereits über eine dokumentierte Cloud-API exportiert.

3.4 Sicherheitskosten über den Lebenszyklus

Über fünf Jahre summiert sich der Sicherheitsaufschlag in unserem Modell auf 24-29 € je Einheit, von 24,09 € bei der Maschine bis 28,92 € beim Gebäudegerät. Er setzt sich aus vier Posten zusammen:

- **Signierte OTA-Updates:** etwa die Hälfte des Aufschlags. Der Preis von Golioth, 0,25 USD je Gerät und Monat, entspricht 0,22 € und damit 48 % des Aufschlags beim Akkuwerkzeug.[199] Über AWS IoT Device Management kosten die OTA-Updates der Maschine 0,15 € im Monat, überwiegend für Secure Tunnels, kaum für die Update-Jobs selbst.[16]
- **CRA-Konformität je Produkt:** 0,175 € im Monat.
- **PKI:** 0,04 € im Monat. Die Monatsgebühr von 400 USD für AWS Private CA verteilt sich auf alle Geräte der Flotte. Ein Zertifikat kostet bis zu einer Menge von 10.000 Stück 0,35-0,75 USD.[19]
- **Sicherheits-Hardware:** unter 0,05 € im Monat, einmalig 1,13-2,56 € je Einheit.[112, 114]

Das Secure Element ist der kleinste Posten. Der ATECC608B kostet zu Rollenpreisen 0,725 USD bei 3.000 Stück, der STSAFE-A110 1,27 USD bei 5.000 und der SE050C2 2,87 USD bei 3.000.[108, 112, 114] Die vorprovisionierte Trust&GO-Variante kostet 1,91 USD, mehr als das Doppelte des unprovisionierten Bauteils. Mit dem Aufpreis bezahlt der Hersteller das Einbringen der Schlüssel in

der Fertigung.[108] Eine Einsparung beim Chip bringt nur wenige Cent im Monat. Die laufenden Dienste bestimmen die Kosten über die Lebensdauer.

3.5 Flottengröße als wichtigster Kostentreiber

Die Flottengröße wiegt schwerer als jedes Bauteil. In unserem Modell steigt der Sicherheitsaufschlag bei 1.000 Einheiten auf rund 2,30 € je Gerät und Monat (2,30-2,38 €), rund das Fünffache des Basisfalls. Bei 100.000 Einheiten sinkt er unter 0,30 € (0,21-0,29 €). In der kleinen Flotte verteilt sich der Kostenblock für die Konformität auf ein Zehntel der Geräte. Allein die CA-Gebühr von 400 USD im Monat macht dann 0,36 € je Gerät aus.[19] Zwei Maßnahmen senken den PKI-Anteil: der AWS-Modus für kurzlebige Zertifikate zu 50 USD im Monat[19] oder eine gemeinsame CA für alle Produktlinien eines Herstellers.

Bei 100.000 Einheiten werden die OTA-Updates zum größten Posten des Aufschlags. Die Wahl des Update-Dienstes wiegt dann schwerer als jede andere Entscheidung. Azure Device Update kostet 0,07 USD je Gerät und Monat,[266] nRF Cloud ab 0,10 USD[285] und Golioth 0,25 USD.[199] balena berechnet 2,00 USD je weiterem Gerät, fast das Dreißigfache des Azure-Preises.[28]

Die Funktechnik verändert die Basiskosten, nicht den Aufschlag. Bei der Maschine senkt der Tarif CMP Mobile Lite von Swisscom zu 1,00 CHF die Basiskosten von 2,70 auf 1,70 €, enthält aber kein Roaming.[376] Beim Gebäudegerät erhöht LTE-M anstelle des Kunden-WLANs die Basiskosten von 0,11 auf 0,57 €, gerechnet mit einem nRF9151 und dem LPWA-Paket der Telekom zu 14,50 €.[96] Beim Tracker kostet LoRaWAN über The Things Stack im Monat etwa so viel wie LTE-M (0,52 gegenüber 0,53 €), braucht aber einen eigenen GNSS-Chip (MAX-M10S, 9,33 USD bei 500).[115, 385] LoRaWAN erreicht Anhänger und Container nur in Reichweite eigener oder per Roaming erreichbarer Gateways.[385] Ein Satellitentarif von Myriota zusätzlich zu LTE-M erhöht die Basiskosten auf 1,41 €, noch ohne das Satellitenmodem, für das Myriota keinen Preis veröffentlicht.[274]

Die Produktklasse verändert die Kosten je Gerät kaum. Eine Bewertung durch Dritte zum Durchschnittswert der Kommission von 25.000 € erhöht den Aufschlag im Basisfall um 0,011 € im Monat.[144] Bei 50.000 €, dem Schätzwert der Kommission für softwarelastige Funkanlagen, sind es 0,053 €.[140] Der Aufschlag sinkt um 0,036 €, wenn die Hälfte der Kosten für sichere Entwicklung ohnehin anfällt.[144] Die Produktklasse ist eine Frage der Vorlaufzeit, nicht der Kosten je Gerät.

KURZ GESAGT

Nicht die gesetzlich verlangte Sicherheit macht ein vernetztes Produkt teuer, sondern eine kleine Flotte, ein Mobilfunktarif und ein eigenes Backend je Produktlinie. Produktplanung und Einkauf legen diese Posten fest, bevor es harmonisierte Normen gibt. Das nächste Kapitel zeigt, welche Bauteile und welche Architektur hinter diesen Kosten stehen.

4 Technologie und Architektur

Ein vernetztes Produkt setzt die Geräteanforderungen der fünf Rechtsakte in sechs technischen Schichten zwischen Funkchip und ERP-System um. Keine dieser Schichten deckt für sich allein einen ganzen Rechtsakt ab. Die meisten Bausteine sind zertifiziert am Markt erhältlich, darunter Secure Elements, Mikrocontroller mit einer der 316 PSA-Zertifizierungen sowie Dienste für Updates und Zertifikate. Die Lücken liegen in Prozessen, die kein Anbieter verkauft, nämlich in der Provisionierung in der Fertigung, in einem Sicherheitsteam, das die 24-Stunden-Meldefrist einhält, und in einem Update-Mechanismus über den gesamten Unterstützungszeitraum. Das Kapitel behandelt die Schichten von der Funkstrecke aufwärts, ordnet ihnen die Pflichten der Rechtsakte zu und fügt sie je Archetyp zu einer Referenzarchitektur zusammen.

4.1 Connectivity

Die Funktechnik entscheidet, wie lange ein Produkt für Updates erreichbar bleibt. Die letzten 2G-Netze in Deutschland und Österreich werden 2028 abgeschaltet, also noch im Unterstützungszeitraum eines Produkts, das 2027 auf den Markt kommt.[6, 77] Die Telekom will ihr 2G-Netz zum 30. Juni 2028 abschalten, Vodafone im September 2028 (einzelne kritische IoT-Anwendungen bis 2030) und Telefónica Ende 2028.[77] A1 in Österreich plant die Abschaltung zum 31. Mai 2028.[6] 3G ist in allen drei Ländern bereits abgeschaltet, in der Schweiz auch 2G.[47, 373, 413] Der Cyber Resilience Act (CRA) verlangt Updates über den gesamten Unterstützungszeitraum.[171] Ein Funknetz, das vorher abgeschaltet wird, macht das Produkt damit zum Compliance-Risiko. Neuentwicklungen kommen ohne 2G-Rückfallebene aus; für Bestandsgeräte mit 2G-Modulen braucht der Hersteller einen Migrationsplan.

LTE-M und NB-IoT sind die stromsparenden Mobilfunkverfahren mit bundesweiter Abdeckung und ohne angekündigtes Abschaltdatum. Die Telekom hat den bundesweiten LTE-M-Ausbau im Juli 2020 abgeschlossen.[94] Vodafone deckte Ende 2020 mit LTE-M mehr als 90 % und mit NB-IoT mehr als 97 % der Fläche Deutschlands ab.[408] LTE-M unterstützt Zellwechsel in Bewegung und überträgt auch Firmware-Images, NB-IoT dringt tiefer in Gebäude ein. Ein System-in-Package wie das Nordic nRF9151 nimmt im Power Saving Mode (PSM) 2,7 µA auf.[284] 5G RedCap (3GPP Release 17)[5] ist der Nachfolger für Geräte mit höherem Bandbreitenbedarf. Der Markt dafür ist noch jung. Das erste kommerzielle RedCap-Gerät in Deutschland war im September 2025 eine Smartwatch.[95] Für 2027 kommt RedCap daher als Option für das Maschinen-Gateway infrage, nicht als Standard.

Drei weitere Netze betreibt der Kunde oder der Versorger, nicht der Gerätehersteller. Die Bundesnetzagentur (BNetzA) teilt seit November 2019 Frequenzen im Band 3,7-3,8 GHz für lokale 5G-Campusnetze zu, gegen eine Gebühr ab 1.000 €.[80] Bis November 2025 zählte sie dort 484 Zuteilungen,[75] im 26-GHz-Band 27.[76] Die 450connect erhielt 2021 die Frequenzen im 450-MHz-Band für die Energie- und Wasserwirtschaft,[73] befristet bis zum 31. Dezember 2040.[72] Über dieses Netz läuft auch Smart-Meter-Verkehr. LoRaWAN (ITU-T Y.4480)[254] arbeitet bei 868 MHz mit einem Tastgrad unter 1 %.[84] Firmware-Updates sind deshalb auf kleine Deltas beschränkt. In Deutschland gibt es kein bundesweites öffentliches LoRaWAN-Netz. Allein Netze BW betreibt bis zu 3.000 Gateways.[255]

Im Nahbereich bestimmt das Recht das Pairing stärker als die Funktechnik. Bluetooth Low Energy (BLE) bietet LE Secure Connections[41] und seit Core 6.0 Channel Sounding zur Abstandsmessung.[42] Die EN 18031-1 begründet keine Konformitätsvermutung, wenn der Nutzer gar kein Passwort setzen

muss.[148] „Just Works“-Pairing reicht daher als einziger Schutz für ein Werkzeug, das Befehle annimmt, nicht aus. Neue Wi-Fi-CERTIFIED-Geräte müssen seit 2020 WPA3 unterstützen.[411] Galileo authentisiert seine Navigationsnachrichten seit dem 24. Juli 2025 mit OSNMA, und ein Tracker erkennt damit gefälschte Positionen.[176]

4.2 Sicherheitsschicht im Gerät

Die Sicherheitsschicht des Geräts stellt den größten Teil der Sicherheitseigenschaften bereit, die der CRA vom Produkt verlangt.[171] Zugriffsschutz, Vertraulichkeit, Integrität und die Abwehr von Exploits hängen von ihr ab. Zugleich ist sie die Schicht, für die das Angebot an zertifizierten Bausteinen am vollständigsten ist. Sie setzt außerdem die Pflicht der Maschinenverordnung um, sicherheitsrelevante Software gegen Korrumpierung zu schützen und Nachweise über Eingriffe zu erfassen.[168]

Die Schlüssel liegen entweder in einem eigenen Baustein, einem Secure Element oder Trusted Platform Module (TPM), oder in einem isolierten Bereich des Hauptmikrocontrollers. Fünf von sieben gängigen Bausteinen sind nach Common Criteria (CC) zertifiziert (Tabelle 7). Das NIST führt FIPS-140-2-Zertifikate seit September 2026 nur noch als historisch. Für bereits eingesetzte Module gelten sie weiter. Neue Ausschreibungen, die FIPS verlangen, setzen aber FIPS 140-3 voraus. Der TA100-Nachfolger TA101 ist nach FIPS 140-3 Level 2 zertifiziert.[261, 276, 277, 278] Der ATECC608B hat kein Zertifikat, und eine seiner Varianten empfiehlt Microchip nicht mehr für Neuentwicklungen.[263] Ein TPM 2.0[394] eignet sich für ein Linux-Gateway mit Measured Boot, ein Secure Element für ein Gerät auf Mikrocontroller-Basis.

BAUSTEIN	HERSTELLER	ZERTIFIZIERUNG	PROVISIONIERUNG
EdgeLock SE050	NXP	CC EAL6+ bis Betriebssystemebene; FIPS 140-2 Level 3 für die Variante SE050F (historisch seit September 2026)	EdgeLock 2GO
EdgeLock SE051	NXP	CC EAL6+ mit AVA_VAN.5; IEC 62443-4-2 für die anwendbaren Anforderungen	EdgeLock 2GO
OPTIGA Trust M	Infineon	CC EAL6+	Trust M Express, vorregistriert für AWS IoT und Azure IoT Hub
ATECC608B	Microchip	kein CC- oder FIPS-Zertifikat	Trust&GO (vorprovisioniert, Mindestmenge 10), TrustFLEX, TrustCUSTOM
TA100	Microchip	FIPS 140-2 Level 2 (historisch seit September 2026; Nachfolger TA101: FIPS 140-3 Level 2); AEC-Q100 Grade 1	TrustFLEX / kundenspezifisch
STSAFE-A110	ST	CC EAL5+ AVA_VAN.5	Personalisierungsdienst von ST
OPTIGA TPM SLB9672	Infineon	TPM 2.0; CC EAL4+ AVA_VAN.4 (BSI-DSZ-CC-1277-2026); FIPS 140-2 Level 2 (historisch seit September 2026)	vorinstallierter Endorsement Key

Tabelle 7: **Zertifizierung gängiger Secure Elements und TPM**
Quellen: [51, 217, 218, 297, 298, 368].

Die PSA-Certified-Stufe ist der maßgebliche Nachweis, wenn die Schlüssel im Mikrocontroller bleiben. Die PSA-Certified-Datenbank enthält 316 Zertifizierungen von 123 Unternehmen, darunter Level 3 für STM32U585, NXP MCX N94x/N54x und Silicon Labs EFR32MG21B.[326] Auf Armv8-M-

Bausteinen trennt TrustZone eine sichere Partition ab. Trusted Firmware-M ist die Referenzimplementierung.[395] Level 2 weist in einer 25-tägigen Laborprüfung nach, dass der Vertrauensanker Softwareangriffen standhält; Level 3 schließt erhebliche Hardwareangriffe ein.[325] Beide Stufen beruhen auf der SESIP-Methodik von GlobalPlatform, das im September 2025 die Trägerschaft von PSA Certified übernommen hat.[194] SESIP ist als EN 17927:2023 veröffentlicht.[83] Nordic bewirbt den nRF54L15 als auf Level 3 ausgelegt, das Zertifikat vom Januar 2026 lautet jedoch auf Level 1.[326] Ein Zertifikat zahlt sich vor allem durch Wiederverwendung aus. NXP zeigt, wie ein Hersteller das Security Target eines Chips als Nachweis für EN 18031 und IEC 62443-4-2 weiterverwendet.[295]

Eine Entwicklung nach IEC 62443 und EN 18031 erbringt solche wiederverwendbaren Nachweise, begründet aber noch keine Konformitätsvermutung nach dem CRA. Die 41 harmonisierten Normen zum CRA entstehen erst unter dem Normungsauftrag M/606, und im Amtsblatt steht noch keine.[151] Die Normenreihe EN 18031 zur Funkanlagenrichtlinie (RED) ist dagegen seit Januar 2025 mit Einschränkungen im Amtsblatt veröffentlicht.[145, 148] IEC 62443-4-1 regelt den Entwicklungsprozess,[208] IEC 62443-4-2 die Anforderungen an Komponenten[117, 209] und ETSI EN 303 645 das Grundschutzniveau für Verbraucher-IoT.[135]

Secure Boot vervollständigt die Schicht. MCUboot ist der gängige quelloffene Bootloader für 32-Bit-Mikrocontroller.[258] Linux-Gateways nutzen U-Boot Verified Boot mit einer vom TPM gemessenen Startkette. Updates folgen der Architektur von RFC 9019[214] mit einem signierten Manifest nach RFC 9124.[215] Der Bootloader prüft die Signatur gegen einen Schlüssel im Vertrauensanker, verweigert ein Downgrade und startet wieder die alte Partition, wenn das neue Image nicht bootet. Damit erfüllt das Gerät zwei Pflichten des CRA, die sichere Verteilung von Updates und automatische Sicherheitsupdates als Voreinstellung.[171]

4.3 Gerätemanagement und PKI

Update-Dienste lassen sich einfach zukaufen, die Identität jedes einzelnen Geräts dagegen nicht. Sie muss feststehen, bevor das Gerät das Werk verlässt. Die meisten Projekte im DACH-Raum setzen 2026 auf fünf Dienste: Mender für Embedded Linux und Mikrocontroller,[292] Memfault mit Absturzberichten,[260] Golioth mit Abrechnung je aktivem Gerät,[199] AWS IoT Device Management mit signierten FreeRTOS-Jobs[20] und Azure Device Update, das allgemein verfügbar bleibt, während Microsoft bereits einen Nachfolger als Vorschau anbietet.[267] Microsofts Edge-Plattform Azure IoT Operations bringt einen eigenen MQTT-Broker mit.[269] Bei mehreren dieser Dienste haben sich 2025 und 2026 Preise und Eigentümer geändert. Memfault gehört heute zu Nordic, Golioth zu Canonical.[198, 286] Der Update-Dienst gehört deshalb hinter eine Abstraktionsschicht. Auf dem Gerät hält ein offenes Format wie MCUboot-Images den Anbieter austauschbar.

Der CRA verlangt sichere Voreinstellungen,[171] und die EN 18031 schließt universelle Standardpasswörter aus.[148] Jedes Gerät braucht deshalb eigene Zugangsdaten. Sie gelangen auf drei Wegen ins Gerät:

1. **Vorprovisionierte Secure Elements.** Der Chiphersteller signiert das Geburtszertifikat: Microchip Trust&GO ab 10 Stück,[263] Infineon Trust M Express,[218] NXP EdgeLock 2GO.[296]
2. **Provisionierung bei der Endprüfung.** Eine Station mit Hardware-Sicherheitsmodul signiert die Zertifikatsanfrage jedes Geräts über die eigene ausstellende CA des Herstellers, etwa mit Diensten von DigiCert, Keyfactor EJBCA oder GlobalSign.[105, 195, 232]
3. **Provisionierung beim ersten Verbindungsaufbau.** AWS Fleet Provisioning per Claim[21] oder der Device Provisioning Service von Azure.[268] Dieser Weg ist der günstigste. Seine Schwachstelle ist der gemeinsam genutzte Claim-Schlüssel.

Die Gültigkeitsdauer der Zertifikate ist eine Designentscheidung. Ein Geburtszertifikat, das über die gesamte Lebensdauer des Produkts gilt, und kurzlebige Betriebszertifikate, die per EST erneuert werden,[212] begrenzen den Schaden eines gestohlenen Schlüssels. BRSKI ergänzt ein Zero-Touch-Bootstrapping.[213] Kurze Laufzeiten sind zudem günstiger. AWS Private CA kostet im Modus für kurzlebige Zertifikate 50 US-Dollar im Monat, im Modus General Purpose 400 US-Dollar.[19]

4.4 SBOM- und PSIRT-Werkzeuge

Werkzeuge decken drei der acht Pflichten des CRA zur Schwachstellenbehandlung ab, nämlich Software-Stückliste (SBOM), Prüfung und Offenlegung.[171] Der Update-Dienst deckt zwei weitere ab. Nur ein Product Security Incident Response Team (PSIRT) erfüllt die übrigen. Dieses Team muss seit dem 11. September 2026 bei einer aktiv ausgenutzten Schwachstelle binnen 24 Stunden eine Frühwarnung abgeben, binnen 72 Stunden eine Meldung erstatten und spätestens 14 Tage, nachdem eine Korrektur verfügbar ist, einen Abschlussbericht vorlegen, auch für Produkte, die bereits auf dem Markt sind.[171] Die Single Reporting Platform der ENISA ging am selben Tag in Betrieb und leitet jede Meldung zugleich an das koordinierende CSIRT und an die ENISA.[133]

Die Formate stehen fest. CycloneDX ist als ECMA-424 genormt,[120] SPDX als ISO/IEC 5962.[253] Die Technische Richtlinie TR-03183-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom August 2025 ist das konkreteste Profil: CycloneDX ab 1.6 oder SPDX ab 3.0.1, ein SHA-512-Hash je Komponente und keine Schwachstelleninformationen in der SBOM selbst.[50] Sicherheitshinweise erscheinen getrennt davon im Format CSAF 2.0, dessen VEX-Profil angibt, ob ein Produkt betroffen ist.[302] Version 2.1 lag im September 2026 als Entwurf vor.[303] CERT-Bund beim BSI veröffentlicht seine Hinweise selbst als CSAF Trusted Provider.[52] CSAF-Hinweise erreichen deutsche Kunden damit über einen Kanal, den sie bereits nutzen.

OWASP Dependency-Track ist kostenlos und gleicht SBOMs laufend mit Schwachstellen-Feeds ab.[321] Zugekaufte Firmware ohne Quellcode, etwa von Funkmodulen, erfordert eine Binäranalyse, wie sie etwa ONEKEY in Düsseldorf anbietet.[308] Kein Werkzeug ersetzt die übrigen Bausteine eines PSIRT: ein benanntes Team, eine veröffentlichte Kontaktstelle, eine Triage mit VEX-Aussagen und einen Freigabeweg in den Update-Dienst.

4.5 Datenschnittstellen für den Data Act

Der Data Act verlangt einen Datenzugang, der schon in der Produktgestaltung angelegt ist, schreibt aber kein Protokoll vor. Die eigentliche Hürde für Gerätehersteller ist daher die Autorisierung, nicht das Format. Produkte, die seit dem 12. September 2026 in Verkehr gebracht werden, müssen ohne Weiteres verfügbare Daten dem Nutzer „standardmäßig einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format“ zugänglich machen.[170] Die Artikel 4 und 5 regeln zusätzlich den Zugang auf Verlangen und den Zugang für Dritte, die der Nutzer benennt.[170] Die FAQ der Kommission vom Januar 2026 stufen auch nur vorübergehend gespeicherte Daten als ohne Weiteres verfügbar ein, verlangen aber nicht in jedem Fall direkten Zugang.[158]

Für die DACH-Industrie kommen vier offene Schnittstellen infrage. OPC UA (IEC 62541)[211] kann Daten über MQTT veröffentlichen,[312] und umati baut auf der Companion Specification des VDMA für Maschinen auf.[398] MQTT 5.0 ist OASIS-Standard.[301] Die Verwaltungsschale (IEC 63278-1),[210] im IDTA-Release 26-01 in Version 3.2,[216] enthält die statischen Produktdaten und verweist auf die Laufzeitdaten. Eine dokumentierte REST-API bedient Nutzer und Dritte in der Cloud.

Der Zugriff Dritter muss auf die Produkte eines Nutzers beschränkt und widerrufbar sein. Dafür greift der Hersteller auf die Identitätsschicht zurück. Das Gerätezertifikat identifiziert das Produkt,

und eine Freigabe nach dem OAuth-Prinzip verknüpft es mit dem Nutzer. Die Daten, die das Produkt verlassen, fallen unter die Pflichten des CRA zu Vertraulichkeit und Datenminimierung.[171]

4.6 Pflichten je Schicht

Auf die Sicherheitsschicht des Geräts und die PKI entfallen mehr rechtliche Anforderungen als auf jede andere Schicht. Gerade diese beiden lassen sich nicht per Firmware-Update nachrüsten. CRA, RED, Maschinenverordnung und Data Act betreffen jeweils mindestens fünf der sechs Schichten (Tabelle 8).

SCHICHT	CRA, EIGENSCHAFTEN (ANH. I TEIL I)	CRA, PROZESSE (ANH. I TEIL II)	RED	MASCHINENVERORDNUNG	DATA ACT
Connectivity	Nr. 2 h Verfügbarkeit, Nr. 2 i Auswirkung auf Netze; Erreichbarkeit für Nr. 2 c	Nr. 7 Update-Kanal über den Unterstützungszeitraum	Art. 3 Abs. 3 d Netzschutz; sicheres Pairing	1.2.1 a Schutz gegen böswillige Versuche auf der Funkstrecke	Übertragung der Daten an Nutzer und Dritte
Sicherheitsschicht	Nr. 2 d Zugriff, Nr. 2 e Vertraulichkeit, Nr. 2 f Integrität, Nr. 2 k Exploit-Abwehr	Nr. 7 Signaturprüfung der Updates	Art. 3 Abs. 3 d, e, f: Authentisierung, sichere Speicherung	1.1.9 Schutz gegen Korrumpierung, Nachweis von Eingriffen	Geräteidentität hinter jedem Datensatz
Gerätemanagement und OTA	Nr. 2 c automatische Sicherheitsupdates, Nr. 2 l Protokollierung	Nr. 2 Behebung, Nr. 7 sichere Verteilung, Nr. 8 kostenlose Updates	Update-Mechanismus, Protokollierung	1.1.9 Nachweis von Software-Eingriffen	Fernkonfiguration des Datenzugangs
Zertifikate und PKI	Nr. 2 b sichere Voreinstellung, Nr. 2 d Authentisierung	Nr. 7 Code-Signing-Schlüssel	keine universellen Standardpasswörter; Verwaltung von Zugangsdaten	1.2.1 a authentisierte Steuerbefehle	Autorisierung Dritter
SBOM und PSIRT	Nr. 2 a keine bekannten ausnutzbaren Schwachstellen	Nr. 1 SBOM, Nr. 3 Prüfungen, Nr. 4 Offenlegung, Nr. 5 CVD, Nr. 6 Kontakt; Art. 14 24 h / 72 h / 14 Tage	Schwachstellenbehandlung für Funk-Stacks	Nachweise zur Zulieferer-Software	entfällt
Datenschnittstellen	Nr. 2 e Vertraulichkeit, Nr. 2 g Datenminimierung, Nr. 2 m Löschung	entfällt	Art. 3 Abs. 3 e Datenschutz	entfällt	Art. 3 Abs. 1 Zugang durch Produktgestaltung, Art. 4 Zugang auf Verlangen, Art. 5 Dritte

Tabelle 8: Rechtliche Anforderungen je Schicht
Anmerkung: Ein Eintrag bedeutet, dass die Schicht die technische Maßnahme umsetzt, nicht, dass ihr Zukauf die Konformität herstellt. Quellen: [141, 148, 168, 170, 171].

Die Schwachstellenbehandlung nach dem CRA ist vor allem eine Prozessaufgabe. Ohne PSIRT ist die Meldefrist nicht zu halten, gleich welche Werkzeuge im Einsatz sind.[133, 171] Der Data Act verlangt dagegen weder neue Funktechnik noch einen neuen Chip. Er fügt eine Autorisierungsschicht hinzu, die auf der Geräteidentität aufbaut, die der CRA ohnehin verlangt.

4.7 Vier Referenzarchitekturen

Die vier Archetypen haben ein gemeinsames Grundgerüst und unterscheiden sich nur dort, wo Physik oder Regulierung es erzwingen. Das Grundgerüst besteht aus fünf Elementen:

- Jedes Gerät hält einen eindeutigen Schlüssel in einem Vertrauensanker und ein in der Fertigung ausgestelltes Zertifikat.
- Jedes Image ist signiert und wird vor dem Start geprüft.
- Ein Update-Dienst bedient alle Produktlinien.
- Ein PSIRT betreut alle Produkte und meldet über die Single Reporting Platform der ENISA.[133]
- Jedes Produkt stellt seine Daten über eine dokumentierte Schnittstelle bereit.[170]

4.7.1 Akkuwerkzeug mit BLE-Tracker

Das Akkuwerkzeug hat kein Mobilfunkmodem und erreicht die Cloud nur über das Smartphone des Nutzers oder ein Baustellen-Gateway. Seine Sicherheitsfunktionen liegen deshalb im BLE-Chip, und Updates erreichen es über einen Vermittler, dem es nicht vertraut (Abbildung 5).

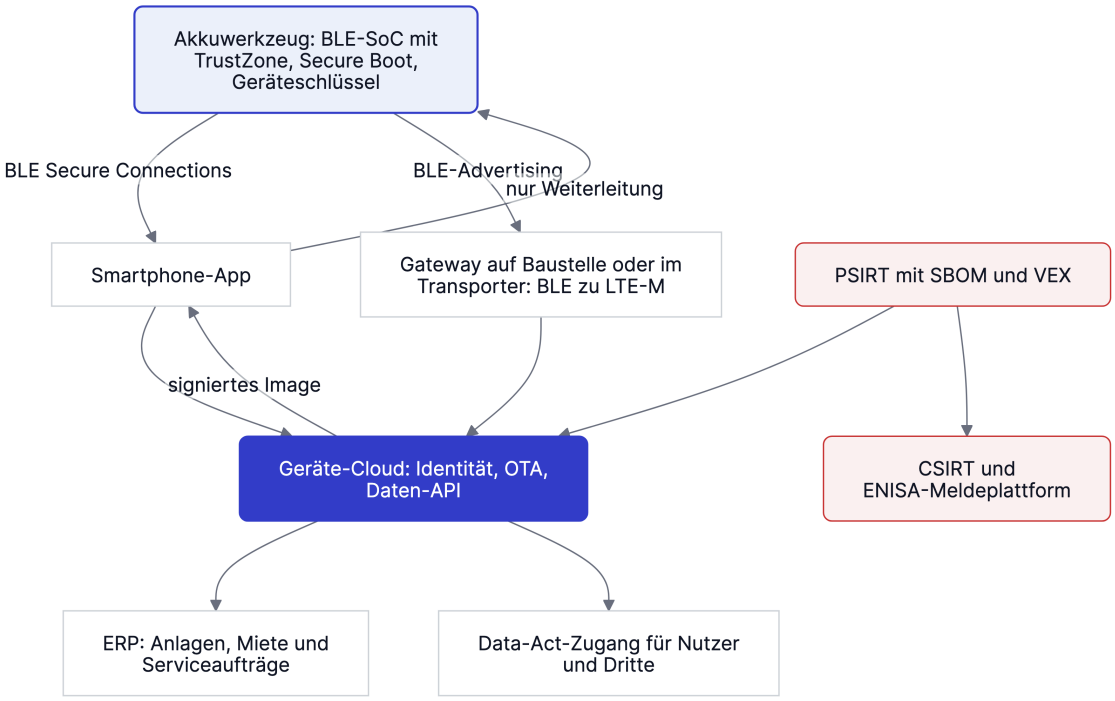


Abbildung 5: **Referenzarchitektur: Akkuwerkzeug mit BLE-Tracker**

FUNK	Bluetooth LE mit LE Secure Connections. Das Werkzeug nimmt Befehle zum Sperren, Entsperren und für Drehmomentvorgaben nur aus einer authentisierten App-Sitzung an.
GATEWAY	Das Smartphone des Nutzers oder ein BLE-zu-LTE-M-Gateway im Transporter, im Baucontainer oder in der Werkzeugausgabe. Jedes Advertising-Paket enthält eine wechselnde, verschlüsselte Kennung.
PLATTFORM	Eine Geräte-Cloud für Mikrocontroller-Flotten, die Identitäten aus dem Fertigungsmanifest registriert, die Eigentümerzuordnung führt und die Daten-API bereitstellt.

ERP	Ereignisgesteuerte Buchung von letztem Standort, Betriebsstunden, Ladezyklen und Fehlercodes. Das ERP fragt keine Werkzeuge ab.
UPDATE-MECHANISMUS	Signiertes Image, von der App weitergeleitet. Der Bootloader prüft Signatur und Version und behält das alte Image, bis das neue erfolgreich gestartet ist.
MELDEPFAD	SBOM von BLE-Stack und Anwendung aus dem Build, mit dem SDK des Funkchip-Herstellers als Drittkomponente, und CSAF-Sicherheitshinweis mit VEX.

Kosten. Nach unserem Kostenmodell kostet das Akkuwerkzeug im Basisfall 0,50 € je Gerät und Monat, der niedrigste Wert der vier Archetypen. Davon entfallen 0,47 € oder 93 % auf den Sicherheitsaufschlag. Signierte OTA-Updates über Golioth machen rund die Hälfte dieses Aufschlags aus.[199]

Worauf zu achten ist. Beim Pairing muss der Nutzer eigene Zugangsdaten festlegen, wie es die Passwortregel der EN 18031 verlangt.[148] Ein Nachweis nach PSA Level 3 ist in der Zertifizierungsdatenbank zu prüfen, nicht im Datenblatt.[326] Automatische Sicherheitsupdates als Voreinstellung hängen beim Akkuwerkzeug davon ab, dass der Nutzer die App öffnet.[171] Der Update-Dienst muss deshalb nachhalten, welche Werkzeuge nicht in Reichweite waren. Das Baustellen-Gateway ist selbst eine Funkanlage mit eigenen Pflichten nach CRA und RED.

4.7.2 Maschine mit Gateway

Das Gateway der Maschine liest Daten aus der Steuerung, hat aber keinen Schreibzugriff auf die Sicherheitssteuerung (Abbildung 6). Auf dieser Trennung beruht der Schutz, den die Maschinenverordnung gegen „vernünftigerweise vorhersehbare böswillige Versuche Dritter“ verlangt, die zu einer Gefährdungssituation führen.[168]

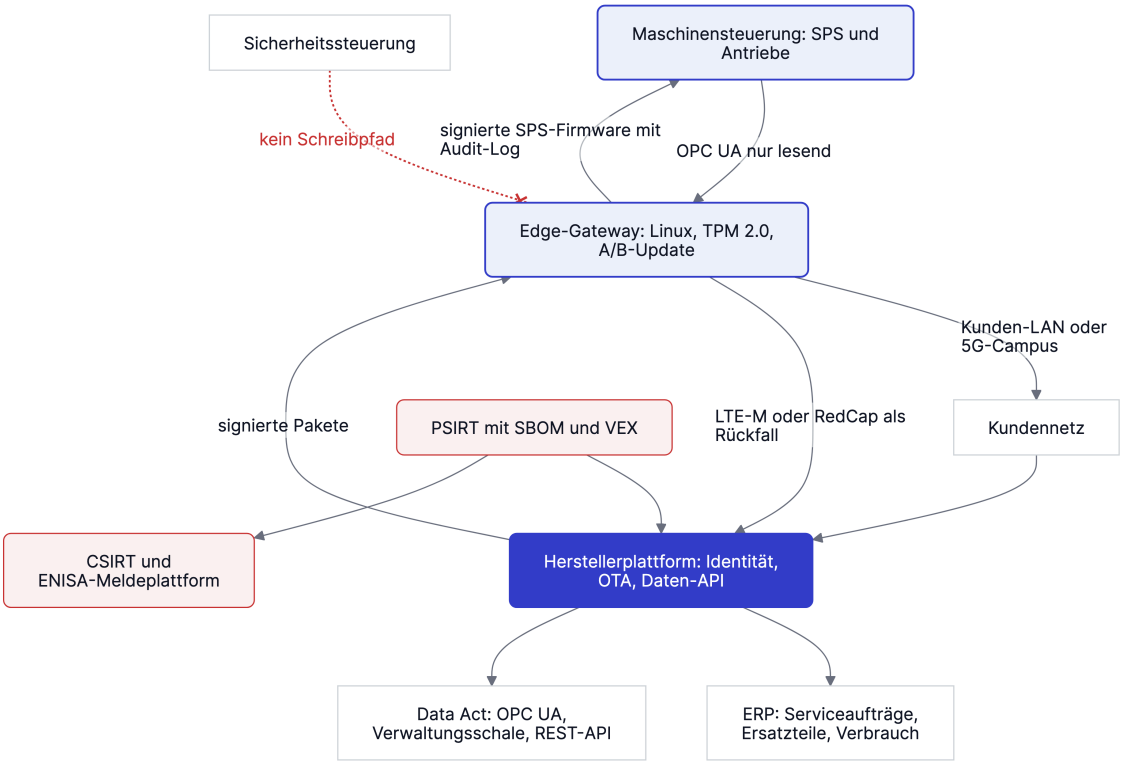


Abbildung 6: **Referenzarchitektur: Maschine mit Gateway**

FUNK	Vorrangig das Kundennetz (Ethernet, WLAN mit WPA3 oder ein 5G-Campusnetz). Als Rückfallebene Mobilfunk mit eSIM über LTE-M, für Video und große Logdateien RedCap. Kein 2G oder 3G.
GATEWAY	Linux-Edge-Gateway mit TPM 2.0, Measured Boot und A/B-Root-Dateisystem. Es liest die Steuerung über OPC UA aus und protokolliert jede Änderung in einem signierten Audit-Log.
PLATTFORM	Azure IoT Hub mit Device Update, AWS IoT Core mit Jobs aus IoT Device Management oder selbst betriebenes Mender.
ERP	Aus Zustandsereignissen werden Serviceaufträge, aus Verbrauchsdaten Ersatzteilvorschläge oder eine nutzungsbasierte Abrechnung. Das ERP des Kunden erhält dieselben Ereignisse über die Data-Act-Schnittstelle.
UPDATE-MECHANISMUS	Gateway-Pakete und SPS-Firmware sind getrennt signiert. SPS-Firmware wird erst im Wartungsfenster eingespielt, Sicherheitskorrekturen laufen über einen eigenen Kanal.
MELDEPFAD	SBOM nach BSI TR-03183-2 für mehrere hundert Linux-Pakete, Binäranalyse der Zulieferfirmware und CSAF-Sicherheitshinweise direkt an die Kunden.

Kosten. Für die Maschine rechnen wir im Basisfall mit 3,10 € je Gerät und Monat, dem höchsten Wert der vier Archetypen. Mobilfunktarif und ständiger Cloud-Verkehr bestimmen die Summe. Der Sicherheitsaufschlag von 0,40 € macht 13 % davon aus.

Worauf zu achten ist. Das Audit-Log auf Gerät und Plattform erbringt den Nachweis über Eingriffe in die Software, den die Maschinenverordnung verlangt.[168] Eine neue SPS-Firmware ist eine sicherheitsrelevante Änderung. Der CRA verlangt, Sicherheitsupdates getrennt von Funktionsupdates bereitzustellen, soweit das technisch möglich ist.[171] Der Kunde kann Korrekturen dann einspielen, ohne den Prozess neu zu qualifizieren. Ein eigenständig verkauftes Gateway der Klasse I braucht eine notifizierte Stelle, solange keine harmonisierte CRA-Norm im Amtsblatt steht.[171] Es sollte nach IEC 62443-4-2 entwickelt werden.[209] Zertifizierte Bausteine dafür sind verfügbar, etwa das NXP SE051[298] oder das TPM SLB9672 mit einem Zertifikat, das bis 2031 gilt.[51]

4.7.3 Gebäudegerät nach § 14a

Das Gebäudegerät empfängt die Steuerbefehle des Netzbetreibers über Smart-Meter-Gateway und Steuerbox des Messstellenbetreibers, nie über die Cloud des Herstellers.[74, 403] Der Hersteller entwickelt deshalb eine EEBUS-Schnittstelle und hält den Cloud-Pfad davon getrennt (Abbildung 7).

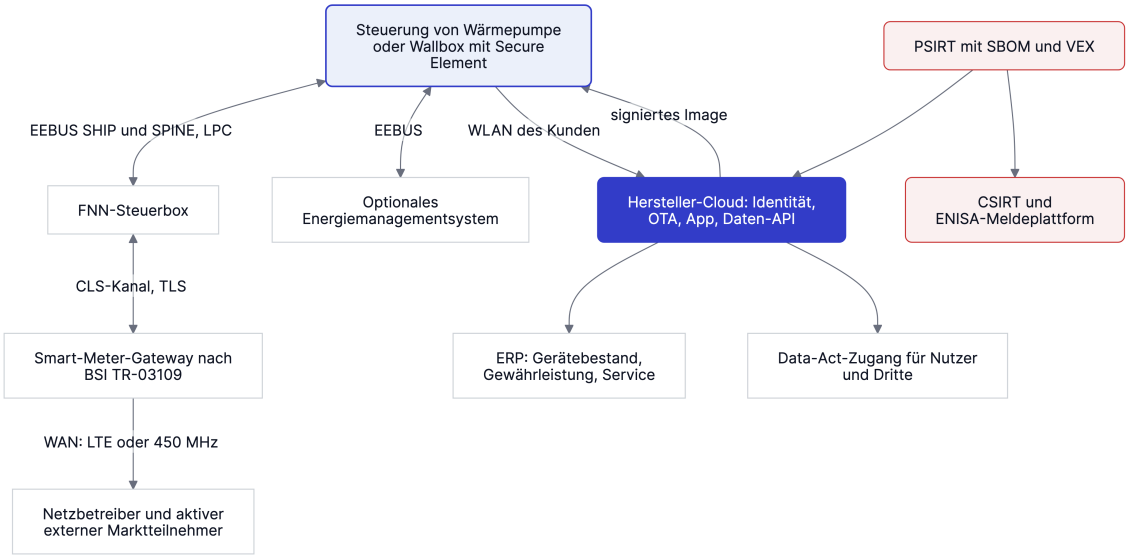


Abbildung 7: **Referenzarchitektur: Gebäudegerät nach § 14a EnWG**

FUNK	Netzseitig nicht Sache des Herstellers. Das Smart-Meter-Gateway nutzt öffentlichen Mobilfunk oder das 450-MHz-Netz. Das Gerät selbst kommuniziert über das WLAN des Kunden.
GATEWAY	Smart-Meter-Gateway nach BSI TR-03109 und FNN-Steuerbox. Das Gerät nutzt EEBUS, wo verfügbar, und hat einen Relaiseingang als Rückfallebene.
PLATTFORM	Hersteller-Cloud über das WLAN des Kunden für App, Ferndiagnose, Updates und Data-Act-Zugang. Über sie läuft keine Netzsteuerung.
ERP	Mit der Inbetriebnahme entsteht der Datensatz im Gerätebestand, auf den sich Gewährleistung, Rückrufe und Sicherheitsupdates beziehen. Serviceereignisse werden als Serviceaufträge gebucht.
UPDATE-MECHANISMUS	Signierte Images, standardmäßig automatisch mit Opt-out, nie während einer laufenden Steuerphase. Mindestleistung und Reaktionszeit werden nach jedem Update geprüft.
MELDEPFAD	Wie bei den anderen Archetypen, dazu koordinierte Offenlegung mit der EEBus Initiative und den Steuerbox-Herstellern, weil ein Fehler im EEBUS-Stack auch Geräte anderer Hersteller trifft.

Kosten. Für das Gebäudegerät kommen wir im Basisfall auf 0,59 € je Gerät und Monat. Davon entfallen 0,48 € oder 81 % auf den Sicherheitsaufschlag.

Worauf zu achten ist. Ein gedrosseltes Gerät behält mindestens 4,2 kW, so die Festlegung BK6-22-300 der BNetzA, die seit dem 1. Januar 2024 gilt.[74] Ein Steuersignal muss binnen fünf Minuten wirken, und Geräte mit Altvereinbarungen wechseln spätestens zum 1. Januar 2029 in das neue Regime.[74] Der Kunde erhält im Gegenzug ein reduziertes Netzentgelt,[61] seit dem 1. April 2025 auch zeitvariabel.[79] Die Steuerkette liegt nicht in der Hand des Herstellers. Sie besteht aus dem Smart-Meter-Gateway,[53] seiner WAN-Anbindung[73] und einer Steuerbox nach dem FNN-Lastenheft vom August 2025, für die die BSI TR-03109-5 gilt.[49, 403] Steuerboxen bieten EEBUS und

Relaiskontakte.[93] Der Rollout soll für diese Messstellen erst Ende 2032 eine Quote von 90 % erreichen.[60] Der Relaiseingang bleibt deshalb noch über Jahre nötig. EEBUS (VDE-AR-E 2829-6)[402] koppelt Geräte über die Schlüsselkennung ihres Zertifikats, die eine Person bestätigen muss.[123] Das Gerät speichert seinen EEBUS-Schlüssel daher geschützt und zeigt die Kennung im Display oder auf dem Typenschild.

4.7.4 Logistik-Tracker

Beim Logistik-Tracker bestimmt das Energiebudget die gesamte Auslegung. Unterwegs überträgt er per LTE-M im Stromsparmodus, auf der Baustelle über ein BLE-Gateway, und eine einzige Tracker-Identität verbindet beide Wege (Abbildung 8). Die Funkübertragung bestimmt die Laufzeit der Batterie, nicht der Ruhezustand oder GNSS.

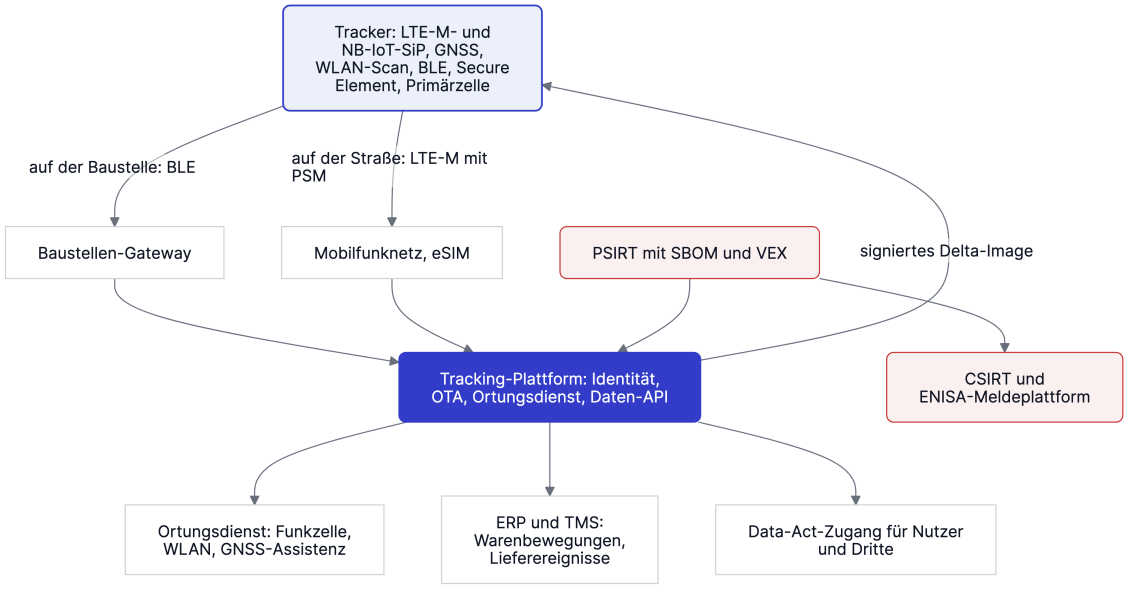


Abbildung 8: **Referenzarchitektur: Logistik-Tracker**

FUNK	LTE-M als primäre Funktechnik für Mobilität und Zellwechsel, NB-IoT als Rückfallebene tief im Gebäude. Eine eSIM, deren Betreiberprofil sich im laufenden Betrieb wechseln lässt.
GATEWAY	Unterwegs keines, auf der Baustelle das BLE-Gateway des Akkuwerkzeugs. Der Positionsverlauf bleibt lückenlos, weil er am Zertifikat des Trackers hängt, nicht an der Funktechnik.
PLATTFORM	Das gemeinsame Grundgerüst, ergänzt um Geofences und einen Ortungsdienst hinter einer Schnittstelle, die der Hersteller kontrolliert.
ERP	Ein- und Ausfahrten an Geofences werden als Warenbewegungen oder Liefereignisse in ERP oder Transportmanagementsystem gebucht. Rohpositionen bleiben in der Plattform.
UPDATE-MECHANISMUS	Signierte Delta-Images über LTE-M, nur im Stillstand, bei guter Netzabdeckung und oberhalb eines Mindestladestands.

MELDEPFAD Wie bei den anderen Archetypen, dazu die Firmware des Mobilfunkmodems als eigene SBOM-Komponente, die sich getrennt aktualisieren lässt.

Kosten. Für den Tracker rechnen wir im Basisfall mit 0,99 € je Gerät und Monat, davon 0,46 € oder 46 % Sicherheitsaufschlag.

Worauf zu achten ist. Die Ortungskette entscheidet über die Batterielaufzeit. Ein Bewegungssensor legt fest, ob ein Fix nötig ist. Aus einem WLAN-Scan berechnet die Cloud die Position auf unter 100 m genau, aus einem Funkzellen-Scan auf unter 700-1.000 m.[287] GNSS mit einer Leistungsaufnahme von rund 25 mW[397] läuft nur, wenn sich das verfolgte Objekt bewegt. Das nRF9151 nimmt in LTE-M mit erweitertem diskontinuierlichem Empfang (eDRX) 18 µA auf.[288] Mit einer eSIM nach GSMA SGP.32 lässt sich der Netzbetreiber eines Trackers am Anhänger wechseln, ohne das versiegelte Gehäuse zu öffnen.[202] Ruhezustand und stündliche GNSS-Fixe verbrauchen im Jahr rund 3 % der Kapazität einer D-Zelle mit 17 Ah (Tabelle 9). Eine A-Zelle hat dagegen nur 3,6 Ah.[340]

POSTEN	BERECHNUNG	LADUNG JE JAHR (MAH)
Ruhezustand im PSM	2,7 µA × 8.760 h	24
GNSS, ein Fix je Stunde	25 mW × angenommene 30 s je Fix = 0,75 J; bei 3,6 V etwa 0,058 mAh je Fix × 8.760 Fixe	507
LTE-M-Meldung, eine je Stunde	Ladung je Übertragung hängt von Netz und Abdeckung ab	im Betrieb messen
Kapazität einer LS 33600	17 Ah nominal	17.000

Tabelle 9: **Jährliches Ladungsbudget des Logistik-Trackers**
Quellen: [284, 341, 397].

Die Ladung je LTE-M-Meldung steht in keinem Datenblatt. Sie hängt von der Netzabdeckung ab und davon, wie lange das Modem verbunden bleibt, bevor es in den PSM zurückkehrt. Sie ist deshalb im Zielnetz zu messen, bei guter und bei schlechter Abdeckung. Die Zelle verliert bei Lagerung bei +20 °C durch Selbstentladung weniger als 1 % im Jahr.[341] Die Nennkapazität von 17 Ah gilt bei 5 mA, +20 °C und 2,0 V Entladeschlussspannung, bei Kälte und höheren Strömen ist sie geringer.[341] Der Hersteller legt die Zelle deshalb gemeinsam mit Saft auf die tiefste Betriebstemperatur und das tatsächliche Pulsstromprofil aus, nicht auf den Nennwert.

Die Batterieverordnung verlangt ab dem 18. Februar 2027, dass Endnutzer Gerätebatterien entnehmen können.[150, 169] Der Hersteller prüft deshalb, ob eine Ausnahme greift, bevor er ein versiegeltes Gehäuse konstruiert. Semtech hat seinen Ortungsdienst LoRa Cloud am 31. Juli 2025 eingestellt.[355] Der Ortungsdienst gehört deshalb hinter eine eigene Schnittstelle des Herstellers. Galileo OSNMA authentisiert die Position, wo sie als Nachweis für Zoll oder Versicherung dient.[176]

KURZ GESAGT

Zusammengenommen liegt der Engpass nicht in der Technik, sondern in der Organisation des Herstellers. Ein Hersteller, der Vertrauensanker und Grundgerüst einmal für alle Produktlinien festlegt, betreibt PSIRT und Update-Mechanismus nur einmal und baut jedes weitere Produkt darauf auf. Das nächste Kapitel zeigt, wo das Logistik-Tracking von diesem Entwurf abweicht.

5 Schwerpunkt Logistik-Tracking

Logistik-Tracker bilden den vierten Archetyp und eröffnen Werkzeug- und Maschinenherstellern ein Servicegeschäft, das bei Anhängern, Containern und Maschinen gerade erst entsteht. Ab dem 18. Februar 2027 müssen Nutzer die meisten Gerätebatterien selbst entnehmen können, und 2028 schalten die deutschen Netzbetreiber 2G ab. Diese beiden Termine bestimmen, welche Tracker ein Hersteller noch bauen kann. Sechs Funkklassen konkurrieren um dieselben Assets, ihre Stückpreise unterscheiden sich rund um den Faktor zehn, ihre Batterielaufzeiten um mehr als den Faktor hundert. Das Kapitel vergleicht die Klassen, beschreibt die Regeln für Tracker und Fahrzeuge und ordnet Anbieter, Markt und Nachfrage ein.

5.1 Tracker- und Tag-Klassen

Zwei Merkmale bestimmen einen Tracker, die Art der Ortung und der Weg, auf dem er seine Position meldet. Sechs Klassen kombinieren beides, und jede erkauft Abdeckung und Genauigkeit mit Batterielaufzeit.

- **Tags mit Bluetooth Low Energy (BLE)** senden nur eine Kennung und übernehmen die Position des Telefons oder Gateways, das sie empfängt. Milwaukee betreibt über die kostenlose ONE-KEY-App ein Community-Netz,[270] und Apples AirTag hält mit einer Knopfzelle mehr als ein Jahr.[22]
- **LoRaWAN-Tracker** halten mit drei AA-Zellen bis zu sieben Jahre,[8] sind aber auf Gateway-Abdeckung angewiesen, und ein bundesweites Netz fehlt in Deutschland. Semtech hat LoRa Cloud, den Ortungsdienst vieler dieser Geräte, am 31. Juli 2025 abgeschaltet.[355]
- **LTE-M- und NB-IoT-Tracker** melden direkt über das Mobilfunknetz und sind der Standard für Ladungsträger und Container. Sensolus nennt bis zu acht Jahre Laufzeit mit austauschbaren Batterien.[358]
- **GNSS-Tracker mit Mobilfunk** orten Anhänger und Geräte ohne eigenen Antrieb im Freien per Satellit auf wenige Meter genau. Die Spanne reicht vom Oyster3 von Digital Matter mit drei tauschbaren AA-Zellen[116] bis zum wiederaufladbaren Solo 5G von Tive mit 50 Tagen Laufzeit und mehr.[389]
- **Ultra-Wideband (UWB)** ortet in Kliniken, Werken und Lagern über fest installierte Anker auf 10 bis 30 cm genau.[272]
- **Satelliten-IoT** erreicht Container auf See. Myriota gibt für sein UltraLite zehn Jahre Laufzeit mit zwei AA-Zellen an,[275] und o2 Telefónica bietet in Deutschland seit März 2025 NB-IoT mit Satelliten-Rückfallebene über Skylo an.[300, 362]

5.2 Preis und Laufzeit je Klasse

Ein BLE-Tag kostet 7,14 € und damit weniger als ein Drittel jeder anderen Tracker-Klasse, ein GNSS-Tracker mit Mobilfunk dagegen 42,01 € netto, mit Akku 84,03 €[271, 322] (Abbildung 9). Die Batterielaufzeit reicht von 20 Tagen bis zu rund zehn Jahren.[116, 322]

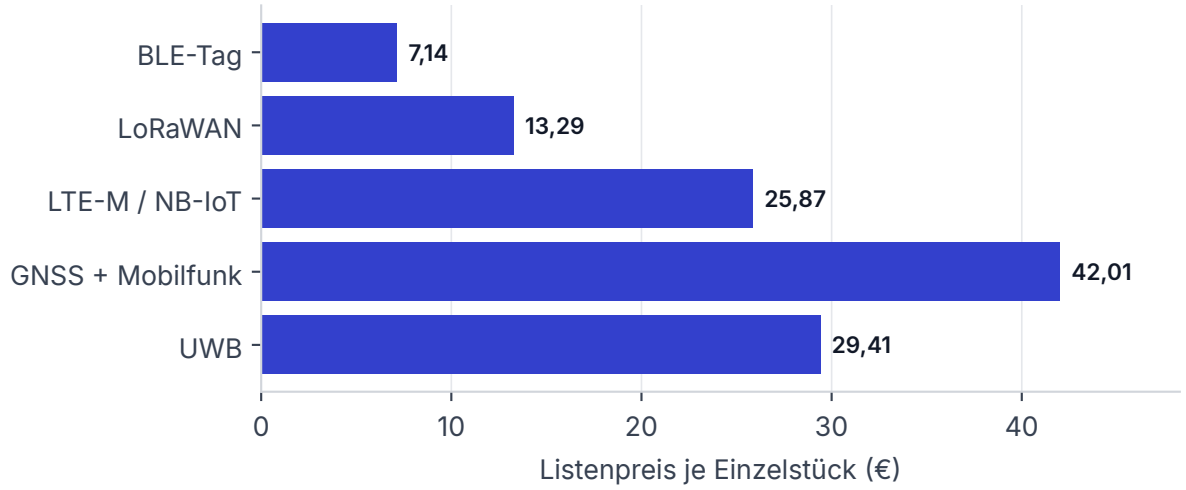


Abbildung 9: **Listenpreis je Tracker-Klasse**
Anmerkung: Für Satelliten-Tracker gibt es keinen öffentlichen Preis. Quellen: [22, 271, 322, 354].

Die meisten B2B-Anbieter nennen Preise nur auf Anfrage. Digital Matter, Tive, Trackunit, Hilti, Bosch und Myriota veröffentlichen keinen Listenpreis.[43, 116, 207, 275, 389, 392] Öffentliche Preise sind deshalb überwiegend Webshop-Preise für Einzelstücke.

Sensolus bietet seine Tracker als Service zum Pauschalpreis an, den BLE-basierten Location Tag für 1 € im Monat bei 1.000 Assets und den Mobilfunk-Tracker Track 1115 für 6 € im Monat bei 500 Assets.[357, 358] Ansonsten fallen laufende Kosten vor allem für Netz und Connectivity an, bei LoRaWAN etwa für den Netzwerkserver von The Things Stack im Tarif Standard.[385] Eine SIM von 1NCE kostet ab 12 € für zehn Jahre und 500 MB, und o2 berechnet für Satelliten-IoT über Skylo 0,70 € je kB.[3, 362] BLE- und UWB-Tags kosten keine Netzgebühr, brauchen aber eine App, ein Gateway oder Anker vor Ort (Tabelle 10).

KLASSE	BEISPIELPRODUKTE	STÜCKPREIS NETTO (€)	KOSTEN JE MONAT (€)	BATTERIELAUFZEIT (JAHRE)
BLE-Tag	Minew E8 und MTB07 (Paletten-Tag), Apple AirTag	7,14-29,41	0	1-8
LoRaWAN	RAKwireless RAK2270 (ohne GNSS), Seeed T1000-A (GNSS, WLAN, BLE), Minew LTB01-G, Abeeway Compact	13,29-40,15	0,19	1-7
LTE-M / NB-IoT	Minew MTB04 (Versandlabel), Sensolus Track 1115, Bosch-Sensoren	25,87	ab 0,10	bis 8
GNSS + Mobilfunk	PAJ COMPACT und POWER Finder 4G, Digital Matter Oyster3	42,01-84,03	5-12	bis 10
UWB	Apple AirTag (BLE + UWB), Minew MBM01/MBS02	29,41	0	über 1
Satellit	Myriota UltraLite (2 AA-Zellen), o2 NB-IoT mit Skylo	k. A.	ab 0,88	10

Tabelle 10: **Kosten und Batterielaufzeit je Tracker-Klasse**
Anmerkung: Preise netto, USD zum EZB-Referenzkurs umgerechnet, k. A. für Preise nur auf Anfrage (so auch bei Oyster3 und den UWB-Tags von Minew), Akkulaufzeit der PAJ-Tracker 20 und 90 Tage, RAK2270 bei stündlichem Uplink. Quellen: [3, 8, 22, 43, 116, 137, 271, 272, 274, 322, 333, 354, 358, 362, 385].

Bei Industriegeräten bilden Shoppreise die Spanne nur unvollständig ab. Berg Insight beziffert die typischen Gerätekosten auf 100 bis 300 € für Trockencontainer, 50 bis 150 € für Paletten und 20

bis 100 € für Fracht.[311] Die Geräte halten an Trockencontainern fünf bis zehn Jahre, an Paletten ein bis zehn Jahre und an Fracht 20 bis 100 Tage je Akkuladung.[311]

Die Batterielaufzeit hängt vom Meldeintervall ab, nicht vom Gerät. Derselbe Oyster3 hält bei einer Meldung pro Tag rund zehn Jahre, bei einer pro Stunde 3,5 Jahre.[116] Eine Laufzeitangabe im Datenblatt ohne Meldeintervall taugt nicht als Grundlage für einen Business Case.

Der Preis verlagert sich von der Hardware auf den Service. Sensolus berechnet je Asset eine laufende Gebühr, die Hardware, Connectivity, Plattform und Support umfasst, und Hilti gibt seine BLE-Tags an Flottenkunden kostenlos ab.[207, 357] Ein Hersteller, der mit Tracking Umsatz erzielen will, konkurriert mit diesen Modellen, nicht mit den Stücklistenkosten eines Tags.

5.3 Regulatorische Termine und Tracker-Design

Die Batterieverordnung verlangt ab dem 18. Februar 2027, dass der Endnutzer die Gerätebatterie eines Produkts mit handelsüblichem Werkzeug leicht entnehmen und ersetzen kann.[169] Die Ausnahmen sind eng gefasst, etwa für Geräte, die für nasse Umgebungen ausgelegt sind und gewaschen werden können. Ein vergossener oder verklebter Tracker erfüllt diese Anforderung nicht, und die meisten Sensormodelle von Bosch haben ein geschlossenes Gehäuse.[43]

Die Abschaltung der deutschen 2G-Netze nimmt vielen Trackern die Rückfallebene. Die Telekom will 2G am 30. Juni 2028 abschalten, Vodafone im September 2028, für einige kritische IoT-Anwendungen erst Ende 2030, und Telefónica Ende 2028.[77] Tives Solo 5G und Boschs Sense I nutzen weiterhin 2G als Rückfallebene.[43, 389] Mobilfunk-Tracker sind aber für bis zu acht Jahre Betrieb ausgelegt.[358] Ein 2027 montiertes Gerät bleibt also länger im Einsatz als seine Rückfallebene. Geräte mit tauschbaren Zellen und LTE-M oder NB-IoT ohne 2G, etwa Oyster3, Abeeway und Sensolus, erfüllen beide Vorgaben.[8, 116, 358] In Österreich schaltet A1 sein 2G-Netz am 31. Mai 2028 ab, in der Schweiz ist 2G bereits abgeschaltet.[6, 47]

Für die Sicherheit gelten dieselben Regeln wie für jedes vernetzte Produkt. Ein Tracker ist eine Funkanlage, die Standortdaten verarbeitet. Er muss deshalb seit dem 1. August 2025 die Anforderungen der RED an den Schutz des Netzes und personenbezogener Daten erfüllen.[141, 145] Ein Tracker ohne Bedienoberfläche braucht ab Werk ein individuelles Zugangsmerkmal statt eines gemeinsamen Standardpassworts.[148] Er übermittelt Standortdaten nur so oft, wie der Zweck es erfordert.[171] Nach unserer Einschätzung braucht ein BLE-Tag, der seine Kennung offen aussendet, zudem rotierende, nicht verknüpfbare Kennungen, damit Dritte ihn nicht verfolgen können.

Für Fahrzeuge gilt ein eigener Zeitplan. Der Smart Tachograph Version 2 (G2V2) ist seit dem 1. Juli 2026 für Transporter über 2,5 t im grenzüberschreitenden Verkehr Pflicht, und ab dem 1. Januar 2027 brauchen neue Pkw und Transporter einen paketvermittelten eCall[146, 172] (Tabelle 11).

DATUM	PFLICHT	RECHTSGRUNDLAGE
21. August 2023	Smart Tachograph Version 2 (G2V2) in neu zugelassenen Fahrzeugen	Durchführungsverordnung (EU) 2021/1228, Art. 2
31. Dezember 2024	Fahrzeuge mit analogem oder digitalem Fahrtenschreiber, die außerhalb ihres Zulassungsstaats fahren, auf G2V2 umgerüstet	VO (EU) Nr. 165/2014, Art. 3 Abs. 4, geändert durch VO (EU) 2020/1054
18. August 2025	Fahrzeuge mit Smart Tachograph Version 1 im grenzüberschreitenden Verkehr auf G2V2 umgerüstet	VO (EU) Nr. 165/2014, Art. 3 Abs. 4a
1. Januar 2026	Neue Typgenehmigungen für eCall-Systeme und Fahrzeuge nur nach den paketver-	Delegierte VO (EU) 2024/1180, Art. 2 Abs. 2

DATUM	PFLICHT	RECHTSGRUNDLAGE
	mittelten Normen CEN/TS 17184:2022 und CEN/TS 17240:2018	
1. Juli 2026	Transporter über 2,5 t im grenzüberschreitenden Verkehr oder in der Kabotage: Lenk- und Ruhezeiten und G2V2	VO (EG) Nr. 561/2006, Art. 2 Abs. 1 Buchst. aa, geändert durch VO (EU) 2020/1054
1. Januar 2027	Übereinstimmungsbescheinigungen neuer Fahrzeuge ohne paketvermittelten eCall nicht mehr gültig	Delegierte VO (EU) 2024/1180, Art. 2 Abs. 3

Tabelle 11: **Pflichten für Fahrtenschreiber und eCall**
Quellen: [139, 146, 172, 173].

Transporter im reinen Inlandsverkehr sind von den Fahrtenschreiber-Pflichten ausgenommen.[163, 164] G2V2 zeichnet Positionen mit einem Empfänger auf, der für Galileos Authentifizierung der Navigationsnachrichten (OSNMA) geprüft ist.[139] Dieser Dienst läuft seit Juli 2025.[176] Ein nachgerüsteter Tracker an einem solchen Transporter erfasst diese Daten also ein zweites Mal, es sei denn, er überwacht Anhänger, Ladung oder Werkzeug. Die Kommission begründet die eCall-Änderung damit, dass alle Mitgliedstaaten ihre 2G- und 3G-Netze zwischen 2025 und 2030 abschalten.[146] Keine dieser Vorschriften gilt für Anhänger, Container, Werkzeuge oder Maschinen.

5.4 Anbieter und Produkte in DACH

Der Markt gliedert sich nach der Art des Assets, nicht nach der Funktechnik. In jedem Segment ist das Netz oder der Service das Produkt, nicht der Tag (Tabelle 36).

Werkzeuge und Geräte. Hiltis ON!Track kombiniert BLE-Tags, einen GPS-Tracker für Maschinen und Anhänger sowie Baustellen- und Fahrzeug-Gateways.[207] Trackunit deckt dieselbe Aufgabe mit Maschinentelematik, Trackern für Geräte ohne eigenen Antrieb, kleinen Tags und Baustellen-Gateways ab.[391] Das Fahrzeug-Gateway des Bauunternehmens erkennt ein Werkzeug mit BLE, nach demselben Prinzip wie beim ersten Archetyp. Würth verkauft seinen Bluetooth-Tag W-CONNECT, der den letzten bekannten Standort in der App ORSY online anzeigt, an Gewerbekunden und veröffentlicht keine Preise.[10] Auf der IAA Transportation im September 2026 zeigte Würth zudem ein Fahrzeug-Gateway mit LTE und eSIM, das prüft, ob die zugeordneten Werkzeuge an Bord sind.[186] Bosch Professional verkauft in Deutschland keinen eigenständigen Tag, sondern nur das Bluetooth-Modul GCY 42 für die eigenen Werkzeuge, zu 35 € netto.[336]

Ladungsträger, Container und Anhänger. Boschs Sense I und Minews BLE-Paletten-Tag MTB07 sind für Ladungsträger und Paletten ausgelegt.[43, 271] Unter den Anbietern von Einweg-Smart-Labels nennt Berg Insight BOX ID und Giesecke+Devrient aus Deutschland sowie Truvami aus der Schweiz.[31] Im Container-Tracking führt Berg Insight Giesecke+Devrient und Sensolus auf, bei Anhängern die deutschen Hersteller Schmitz Cargobull und Krone.[32]

Anbieterrisiko. Eine Tracker-Flotte bleibt oft länger im Einsatz, als ihre Anbieter am Markt sind. Inzwischen steht die Domain von Kizy zum Verkauf, Roambee firmiert als Decklar, und Teltonika führt seinen Tracker TAT141 als abgekündigt.[92, 240, 382] Geräteidentität, Update-Schlüssel und Ortungsdienst müssen deshalb in der Hand des Herstellers bleiben.

5.5 Bestand und Wachstum bis 2028

Berg Insight erwartet, dass sich der Bestand an Trackern auf Ladungsträgern verdoppelt, von 11,1 Mio. Ende 2023 auf 22,4 Mio. im Jahr 2028, ein Plus von 15,0 % pro Jahr.[32] Er wächst damit schneller als das Flottenmanagement in Europa mit 11,0 % pro Jahr bis 2029[30] (Tabelle 12).

Einweg-Smart-Labels wachsen am schnellsten, von 400.000 weltweit ausgelieferten Stück im Jahr 2024 auf erwartete 31,8 Mio. pro Jahr bis 2029.[31]

SEGMENT UND KENNZAHL	REGION	BASISJAHR	BASISWERT	PROGNOSEJAHR	PROGNOSEWERT	JÄHRLICHES WACHSTUM (CAGR)
Ladungsträger: Auslieferungen von Ortungsgeräten	Weltweit	2023	4,0 Mio.	2028	6,6 Mio.	10,2 %
Ladungsträger: Bestand	Weltweit	2023	11,1 Mio.	2028	22,4 Mio.	15,0 %
Ladungsträger und Fracht: Umsatz, 12. Ausgabe	Weltweit	2023	2,1 Mrd. €	2028	3,5 Mrd. €	10,2 %
Ladungsträger und Fracht: Umsatz, 13. Ausgabe	Weltweit	2024	2,7 Mrd. €	2029	4,5 Mrd. €	10,8 %
Aktive Geräte an Anhängern	Weltweit	2024	5,8 Mio.	-	-	-
Aktive Geräte an Seecontainern	Weltweit	2024	5,3 Mio.	-	-	-
Aktive Geräte für allgemeine Fracht	Weltweit	2024	3,2 Mio.	-	-	-
Smart Labels: Auslieferungen	Weltweit	2024	0,4 Mio.	2029	31,8 Mio.	140 %
Smart Labels: Marktvolumen	Weltweit	2024	11,2 Mio. €	2029	181,6 Mio. €	75 %
Flottenmanagement: aktive Systeme	Europa	2024	18,1 Mio.	2029	30,5 Mio.	11,0 %
Flottenmanagement: Anteil an gewerblichen Nutzfahrzeugen und Pkw	Europa	2024	26,7 %	2029	42,8 %	-

Tabelle 12: **Größe des Tracking-Markts nach Segment**
Anmerkung: Keine der Prognosen weist DACH gesondert aus. Quellen: [30, 31, 32, 33, 311].

Der Markt ist bei Weitem nicht ausgeschöpft. Nur etwa ein Fünftel (20 %) der rund 30 Mio. Seecontainer, 15,7 Mio. Anhänger und 5,5 Mio. Güterwagen ist mit einem Ortungsgerät ausgestattet.[32] Auf Anhänger entfallen 45,8 % des Bestands an Trackern auf Ladungsträgern, auf Seecontainer 40,6 %.[32] Maersk hat alle 360.000 Kühlcontainer mit Ortungsgeräten ausgerüstet.[32]

5.6 Werksausstattung und Nachrüstung

Lkw werden ab Werk mit Telematik ausgeliefert, Anhänger, Container und Maschinen dagegen nicht. Dort liegt der Nachrüstmarkt.[30] Daimler Truck baut Fleetboard in alle mittleren und schweren Lkw ein, MAN RIO in neue Lkw.[30] Gemessen an aktiven Abonnenten in Europa führten Ende 2024 unter den Nachrüstanbietern Targa Telematics mit 900.000, Webfleet mit 752.000 und CalAmp mit 600.000, unter den Lkw-Herstellern Scania mit 461.000, Daimler Truck mit 382.000, Volvo mit 364.000 und MAN mit 264.000.[30] Geotab hat das verbliebene Europageschäft von Verizon

Connect einschließlich Deutschland übernommen.[30] Berg Insight zählt im Markt für 2025 bis November elf Übernahmen und Fusionen.[30]

Deutsche Fuhrparks bieten noch viel Potenzial. In einer Dataforce-Umfrage unter mehr als 530 Fuhrparkbetreibern (September bis Dezember 2024) nutzte rund ein Fünftel (21 %) der befragten Fuhrparks ab fünf Fahrzeugen Telematik. Bei Fuhrparks ab 16 Nutzfahrzeugen waren es etwa 40 %, im Bereich Verkehr und Lagerei 60 %.[407] Die meistgenutzte Funktion ist die GPS-Ortung, bei Transportern mit 84 %. Unter den befragten Fuhrparks mit Telematik stieg der Anteil derer, die auch ihre Transporter einbinden, von 51 % im Jahr 2018 auf 78 % im Jahr 2024.[407]

5.7 Die Nachfrageseite

Verteidigung, Kliniken und Baustellen müssen ihre Assets orten können, doch keiner dieser Bereiche hat einen eigenen Haushaltsposten für Tracking. Das Bundesministerium der Verteidigung veranschlagt für 2026 mehr als 108 Mrd. €, ohne Logistik oder Materialverfolgung gesondert auszuweisen.[65]

Verteidigungslieferketten. Keine seit Januar 2025 veröffentlichte Ausschreibung der Bundeswehr verlangt die Ortung von Assets, Containern oder Fahrzeugen.[329] Nach unserer Einschätzung ergeben sich stattdessen zwei Designanforderungen aus der Technik. Positionsnachweise setzen authentifiziertes GNSS voraus, wie es Galileo OSNMA bietet,[176] und ein Tracker, der sich per Befehl stummschalten lässt, braucht einen signierten Befehlskanal.

Kliniken. Das Krankenhauszukunftsgesetz förderte die Digitalisierung mit bis zu 4,3 Mrd. €. Die Antragsfrist endete jedoch am 31. Dezember 2021, und keiner der elf Fördertatbestände nennt Ortung oder Tracking.[64, 69] Einem Krankenhaus ohne die geforderten digitalen Dienste droht seit dem 1. Januar 2025 ein Abschlag von bis zu 2 % je stationärem Fall.[63] Tracking gelangt deshalb als Teil dieser Prozesse in die Kliniken, per UWB oder BLE.

Baustellen. Diebstähle treiben die Nachfrage. In Österreich erreichte der polizeilich erfasste Schaden durch Baustellendiebstähle 2017 mit 18,7 Mio. € seinen Höchststand und lag 2018 und 2019 bei rund 17 Mio. €.[324] Fast neun von zehn (88 %) der 150 im Juni 2021 befragten Bauunternehmen und Baumaschinenvermieter waren bereits Opfer eines Diebstahls geworden.[324] Die Lösungen der Anbieter laufen auf ein Baustellen-Gateway hinaus, das BLE-Tags erfasst, ergänzt um GNSS-Tracker an großen Geräten.[207, 391] Für Werkzeug- und Maschinenhersteller kommt es deshalb auf die Integration an. Jedes Gateway des Bauunternehmens erkennt ein Werkzeug mit rotierender BLE-Kennung, und die Daten des Werkzeugs müssen dem Nutzer zugänglich sein.[170]

KURZ GESAGT

Im Ergebnis braucht ein Tracker, der ab 2027 verkauft wird, eine tauschbare Batterie, die zum Meldeintervall passt, und ein Funknetz, das auch nach 2028 noch betrieben wird. Für Werkzeug- und Maschinenhersteller liegt das Geschäft im Service rund um das Gerät, nicht im Gerät selbst. Das nächste Kapitel zeigt, was sich für Hersteller in Österreich und der Schweiz ändert.

6 Schwerpunkt Österreich und Schweiz

Österreich und die Schweiz stellen 718 der 4.410 Hersteller der DACH-Grundgesamtheit. Ein Hersteller, der in alle drei Länder liefert, trifft auf zwei weitere Regelwerke für die Netzsteuerung und an der Schweizer Grenze auf die Drittlandregeln der EU. Österreich teilt mit Deutschland das EU-Produktrecht, schreibt mit seinem neuen Elektrizitätswirtschaftsgesetz aber nur für Erzeugungsanlagen die Steuerbarkeit vor und überlässt die Steuerung von Wärmepumpen vertraglichen Vereinbarungen. Schweizer Hersteller gelten nach dem Cyber Resilience Act (CRA) als Drittlandhersteller und brauchen nach dem Data Act einen gesetzlichen Vertreter in der EU, unabhängig davon, wie es mit dem Abkommen über die gegenseitige Anerkennung (MRA) weitergeht. Für Maschinen brauchen sie ab 2027 zusätzlich einen Wirtschaftsakteur in der EU, solange das Maschinenkapitel des MRA nicht aktualisiert ist. Das Kapitel beschreibt beide Länder nach demselben Schema, von den Unterschieden über die wichtigsten Termine bis zu den Folgen für Hersteller, und schließt mit den Regeln für Schweizer Hersteller auf dem EU-Markt.

6.1 Österreich

6.1.1 Unterschiede zu Deutschland

Österreich wendet dasselbe EU-Produktrecht an wie Deutschland, kennt aber kein Gegenstück zu § 14a EnWG. Das neue Elektrizitätswirtschaftsgesetz (ElWG) schreibt die Steuerbarkeit nur für Erzeugungsanlagen vor, nicht für Verbrauchsgeräte.[335] Eine in Österreich verkaufte Wärmepumpe braucht deshalb von Gesetzes wegen keine Steuerschnittstelle für den Netzbetreiber. Verbrauchsgeräte lassen sich über Verträge zum flexiblen Netzzugang, über Aggregatoren oder über die marktgestützte Beschaffung von Flexibilität steuern.[335] In Deutschland dagegen erlaubt § 14a EnWG dem Netzbetreiber, neue Wärmepumpen und Wallboxen zu dimmen.[61]

Smart Meter sind in Österreich fast flächendeckend installiert, ihre Daten fließen aber kaum. Ende 2024 waren 96,9 % der 6,74 Mio. österreichischen Zählpunkte mit einem Smart Meter ausgestattet, aber nur jeder achte dieser Zähler (12,6 %) arbeitete in der Opt-in-Konfiguration, die Viertelstundenwerte überträgt.[132]

In Österreich haben 318 Hersteller der Grundgesamtheit ihren Sitz.[175] Nach unserer Schätzung stellen 132 bis 248 davon vernetzte Produkte her. Der Maschinenbau bildet den Kern der österreichischen Grundgesamtheit. Abteilung 28 hat mehr Beschäftigte als die Abteilungen 26 und 27 zusammen[175] (Tabelle 13).

ÖNACE	ERZEUGNISSE	UNTERNEHMEN	DAVON 50-249	DAVON 250+	BESCHÄFTIGTE
26	Elektronische und optische Erzeugnisse	704	54	19	34.888
27	Elektrische Ausrüstungen	625	71	42	52.050
28	Maschinenbau	1.426	192	98	104.506
32.5	Medizinische und zahnmedizinische Apparate	877	13	4	9.121

Tabelle 13: **Hersteller in Österreich nach Abteilung, 2023**
Quelle: [175].

Die Metalltechnische Industrie (FMTI) erzielte 2025 einen vorläufigen Produktionswert von 47,0 Mrd. € und exportierte davon 79,0 %.[182] Die Elektro- und Elektronikindustrie setzte 2025 mit

71.932 Beschäftigten Waren im Wert von 23,6 Mrd. € ab, rund halb so viel wie die Metalltechnische Industrie.[181]

Für österreichische Hersteller kommt ein zweites Cybersicherheitsgesetz hinzu. Die NIS-2-Richtlinie erfasst mittlere und große Einrichtungen, die elektronische und optische Erzeugnisse oder elektrische Ausrüstungen herstellen oder Maschinen bauen (NACE C26, C27 und C28).[166] Jedes Unternehmen der österreichischen Grundgesamtheit hat mindestens 100 Beschäftigte.

6.1.2 Die wichtigsten Termine

Drei österreichische Termine fallen in die Lebensdauer eines 2027 eingeführten Produkts: die Steuerbarkeit von Erzeugungsanlagen seit dem 1. Juni 2026, das neue NIS-Gesetz seit dem 1. Oktober 2026 und die Abschaltung des 2G-Netzes von A1 am 31. Mai 2028.[6, 334, 335] Der Nationalrat beschloss das ElWG am 12. Dezember 2025 mit 116 zu 47 Stimmen, also mit der erforderlichen Zweidrittelmehrheit.[323] Die meisten seiner Bestimmungen zu Zählern und Flexibilität sind bereits in Kraft, einzelne gelten ab späteren Stichtagen[335] (Tabelle 14).

BESTIMMUNG	REGEL	GILT AB
§ 49	Intelligente Messgeräte an allen Zählpunkten; auf Verlangen binnen zwei Monaten	in Kraft
§ 50 Abs. 2	Mindestfunktionen: Viertelstundenwerte, mindestens 60 Tage gespeichert; tägliche Fernauslesung über eine bidirektionale Schnittstelle; Abschaltung aus der Ferne; eine unidirektionale Schnittstelle, die der Kundin oder dem Kunden die Messwerte bereitstellt	in Kraft
§ 54 Abs. 2	Haushalte können Viertelstundenwerte ablehnen, außer an Zählpunkten mit Wärmepumpe, Ladepunkt, Speicher oder Erzeugungsanlage	in Kraft
§ 63	Endkunden und Erzeuger dürfen Last- und Einspeisesteuerung an allen Strommärkten anbieten, allein oder über Aggregatoren	in Kraft
§ 76	Neue oder wesentlich geänderte Erzeugungsanlagen ab 3,68 kW brauchen eine Steuereinrichtung mit standardisierter Schnittstelle; Ansteuerbarkeit durch den Netzbetreiber bis 1. Juni 2028 (> 25 kW), 1. Juni 2029 (3,68-25 kW), 1. Jänner 2030 (0,8-3,68 kW, auf Verlangen)	1. Juni 2026
§ 101	Spitzenkappung: PV-Einspeisung nicht unter 70 % der Modulspitzenleistung begrenzt; Windkraft höchstens 1 % der Jahresenergie	PV in Kraft; Wind 1. Jänner 2027
§ 103	Flexibler Netzzugang: Bei fehlender Kapazität darf der Netzbetreiber die netzwirksame Leistung begrenzen; Verbrauchs- und Speicheranlagen können dies vereinbaren	in Kraft
§ 139	Marktgestützte Beschaffung von Flexibilität, wenn günstiger als Netzausbau; gemeinsamer Vorschlag an die Regulierungsbehörde binnen neun Monaten	in Kraft

Tabelle 14: **ElWG-Bestimmungen für vernetzte Gebäudegeräte**
Quelle: [335].

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) setzt NIS 2 um und errichtet das Bundesamt für Cybersicherheit als Aufsichtsbehörde. Seine materiellen Bestimmungen gelten seit dem 1. Oktober 2026.[334] Alle österreichischen Mobilfunkbetreiber haben ihre 3G-Netze bis 2025 abgeschaltet, und die Wirtschaftskammer Österreich erwartet, dass die übrigen Betreiber dem Beispiel von A1 folgen und 2G bis 2028 abschalten.[413]

6.1.3 Folgen für Hersteller

Ein Gebäudegerät für Deutschland und Österreich braucht eine Hardwareplattform mit zwei Steuerpfaden: eine Schnittstelle nach § 14a für Deutschland und eine Aggregator- oder Energiemanagementschnittstelle für Österreich.[335] Ein Hybridsystem mit PV oder Batterie ab 3,68 kW braucht seit dem 1. Juni 2026 zusätzlich die Steuereinrichtung nach § 76.[335] Der Netzbetreiber gibt aber nur die Leistung am Netzanschlusspunkt vor, und die Optimierung hinter dem Zählpunkt bleibt Sache des Anlagenbetreibers.[335]

Die Technischen und Organisatorischen Regeln (TOR) der Regulierungsbehörde E-Control legen die standardisierte Schnittstelle fest, nicht das Gesetz.[335] Die TOR für Stromerzeugungsanlagen des Typs A gelten seit dem 1. Juni 2026. Sie verlangen eine digitale Schnittstelle, die der Netzbetreiber über die Internetverbindung des Netzbenutzers mit einem OpenADR-Protokoll nach IEC 62746-10-1 anspricht, schließen Drittsysteme als Übertragungsweg aus und schreiben vor, dass die Anlage den Sollwert innerhalb einer Minute erreicht.[121] Das Signal des Netzbetreibers darf also nicht über die Cloud des Herstellers laufen. Die Netzbetreiber spezifizieren das österreichische OpenADR-Profil bis zum 31. Oktober 2026 und veröffentlichen es bis zum 31. Dezember 2026.[121]

Der Smart Meter ist die Datenquelle. Er muss der Kundin oder dem Kunden die Messwerte über eine unidirektionale Schnittstelle bereitstellen, und an Zählpunkten mit Wärmepumpe oder Ladepunkt lassen sich seine Viertelstundenwerte nicht abschalten.[335] Bei der Sicherheit regelt NIS 2 die eigenen Netze des Unternehmens, einschließlich der Entwicklungs- und Update-Infrastruktur, auf die der CRA angewiesen ist.[166] Der CRA regelt das Produkt.[171] Ein gemeinsamer Meldeprozess kann beides abdecken, wenn er Produktschwachstellen an die CRA-Meldeplattform und Vorfälle in den eigenen Systemen an die nationale Behörde leitet.

6.2 Schweiz

6.2.1 Unterschiede zu Deutschland

Die Schweiz ist bei der Netzsteuerung das Gegenmodell zu Deutschland. Seit dem 1. Januar 2026 gehört die Flexibilität einer Anlage ihrem Inhaber. Jeder Dritte, auch der Netzbetreiber, braucht für ihre Nutzung einen Vertrag mit ihm.[344]

Die Stromversorgungsverordnung (StromVV) regelt die Einzelheiten. Die Verträge regeln Steuersystem, Umfang, Vergütung und Laufzeit, und die Netzbetreiber veröffentlichen ihre Vergütungsansätze jährlich.[345] Ohne Zustimmung und Vergütung darf der Netzbetreiber nur die Einspeisung am Anschlusspunkt abregeln, höchstens um 3 % der dort jährlich erzeugten Energie, und bei unmittelbarer Gefährdung des sicheren Netzbetriebs eingreifen.[345] Die vor 2026 genutzte Rundsteuerung von Wärmepumpen läuft weiter, solange der Inhaber nicht widerspricht.[345]

In der Schweiz haben 400 Hersteller der Grundgesamtheit ihren Sitz.[56] Nach unserer Schätzung stellen 153 bis 313 davon vernetzte Produkte her. Die meisten Beschäftigten der Schweizer Abteilungen entfallen auf die Elektronik einschließlich der Uhren und auf den Maschinenbau[56] (Tabelle 15). Auf die Uhrenindustrie entfällt fast die Hälfte der Beschäftigten von Abteilung 26.[55] Die Medizintechnik mit rund 1.400 Unternehmen und knapp 72.000 Beschäftigten wickelt mehr als die Hälfte ihrer Exporte und Importe mit der EU ab, und 43 % der befragten Unternehmen planen keine Investitionen, so viele wie nie seit Beginn der Erhebung.[371]

NOGA	ERZEUGNISSE	UNTERNEHMEN	DAVON 50-249	DAVON 250+	BESCHÄFTIGTE
26	Elektronische und optische Erzeugnisse, Uhren	1.920	260	82	124.075

NOGA	ERZEUGNISSE	UNTERNEHMEN	DAVON 50-249	DAVON 250+	BESCHÄFTIGTE
27	Elektrische Ausrüstungen	816	90	24	27.831
28	Maschinenbau	1.850	292	58	81.810
32	Sonstige Waren, inkl. Medizinprodukte	3.647	62	20	30.813

Tabelle 15: **Hersteller in der Schweiz nach Abteilung, 2024**
Quelle: [56].

Die Schweizer Tech-Industrie (Maschinen-, Elektro- und Metallindustrie) steigerte ihre Exporte 2025 um 0,7 % auf 68,1 Mrd. CHF. Die Ausfuhren in die EU stiegen um 3,5 %, die in die USA sanken um 7,6 %.[378] Ihre Kapazitätsauslastung lag mit 81,5 % im vierten Quartal 2025[378] und 81,1 % im zweiten Quartal 2026[377] unter dem langjährigen Mittel von 85,6 %.

6.2.2 Die wichtigsten Termine

Die für Hersteller wichtigen Schweizer Termine liegen zwischen Januar 2026 und Dezember 2027:

- **Bereits vollzogen.** 2G ist abgeschaltet, und Swisscom hat 3G Ende 2025 eingestellt. Sunrise hatte die Abschaltung für denselben Zeitpunkt geplant.[47, 373]
- **1. Januar 2026.** Die Flexibilitätsregeln von StromVG und StromVV treten in Kraft.[344]
- **31. Januar 2026.** Frist der Netzbetreiber für Richtlinien zu den Datenformaten der Smart Meter.[345]
- **20. Januar 2027.** Die EU-Maschinenverordnung wird anwendbar.[168]
- **Ende 2027.** 80 % der Messeinrichtungen jedes Netzgebiets müssen intelligent sein.[345]
- **11. Dezember 2027.** Die Hauptpflichten des CRA werden für Schweizer Produkte auf dem EU-Markt anwendbar.[171]

6.2.3 Folgen für Hersteller

Ein Gerät für den Schweizer Markt braucht eine Schnittstelle, die ein Netzbetreiber oder ein Dritter auf vertraglicher Grundlage nutzen kann, eine bestimmte Schnittstelle ist aber nicht vorgeschrieben.[344, 345] Ein Wärmepumpenhersteller plant für die Schweiz also eine freiwillige und vergütete Steuerung mit Vetorecht des Eigentümers, nicht das Dimmen durch den Netzbetreiber nach § 14a EnWG.

Der Zähler wird zur Datenquelle des Geräts. Art. 8a^{decies} StromVV verlangt eine Kundenschnittstelle, die Messdaten unmittelbar bei ihrer Erfassung in einem international gebräuchlichen Datenformat bereitstellt, und aktualisierbare Zählersoftware.[345] Spätestens ab 2028 haben damit die meisten Schweizer Haushalte und Betriebe einen Zähler, den ein Energiemanager, eine Wärmepumpe oder eine Wallbox ohne eigenen Zähler auslesen kann.[345] Ende 2024 waren 2,94 Mio. Smart Meter in Betrieb, die Hälfte (50,2 %) aller Zähler, gegenüber 26,1 % im Jahr 2021.[46]

6.3 Schweizer Hersteller auf dem EU-Markt

Die fünf Rechtsakte gelten für jedes Produkt, das in der EU in Verkehr gebracht wird, gleich, wo sein Hersteller sitzt. Der Data Act erfasst Hersteller vernetzter Produkte ausdrücklich „unabhängig vom Ort ihrer Niederlassung“.[170, 171] Für einen Schweizer Hersteller ändert sich, wer zusätzlich in der Pflicht steht, mit welcher Behörde er zu tun hat und ob das Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) seine Maschinenbewertungen unter der neuen Maschinenverordnung noch anerkennt.

Einführer. Der EU-Einführer eines Schweizer Produkts darf es erst in Verkehr bringen, wenn er sichergestellt hat, dass die CRA-Konformitätsbewertung durchgeführt wurde und die technische

Dokumentation vorliegt. Das Produkt muss außerdem die CE-Kennzeichnung tragen und mit der EU-Konformitätserklärung und den vorgeschriebenen Nutzerinformationen ausgeliefert werden.[171] Der Einführer bringt seinen eigenen Namen und seine Kontaktdaten auf Produkt, Verpackung oder Begleitdokument an und informiert den Hersteller über ihm bekannt gewordene Schwachstellen. Er bewahrt die Erklärung mindestens zehn Jahre oder für den Unterstützungszeitraum auf, je nachdem, welcher Zeitraum länger ist.[171]

Bevollmächtigter. Nach dem CRA ist die Benennung eines Bevollmächtigten freiwillig und erfolgt durch schriftlichen Auftrag. Der Auftrag muss mindestens die Bereithaltung von Erklärung und Dokumentation, Auskünfte an Behörden und die Mitwirkung an Korrekturmaßnahmen umfassen. Er darf aber die Pflichten des Herstellers zu Design und Schwachstellenbehandlung nicht einschließen.[171] Für Funkanlagen, elektrische Betriebsmittel und Maschinen verlangt Artikel 4 der Marktüberwachungsverordnung einen in der Union niedergelassenen Wirtschaftsakteur, also Einführer, Bevollmächtigten oder Fulfilment-Dienstleister, dessen Name auf dem Produkt steht.[165] Für Maschinen bleibt diese Pflicht unter der Maschinenverordnung bestehen.[167, 168] Die MRA-Kapitel für Funkanlagen und für elektrische Betriebsmittel verweisen auf die geltenden Richtlinien und lassen für Kennzeichnung und Aufbewahrung der Unterlagen einen in der Schweiz ansässigen Hersteller oder Einführer genügen.[343] Ein Schweizer Hersteller braucht deshalb weder einen Vertrag mit einem Wirtschaftsakteur in der EU noch dessen Kontaktdaten auf dem Produkt, solange das MRA-Kapitel für sein Produkt aktuell ist.[125] Der Data Act fügt unabhängig vom MRA eine eigene Pflicht hinzu. Ein Unternehmen ohne Niederlassung in der Union, das dort vernetzte Produkte bereitstellt, muss einen gesetzlichen Vertreter in einem Mitgliedstaat benennen und unterliegt der Zuständigkeit dieses Mitgliedstaats.[170]

Meldungen. Die Meldepflichten nach Artikel 14 gelten seit dem 11. September 2026 und treffen den Schweizer Hersteller unmittelbar.[171] Ein Hersteller ohne Hauptniederlassung in der Union meldet an das CSIRT des Mitgliedstaats, in dem sein Bevollmächtigter niedergelassen ist. Ersatzweise ist der Mitgliedstaat des Einführers zuständig, der die meisten seiner Produkte in Verkehr bringt, dann der des Händlers und zuletzt der Mitgliedstaat mit den meisten Nutzern.[171] Die Benennung eines Bevollmächtigten in Deutschland oder Österreich legt damit fest, mit welchem CSIRT der Hersteller zu tun hat.

Schweizer Recht im Inland. In der Schweiz gilt kein Gesetz, das dem CRA oder dem Data Act entspricht. Im August 2025 hatte der Bundesrat das Bundesamt für Cybersicherheit (BACS) beauftragt, ein Cybersicherheitsgesetz auszuarbeiten.[45] Am 25. September 2026 übertrug er diese Aufgabe an das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), das bis Juni 2027 einen Entwurf vorlegen soll.[351] Das Gesetz soll sich am CRA orientieren, Hersteller, Importeure und Händler verpflichten und ein Vertriebsverbot für unsichere Produkte ermöglichen.[45, 351] Bis zum Inkrafttreten stehen noch Vernehmlassung, parlamentarische Beratung und ein mögliches Referendum aus. Wir erwarten deshalb nicht, dass das Gesetz vor dem 11. Dezember 2027 gilt.

Zwei sektorale Verordnungen übernehmen EU-Anforderungen an die Cybersicherheit, eine geplante und eine geltende. Für Maschinen würde die revidierte Schweizer Maschinenverordnung (MaschV) die Anforderungen der EU-Maschinenverordnung an den Schutz gegen Korrumpierung und an Sicherheit und Zuverlässigkeit der Steuerungen übernehmen, samt der Konformitätsvermutung für Maschinen, die unter einem EU-Schema für die Cybersicherheitszertifizierung zertifiziert sind.[125, 168] Solche Schweizer Zertifikate gibt es nicht.[125] Für Funkanlagen übernehmen die Verordnung über Fernmeldeanlagen (FAV) und die Verordnung des BAKOM über Fernmeldeanlagen (VFAV) die drei Anforderungen der delegierten Verordnung 2022/30.[125, 346] Funkanlagen, die sie nicht erfüllen, dürfen in der Schweiz seit dem 1. August 2025

nicht mehr in Verkehr gebracht werden, zum selben Stichtag wie in der EU.[346] Eine CE-Kennzeichnung ist in der Schweiz grundsätzlich nicht vorgeschrieben.[365] Ein Schweizer Hersteller, der im gesamten DACH-Raum verkauft, entwickelt also für Deutschland und Österreich nach EU-Recht und verwendet dasselbe Design im Inland.

6.3.1 Die MRA-Frage

Das MRA umfasst 20 Produktsektoren, darunter Maschinen (Kapitel 1), Medizinprodukte, elektrische Geräte sowie Funkanlagen und Telekommunikationsendgeräte (Kapitel 7), und deckt damit 73 % der Schweizer Industrieprodukte ab, die in die EU ausgeführt werden.[349, 365] Im Kern sieht es vor, dass die Konformität nur einmal bewertet wird, in der Schweiz oder in der EU.[349] Der CRA fällt unter keines seiner Kapitel. Eine CRA-Konformitätsbewertung durch eine Schweizer Stelle wird über das MRA daher nicht anerkannt.[365] Ein Produkt der Klasse I oder II, das eine notifizierte Stelle braucht, muss von einer in der EU notifizierten Stelle bewertet werden.[365] Seit dem 26. Mai 2021 verweigert die EU die Aktualisierung des Abkommens, weil institutionelle Fragen offen waren. Das Kapitel für Medizinprodukte wurde deshalb nicht aktualisiert, und Medizinprodukthersteller haben seitdem Drittlandstatus.[349]

Das Paket Schweiz-EU (Bilaterale III) soll diese Blockade beenden und nimmt dazu institutionelle Elemente in das MRA auf, damit es regelmäßig an das EU-Recht angepasst wird.[349] Die Abkommen wurden am 2. März 2026 unterzeichnet und im selben Monat dem Parlament überwiesen. Ein Datum für das Inkrafttreten steht nicht fest.[124] Das Änderungsprotokoll zum MRA fasst die institutionellen Artikel des Abkommens und die Kapitel 4, 5, 11 und 15 seines Anhangs neu, nicht das Maschinenkapitel. Es tritt nur zusammen mit den übrigen Abkommen des Pakets in Kraft.[85, 124]

Für Maschinenbauer ist der 20. Januar 2027 der Stichtag.[168] Das Maschinenkapitel des MRA verweist in der Fassung vom 22. Dezember 2017 noch auf die Maschinenrichtlinie und die MaschV vom 2. April 2008.[343] Seine Aktualisierung auf die Verordnung 2023/1230 setzt eine gleichwertige Schweizer Verordnung und die Zustimmung beider Vertragsparteien im Gemischten Ausschuss voraus.[125] Die totalrevidierte MaschV übernimmt die Verordnung durch Verweis und soll am selben Tag in Kraft treten.[125] Die Vernehmlassung lief vom 19. September bis zum 19. Dezember 2025.[342, 350] Der erläuternde Bericht geht davon aus, dass das MRA-Kapitel rechtzeitig aktualisiert wird, und beauftragt das Eidgenössische Departement für Wirtschaft, Bildung und Forschung (WBF), andernfalls die Folgen zu prüfen.[125]

Bislang hat der Bundesrat die revidierte Verordnung nicht verabschiedet und der Gemischte Ausschuss das Kapitel nicht aktualisiert. Die geltende MaschV ist die Fassung vom 20. Januar 2024, und auch die Bezeichnung technischer Normen für Maschinen, die das SECO am 9. Oktober 2026 veröffentlicht hat, verweist noch auf die Verordnung von 2008 und die unter der Richtlinie zitierten Normen.[343, 347, 364] Der Bundesrat kann die Verordnung noch rechtzeitig verabschieden, die Aktualisierung des Kapitels erfordert aber zusätzlich die Zustimmung der EU. Bis dahin braucht ein Schweizer Maschinenbauer, der in die EU liefert, einen auf dem Produkt genannten Wirtschaftsakteur in der EU und für Maschinen nach Anhang I eine notifizierte Stelle in der EU[349] (Tabelle 16).

BEREICH	MRA AKTUALISIERT	MASCHINENKAPITEL NICHT AKTUALISIERT
Konformitätsbewertung Maschinen	einmal, in der Schweiz, in der EU anerkannt	Konformitätsbewertung in der EU nötig
Wirtschaftsakteur in der EU, Kennzeichnung	für Maschinen nicht nötig	Einführer oder Bevollmächtigter in der EU; neue Etikettierung

BEREICH	MRA AKTUALISIERT	MASCHINENKAPITEL NICHT AKTUALISIERT
CRA (Cybersicherheit)	außerhalb des MRA: EU-Recht gilt voll, Pflichten des Einführers gelten	ebenso
Medizinprodukte	Aktualisierung nach Inkrafttreten möglich	Drittlandstatus wie seit 2021

Tabelle 16: **Folgen der beiden MRA-Ausgänge für Schweizer Hersteller**
Anmerkung: „MRA aktualisiert“ setzt das Inkrafttreten des Pakets Schweiz-EU voraus. Quellen: [349, 365].

KURZ GESAGT

Im Ergebnis lässt sich ein nach EU-Recht gebautes Produkt in allen drei Ländern verkaufen, doch jedes Stromnetz verlangt einen eigenen Steuerpfad, und jeder Schweizer Hersteller braucht einen Partner in der EU, der eigene Pflichten übernimmt. Beides hängt weder vom MRA noch von einem künftigen Schweizer Cybersicherheitsgesetz ab. Das nächste Kapitel zeigt, welche Anbieter die Technik liefern, mit der Hersteller diese Regeln erfüllen.

7 Anbieterlandschaft

Ein Hersteller vernetzter Produkte kauft die meisten Schichten seiner Systemarchitektur zu, vom Secure Element über den Update-Dienst bis zur IoT-Plattform, und ist während des gesamten Unterstützungszeitraums seiner Produkte auf diese Anbieter angewiesen. Für jede Schicht gibt es etablierte Anbieter, doch viele von ihnen haben 2025 und 2026 den Eigentümer gewechselt, und die drei großen US-Cloud-Anbieter haben IoT-Dienste eingestellt. Unter dem CRA ist bisher keine einzige Stelle notifiziert. Für Gateways, die auf eine solche Stelle angewiesen sind, gibt es damit noch keinen Weg zur Konformität. Das Kapitel beschreibt die Konsolidierung je Schicht, die Abkündigungen der Cloud-Anbieter und den Stand der notifizierten Stellen.

7.1 Marktkonsolidierung 2025-2026

Der Anbietermarkt hat sich zwischen 2024 und 2026 in vier Schichten konsolidiert. Das Gerätemanagement ging an Chip- und Betriebssystemanbieter, Kapital floss in die Firmware-Sicherheit, PKI-Anbieter wurden von Finanzinvestoren übernommen, und unabhängige Plattformen wechselten den Eigentümer (Anbieter je Schicht in Anhang D).

Ein 2026 gewählter Anbieter kann deshalb einen neuen Eigentümer, eine neue Produktlinie oder eine neue Preisliste haben, bevor ein 2027 verkauftes Produkt das Ende seines Unterstützungszeitraums erreicht.

7.1.1 Gerätemanagement und OTA

Drei der fünf OTA-Produkte, auf denen die meisten DACH-Projekte beruhen, wechselten zwischen Juni 2025 und März 2026 den Eigentümer. Nordic Semiconductor übernahm Memfault am 24. Juni 2025 und integriert es in nRF Cloud. Nordic hat zugesagt, auch Gerätehersteller mit Hardware anderer Anbieter weiterhin zu betreuen.[286] Golioth gehört seit dem 3. März 2026 zu Canonical,[198]

und Canonicals Zephyr 26.04 LTS enthält seit September 2026 Golioth-OTA.[200] Die Wahl des OTA-Dienstes ist damit enger als bisher an einen Chip- oder Betriebssystemanbieter gebunden.

Zwei Anbieter legen den Schwerpunkt auf Compliance für den deutschsprachigen Markt. qdCloud ordnet seine Funktionen den CRA-Anforderungen zu und stellt klar, dass dies die Konformitätsbewertung des Produkts nicht ersetzt.[332] Kontron aus Linz verkauft Betriebssystem und Update-Dienst im Paket[241] und hat seit 2026 mit Ennoconn einen Ankeraktionär.[243]

7.1.2 SBOM, Schwachstellenmanagement und PSIRT

Anbieter von Binäranalysen untersuchen kompilierte Firmware und erfassen damit auch zugekaufte Funkmodule und Platinen von Zulieferern. Sie haben mehr Kapital eingesammelt als jede andere Anbietergruppe. Allein Exein aus Rom erhielt im Juli 2025 70 Mio. €, im Dezember 2025 100 Mio. € und im September 2026 270 Mio. US-Dollar bei einer Bewertung von 1,7 Mrd. US-Dollar.[177, 178, 180] Dragos übernahm NetRise, und Keysight vertreibt die SBOM-Plattform von Cybeats unter eigenem Namen.[89, 118]

Kein Anbieter von Analysewerkzeugen liefert das PSIRT-Team, die Richtlinie zur Offenlegung von Schwachstellen und den 24-Stunden-Meldeweg mit. Diese Leistungen bieten Ingenieurdienstleister an. Ginzinger electronic systems und sein Partner LIMES Security etwa bieten sichere Updates und den zugehörigen CVE-Prozess als Teil eines Lebenszyklus-Services an.[192] Die Werkzeuge lassen sich kaufen, für den Prozess bleibt der Hersteller oder sein Dienstleister verantwortlich.

7.1.3 Secure Element und PKI

Vier börsennotierte Chiphersteller liefern die gängigen Secure Elements und ihre Provisionierungsdienste, darunter NXP EdgeLock 2GO, Infineon Trust M Express und Microchip Trust&GO.[218, 263, 296] Die Anbieter ausstellender CAs haben sich unter dem Dach von Finanzinvestoren konsolidiert. Keyfactor übernahm InfoSec Global, DigiCert übernahm Vercara und Valimail, und Sectigo übernahm das Geschäft von Entrust mit öffentlichen Zertifikaten.[103, 104, 231, 352] Keyfactor erhielt 2026 zudem eine Wachstumsinvestition von über 1 Mrd. US-Dollar.[233] Die PKI- und HSM-Anbieter aus dem DACH-Raum sind kleiner, mehrere gehören Finanzinvestoren oder dem Staat.

7.1.4 IoT-Connectivity

Zwei MVNOs mit Sitz in Deutschland konkurrieren mit den Netzbetreibern. 1NCE aus Köln gibt über 40 Mio. SIM-Verbindungen an,[4] emnify aus Berlin über 23 Mio.[130] Beide finanzieren sich über Investoren. 1NCE sammelte im April 2025 60 Mio. US-Dollar ein, unter anderem bei der Deutschen Telekom.[1] Beide bieten eSIM nach SGP.32 an, den Standard für den Profilwechsel bei bereits ausgelieferten Geräten.[129]

7.1.5 IoT-Plattformen

Die unabhängigen Plattformen wechselten den Eigentümer, die deutschen Industrieplattformen blieben bei ihren Konzernen. Das Management von Cumulocity kaufte die Plattform im Januar 2025 von der Software AG zurück,[86] und PTC verkaufte ThingWorx und Kepware an TPG, die Transaktion wurde am 13. März 2026 abgeschlossen.[327] Siemens hat MindSphere in Insights Hub umbenannt,[361] für die Bosch IoT Suite liegt keine Abkündigung vor,[44] und Device Insight ist seit 2019 eine hundertprozentige Tochter von KUKA.[102]

7.1.6 Tracker und Telematik

Zwei wichtige Zulieferer für Tracker und Telematik gingen 2025 an Finanzinvestoren. Advent International schloss am 26. November 2025 die Übernahme von u-blox ab, dem Schweizer

Hersteller von GNSS- und Mobilfunkmodulen.[11] Goldman Sachs Alternatives ist seit Juni 2025 Mehrheitsinvestor beim Baumaschinen-Telematikanbieter Trackunit.[390]

7.1.7 Ingenieurdienstleister

Die beiden börsennotierten Ingenieurdienstleister mit großem Deutschlandgeschäft, Bertrandt und EDAG, meldeten für ihre im Jahr 2025 abgelaufenen Geschäftsjahre Umsatzrückgänge von 18 % und 13 %.[34, 122] Die spezialisierten Embedded-Dienstleister in Österreich und der Schweiz sind kleiner und arbeiten näher an der Gerätetechnik.

7.2 Eingestellte IoT-Dienste als Plattformrisiko

Alle drei großen US-Cloud-Anbieter haben seit 2023 IoT-Dienste eingestellt oder für Neukunden geschlossen. Google beendete IoT Core 2023, AWS und Microsoft folgten ab 2024 mit mehreren Diensten, insgesamt sechs Änderungen in vier Jahren[14, 201, 264] (Tabelle 17). Für ein Produkt mit einem Unterstützungszeitraum von mindestens fünf Jahren ist jede davon ein Plattformrisiko.[171]

DIENST	ANBIETER	ÄNDERUNG	DATUM
Google Cloud IoT Core	Google	Eingestellt	August 2023
AWS IoT Analytics	AWS	Seit 24. Juli 2024 keine Neukunden; Ende des Supports	15. Dez. 2025
AWS IoT Events	AWS	Seit 20. Mai 2025 keine Neukunden; Ende des Supports	20. Mai 2026
AWS IoT FleetWise	AWS	Keine Neukunden; Supportende nicht angekündigt	30. Apr. 2026
Azure IoT Central	Microsoft	Keine neuen Anwendungen; nach dem 20. Sept. 2029 nicht mehr verfügbar	23. Sept. 2026
Azure IoT Edge 1.5 LTS	Microsoft	Ende des Supports; keine Nachfolge-LTS gelistet	11. Nov. 2026
Azure Device Update for IoT Hub	Microsoft	Bleibt allgemein verfügbar; Updates über Azure Device Registry in Vorschau	Oktober 2026

Tabelle 17: **Abkündigungen von Cloud-IoT-Diensten seit 2023**
Quellen: [14, 17, 18, 201, 264, 265, 267].

Die Kerndienste sind nicht betroffen. Für AWS IoT Core und Azure IoT Hub ist keine Abkündigung bekannt, und Microsoft nennt IoT Hub, den Device Provisioning Service und Fabric als Migrationsweg aus IoT Central.[264] Das Risiko liegt bei den darauf aufbauenden Diensten. Der Update-Dienst sollte deshalb über eine eigene Abstraktionsschicht angebunden sein.

7.3 Notifizierte Stellen unter dem CRA

Derzeit verzeichnet NANDO keine einzige nach Verordnung (EU) 2024/2847 notifizierte Stelle, unabhängig vom Status.[161] Kapitel IV des CRA gilt seit dem 11. Juni 2026, und die Kommission veröffentlicht jede Stelle nach ihrer Notifizierung in NANDO.[157]

Auch die Behörden stehen noch nicht überall bereit. Für den CRA sind 14 notifizierende Behörden in 13 Mitgliedstaaten eingetragen, in Deutschland das BSI.[161] Österreich hat keine eingetragen. Das Bundeskanzleramt erklärt, es werde diese Aufgabe übernehmen.[59] Das parlamentarische Verfahren zum deutschen CRA-Durchführungsgesetz ist noch nicht abgeschlossen.[100, 220] Der CRA fällt nicht unter das MRA zwischen der EU und der Schweiz.[365] Schweizer Stellen können deshalb nicht notifiziert werden.[365]

Zwei Stellen haben ihre Notifizierung öffentlich angekündigt. SGS Brightsight in den Niederlanden ist nach ISO/IEC 17065 für CRA-Modul B akkreditiert und strebt die Notifizierung über die niederländische notifizierende Behörde an.[360] TÜV NORD wird beim BSI die Benennung unter dem CRA beantragen.[396]

Ein Produkt der Klasse I wie ein eigenständig verkauftes Gateway braucht deshalb eine notifizierte Stelle, die es noch nicht gibt, solange keine harmonisierte CRA-Norm im Amtsblatt zitiert ist. Für Bewertungen nach EN 18031 unter der RED stehen dagegen schon heute 55 aktive Stellen bereit, 12 davon in Deutschland.[160]

KURZ GESAGT

Ein Hersteller kann die Technik zukaufen, muss sein System aber so auslegen, dass er Update-Dienst, PKI und Cloud wechseln kann, ohne in bereits ausgelieferte Geräte eingreifen zu müssen. Normung und Notifizierung entscheiden über den Marktzugang eigenständig verkaufter Gateways, nicht der Hersteller. Das letzte Kapitel leitet aus der Analyse Maßnahmen je Rolle, einen Zwölfmonatsplan und fünf Leitfragen ab.

8 Handlungsempfehlungen

Ein Hersteller vernetzter Produkte hat weniger als ein Jahr, bis der CRA am 11. Dezember 2027 vollständig gilt. Die Meldepflicht für Schwachstellen besteht bereits. Der Hersteller sollte bis Ende März 2027 eine aktiv ausgenutzte Schwachstelle binnen 24 Stunden melden können und die CRA-Klasse jedes Produkts kennen. Bis zur Jahresmitte folgt die Architektur, bis zum Herbst ein Pilot an einer Produktlinie und vor dem Stichtag die Konformitätsbewertung. Das Kapitel ordnet die Maßnahmen drei Rollen zu, legt sie in einem Zwölfmonatsplan fest, nennt die Förderprogramme, die einen Teil der Kosten übernehmen, und schließt mit fünf Leitfragen.

8.1 Geschäftsführung

Die Geschäftsführung entscheidet über die Größe der Flotte, auf die sich die Sicherheitskosten verteilen, und über das Backend, das Updates, Zertifikate und Meldungen abwickelt. Beides bestimmt die Kosten (F4, F5).

- Ein gemeinsames Geräte-Backend für alle Produktlinien zur Regel machen, mit einem Update-Dienst, einer PKI und einem Schwachstellenprozess. Nach unserem Kostenmodell sinkt der Sicherheitsaufschlag von rund 2,30 € je Gerät und Monat bei 1.000 Einheiten auf unter 0,30 € bei 100.000 (F5).
- Sicherheit nicht als einmaliges Projekt budgetieren, sondern als laufende Kosten von rund einem halben Euro je Gerät und Monat, und diese in Produktpreis und Serviceverträge einkalkulieren (F4). Den Data Act einmal für das ganze Unternehmen budgetieren, für eine Exportschnittstelle und einen Prozess zur Datenweitergabe.[143]
- Die Verantwortung für Produktsicherheit einer Person übertragen und ihr die Befugnis geben, eine Meldung ohne weitere Freigabe abzugeben (F1).
- Den folgenden Zwölfmonatsplan ab Januar 2027 finanzieren und quartalsweise überprüfen. Die Fristen verschieben sich nicht, wenn die Normen sich verspäten (F1, F2).

- OTA-Dienst und Mobilfunktarif nach ihren Kosten über fünf Jahre auswählen, nicht nach dem Chippreis (F4). Von jedem Plattform- und OTA-Anbieter eine schriftliche Zusage für den Unterstützungszeitraum der eigenen Produkte und einen dokumentierten Exportweg verlangen.
- Entscheiden, ob Tracking als Service verkauft wird, und den Preis an Pauschalen je Asset ausrichten, nicht an den Stücklistenkosten des Tags.[357] Werkzeugortung als Integration in die Baustellen-Gateways der Bauunternehmen planen, nicht als eigenes Gateway-Netz.[207, 391]

8.2 Produkt und Entwicklung

Die Entwicklung trifft die Designentscheidungen, die sich nach der Auslieferung nicht mehr ändern lassen (F3, F4, F6).

- Secure Boot, einen Hardware-Vertrauensanker, eine eindeutige Geräteidentität und den Provisionierungsweg in der Fertigung für jedes Produkt, das 2027 auf den Markt kommt, vor dem Platinenlayout festlegen. Keines davon lässt sich per Firmware-Update nachrüsten, und in unserem Kostenmodell ist das Secure Element der kleinste Kostenposten (F4, F5).
- Gateways als Teil der Maschine auslegen, zusammen mit ihr verkaufen und dokumentieren und ihre Kernfunktion als Maschinenanbindung beschreiben, nicht als Netzschutz, damit sie in der Standardklasse des CRA bleiben[149] (F3).
- Schreibzugriffe des Gateways auf Sicherheitsfunktionen konstruktiv ausschließen und SPS-Firmware getrennt von den Paketen des Gateways signieren, damit Kunden Sicherheitskorrekturen einspielen können, ohne ihren Prozess neu zu qualifizieren.[168, 171]
- Kein Firmware-Release ohne SBOM im Format der BSI TR-03183 und ohne Abgleich mit bekannten Schwachstellen freigeben[54] und jeden Treffer an ein benanntes Sicherheitsteam leiten, das binnen 24 Stunden an die ENISA melden kann (F1).
- Geräteidentitäten, Update-Schlüssel, Update-Dienst und Ortungsdienst hinter einer eigenen Schnittstelle betreiben, die den Verkauf eines Anbieters oder die Abkündigung eines Cloud-Dienstes übersteht.
- Den 2G-Fallback aus Tracker- und Gateway-Designs streichen und Batterien für den Nutzer entnehmbar machen oder die Ausnahme dokumentieren, bevor das Design eingefroren wird[77, 169] (F6).

8.3 Compliance

Compliance verantwortet die Pflicht, die heute gilt, und die Einstufung, die alle späteren Kosten bestimmt (F1, F3).

- Den Meldeweg über die zentrale Meldeplattform der ENISA verantworten und in einer Übung testen, bevor ein echter Fall eintritt[133, 171] (F1). Einen gemeinsamen Meldeprozess für CRA und NIS 2 einrichten, wenn das Unternehmen auch unter NIS 2 fällt. Er leitet Produktschwachstellen an die Meldeplattform und Vorfälle in den eigenen Systemen an die nationale Behörde.[166]
- Die bereits ausgelieferten Geräte in die Meldepflicht einbeziehen, nicht nur die laufende Produktion (F1).
- Die CRA-Einstufung aller Produkte verantworten und an der Durchführungsverordnung der Kommission zu den Produktkategorien ausrichten[149] (F3).
- Die Konformität jetzt an den grundlegenden Anforderungen aus Anhang I bewerten, statt auf harmonisierte Normen zu warten, und die Nachweise je Anforderung ablegen (F3). Zertifizierte Funkmodule und Secure Elements sparen Arbeit, ersetzen aber nicht die Bewertung des ganzen Produkts.[171]
- Für wichtige Produkte frühzeitig Kontakt zu den Stellen aufnehmen, die eine CRA-Notifizierung angekündigt haben (F3).

- Für Schweizer Produkte den gesetzlichen Vertreter nach dem Data Act benennen und die CRA-Pflichten in jeden Vertrag mit einem EU-Einführer aufnehmen: Dokumentation, Kontaktangaben auf dem Produkt, Mitwirkung bei Schwachstellen.[170, 171] Für Schweizer Maschinen zusätzlich einen Einführer oder Bevollmächtigten in der EU benennen und für Maschinen nach Anhang I eine notifizierte Stelle in der EU als Rückfalloption vorhalten, solange das Maschinenkapitel des Abkommens über die gegenseitige Anerkennung nicht an die neue Maschinenverordnung angepasst ist.[343, 349]

8.4 Der Zwölfmonatsplan

Die Pflichten bestimmen die Reihenfolge des Plans. Die bereits geltende Meldepflicht kommt zuerst, die Konformitätsbewertung für Produkte, die nach dem 11. Dezember 2027 in Verkehr kommen, zuletzt[171] (Tabelle 18). Der Plan beginnt im Januar 2027 und richtet sich an einen Hersteller mit einer bis fünf vernetzten Produktlinien und einer gemeinsamen Entwicklungsorganisation.

MONAT AB ERSCHEINEN	PHASE	ERGEBNIS	ZUGEHÖRIGE FRIST	BERUHT AUF
1-3	Meldung und Einstufung	Ein funktionierender CRA-Meldeprozess; jedes Produkt einer CRA-Klasse und einer Kategorie der Maschinenverordnung zugeordnet	CRA-Meldepflicht, gilt seit 11.09.2026; Maschinenverordnung, 20.01.2027	F1, F3
4-6	Lückenanalyse und Architektur	Eine Lückenliste je Produkt gegen die Anforderungsmatrix; eine Zielarchitektur und eine kalkulierte Stückliste	Gestaltungspflicht des Data Act für neue Produkte, gilt seit 12.09.2026	F4, F5
7-9	Pilot	Eine Produktlinie in der Zielarchitektur: Secure Element, signierte OTA-Updates, SBOM je Release, Datenschnittstelle	Batterieverordnung, 18.02.2027; 2G-Abschaltung, 2028	F6
10-12	Bewertung und CE-Kennzeichnung	Technische Dokumentation, Konformitätsbewertung und EU-Konformitätserklärung für jedes Produkt, das nach dem 11.12.2027 in Verkehr kommt	CRA vollständig, 11.12.2027	F3

Tabelle 18: **Maßnahmenplan für die ersten zwölf Monate**

8.4.1 Monate 1-3: Meldung und Einstufung

Das erste Quartal gilt der Pflicht, die bereits besteht. Bei einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Vorfall muss der Hersteller binnen 24 Stunden eine Frühwarnung abgeben, binnen 72 Stunden eine Meldung und danach einen Abschlussbericht, über die zentrale Meldeplattform der ENISA und auch für Produkte, die bereits am Markt sind.[133, 156, 171]

A1 Die verantwortliche Person und ihre Vertretung benennen und sicherstellen, dass eine von beiden binnen 24 Stunden über eine Meldung entscheiden kann.

A2	Sich auf der Meldeplattform der ENISA registrieren und klären, welches CSIRT zuständig ist. Bei einem Schweizer Hersteller richtet sich das nach dem Wirtschaftsakteur in der EU, mit dem er zusammenarbeitet.
A3	Eine Richtlinie zur Offenlegung von Schwachstellen und eine Kontaktadresse für Sicherheitsmeldungen auf der Website veröffentlichen.
A4	Ein Verzeichnis aller Produkte mit digitalen Elementen am Markt anlegen, mit den Firmware-Ständen der Geräte im Einsatz.
A5	Jedes Produkt einer CRA-Klasse zuordnen (Standard, wichtig Klasse I oder II, kritisch) und bei Maschinen prüfen, ob sie unter Anhang I der Maschinenverordnung fallen.
A6	Jede Einstufung mit Ermessensspielraum, etwa bei einem eigenständig verkauften Gateway, samt Begründung dokumentieren.

Die Einstufung bestimmt die Kosten aller weiteren Schritte. Ein Produkt der Standardklasse darf sich nach Modul A selbst bewerten, ein wichtiges Produkt braucht eine harmonisierte Norm oder eine notifizierte Stelle.[171] Die Durchführungsverordnung der Kommission zu den Kategorien gilt seit dem 21. Dezember 2025 und entscheidet über Grenzfälle.[149]

8.4.2 Monate 4-6: Lückenanalyse und Architektur

Im zweiten Quartal prüft der Hersteller jedes Produkt gegen die Anforderungsmatrix der fünf Rechtsakte und legt das Zieldesign fest. Anhang I des CRA setzt den Maßstab: sichere Voreinstellungen, Integrität und Vertraulichkeit, ein erklärter Unterstützungszeitraum und eine Schwachstellenbehandlung mit SBOM[171] im Format der BSI TR-03183.[54]

A7	Je Produktlinie eine Lückenanalyse gegen die Matrix durchführen, eine Zeile je Anforderung, mit den heute vorhandenen Nachweisen.
A8	Den Unterstützungszeitraum je Produkt festlegen und veröffentlichen, denn der CRA verlangt, ihn beim Kauf anzugeben.
A9	Die Bausteine der Zielarchitektur wählen: Funk, Secure Element oder TPM, Geräteidentität und PKI, OTA-Dienst, SBOM-Werkzeug, Datenschnittstelle.
A10	Die Zielarchitektur für die geplante Flottengröße kalkulieren, einschließlich des Sicherheitsaufschlags.
A11	Die gewählte Funktechnik auf die 2G-Abschaltung prüfen.
A12	Die Data-Act-Schnittstelle für Produkte entwerfen, die ab jetzt in Verkehr kommen, mit den entstehenden Produktdaten, dem Zugriffsweg des Nutzers und dem Format.

Diese Entscheidungen lassen sich später nicht mehr korrigieren. Die deutschen 2G-Netze werden zwischen dem 30. Juni 2028 und Ende 2028 abgeschaltet. Ein 2027 verkauftes Produkt mit fünf Jahren Lebensdauer ist dann noch im Einsatz.[77] Die Sicherheitsfunktionen des Geräts lassen sich nach der Auslieferung nicht nachrüsten. Die Pflicht des Data Act zum Datenzugang ab Werk gilt für vernetzte Produkte, die nach dem 12. September 2026 in Verkehr gebracht werden.[170]

8.4.3 Monate 7-9: Pilot

Im dritten Quartal muss sich das Design an einer Produktlinie bewähren, von der Provisionierung im Werk über ein signiertes Update an ausgelieferte Geräte bis zu einer Testmeldung über den Meldeprozess aus dem ersten Quartal.

A13	Für eine Fertigungscharge die Geräteidentitäten im Werk provisionieren und in der PKI registrieren.
A14	Ein signiertes und, wo nötig, verschlüsseltes Firmware-Update an die Pilotflotte ausrollen und einen Rollback testen.
A15	Die SBOM-Erzeugung in der Build-Pipeline der Pilotlinie automatisieren.
A16	Eine Meldeübung mit einer simulierten, aktiv ausgenutzten Schwachstelle durchführen, von der Erkennung bis zur Frühwarnung innerhalb von 24 Stunden.
A17	Die Data-Act-Schnittstelle mit einem Nutzer und, falls relevant, einem vom Nutzer benannten Dritten testen.
A18	Bei batteriebetriebenen Produkten prüfen, dass der Endnutzer Gerätebatterien entnehmen und ersetzen kann und Industriebatterien über 2 kWh einen Batteriepass haben, beides Pflicht ab dem 18. Februar 2027.

Die Batterieregel trifft vor allem Werkzeuge und Tracker. Viele Tracker sind vergossen oder versiegelt und verstoßen damit gegen die Pflicht zur Entnehmbarkeit, sofern keine Ausnahme greift[169] (F6).

8.4.4 Monate 10-12: Bewertung und CE-Kennzeichnung

Im letzten Quartal entstehen Dokumentation und Konformitätsbewertung, damit jedes Produkt am Tag der vollen Geltung des CRA die CE-Kennzeichnung tragen kann.[171] Neue Maschinen unterliegen bereits ab dem 20. Januar 2027 der Maschinenverordnung.[168]

A19	Je Produkt die technische Dokumentation zusammenstellen: Risikobeurteilung, Anforderungsmatrix mit Nachweisen, SBOM, Unterstützungszeitraum, Prüfberichte.
A20	Für Produkte der Standardklasse die interne Kontrolle nach Modul A durchführen und die EU-Konformitätserklärung ausstellen.
A21	Für wichtige Produkte ohne zitierte harmonisierte Norm einen Termin bei einer notifizierten Stelle sichern, sobald die erste notifiziert ist.
A22	Die Nutzerinformation aktualisieren: Unterstützungszeitraum, Sicherheitskontakt, sichere Außerbetriebnahme, Datenzugang.
A23	Vertrieb und Service darüber informieren, was sich für ausgelieferte Produkte und für Ersatzteile ändert.
A24	Die erste jährliche Überprüfung planen. Harmonisierte Normen können die nächste Bewertung vereinfachen, sobald die ersten zitiert sind.

Der Normungsauftrag sieht die harmonisierten CRA-Normen für Router, Modems, Switches und Firewalls zum 30. Oktober 2026 vor.[147] Die Veröffentlichung ihrer Fundstellen im Amtsblatt folgt erst danach. Ein Plan für 2027 kann deshalb nicht mit ihnen rechnen. Schweizer Hersteller folgen demselben Plan und benennen im ersten Quartal zusätzlich einen Wirtschaftsakteur in der EU.

8.5 Förderung der CRA-Umsetzung

Es gibt weder in Deutschland noch in Österreich oder der Schweiz einen nationalen Zuschuss für die CRA-Umsetzung (Anhang E). Die beiden offenen Ausschreibungen, die den CRA ausdrücklich nennen, sind europäisch. SECURE fördert KMU mit bis zu 30.000 € bei einer Förderquote von 50 %,[353] und ein Ausschreibungsthema im Programm Digitales Europa fördert die Umsetzung der EU-Rechtsakte zur Cybersicherheit.[280]

2026 ist das Angebot weiter geschrumpft. Das ZIM nimmt seit dem 7. Juli 2026 keine neuen Anträge mehr an,[387] KMU.DIGITAL wird 2027 nicht fortgeführt,[414] und in Baden-Württemberg, Niedersachsen und Thüringen endeten die Digitalisierungszuschüsse der Länder.[250, 282, 386] Die Nachfolger des KfW ERP-Digitalisierungs- und Innovationskredits zahlen einen Zuschuss von 3 oder 5 % erst ab Stufe 2.[235, 237]

Nur wenige Programme haben noch eine Antragsfrist mit festem Datum. MID-Digitale Prozesse öffnete am 19. Oktober 2026.[294] SECURE schließt am 11. Dezember 2026,[353] die Ausschreibung 2026 des FFG-Basisprogramms am 31. Dezember 2026,[313] KIRAS am 26. Februar 2027[317] und der Digitalbonus.Bayern Ende 2027.[29] Die übrigen Programme sind geschlossen oder laufen ohne Frist. Ein Hersteller kann etwa den ERP-Förderzuschuss der KfW jederzeit zusammen mit dem Kredit über seine Hausbank beantragen,[237, 238] und auch L-Bank, aws erp-Kredit, Innosuisse und die steuerliche Förderung kennen keine Frist.

Ein deutscher Hersteller finanziert die CRA-Umsetzung deshalb realistischerweise über einen KfW-Kredit der Stufe 2 oder 3 mit Zuschuss und über die Forschungszulage, deren Bemessungsgrundlage auf 12 Mio. € im Jahr gestiegen ist.[35, 62] Ein österreichischer Hersteller nutzt das FFG-Basisprogramm und die Forschungsprämie, ein Schweizer ein Innosuisse-Projekt mit Forschungspartner.

8.6 Fünf Leitfragen

Fünf Fragen zeigen, ob ein Unternehmen bereit ist. Jede sollte sich mit Ja beantworten lassen.

1. Erreicht eine Frühwarnung zu einer ausgenutzten Schwachstelle heute innerhalb eines Tages die ENISA, auch für ein Produkt, das vor Jahren verkauft wurde?
2. Könnten Sie die CRA-Klasse jedes Gateways und jedes anderen Grenzfalls heute gegenüber einer Marktüberwachungsbehörde begründen?
3. Ist in jedem Produkt, das Sie 2027 auf den Markt bringen, die Sicherheit in Hardware verankert, vom Bootvorgang bis zur Geräteidentität?
4. Wickelt ein einziges Backend die Updates, Zertifikate und Schwachstellenmeldungen aller Ihrer Produktlinien ab?
5. Funktioniert jeder Tracker und jedes Gateway, das Sie 2027 verkaufen, auch nach der 2G-Abschaltung, und kann der Nutzer die Batterie wechseln, wo keine Ausnahme greift?

Ein Nein bei der ersten Frage bedeutet, dass eine geltende Pflicht nicht erfüllt ist. Ein Nein bei einer der übrigen Fragen bedeutet ein Kosten- oder Marktrisiko für die Produkte des Jahrgangs 2027.

KURZ GESAGT

Die Fristen bestimmen die Reihenfolge der Arbeit, nicht der Stand der Normen. Ein Hersteller, der auf die Veröffentlichung harmonisierter Normen im Amtsblatt wartet, beginnt die Konformitätsbewertung zu spät für seine Produkte des Jahres 2027. Er finanziert die Umsetzung im Wesentlichen aus eigenen Mitteln. Kredite und steuerliche Forschungsförderung entlasten ihn nur geringfügig.

Anhang

A Methodik

Alle Zahlen des Berichts beruhen auf veröffentlichten Quellen oder auf ausdrücklich gekennzeichneten Annahmen. Eigene Umfragen und verhandelte Preise fließen nicht ein. Unser Kostenmodell und unsere Schätzung der Zahl der Hersteller vernetzter Produkte (Kapitel 1.5) beruhen zum Teil auf Annahmen.

A.1 Quellen

Die Quellen lassen sich sechs Arten zuordnen:

- **Rechtstexte.** Fristen und Pflichten stammen aus den Rechtstexten in ihrer berichtigten Fassung, die Fristen aus den Artikeln zum Geltungsbeginn.[141, 167, 168, 169, 170, 171] Der Stand der harmonisierten Normen und der notifizierten Stellen ist dem Amtsblatt, der NANDO-Datenbank der Kommission und den Veröffentlichungen der europäischen Normungsorganisationen entnommen.
- **Amtliche Statistik.** Die Unternehmenszahlen stammen aus der deutschen Kostenstrukturerhebung 2023, der europäischen Strukturstatistik der Unternehmen für Österreich (2023) und der Schweizer Statistik der Unternehmensstruktur STATENT (2024).[56, 175, 367]
- **Umfragen.** Der Anteil der Unternehmen mit vernetzten Funktionen und die Angaben zum Umsetzungsstand stammen aus veröffentlichten Umfragen von Forschungsinstituten, Verbänden, Beratungsunternehmen und Anbietern unter jeweils 100 bis 1.003 Unternehmen.[36, 37, 190, 307, 330] Sie geben die Selbsteinschätzung der Unternehmen wieder.
- **Preise.** Alle Preise sind Listenpreise, die Anbieter und Distributoren derzeit veröffentlichen. Anbieter ohne veröffentlichten Preis nehmen wir nicht in unser Kostenmodell auf, und wir schätzen für sie auch keinen Preis.
- **Schätzungen der Konformitätskosten.** Die Kosten des CRA je Produkt und die Kosten der Prüfung durch Dritte stammen aus den Folgenabschätzungen und der Begleitstudie der Kommission.[140, 143, 144, 410]
- **Marktereignisse.** Angaben zu Übernahmen, Produkteinführungen und eingestellten Diensten stammen aus Mitteilungen der Unternehmen sowie aus der Wirtschafts- und Rechtspresse.

A.2 Messwerte und Annahmen

Wir berechnen die Kosten je Gerät mit einem eigenen Kostenmodell für die vier Archetypen (Anhang C). Als Annahmen gehen darin nur Funktechnik, Datenverkehr, Sicherheits-Hardware und Update-Dienst je Archetyp ein, jede andere Zahl des Modells ist ein Listenpreis mit Quelle.

Unsere Schätzung der Grundgesamtheit geht von den amtlich gezählten Unternehmen aus. Annahmen sind der Anteil der Unternehmen, die vernetzte Produkte bauen, die Aufteilung der deutschen Klasse 100-499 nach dem Verhältnis von 2017, die Größenstruktur für Österreich und die Schweiz und zwei beschäftigungsgewichtete Näherungen für die Schweiz.

A.3 Schätzung der Grundgesamtheit

Kein Statistikamt weist „Hersteller vernetzter Produkte“ aus. Wir schätzen die Zahl solcher Hersteller deshalb auf 1.750-3.440. Dafür multiplizieren wir amtliche Unternehmenszahlen nach Wirtschaftszweig und Größenklasse[56, 175, 367] mit einem unteren und einem oberen Anteil aus

Umfragen. Der Anteil vernetzter Hersteller beruht auf Umfragen, nicht auf Registern, und ist deshalb der unsicherste Schritt. In einer späteren Ausgabe wollen wir ihn durch Signale aus der RUBINLAKE-Plattform ersetzen.

A.3.1 Vorgehen in vier Schritten

Schritt 1: Wirtschaftszweige. Wir zählen Unternehmen in vier Positionen der WZ 2008 (Deutschland), der ÖNACE 2008 (Österreich) und der NOGA 2008 (Schweiz), die auf dieser Ebene mit der NACE Rev. 2 übereinstimmen: Abteilung 26 (Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse, darunter Mess-, Kontroll- und Navigationsinstrumente), Abteilung 27 (elektrische Ausrüstungen, darunter Motoren, Schaltgeräte, Installationsmaterial und Haushaltsgeräte), Abteilung 28 (Maschinenbau, darunter Elektrowerkzeuge, Wärmepumpen und Werkzeugmaschinen) sowie Gruppe 32.5 (medizinische und zahnmedizinische Apparate). Die Abteilungen 29 und 30 (Fahrzeugbau) lassen wir weg, weil Fahrzeuge mit EU-Typgenehmigung nicht unter den CRA fallen.[171] Die Gruppen 26.1 (Bauelemente und Leiterplatten) und 27.3 (Kabel und Installationsmaterial) behalten wir in der Basis, weil auch ihre Bauteile nach dem CRA Produkte mit digitalen Elementen sein können.[171]

Schritt 2: Größenklassen. Die deutsche Kostenstrukturerhebung (KSE) zählt rechtliche Einheiten mit 20 und mehr tätigen Personen in den Klassen 20-49, 50-99, 100-499, 500-999 sowie 1.000 und mehr.[367] Wir teilen die Klasse 100-499 nach dem Verhältnis der letzten KSE-Ausgabe, die beide Klassen getrennt auswies (Berichtsjahr 2017), in 100-249 und 250-499 auf. Damals hatten 73 % der Unternehmen mit 100-499 Beschäftigten in Abteilung 26 weniger als 250 Beschäftigte, je 71 % in den Abteilungen 27 und 28 und 74 % im gesamten Verarbeitenden Gewerbe.[366] Für Gruppe 32.5 verwenden wir den Wert des gesamten Verarbeitenden Gewerbes. Österreich und die Schweiz veröffentlichen nur die Klassen 50-249 sowie 250 und mehr.[56, 175] Wir übertragen die deutsche Struktur auf beide Länder. In den vier Wirtschaftszweigen haben 47 % der deutschen Unternehmen der Klasse 50-249 mindestens 100 Beschäftigte und 18 % der Unternehmen der Klasse 250+ mindestens 1.000.[367] Die Übertragung ist eine Annahme. Österreichische und Schweizer Unternehmen der Klasse 250+ sind im Schnitt kleiner. Unsere Werte für die Klasse 1.000+ beider Länder fallen daher eher zu hoch als zu niedrig aus.

Schritt 3: Länderanpassungen. Die Schweizer Abteilung 26 enthält die Uhrenindustrie (NOGA 26.52), auf die 47,7 % der 117.217 Beschäftigten der Abteilung entfallen.[55] Wir ziehen diesen Anteil von den Schweizer Zahlen der Abteilung 26 ab. Die Schweiz weist Gruppe 32.5 nicht nach Größenklassen aus. Wir gewichten Abteilung 32 deshalb mit dem Anteil von 66,8 % ihrer Beschäftigten, der auf Gruppe 32.5 entfällt.[55] Beides sind beschäftigungsgewichtete Näherungen.

Schritt 4: Anteil vernetzter Hersteller. Dieser Anteil bestimmt die Breite der Spanne. Wir rechnen mit einem unteren und einem oberen Anteil von Unternehmen, die vernetzte Produkte herstellen:

- **Untergrenze:** der Anteil der Betriebe, die 2018 IoT-Serviceplattformen für digitale Dienste nutzten oder bis 2021 nutzen wollten, laut der Erhebung Modernisierung der Produktion des Fraunhofer ISI 17 % plus 14 % bei 50-249 Beschäftigten und 37 % plus 15 % bei 250 und mehr.[190] Wir verwenden 31 % für die Klasse 100-249 und 52 % für die größeren Klassen. Die Zahl ist alt und misst die Nutzung von Plattformen, nicht Merkmale der Produkte. Wir setzen sie deshalb als Untergrenze an.
- **Obergrenze:** der Anteil der deutschen Industrieunternehmen ab 100 Beschäftigten, die IoT-Plattformen einsetzen (45 %) oder deren Einsatz planen (33 %), laut Bitkom 2026 (n = 555).[37] Daraus ergeben sich 78 %, die wir auf alle Klassen anwenden. Die Frage erfasst IoT-Plattformen in der Produktion ebenso wie im Produkt. Der Wert markiert daher die Obergrenze.

Jede Schätzung je Land und Größenklasse ergibt sich als Basiszahl mal Anteil. Die 277 deutschen rechtlichen Einheiten mit 1.000 und mehr Beschäftigten ergeben 144 Hersteller bei 52 % und 216 bei 78 %.[37, 190, 367]

Oberste Klasse. Keine amtliche Quelle trennt bei 5.000 Beschäftigten. Die oberste Klasse 1.000-4.999 enthält deshalb auch Unternehmen mit 5.000 und mehr Beschäftigten. Die Klasse 1.000+ der KSE umfasst in den vier Zweigen 277 deutsche rechtliche Einheiten mit 867.062 tätigen Personen, im Schnitt 3.130.[367] Die KSE zählt rechtliche Einheiten. Tochtergesellschaften großer Konzerne erscheinen deshalb einzeln, und die meisten von ihnen haben weniger als 5.000 Beschäftigte. Wir ziehen keine Klasse 5.000+ ab und überschätzen die oberste Klasse damit leicht.

A.3.2 Nach Land und Größenklasse

Auf Deutschland entfallen mehr als vier Fünftel der Grundgesamtheit, 3.692 der 4.410 Unternehmen der Basis und 1.465-2.879 der 1.750-3.440 geschätzten Hersteller vernetzter Produkte. Österreich kommt auf 132-248 Hersteller, die Schweiz auf 153-313 (Tabelle 19).

LAND	UNTERNEHMEN	100-249	250-999	1.000-4.999	GESAMT
Deutschland	in der Basis	2.170	1.245	277	*3.692*
	davon vernetzt	673-1.692	648-971	144-216	*1.465-2.879*
Österreich	in der Basis	155	133	30	*318*
	davon vernetzt	48-121	69-104	15-23	*132-248*
Schweiz	in der Basis	262	113	25	*400*
	davon vernetzt	81-205	59-88	13-20	*153-313*

Tabelle 19: **Grundgesamtheit und Spanne nach Land und Größenklasse**
Anmerkung: Größenklassen nach Beschäftigten, Basisjahr Deutschland und Österreich 2023, Schweiz 2024, Deutschland in rechtlichen Einheiten, Rundungsdifferenzen möglich. Quellen: [37, 56, 175, 190, 367].

Die 159 österreichischen Unternehmen mit 250 und mehr Beschäftigten in den Abteilungen 26 bis 28 beschäftigen 136.695 Personen.[175] Die Schweiz zählt 82 Unternehmen mit mehr als 249 Beschäftigten in Abteilung 26 (einschließlich Uhrenindustrie), 24 in Abteilung 27 und 58 in Abteilung 28.[56]

A.3.3 Nach Branche

Auf den Maschinenbau (WZ 28) entfallen mit 2.075 der 3.692 deutschen Hersteller ab 100 Beschäftigten mehr als die Hälfte, und er stellt Geräte von drei der vier Archetypen her.[367] Nur Deutschland veröffentlicht Größenklassen unterhalb der Abteilungsebene. Die Aufschlüsselung gilt daher nur für Deutschland (Tabelle 20).

WZ 2008	ERZEUGNISSE	100-499	500-999	1.000+	SUMME 100+	ZUGEORDNETE ARCHETYPEN
26	Elektronische und optische Erzeugnisse	533	64	52	649	Logistik-Tracker
26.5	davon Mess-, Kontroll-, Navigationsinstrumente	262	29	22	313	Maschine, Logistik-Tracker
27	Elektrische Ausrüstungen	568	94	58	720	Gebäudegerät
27.1	davon Motoren, Transformatoren, Schaltgeräte	238	29	25	292	Maschine, Gebäudegerät
27.5	davon Haushaltsgeräte	27	6	8	41	Gebäudegerät

WZ 2008	ERZEUGNISSE	100-499	500-999	1.000+	SUMME 100+	ZUGEORDNETE ARCHETYPEN
28	Maschinenbau	1.724	207	144	2.075	Akkuwerkzeug, Maschine, Gebäudegerät
28.1	davon nicht wirtschafts-zweigspezifische Maschi-nen (Pumpen, Armaturen, Antriebe, Hydraulik)	381	58	45	484	Maschine
28.2	davon sonstige nicht wirt-schaftszweigspezifische Maschinen	533	50	46	629	Akkuwerkzeug, Maschine, Gebäudegerät
28.24	davon handgeführte Werk-zeuge mit Motorantrieb	13	0	4	17	Akkuwerkzeug
28.25	davon Kälte- und Lufttech-nik, inkl. Wärmepumpen	108	g.	g.	g.	Gebäudegerät
28.4	davon Werkzeugmaschinen	192	27	12	231	Maschine
28.9	davon Maschinen für be-stimmte Wirtschaftszweige	558	64	32	654	Maschine
32.5	Medizinische und zahnme-dizinische Apparate	201	24	23	248	Maschine
	Summe	**3.026**	**389**	**277**	**3.692**	

Tabelle 20: **Deutsche Hersteller nach WZ-Gruppe, 2023**
Anmerkung: „g." kennzeichnet Felder, die aus Geheimhaltungsgründen gesperrt sind. Quelle: [367].

Akkuwerkzeug mit BLE-Tracker. WZ 28.24 ist eine kleine Klasse, die von großen Unternehmen geprägt ist. Sie umfasst 31 rechtliche Einheiten mit 20 und mehr Beschäftigten, und auf die vier mit 1.000 und mehr entfallen 11.841 der 16.054 tätigen Personen der Klasse.[367] Auch Unternehmen anderer Zweige verkaufen Akkuwerkzeuge mit Tracker, etwa aus der Herstellung von Metallerzeugnissen (Abteilung 25). Die Klasse bildet den Archetyp deshalb nicht vollständig ab.

Maschine mit Gateway. Allein Abteilung 28 zählt 2.075 rechtliche Einheiten mit 100 und mehr Beschäftigten und 1,10 Mio. tätige Personen in allen Einheiten ab 20 Beschäftigten.[367] Maschinenbauer weisen zudem den höchsten Anteil vernetzter Hersteller auf. Im Jahr 2018 nutzten 24 % von ihnen IoT-Serviceplattformen, weitere 20 % planten deren Einsatz.[190]

Gebäudegerät nach § 14a EnWG. Der Archetyp findet sich vor allem in 28.25 (395 rechtliche Einheiten mit 20 und mehr Beschäftigten, davon 108 mit 100-499), in 28.21 (Öfen und Brenner, 127) und in Abteilung 27.[367] Der Absatz von Wärmepumpen in Deutschland stieg 2025 um 55 % auf 299.000 Geräte und übertraf damit den Absatz von Gas-Brennwertkesseln (229.000).[81] Jede Wärmepumpe, die ein Netzbetreiber nach § 14a EnWG steuern kann, hat eine Kommunikationsschnittstelle und ist damit ein Produkt mit digitalen Elementen.[171]

Logistik-Tracker. Hersteller von Ausrüstung und Trackern verteilen sich auf die Abteilungen 26 und 27. Spezialisierte Tracker-Hersteller liegen oft unter der Schwelle von 100 Beschäftigten. Die großen Abnehmer von Trackern sind die Werkzeug- und Maschinenhersteller dieser Grundgesamtheit.

A.3.4 Abgleich mit den Verbänden

Die Verbände grenzen ihre Branchen anders ab als die amtliche Statistik. Ihre Zahlen bestätigen deshalb die Größenordnung der amtlichen Basis, nicht aber einzelne Tabellenfelder (Tabelle 21).

VERBAND	VERBANDSZAHL	AMTLICHE VERGLEICHSZAHL
VDMA (Deutschland, Maschinenbau)	6.459 Unternehmen, im Schnitt 178,9 Beschäftigte (2016); 6.653 Unternehmen, im Schnitt 182,8 (2018)	WZ 28: 5.688 rechtliche Einheiten ab 20 Beschäftigten, 1.102.436 tätige Personen, im Schnitt 194 (2023)
ZVEI (Deutschland, Elektro- und Digitalindustrie)	872.700 Beschäftigte Ende 2025; Umsatz 226,8 Mrd. € 2025	WZ 26 + 27: 858.294 tätige Personen in rechtlichen Einheiten ab 20 Beschäftigten (2023)
FEEI (Österreich, Elektro- und Elektronikindustrie)	71.932 Beschäftigte, Produktion 23,6 Mrd. € (2025)	ÖNACE 26 + 27: 86.938 Beschäftigte (2023)
FMTI (Österreich, Metalltechnische Industrie)	130.694 Beschäftigte (Dezember 2025), Produktion 47,0 Mrd. €	ÖNACE 28: 104.506 Beschäftigte (2023)
Swissmem (Schweiz, Tech-Industrie)	322.900 Beschäftigte im 4. Quartal 2025; Exporte 68,1 Mrd. CHF 2025	NOGA 26-28: 233.716 Beschäftigte (2024)
Swiss Medtech (Schweiz, Medizintechnik)	rund 1.400 Unternehmen, rund 72.000 Beschäftigte	NOGA 32.5: 1.472 institutionelle Einheiten, 19.990 Beschäftigte (2022)

Tabelle 21: **Verbandszahlen und amtliche Basis im Vergleich**
Quellen: [55, 56, 175, 181, 182, 367, 371, 378, 404, 405, 416].

VDMA. Die amtliche Zahl für 2023 liegt unter der Zählung des VDMA, doch die Reihen sind nicht vergleichbar. Die KSE erfasst nur rechtliche Einheiten mit 20 und mehr tätigen Personen, jeweils nach ihrem wirtschaftlichen Schwerpunkt eingeordnet.[367] Der VDMA kombiniert dagegen Daten von Destatis mit eigenen Erhebungen.[404] Er selbst vertritt rund 3.500 deutsche und europäische Mitgliedsunternehmen.[406] Unabhängig von der Abgrenzung haben rund 2.000 deutsche Maschinenbauer 100 und mehr Beschäftigte.[367]

ZVEI. Die amtlich erfasste Beschäftigung der Abteilungen 26 und 27 liegt in derselben Größenordnung wie die Zahl des ZVEI.[367] Die Elektro- und Digitalindustrie beschäftigte Ende 2025 1,9 % weniger Menschen als ein Jahr zuvor.[416] Der ZVEI erwartet für 2026 ein reales Produktionsplus von 2 %, bei einer Kapazitätsauslastung von 78 % gegenüber einem langjährigen Mittel von 83 %.[417]

FEEI, FMTI und Swissmem. Swissmem und der FMTI grenzen ihre Branchen weiter ab als die Wirtschaftszweige dieser Schätzung. Swissmem schließt die Metallverarbeitung ein, der FMTI die Metallwaren. Die Zahl des FEEI liegt unter der Summe der ÖNACE-Abteilungen 26 und 27, weil nicht jedes dort eingeordnete Unternehmen Mitglied des FEEI ist.[175, 181]

B Rechtsgrundlagen

Die acht Gerätefunktionen aus Kapitel 2 gehen jeweils auf einzelne Artikel oder Anhangsnummern aus bis zu vier Rechtsakten zurück (Tabelle 22).

GERÄTEFUNKTION	RECHTSAKT	FUNDSTELLE
Firmware-Integrität (Secure Boot)	CRA	Anh. I Teil I Nr. 2 lit. f, k
	RED (VO 2022/30)	Art. 3 Abs. 3 lit. d, Nachweis über EN 18031-1
	Maschinenverordnung	Anh. III 1.1.9
Update-Mechanismus und Unterstützungszeitraum	CRA	Anh. I Teil I Nr. 2 lit. c; Teil II Nr. 7, 8; Art. 13 Abs. 8, 9
	Maschinenverordnung	Anh. III 1.2.1 lit. f: Protokoll der Versionen sicherheitsrelevanter Software
Software-Stückliste (SBOM)	CRA	Anh. I Teil II Nr. 1
	Maschinenverordnung	Anh. III 1.1.9: Liste der sicherheitsrelevanten Software
Schwachstellenmanagement und Meldung	CRA	Anh. I Teil II Nr. 2-6; Art. 14
Authentifizierung, keine leeren Passwörter	CRA	Anh. I Teil I Nr. 2 lit. b, d
	RED (VO 2022/30)	Einschränkung der EN 18031 zu Abschnitt 6.2.5.1/6.2.5.2
	Data Act	„Sicherer" Zugang (Art. 3 Abs. 1)
	Maschinenverordnung	Anh. III 1.1.9
Datenexport-Schnittstelle	CRA	Anh. I Teil I Nr. 2 lit. m: sichere Übertragung
	Data Act	Art. 3 Abs. 1, 3 Abs. 2, 4, 5
	Batterieverordnung	Art. 77: Daten des Batteriepasses
Protokollierung von Eingriffen und Zugriffen	CRA	Anh. I Teil I Nr. 2 lit. d, l
	Maschinenverordnung	Anh. III 1.1.9; 1.2.1 lit. f: Eingriffsprotokoll, fünf Jahre aufzubewahren
Produktidentifikation	CRA	Anh. II Nr. 3, 7
	Data Act	Art. 3 Abs. 2
	Maschinenverordnung	Anh. III 1.1.9
	Batterieverordnung	Art. 13 Abs. 6: QR-Code

Tabelle 22: **Rechtsgrundlage je Gerätefunktion**
Quellen: [141, 148, 168, 169, 170, 171].

C Kostenmodell

Für die Kosten je Gerät in Kapitel 3 haben wir ein eigenes Kostenmodell aufgebaut. Es rechnet ausschließlich mit den bei Veröffentlichung gültigen öffentlichen Listenpreisen und mit wenigen Annahmen.

C.1 Modellannahmen

Funktechnik, Datenverkehr, Sicherheits-Hardware und Update-Dienst je Archetyp haben wir festgelegt, nicht gemessen (Tabelle 23). Im Basisfall rechnen wir mit 10.000 Einheiten über 60 Monate. USD- und CHF-Preise rechnen wir zu den EZB-Referenzkursen vom 15. Oktober 2026 um, 1 € = 1,1208 USD = 0,9305 CHF.[137] Die Preise verstehen sich ohne Mehrwertsteuer, soweit der Anbieter dies ausweist. Die meisten B2B-Preislisten weisen es nicht aus.

Für Bauteile setzen wir die höchste Mengenstaffel an, die DigiKey veröffentlicht (500 bis 5.000 Stück), keinen verhandelten Preis für 10.000 Stück. Vertragspreise für eine Bestellung dieser Größe liegen in der Regel darunter. Die Hardware-Positionen sind deshalb eine Obergrenze. Wir zinsen nicht ab, rechnen ohne Inflation, erfassen Personalaufwand nur über die Schätzungen der Kommission je Produkt und setzen die Kosten des Data Act je Unternehmen an, nicht je Gerät.

ARCHETYP	FUNK UND WEG IN DIE CLOUD	DATENVERKEHR JE GERÄT	SICHERHEITS-HARDWARE	UPDATE-DIENST
Akkuwerkzeug mit BLE-Tracker	BLE-SoC, weitergeleitet über die App des Nutzers oder ein Baustellen-Gateway	20 Nachrichten am Tag, 60 Minuten am Tag verbunden	ATECC608B Trust&GO, vorprovisioniert	Golioth
Maschine mit Gateway	LTE Cat-1, IoT-SIM mit 100 MB im Monat	eine Nachricht alle 10 s, dauerhaft verbunden	TPM 2.0 SLB9672	AWS IoT Device Management, 12 Jobs im Jahr
Gebäudegerät nach § 14a EnWG	WLAN über das Netz des Kunden	eine Nachricht je Minute, dauerhaft verbunden	SE050	Golioth
Logistik-Tracker für Assets, Container und Anhänger	LTE-M/NB-IoT mit GNSS, Energiesparmodus	24 Nachrichten am Tag, 30 Cloud-Ortungen im Monat	STSAFE-A110	Golioth

Tabelle 23: **Modellannahmen je Archetyp**
Anmerkung: Nachrichten von höchstens 5 KB. Quelle: RUBINLAKE-Kostenmodell.

C.2 Erhobene Listenpreise

Mobilfunktarife streuen stärker als jede andere Eingangsgröße, von 10 € je SIM für zehn Jahre bei o2 bis 2,07 € je SIM und Monat bei der Telekom.[97, 381]

Connectivity-Tarife. Die IoT-Tarife in der DACH-Region folgen drei Preismodellen:

- **Einmalpakete für die Lebensdauer des Geräts.** 1NCE IoT Lifetime Flat: 12 € je SIM für 500 MB und 250 SMS über zehn Jahre. Eine gleich große Aufladung kostet ebenfalls 12 € netto.[3] o2 Business Easy IoT (Telefónica): 10 € netto je SIM für zehn Jahre mit 750 MB (Welt), 1.000 MB (Europa) oder 1.500 MB (Deutschland), ohne Mindestbestellmenge, nur für Geschäftskunden mit Sitz in Deutschland.[381] Telekom IoT Business LPWA: einmalig 14,50 € je SIM für zehn Jahre mit

6,5 MB im Monat in Europa über NB-IoT und LTE-M.[96] Magenta (Österreich): IoT Tarif 5 zu 9,99 € für 60 Monate (6,5 MB) und IoT Tarif 10 zu 18,99 € für 120 Monate (8,33 MB), mindestens 10 SIM-Karten.[256]

- **Monatsgebühren je SIM.** Telekom IoT Business Classic: 2,07 € im Monat je SIM mit 100 MB, mindestens 10 SIM-Karten und 12 Monate Laufzeit.[97] Die Tariffamilie beginnt bei 1,43 €.[96] Swisscom CMP Mobile Lite: ab 1,00 CHF je SIM, 69 CHF Aktivierung, ohne Roaming.[376] Sunrise IoT Starter Services zur Einführung im Juni 2022: 1,50 bis 9,00 CHF je SIM und Monat für 2 MB bis 5 GB, dazu einmalig 205 CHF, Mindestlaufzeit 12 Monate.[370]
- **Nutzungsabhängige Preise.** Onomondo: Daten ab 0,0025 € je MB, Grundgebühren auf Anfrage.[310]

LPWAN und Satellit.

- **The Things Stack Cloud:** Standard-Plan 190 € im Monat mit einer Lizenz für 1.000 Endgeräte, also 0,19 € je Gerät. Der Plan umfasst nur den Netzwerkserver, ohne Gateways und Roaming.[385]
- **Swisscom LPN:** LoRaWAN-Connectivity zu 1,00 CHF je Gerät im Lite-Plan oder ab 0,45 CHF im Smart-Plan mit 49 CHF Plattformgebühr im Monat.[376]
- **Myriota:** Satellitentarife ab 0,99 USD je Gerät und Monat.[274]

Cloud. AWS IoT Core in Frankfurt:[15]

- 0,096 USD je Million Verbindungsminuten
- 1,20 USD je Million Nachrichten für die erste Milliarde im Monat, abgerechnet in 5-KB-Schritten
- 0,18 USD je Million ausgelöster Regeln und noch einmal so viel je Million Aktionen
- 1,50 USD je Million Shadow- und Registry-Operationen
- 0,001 USD je Ortung

Azure IoT Hub, je Einheit und Monat, in den kostenpflichtigen Stufen in 4-KB-Blöcken abgerechnet:[266]

- S1: 25 USD für 400.000 Nachrichten am Tag
- S2: 250 USD für 6 Mio. Nachrichten am Tag
- S3: 2.500 USD für 300 Mio. Nachrichten am Tag

Bei 8.640 Nachrichten je Maschine und Tag passen 10.000 Maschinen in eine S3-Einheit. Das sind 0,25 USD je Gerät und Monat gegenüber 0,41 USD bei AWS.[15, 266] Für die anderen drei Archetypen kosten beide Clouds weniger als 0,07 € im Monat.

Gerätemanagement und OTA.

- **Golioth:** 0,25 USD je aktivem Gerät und Monat, ohne Plattformstufen.[199]
- **AWS IoT Device Management:** 0,003 USD je Remote-Aktion (Job), 2,25 USD je Million Index-Updates, 1,00 USD je Secure Tunnel.[16]
- **Azure Device Update:** 0,07 USD je Gerät und Monat plus 70 USD je Instanz.[266]
- **nRF Cloud:** ab 0,10 USD je Gerät und Monat.[285]
- **balena:** Production-Plan 1.439 USD im Monat für 110 Geräte plus 2 USD je weiterem Gerät.[28]
- **Mender:** 291 USD im Monat für bis zu 250 Geräte, Flotten über 2.000 Geräte auf Anfrage.[292]
- **Memfault:** ab 3.495 USD im Monat für 1.000 monatlich aktive Geräte.[260]

PKI und SBOM. AWS Private CA:[19]

- 400 USD je Zertifizierungsstelle und Monat im General-Purpose-Modus oder 50 USD im Modus für kurzlebige Zertifikate
- Zertifikate zu je 0,75 USD für die ersten 1.000, 0,35 USD bis 10.000 und 0,001 USD darüber

Wir setzen ein vorprovisioniertes Trust&GO-Bauteil anstelle eines Provisionierungsdienstes in der Fertigung an, wo ein solches Bauteil im Handel ist. OWASP Dependency-Track ist kostenlos.[321] FOSSA Business kostet 20 USD je Projekt und Monat, der Beispielplan des Anbieters 207 USD im Monat.[189] Snyk Team beginnt bei 25 USD im Monat.[363]

C.3 Positionen je Archetyp

Der Mobilfunktarif der Maschine ist mit 2,07 € je Gerät und Monat die größte Einzelposition aller Archetypen.[97] Die Monatswerte setzen sich aus den laufenden Gebühren und jeder Einmalposition geteilt durch 60 zusammen.

Beim Akkuwerkzeug macht der Aufschlag fast die gesamten Kosten aus (Tabelle 24).

POSITION	KATEGORIE	EINMALIG JE GERÄT (€)	MONATLICH JE GERÄT (€)
BLE-SoC nRF54L15, 2,40 USD bei 3.000[110]	Basis	2,14	0,036
Connectivity über App oder Baustellen-Gateway (Annahme)	Basis	0	0
AWS IoT Core: Nachrichten, Verbindung, Shadow[15]	Basis	0	0,001
ATECC608B Trust&GO, 1,91 USD bei 100[108]	Aufschlag	1,70	0,028
Gerätezertifikat und CA-Anteil[19]	Aufschlag	0,35	0,041
Signierte OTA-Updates, Golioth[199]	Aufschlag	0	0,223
CRA-Konformität je Produkt (Tabelle 28)	Aufschlag	7,37	0,175
Basiskosten			**0,037**
Sicherheitsaufschlag			**0,468**

Tabelle 24: **Kostenpositionen des Akkuwerkzeugs**
Anmerkung: Rundungsdifferenzen möglich. Quelle: RUBINLAKE-Kostenmodell.

Bei der Maschine macht der Mobilfunktarif zwei Drittel der Kosten aus (Tabelle 25).

POSITION	KATEGORIE	EINMALIG JE GERÄT (€)	MONATLICH JE GERÄT (€)
LTE Cat-1 Quectel EG915U, 17,61 USD bei 500[113]	Basis	15,71	0,262
Telekom IoT Business Classic, 100 MB[97]	Basis	0	2,070
AWS IoT Core: 259.200 Nachrichten im Monat, Regeln, Shadow[15]	Basis	0	0,366
TPM 2.0 SLB9672, 2,19 USD bei 5.000[107]	Aufschlag	1,95	0,032
Gerätezertifikat und CA-Anteil[19]	Aufschlag	0,35	0,041
Signierte OTA-Updates, Jobs, Flottenindex, Tunnel[16]	Aufschlag	0	0,153
CRA-Konformität je Produkt (Tabelle 28)	Aufschlag	7,37	0,175
Basiskosten			**2,698**
Sicherheitsaufschlag			**0,401**

Tabelle 25: **Kostenpositionen der Maschine**
Anmerkung: Rundungsdifferenzen möglich. Quelle: RUBINLAKE-Kostenmodell.

Beim Gebäudegerät sind die signierten OTA-Updates der größte Posten (Tabelle 26).

POSITION	KATEGORIE	EINMALIG JE GERÄT (€)	MONATLICH JE GERÄT (€)
WLAN-6/BLE-Modul ESP32-C6-WROOM-1, 3,13 USD bei 650[106]	Basis	2,79	0,047
Connectivity über das Netz des Kunden (Annahme)	Basis	0	0
AWS IoT Core: 43.200 Nachrichten im Monat, Regeln, Shadow[15]	Basis	0	0,064
Secure Element SE050C2, 2,87 USD bei 3.000[112]	Aufschlag	2,56	0,043
Gerätezertifikat und CA-Anteil[19]	Aufschlag	0,35	0,041
Signierte OTA-Updates, Golioth[199]	Aufschlag	0	0,223
CRA-Konformität je Produkt (Tabelle 28)	Aufschlag	7,37	0,175
Basiskosten			**0,111**
Sicherheitsaufschlag			**0,482**

Tabelle 26: **Kostenpositionen des Gebäudegeräts**
Anmerkung: Rundungsdifferenzen möglich. Quelle: RUBINLAKE-Kostenmodell.

Beim Logistik-Tracker machen Funkchip und SIM die Hälfte der Kosten aus (Tabelle 27).

POSITION	KATEGORIE	EINMALIG JE GERÄT (€)	MONATLICH JE GERÄT (€)
LTE-M/NB-IoT und GNSS nRF9151, 17,46 USD bei 500[111]	Basis	15,58	0,260
1NCE Lifetime Flat (12 €) und Chip-SIM (2,50 €)[3]	Basis	14,50	0,242
AWS IoT Core und 30 Ortungen im Monat[15]	Basis	0	0,028
Secure Element STSAFE-A110, 1,27 USD bei 5.000[114]	Aufschlag	1,13	0,019
Gerätezertifikat und CA-Anteil[19]	Aufschlag	0,35	0,041
Signierte OTA-Updates, Golioth[199]	Aufschlag	0	0,223
CRA-Konformität je Produkt (Tabelle 28)	Aufschlag	7,37	0,175
Basiskosten			**0,529**
Sicherheitsaufschlag			**0,458**

Tabelle 27: **Kostenpositionen des Logistik-Trackers**
Anmerkung: Rundungsdifferenzen möglich. Quelle: RUBINLAKE-Kostenmodell.

Der Tracker verbraucht etwa 1 MB im Monat. Das 1NCE-Paket erlaubt über fünf Jahre 8,3 MB im Monat und reicht damit für die ganze Lebensdauer.[3] Akkuwerkzeug und Gebäudegerät haben keine SIM. Ihre Basiskosten bestehen aus Funkchip und Cloud-Verkehr.

C.4 Konformitätskosten je Produkt

Die CRA-Konformität kostet in unserem Modell 104.781 € je Produkt über fünf Jahre, für alle vier Archetypen gleich (Tabelle 28). Wir übernehmen die Schätzungen der Kommission je Produkt für den CRA vollständig.[144] Für sichere Entwicklung setzen wir den zentralen Schätzwert der Kommission von 30,5 % an, aus einer Spanne von 19 bis 42 % in ihrem Modell.[144] Die Kommission beziffert die wiederkehrenden Prüfungen auf 3.000 bis 5.000 € je Produkt, ohne einen Zeitraum zu nennen. Wir setzen den Mittelwert von 4.000 € als jährliche Kosten an.[144] Für die Werkzeuge rechnen wir mit einem FOSSA-Business-Abonnement, das eine einzige Produktlinie bezahlt.[189]

KOSTENPOSITION	JE PRODUKT (€)	JE GERÄT UND MONAT (€)
Sichere Entwicklung (+30,5 % von 140.000 €)	42.700	0,071
Dokumentation, Konformitätserklärung, CE-Kennzeichnung, Meldungen	12.600	0,021
Konformitätsbewertung (Selbstbewertung)	18.400	0,031
Wiederkehrende Prüfungen, 4.000 € im Jahr über 5 Jahre (Annahme)	20.000	0,033
Werkzeuge für SBOM und Schwachstellenmanagement, 207 USD im Monat über 5 Jahre	11.081	0,018
Summe	**104.781**	**0,175**

Tabelle 28: **Kosten der CRA-Konformität je Produkt**
Anmerkung: Rundungsdifferenzen möglich. Quellen: RUBINLAKE-Kostenmodell; [144, 189].

C.5 Gebühren für die Konformitätsbewertung

Notifizierte Stellen veröffentlichen ihre Gebühren selten. Das einzige öffentliche Angebot ist eine EU-Baumusterprüfung durch LCIE (notifizierte Stelle 0081), die Serma Safety & Security ab 3.900 € anbietet.[359] Es liegt unter jeder Schätzung der Kommission für eine Bewertung durch Dritte[140, 144, 410] (Tabelle 29).

ANBIETER ODER SCHÄTZUNG	LEISTUNG ODER PRODUKTART	ART DER ANGABE	BETRAG (€)
Serma Safety & Security[359]	EU-Baumusterprüfung durch LCIE	veröffentlichtes Angebot, ab	3.900
Serma Safety & Security[359]	Gap-Analyse gegen EN 18031 oder ETSI EN 303 645	veröffentlichtes Angebot, ab	3.750
Serma Safety & Security[359]	Gap-Analyse mit Penetrationstest	veröffentlichtes Angebot, ab	13.500
RED-Folgenabschätzung[140]	Prüfung durch Dritte, einfache Produkte	Schätzung je Modell	5.000-15.000
RED-Folgenabschätzung[140]	Prüfung durch Dritte, komplexe Produkte	Schätzung je Modell	20.000-30.000
RED-Folgenabschätzung[140]	Prüfung durch Dritte, stark softwareabhängige Geräte	Schätzung je Modell	50.000+
CRA-Begleitstudie, 2021[410]	Bewertung durch Dritte	Schätzung	15.000-50.000
CRA-Folgenabschätzung[144]	Selbstbewertung (Basisfall unseres Modells)	Schätzung	18.400
CRA-Folgenabschätzung[144]	Bewertung durch Dritte (Sensitivitätsfall unseres Modells)	Schätzung	25.000

Tabelle 29: **Gebühren für die Konformitätsbewertung**

Je verkaufter Einheit beziffert die Kommission die Prüfung durch Dritte nach der RED auf 3 bis 13 € bei einem vernetzten Rasenmäher und 0,35 € bei einem Router.[140] Bewertungen durch Dritte zu 25.000 € und 50.000 € erhöhen den Aufschlag um 0,01 € beziehungsweise 0,05 € je Gerät und Monat (Tabelle 30).

C.6 Sensitivität

Die Flottengröße verändert den Aufschlag stärker als jede andere Eingangsgröße. Der Weg der Konformitätsbewertung verschiebt ihn nur um Cent. Die Funktechnik lässt ihn unverändert und wirkt allein auf die Basiskosten (Tabelle 30).

FALL (€ JE GERÄT UND MONAT)	AKKUWERKZEUG	MASCHINE	GEBÄUDEGERÄT	LOGISTIK-TRACKER
Aufschlag, 10.000 Einheiten (Basisfall)	0,47	0,40	0,48	0,46
Aufschlag, 1.000 Einheiten	2,37	2,30	2,38	2,36
Aufschlag, 100.000 Einheiten	0,27	0,21	0,29	0,26
Aufschlag, Bewertung durch Dritte zu 25.000 €[144]	0,48	0,41	0,49	0,47
Aufschlag, Bewertung durch Dritte zu 50.000 €[140]	0,52	0,45	0,53	0,51
Aufschlag, Hälfte der sicheren Entwicklung schon vorhanden[144]	0,43	0,37	0,45	0,42
Basiskosten, Basisfall	0,04	2,70	0,11	0,53
Basiskosten, Swisscom CMP Mobile Lite statt Telekom[376]	entfällt	1,70	entfällt	entfällt
Basiskosten, nRF9151 und Telekom LPWA statt WLAN[96]	entfällt	entfällt	0,57	entfällt
Basiskosten, LoRaWAN über The Things Stack statt LTE-M[109, 115, 385]	entfällt	entfällt	entfällt	0,52
Basiskosten, Myriota-Tarif zusätzlich zu LTE-M, ohne Modem[274]	entfällt	entfällt	entfällt	1,41

Tabelle 30: Sensitivität von Aufschlag und Basiskosten
Quelle: RUBINLAKE-Kostenmodell.

Der Swisscom-Fall lässt die Aktivierungsgebühr von 69 CHF außen vor und enthält kein Roaming.[376] Im LoRaWAN-Fall setzen wir ein Murata-Modul Type 1SJ zu 11,11 USD und ein u-blox MAX-M10S zu 9,33 USD an, beide über DigiKey, dazu 0,19 € im Monat für den Netzwerkserver.[109, 115, 385]

D Anbieterverzeichnis

Wir bewerten und empfehlen keinen der Anbieter. Die Auswahl erhebt keinen Anspruch auf Vollständigkeit.

D.1 Benötigte Anbieter je Archetyp

Jeder Archetyp braucht nur einen Teil der Schichten und Anbietergruppen.

1. **Akkuwerkzeug mit BLE-Tracker.** Anbieter von BLE-SoC und Secure Element (Tabelle 33), ein OTA-Dienst für Mikrocontroller (Tabelle 31), SBOM-Werkzeuge für Binär- oder Quellcode des Funkstacks (Tabelle 32) und eine nach der RED notifizierte Stelle für EN 18031 (Tabelle 38). Eine SIM ist nicht nötig.
2. **Maschine mit Gateway.** TPM- und PKI-Anbieter, ein Linux-OTA-Dienst, eine IoT-Plattform oder Cloud (Tabelle 35), ein Mobilfunkanbieter (Tabelle 34) und eine nach dem CRA notifizierte Stelle (Tabelle 38), falls das Gateway nach dem CRA in Klasse I fällt.
3. **Gebäudegerät nach § 14a EnWG.** Secure Element, OTA über WLAN oder Ethernet, SBOM-Werkzeuge und eine nach der RED notifizierte Stelle. Für das Smart-Meter-Gateway gelten eigene Vorgaben.
4. **Logistik-Tracker für Assets, Container und Anhänger.** Lieferanten für Mobilfunkmodule und GNSS (Tabelle 36), ein MVNO mit eSIM nach SGP.32 (Tabelle 34), OTA für Mikrocontroller und eine nach der RED notifizierte Stelle.

D.2 Gerätemanagement und OTA

Für Gerätemanagement und OTA reicht die Auswahl vom Open-Source-Projekt Eclipse hawkBit bis zu den Diensten von AWS und Microsoft (Tabelle 31). Kontron bewirbt KontronOS als konform mit CRA, EN 18031 und NIS-2 und stellt viermal im Jahr Delta-Updates bereit.[241]

ANBIETER (PRODUKT)	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
Northern.tech (Mender)	Rechtsträger in Oslo; Büros in Palo Alto, Oslo, Shanghai	Gegründet 2008; Kunden in über 70 Ländern	NVIDIA-Jetson-Integration (Aug. 2024); MCU-Unterstützung (Mai 2026); Tochtergesellschaft in Shanghai (2025)
Memfault	San Francisco	Series B 24 Mio. US-Dollar (Jan. 2023, angeführt von Stripes)	Von Nordic Semiconductor übernommen (24. Juni 2025); Kaufpreis nicht genannt
Golioth	San Francisco	Pre-Seed und Seed zusammen 7,1 Mio. US-Dollar (bis Mai 2023)	Seit dem 3. März 2026 Teil von Canonical
balena	Dezentral organisiert, ohne Hauptsitz	-	-
AWS IoT Device Management	Seattle	Teil von Amazon Web Services	IoT Analytics, IoT Events und FleetWise eingestellt oder für Neukunden geschlossen (2024-2026)

ANBIETER (PRODUKT)	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
Azure Device Update for IoT Hub	Redmond	Teil von Microsoft	Allgemein verfügbar; Updates über Azure Device Registry als Vorschau (2026)
Bosch IoT Rollouts / Eclipse hawkBit	Bosch Global Software Technologies; Eclipse Foundation	Open Source, EPL-2.0	hawkBit 1.0.0 (30. März 2026), 1.1.0 (3. Juli 2026)
Kontron (KontronOS, susietec)	Linz, Österreich	Rund 7.000 Beschäftigte; Umsatz 2025 1.607,3 Mio. €	Ennoconn hält nach einem Pflichtangebot zu 23,50 € je Aktie 48,36 % (Aug. 2026)
emteria	Aachen	-	Partnerprogramm u. a. mit Raspberry Pi, PHYTEC, Intel
querdenker engineering (qdCloud)	Offenburg	-	OTA, SBOM je Firmware-Version und Schwachstellenverfolgung in einem Produkt

Tabelle 31: **Anbieter für Gerätemanagement und OTA**
Quellen: [14, 17, 18, 28, 44, 119, 131, 197, 198, 241, 242, 243, 259, 267, 286, 289, 290, 291, 332].

Zu Menders Kunden gehören Siemens, Volkswagen und die ZF Group.[291]

D.3 SBOM, Schwachstellenmanagement und PSIRT

Für SBOM, Firmware-Analyse und Schwachstellenmanagement reicht die Auswahl vom Open-Source-Projekt OWASP Dependency-Track bis zu Exein (Tabelle 32). Synopsys verkaufte Black Duck zum 1. Oktober 2024 an Clearlake Capital und Francisco Partners, Finite State übernahm MergeBase, und FOSSA übernahm StackShare und EdgeBit.[38, 184, 187, 188]

ANBIETER	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
ONEKEY	Düsseldorf	Ausgründung von SEC Consult (2020, als IoT Inspector); im Beteiligungsportfolio von PwC Deutschland	Gemeinsame Lösung mit ETAS/ESCRYPT CycurRISK (Mai 2024)
Cybellum	Tel Aviv; Büros in Frankfurt, Peking, Tokio, Taipeh	LG Electronics übernahm rund 64 % (Sept. 2021, Bewertung 140 Mio. US-Dollar)	-
Finite State	Columbus, Ohio	Wachstumsrunde von 20 Mio. US-Dollar, angeführt von Energy Impact Partners (März 2024)	Übernahme von MergeBase (Juni 2024)
Black Duck	Burlington, Massachusetts	Eigentümer Clearlake Capital und Francisco Partners; seit dem 1. Okt. 2024 unabhängig von Synopsys	STMicroelectronics nutzt Black Duck SCA zur SBOM-Erzeugung (März 2025)

ANBIETER	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
FOSSA	-	Series B 23,2 Mio. US-Dollar (2020)	Übernahme von StackShare (Aug. 2024) und EdgeBit (Sept. 2025)
Exein	Rom; Büros in Karlsruhe, San Francisco, Taipeh	70 Mio. € (Juli 2025), 100 Mio. € (Dez. 2025), 270 Mio. US-Dollar bei einer Bewertung von 1,7 Mrd. US-Dollar (Sept. 2026)	Partnerschaft mit der Deutschen Telekom IoT (Sept. 2026)
Cybeats	Toronto (an der CSE notiert)	Kleinere Platzierungen 2025-2026	OEM-Vertrag: Keysight vertreibt die Plattform als Keysight SBOM Manager (Feb. 2026)
NetRise	-	Series A 10 Mio. US-Dollar (2025)	Von Dragos übernommen (Sept. 2026)
OWASP Dependency-Track	Open Source	OWASP-Flagship-Projekt, Apache 2.0	Von über 20.000 Organisationen genutzt

Tabelle 32: **Anbieter für SBOM und Schwachstellenmanagement**
Quellen: [38, 39, 40, 89, 90, 91, 118, 177, 178, 179, 180, 184, 185, 187, 188, 252, 304, 305, 306, 308, 321].

Im vierköpfigen Board von Cybellum sitzen die beiden Gründer und zwei Führungskräfte von LG Electronics.[90] PwC Deutschland stieg im Dezember 2023 als Minderheitsgesellschafter bei ONEKEY ein, an dem eCAPITAL bereits beteiligt war, und nannte keinen Betrag.[101] JFrog übernahm 2021 Vdoo, das seitdem kein eigenständiger Anbieter mehr ist.[230]

D.4 Secure Element und PKI

Die Hersteller von Secure Elements sind die größten Unternehmen im Verzeichnis (Tabelle 33). Infineon meldete für das Geschäftsjahr bis zum 30. September 2025 einen Umsatz von 14.662 Mio. €, NXP für das Jahr 2025 einen Umsatz von 12.269 Mio. US-Dollar.[219, 299]

ANBIETER	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
Infineon	Neubiberg	Umsatz GJ 2025 (bis 30. Sept. 2025) 14.662 Mio. €; 57.077 Beschäftigte	Übernahme des Automotive-Ethernet-Geschäfts von Marvell für 2,5 Mrd. US-Dollar in bar (Abschluss 14. Aug. 2025)
NXP	Eindhoven	Umsatz 2025 12.269 Mio. US-Dollar; rund 32.169 Beschäftigte	Übernahmen 2025: TTTech Auto (766 Mio. US-Dollar), Aviva Links (222 Mio.), Kinara (284 Mio.); MEMS-Sensorik an ST verkauft (Feb. 2026)
STMicroelectronics	Schiphol (NL), operative Zentrale in Genf	Umsatz 2025 11.800 Mio. US-Dollar	Übernahme der MEMS-Sensorik von NXP (2. Feb. 2026)
Microchip	Chandler, Arizona	Umsatz GJ 2026 (bis 31. März 2026) 4.713,1 Mio. US-Dollar; rund 17.900 Beschäftigte	-

ANBIETER	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
Giesecke+Devrient	München	Umsatz 2025 3.173 Mio. €; 14.561 Vollzeitäquivalente	eSIM und IoT-Connectivity im Geschäftsbereich Connectivity & IoT
Thales (Cyber & Digital)	Meudon, Frankreich	Segmentumsatz 2025 3.852 Mio. €, davon Digital Identity 2.397 Mio. €	SGP.32-eSIM für IoT mit AT&T (Okt. 2025)
achelos	Paderborn	Gegründet 2008; Größe und Gesellschafter nicht veröffentlicht	Partner u. a. Keyfactor, Sectigo, Thales
Kudelski Group (Kudelski IoT)	Cheseaux-sur-Lausanne, Schweiz	Umsatz 2025 371,0 Mio. US-Dollar, davon IoT 39,1 Mio.; rund 1.671 Beschäftigte	SKIDATA an ASSA ABLOY verkauft (340 Mio. € Unternehmenswert, Sept. 2024); Matter-Partnerschaft mit Silicon Labs (Okt. 2024)
Utimaco	Aachen und Campbell, Kalifornien	Über 400 Beschäftigte; Investor SGT Capital	Bereich Lawful Interception verkauft (Sept. 2025); Partnerschaft mit Keyfactor (März 2025)
Keyfactor	Atlanta und Stockholm	ARR über 200 Mio. US-Dollar (Sept. 2026)	Übernahme von InfoSec Global und CipherInsights (Mai 2025); Wachstumsinvestition über 1 Mrd. US-Dollar unter Führung von Summit Partners (Juli 2026)
DigiCert	Lehi, Utah	Nicht veröffentlicht	Übernahme von Vercara (Sept. 2024) und Valimail (Sept. 2025)
GlobalSign (GMO GlobalSign Holdings)	Tokio	Holding: 962 Vollzeitbeschäftigte; Umsatz 2025 20.670 Mio. Yen	-
Sectigo	Scottsdale, Arizona	Mehrheitseigner GI Partners	Übernahme des Geschäfts mit öffentlichen Zertifikaten von Entrust (Jan. 2025)
Bundesdruckerei (D-Trust)	Berlin	Umsatz 2024 1.111,9 Mio. €; rund 4.577 Beschäftigte; im Bundeseigentum	D-Trust-Zertifikate für die Delos Cloud (Mai 2025)
Swissbit	Bronschhofen, Schweiz	Über 500 Beschäftigte; eigenes Werk in Berlin	Post-Quanten-Authentisierung mit Intercede (Juni 2026)

Tabelle 33: Anbieter für Secure Element, HSM und PKI
Quellen: [9, 58, 103, 104, 191, 196, 219, 231, 233, 234, 244, 245, 246, 248, 257, 262, 299, 352, 369, 372, 383, 384, 399, 400, 401].

Das Segment Cyber & Digital von Thales schrumpfte 2025 um 4,3 %, der Umsatz mit Digital Identity um 2,5 %.[384] achelos wird von drei Geschäftsführern geleitet und veröffentlicht seine Gesellschafter nicht.[9] Kudelskis IoT-Segment wuchs im ersten Halbjahr 2026 um 5,1 % auf 20,3 Mio. US-Dollar.[247]

D.5 IoT-Connectivity

Nur die MVNOs und Vodafone veröffentlichen ihre IoT-Verbindungszahlen (Tabelle 34).

ANBIETER	SITZ	GRÖSSE, EIGENTÜMER UND FINANZIERUNG	ENTWICKLUNGEN 2024-2026
1NCE	Köln	Über 40 Mio. SIM-Verbindungen; über 280 Beschäftigte	Finanzierungsrunde von 60 Mio. US-Dollar (Apr. 2025), Deutsche Telekom unter den Investoren
emnify	Berlin	Über 23 Mio. Verbindungen; ARR über 50 Mio. €	Neuer CEO (Sept. 2026), CFO und CRO (Okt. 2026); SGP.32-eSIM (März 2026)
Onomondo	Kopenhagen	Über 500 Kunden	Aspirity Partners übernimmt die Mehrheit, Gesamtinvestition über 100 Mio. € (Sept. 2026)
Deutsche Telekom IoT	Bonn	LTE-M/NB-IoT-Abdeckung in Deutschland über 99 %; 600 Roaming- und Satellitenpartner	Satellitenpartner Skylo, Sateliot, OQ Technology
Vodafone IoT	Newbury, Großbritannien	244 Mio. IoT-Verbindungen im Konzern (GJ bis März 2026)	-
Telefónica Deutschland (o2 Business)	München	742.000 M2M-Nettozugänge 2025	-
Swisscom	Schweiz	Nicht veröffentlicht	LoRaWAN, NB-IoT und LTE-M auf einer Plattform
A1 Digital	Wien	Über 200 Beschäftigte	Managed IoT Connectivity

Tabelle 34: Anbieter für IoT-Connectivity
Quellen: [1, 4, 7, 98, 99, 127, 128, 129, 130, 309, 375, 380, 409].

1NCE wurde 2017 zusammen mit der Deutschen Telekom gegründet und nennt über 30.000 Kunden.[4] An der Finanzierungsrunde vom April 2025 beteiligten sich Deutsche Telekom, iSquared, Kensington, SoftBank Corp., Vicenda und der Gründer. Damit stieg die Gesamtfinanzierung auf rund 160 Mio. US-Dollar.[1] emnify nennt ein Wachstum von 30 %.[127, 130] In der Series B sammelte emnify im Januar 2022 bei One Peak 57 Mio. US-Dollar ein.[126]

Weder die Deutsche Telekom noch Swisscom weisen eine Zahl ihrer IoT-Verbindungen aus. Die Telekom zählte Ende 2025 in Deutschland 46,75 Mio. Prepaid-Kunden einschließlich M2M-Karten. Die Zahl wuchs um 11,3 %, vor allem durch M2M-SIM-Karten in der Automobilindustrie.[98] Swisscom nennt IoT als Wachstumsfeld, veröffentlicht aber keine Zahl.[374]

D.6 IoT-Plattformen

Drei der fünf Plattformen gehören Industriekonzernen, nämlich Siemens, Bosch und KUKA[44, 102, 361] (Tabelle 35).

PLATTFORM	EIGENTÜMER UND SITZ	GRÖSSE	ENTWICKLUNGEN 2024-2026
Cumulocity	Unabhängig, Düsseldorf	Über 1.000 Kundenunternehmen in 28 Ländern	Management-Buy-out aus der Software AG (Jan. 2025); im ersten Ma-

PLATTFORM	EIGENTÜMER UND SITZ	GRÖSSE	ENTWICKLUNGEN 2024-2026
			gic Quadrant von Gartner für industrielle AIoT-Plattformen als Visionary eingestuft (Sept. 2026)
ThingWorx und Kepware	TPG	Nicht veröffentlicht	Von PTC an TPG verkauft, Abschluss am 13. März 2026
Insights Hub (vormals MindSphere)	Siemens	Nicht veröffentlicht	Umbenannt
Bosch IoT Suite (Remote Manager, Rollouts, Insights, Edge)	Bosch	Nicht veröffentlicht	Release Notes bis Aug. 2026; keine Abkündigung
Device Insight	KUKA, München	Nicht veröffentlicht	Seit 2019 hundertprozentige KUKA-Tochter

Tabelle 35: **Anbieter von IoT-Plattformen**
Quellen: [44, 86, 87, 88, 102, 327, 361].

Avedon, Schroders Capital und Verso Capital finanzierten den Buy-out von Cumulocity.[249] TPG zahlt PTC für ThingWorx und Kepware bis zu 725 Mio. US-Dollar, davon bis zu 600 Mio. bei Abschluss und bis zu 125 Mio., falls TPG das Geschäft später weiterverkauft.[328]

D.7 Tracker-Anbieter

Der Tracker-Markt gliedert sich nach den Assets, die ein Anbieter abdeckt, nicht nach der Funktechnik (Tabelle 36). Sensolus in Gent, einer der Spezialisten für Container und Anhänger, verfolgt über 1,5 Mio. Assets für 500 Unternehmen.[356]

ASSET-TYP	ANBIETER UND PRODUKT	TRACKER-KLASSE	KONDITIONEN UND BESONDERHEITEN
Werkzeuge und Kleingeräte	Hilti ON!Track (Smart Tag AI T320, Geo Tag AI T400, Gateways)	BLE, GNSS + Mobilfunk	Software auch für Geräte anderer Hersteller; Preis auf Anfrage
Werkzeuge und Kleingeräte	Milwaukee ONE-KEY	BLE	Kostenlose App, Community-Netz
Bau- und Mietgeräte	Trackunit (Raw, Spot, Kin, Beam, Pass)	Telematik, BLE	Vertragslaufzeiten 36 oder 42 Monate
Ladungsträger, Paletten, Mehrwegbehälter	Bosch Sense I mit All-in-One-Gateways	LTE-M / NB-IoT, 2G-Rückfallebene	KLT, GLT, Paletten, Sonderladungsträger; ATEX-Varianten
Container, Anhänger, Mehrwegbehälter	Sensolus	LTE-M / NB-IoT, BLE	Pauschal 6 € / 1 € pro Monat
Fracht und Sendungen	Tive; Decklar (früher Roambee); Arviem (Baar, CH)	Mobilfunk	Tive: LTE-M mit 2G-Rückfallebene; Arviem als Managed Service
Geräteplattformen	Digital Matter; Teltonika; Abeeway; Minew	BLE, LoRaWAN, LTE-M, GNSS, UWB	Hardware für Integratoren und Plattformen

Tabelle 36: **Tracker-Anbieter in DACH nach Asset-Typ**
Quellen: [8, 23, 43, 92, 116, 207, 270, 271, 357, 382, 389, 391, 392].

Hilti meldete für 2025 einen Konzernumsatz von 6.297 Mio. Franken.[206] Bei Trackunit hat der bisherige Investor Hg erneut investiert.[390] Tive in Boston meldete 2026 einen gebuchten ARR von

100 Mio. US-Dollar und eine Finanzierungsrunde von 20 Mio. US-Dollar unter Führung der Lightsmith Group.[388]

D.8 Ingenieurdienstleister

Die Auswahl reicht von börsennotierten Konzernen mit einem Umsatz in der Größenordnung von 1 Mrd. € (Bertrandt 978 Mio. €, EDAG 714,0 Mio. €) bis zu familiengeführten Embedded-Spezialisten in Österreich und der Schweiz[34, 122, 193] (Tabelle 37). RUBINLAKE ist selbst als Ingenieurberatung für IoT tätig. Wir führen uns deshalb nicht auf.

DIENSTLEISTER	SITZ	GRÖSSE (LETZTES VERÖFFENTLICHTES JAHR)
Bertrandt	Ehningen	Umsatz GJ 2024/25 978 Mio. € (−18 %); 11.932 Beschäftigte zum 31. Dez. 2025
EDAG Group	Arbon, Schweiz; operative Zentrale in Fulda	Umsatz 2025 714,0 Mio. € (−13 %); 8.303 Beschäftigte
FERCHAU	Gummersbach	Rund 10.000 Beschäftigte
Akkodis (Adecco Group)	-	Über 40.000 Ingenieurinnen und Ingenieure weltweit
ALTEN (in Deutschland ALTEN GmbH)	Paris (Konzern)	Konzernumsatz 2025 4.099,0 Mio. €; 57.400 Beschäftigte; keine Zahlen für Deutschland veröffentlicht
Ginzinger electronic systems	Weng im Innkreis, Österreich	Familienunternehmen, gegründet 1991; Größe nicht veröffentlicht
Zühlke	Schlieren, Schweiz	Gegründet 1968; im Besitz der Partner; Nettoumsatz 2023 246 Mio. Franken, rund 1.900 Beschäftigte
Noser Group	Schweiz	Über 600 Beschäftigte in acht Gesellschaften
Kontron (susietec)	Linz, Österreich	Siehe Tabelle 31
Device Insight (KUKA)	München	Siehe Tabelle 35

Tabelle 37: **Ingenieurdienstleister in DACH**
Anmerkung: Auswahl. Quellen: [12, 13, 34, 122, 183, 193, 283, 293, 415].

ALTEN zählt Deutschland zu den Ländern, deren Wirtschaftslage 2025 auf die operative Marge drückte.[13] Vodafone Deutschland kündigte im Dezember 2024 die Schließung von grandcentrix an. Den IoT-Entwickler hatte Vodafone rund fünf Jahre zuvor übernommen.[379]

D.9 Notifizierte Stellen für RED und CRA

Acht der 13 aufgeführten Stellen sind für die RED aktiv, sieben für die Maschinenverordnung[160] (Tabelle 38). TÜV NORD CERT und die DEKRA Testing and Certification GmbH in Deutschland sind für die Maschinenverordnung notifiziert, nicht aber für die RED.

STELLE	LAND	KENNNUMMER	RED	MASCHINENVERORDNUNG	CRA
TÜV SÜD Product Service GmbH	Deutschland	0123	Aktiv	Aktiv	Nicht notifiziert

STELLE	LAND	KENNNUMMER	RED	MASCHINENVERORD-NUNG	CRA
TÜV Rheinland LGA Products GmbH	Deutschland	0197	Aktiv	Aktiv	Nicht notifiziert
TÜV NORD CERT GmbH	Deutschland	0044	Nicht notifiziert	Aktiv	Nicht notifiziert; TÜViT plant den Antrag
TÜV AUSTRIA GMBH	Österreich	0408	Aktiv	Aktiv	Nicht notifiziert
DEKRA Testing and Certification GmbH	Deutschland	0158	Nicht notifiziert	Aktiv	Nicht notifiziert
VDE Prüf- und Zer-tifizierungsinstitut GmbH	Deutschland	0366	Aktiv	Aktiv	Nicht notifiziert
SGS-TÜV Saar GmbH	Deutschland	1637	Nicht notifiziert	Aktiv	Nicht notifiziert
SGS Fimko Oy	Finnland	0598	Abgelaufen	Abgelaufen	Nicht notifiziert
SGS Brightsight	Niederlande	-	-	-	Für Modul B akkre-ditiert; Notifizierung ausstehend
Eurofins Product Service GmbH	Deutschland	0681	Aktiv	Nicht notifiziert	Nicht notifiziert
cetecom advanced GmbH	Deutschland	0682	Aktiv	Nicht notifiziert	Nicht notifiziert
NMi Testlab GmbH (vormals Phoenix Testlab)	Deutschland	0700	Aktiv	Nicht notifiziert	Nicht notifiziert
Bureau Veritas CPS Germany GmbH	Deutschland	2004	Aktiv	Nicht notifiziert	Nicht notifiziert

Tabelle 38: **Notifizierte Stellen nach Rechtsakt**
Quellen: [160, 161, 162, 360, 396].

Die niederländische DEKRA-Gesellschaft ist ebenfalls nicht für die RED notifiziert, und die Notifizierung der spanischen mit der Kennnummer 1909 ist für die RED bis zum 1. Dezember 2026 ausgesetzt.[160] NANDO führt die Notifizierungen von SGS Fimko für die RED und die Maschinenverordnung als abgelaufen, mit dem Enddatum 20. März 2030 und ohne Begründung.[162] In Österreich sind zwei Stellen für die RED aktiv, TÜV AUSTRIA und OVE. In der Schweiz ist keine Stelle für die RED notifiziert, obwohl das MRA zwischen der Schweiz und der EU die RED einschließt.[160] Die Stellen veröffentlichen ihre Gebühren selten[359] (Tabelle 29).

D.10 Listenpreise

Die veröffentlichten Einstiegspreise reichen von 12 € einmalig für eine 1NCE-SIM mit zehn Jahren Laufzeit bis zu 6.695 US-Dollar im Monat für Memfaults Scale-Tarif.[2, 260] Gebühren je Gerät für OTA, Pauschalen je Tarif und Preise je Megabyte lassen sich nur an einer konkreten Gerätezahl vergleichen (Tabelle 39).

ANBIETER	TARIF	VERÖFFENTLICHTER PREIS	EINHEIT UND STUFE
Mender	Basic	34 US-Dollar im Monat	Bis 50 Geräte

ANBIETER	TARIF	VERÖFFENTLICHTER PREIS	EINHEIT UND STUFE
Mender	Professional	291 US-Dollar im Monat	Bis 250 Geräte
Memfault	Growth / Scale	3.495 / 6.695 US-Dollar im Monat	Je Tarif
Golioth	Connect / Fleet Control	0,25 US-Dollar je aktivem Gerät und Monat; 0,0095 US-Dollar je MB OTA	Nutzungsbasiert, ohne Stufen
balena	Prototype / Pilot / Production	159 / 329 / 1.439 US-Dollar im Monat	30 / 60 / 110 Geräte, darüber 2-3 US-Dollar je weiteres Gerät
emteria	Small / Medium / Large	Ab 80 / 360 / 890 € im Monat	Gerätezahl je Stufe nicht veröffentlicht
qdCloud	Hosting	0,01 € je GB Datenverkehr, 0,10 € je GB Speicher	Lizenz je aktivem Gerät und Jahr, Betrag nicht veröffentlicht
1NCE	Lifetime Flat	12 € einmalig	10 Jahre, 500 MB, 250 SMS; High-Data-Option 5 € je GB
Onomondo	Daten	Ab 0,0025 € je MB	Grundgebühr auf Anfrage
FOSSA	Business	20 US-Dollar je Projekt und Monat	Je Projekt

Tabelle 39: **Veröffentlichte Einstiegspreise**
Anmerkung: Listenpreise ohne Umsatzsteuer, soweit angegeben, nur für Anbieter, die in unserem Kostenmodell (Anhang C) fehlen oder dort nur mit einer Stufe vorkommen. Quellen: [2, 28, 131, 189, 199, 260, 292, 310, 332].

Die meisten Anbieter veröffentlichen keine Preise, darunter ONEKEY, Cybellum, Finite State, Exein, emnify, alle PKI-Anbieter für Gerätezertifikate, alle notifizierten Stellen sowie Cumulocity, Bosch IoT Suite und Insights Hub.

E Förderprogramme

Die Förderprogramme zu Kapitel 8 decken Digitalisierung, IoT und Produkt-Cybersicherheit in Deutschland, Österreich, der Schweiz und der EU ab. Bei fast allen muss der Antrag vor Projektbeginn gestellt werden.

E.1 Deutschland: Bundesprogramme

KfW ERP-Förderkredit Digitalisierung (511, 512) und Innovation (513, 514). Diese beiden ERP-Förderkredite ersetzen seit dem 1. Juli 2025 den ERP-Digitalisierungs- und Innovationskredit (380, 390, 391),[235] den viele Förderratgeber noch nennen, für den aber keine Anträge mehr möglich sind.[236] Beide werden über die Hausbank beantragt und in drei Stufen vergeben:[237]

- **Stufe 1 (Basis):** bis 7,5 Mio. €, nur für KMU und Freiberufler nach dem KfW-Digitalisierungs-Check, ohne Zuschuss.
- **Stufe 2 (LevelUp):** bis 25 Mio. €, mit einem ERP-Förderzuschuss von 3 % des ausgezahlten Betrags.
- **Stufe 3 (HighEnd):** bis 25 Mio. €, mit einem Zuschuss von 5 % des ausgezahlten Betrags.

Der Zuschuss ist auf 200.000 € begrenzt und wird erst nach vollständigem Abruf des Kredits ausgezahlt.[237] Unternehmen mit einem Gruppenumsatz von bis zu 500 Mio. € im Jahr und Sitz oder Niederlassung in Deutschland sind antragsberechtigt. Programm 512 enthält zusätzlich eine Haftungsfreistellung der Bank von 50 %.[237] Der Digitalisierungskredit nennt für Stufe 2 IT-Sicherheit, Sicherheitsstandards, Datensicherheitskonzepte und den Aufbau digitaler Geschäftsmodelle und finanziert neben Investitionen auch Betriebsmittel.[237] Die Sicherheitsmaßnahmen für den CRA und die Geräteplattform eines vernetzten Produkts fallen unter Stufe 2, die Entwicklung des Produkts selbst unter den Innovationskredit.[238] Für keinen der beiden Kredite gilt eine Antragsfrist. Der Kredit muss innerhalb von 24 Monaten (511) bzw. 12 Monaten (512) nach Zusage abgerufen werden.[237] Der Zinssatz hängt von der Preisklasse ab, die die Hausbank vergibt. Der Sollzins für 511, gültig ab dem 9. Oktober 2026, lag bei zehn Jahren Laufzeit, zwei tilgungsfreien Jahren und zehnjähriger Zinsbindung in Stufe 1 zwischen 4,48 % in der besten und 10,88 % in der schlechtesten von neun Preisklassen.[239] In Stufe 2 reichte er von 4,33 bis 10,73 %, in Stufe 3 von 4,18 bis 10,58 %.[239]

BAFA EEW Modul 3. Die Bundesförderung für Energie- und Ressourceneffizienz fördert Mess-, Steuer- und Regelungstechnik, Sensorik und Energiemanagement-Software im eigenen Betrieb, mit Förderquoten von 45 % für kleine, 35 % für mittlere und 25 % für große Unternehmen.[57] Das BAFA führt das Programm ohne Antragsstopp weiter. Gefördert werden Soft- und Hardware für Aufbau und Betrieb eines Energie- oder Umweltmanagementsystems im eigenen Betrieb des Antragstellers, nicht Sensorik oder Software in Produkten für Kunden.[57] Ein Hersteller kann damit den Energieverbrauch der eigenen Fertigung erfassen, nicht aber seine vernetzten Produkte entwickeln.

Digital Jetzt. Der Investitionszuschuss des Wirtschaftsministeriums lief bis zum 31. Dezember 2023.[70]

Digital-Tech-to-Product. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) fördert Start-ups und KMU, die allein oder im Verbund eine digitale Technologie vom Proof of Concept bis zum Reifegrad TRL 8 weiterentwickeln. Antragsteller müssen ein Geschäftsmodell vorlegen und darlegen, wie ihr Technologie-Stack zur digitalen Souveränität beiträgt.[66, 68] Das

BMDS vergibt je Vorhaben bis zu 5 Mio. € in einem zweistufigen Verfahren. Der erste Aufruf setzte die Schwerpunkte KI, Datenökosysteme, Cybersicherheit sowie Cloud und Edge Computing.[68] Der erste Förderaufruf endete am 11. Oktober 2026, weitere Aufrufe will das Ministerium in den kommenden Monaten veröffentlichen.[66]

InnoNT+ (Smarte Konnektivität für die Wirtschaft). Das BMDS stellt bis 2029 mindestens 60 Mio. € für branchenspezifische Anwendungszentren bereit, in denen Unternehmen Connectivity-Lösungen im Realbetrieb erproben. Verbünde konnten Projektskizzen bis zum 13. April oder 6. Mai 2026 einreichen.[67] Das Programm fördert Zentren, nicht das Produkt eines Herstellers. Ein Hersteller kann sich aber einem Verbund anschließen oder ein Zentrum nutzen.

ZIM. Das Zentrale Innovationsprogramm Mittelstand läuft seit dem 1. Januar 2025 nach einer Richtlinie vom 28. November 2024.[71] Es übernimmt je nach Unternehmensgröße und Region 25 bis 45 % der zuwendungsfähigen Kosten für Einzelprojekte und 30 bis 55 % für Kooperationsprojekte (40 bis 60 % mit ausländischem Partner).[71] Die zuwendungsfähigen Kosten sind auf 690.000 € je Einzelprojekt und 560.000 € je Unternehmen in einer Kooperation begrenzt.[71] KMU und weitere mittelständische Unternehmen mit weniger als 500 Beschäftigten sind antragsberechtigt, Unternehmen mit weniger als 1.000, wenn sie mit einem geförderten KMU kooperieren.[71] Das Bundesministerium für Wirtschaft und Energie (BMWE) hat am 7. Juli 2026 die Annahme neuer Anträge gestoppt. Es begründet den Stopp mit der seit dem vierten Quartal 2025 deutlich gestiegenen Nachfrage und den begrenzten Haushaltsmitteln des Bundes. Die für 2026 vorgesehenen Mittel waren bereits zur Jahresmitte ausgeschöpft.[387]

Forschungszulage. Die steuerliche Forschungszulage beträgt 25 % der Bemessungsgrundlage, KMU können zehn Prozentpunkte mehr beantragen.[62] Für Aufwendungen ab dem 1. Januar 2026 stieg die maximale Bemessungsgrundlage auf 12 Mio. € jährlich.[35, 62] Der Pauschalsatz für Eigenleistungen stieg von 70 auf 100 € je Stunde, und Gemeinkosten werden für Vorhaben mit Beginn nach dem 31. Dezember 2025 pauschal mit 20 % anerkannt.[35, 62] Nach unserer Einschätzung kann die Entwicklung eines neuen vernetzten Produkts mit echter technischer Unsicherheit begünstigt sein, routinemäßige Compliance-Arbeit dagegen nicht.

Transferstelle Cybersicherheit im Mittelstand. Sie bietet KMU, Start-ups und Handwerksbetrieben kostenfreie Checks, Erstberatung und Notfallhilfe.[393] Das Angebot ist Beratung statt Geld und betrifft die IT des Unternehmens, nicht seine Produkte.

E.2 Deutschland: Landesprogramme

Die Länder vergeben seit dem Ende von Digital Jetzt 2023 den größten Teil der Zuschüsse für Digitalisierung.[70] Die meisten ihrer Zuschüsse sind kleinen oder mittleren Unternehmen vorbehalten, und mehrere Programme sind geschlossen oder pausieren.

- **Baden-Württemberg.** Die Digitalisierungsprämie Plus ist zum 30. Juni 2025 ausgelaufen.[250] Nachfolger ist die **Digitalisierungsfinanzierung** der L-Bank, ein Förderdarlehen mit Zinsverbilligung und einem Tilgungszuschuss von bis zu 5 % für KMU, von 10.000 € bis 5 Mio. €, für größere Unternehmen bis 25 Mio. €. Sie lässt sich in den Stufen 2 und 3 mit dem KfW-Zuschuss kombinieren.[251]
- **Bayern.** Der **Digitalbonus.Bayern** läuft bis zum 31. Dezember 2027. Kleine Unternehmen mit Betriebsstätte in Bayern erhalten bis zu 7.500 € (Standard, 2026 auf diesen Betrag gesenkt) oder bis zu 30.000 € (Plus, für Maßnahmen mit besonderem Innovationsgehalt), höchstens jedoch 50 % der förderfähigen Ausgaben.[29] IT-Sicherheit ist ein eigener Förderbereich, der Sicherheitsprozesse und Hardware wie Firewalls umfasst.[29]

- **Berlin.** Die **Digitalprämie Berlin** ist mit Ablauf der Antragsfrist am 31. Dezember 2023 ausgelaufen.[229]
- **Hamburg.** Der **Hamburg Digital Check** der IFB Hamburg bezuschusst Beratung zu Informationssicherheit und digitalem Wandel mit bis zu 50 %, höchstens 7.500 €, für KMU mit Betriebsstätte in Hamburg.[203] Der **Hamburg-Kredit Digital** in der Fassung vom 15. April 2026 verbindet ein Darlehen von 25.000 € bis 2,5 Mio. €, refinanziert aus dem KfW-Programm 511, mit einem Hamburger Zuschuss von bis zu 12 % des Darlehens, höchstens 20.000 €, zusätzlich zum KfW-Zuschuss. Er steht KMU offen und läuft längstens bis zum 31. Dezember 2028.[204]
- **Hessen.** Der **DIGI-Zuschuss** zahlt KMU bis zu 50 % der Ausgaben für externe Leistungen, höchstens 10.000 €. Vorhaben über 50.000 € sind ausgeschlossen, Maßnahmen zur IKT-Sicherheit förderfähig. Ein Antragsteller muss zuvor an einem Förderaufruf der WIBank teilnehmen.[205] **Distr@l** fördert digitale Produktinnovationen mit bis zu 500.000 € und einer Förderquote von 50 % für KMU.[412] Das Verfahren beginnt mit einer Projektskizze an das Hessische Digitalministerium.[412]
- **Niedersachsen.** Der **Digitalbonus.Niedersachsen-innovativ** ist zum 31. Dezember 2025 ausgelaufen. Die NBank hat eine Neuauflage angekündigt, aber noch keine Konditionen veröffentlicht.[282]
- **Nordrhein-Westfalen. Mittelstand Innovativ & Digital (MID)** zahlt bis zu 15.000 € für Investitionen in digitale Produkte, Sicherheit und Prozesse und bis zu 48.000 € für die Einstellung von Hochschulabsolventen für ein Innovationsprojekt. Die NRW.BANK betreut das Programm seit 2026.[294] MID-Digitalisierung und MID-Digitale Sicherheit werden per Los vergeben, MID-Assistent(in) über einen Wartesaal. Das Kontingent für MID-Digitale Prozesse war wegen der hohen Nachfrage erschöpft. Das Land hat es um 650.000 € aufgestockt. Anträge sind ab dem 19. Oktober 2026, 10:00 Uhr, im Kundenportal der NRW.BANK möglich.[294] Das Vorhaben darf erst nach der Bewilligung beginnen.
- **Rheinland-Pfalz.** Das Land hat keinen Digitalisierungszuschuss. DigiBoost gehört nicht mehr zu den Programmen der ISB für Innovation und Digitalisierung.[228] Es bleiben zwei Programme. **InnoTop** ist ein FuE-Zuschuss für KMU und Unternehmen bis 499 Beschäftigte.[226] Die Grundförderung für experimentelle Entwicklung beträgt 25 %, zuzüglich bis zu 20 Prozentpunkten nach Unternehmensgröße und 15 Prozentpunkten für die Zusammenarbeit mit der Forschung, insgesamt höchstens 80 %.[226] **IBI-EFRE** ist ein Investitionszuschuss für Produkt- und Prozessinnovationen von 50.000 € bis 5 Mio. €, mit bis zu 20 % für kleine und 10 % für mittlere Unternehmen.[227]
- **Sachsen** bietet ein Digitalisierungsdarlehen (**Digi-D**) von 30.000 bis 250.000 € für KMU.[339]
- **Schleswig-Holstein.** Die seit Juni 2026 geltende Richtlinie **DKU** erstattet kleinen Unternehmen mit weniger als 50 Beschäftigten 40 % der Ausgaben, bei Ausgaben bis 20.000 € für Beratung und bis 200.000 € für die Umsetzung.[273] Jedes Vorhaben muss die IT- und Informationssicherheit verbessern. Die Richtlinie gilt bis zum 30. Juni 2027.[273] Hersteller mit 100 bis 4.999 Beschäftigten sind damit nicht antragsberechtigt.
- **Thüringen.** Die Mittel des **Digitalbonus Thüringen** sind ausgeschöpft. Das Programm nimmt keine Anträge mehr an.[386]

E.3 Österreich: aws und FFG

Die Budgetkonsolidierung des Bundes hat die Digitalisierungsförderung in Österreich direkt getroffen. **KMU.DIGITAL**, ein Programm von WKO und aws, förderte Beratung und Umsetzung, auch in einer eigenen Schiene für IT- und Cybersecurity.[24] Die Umsetzung wurde mit bis zu 30 % und höchstens 6.000 € je Förderschiene gefördert.[24] Das Budget von KMU.DIGITAL 4.0 ist

vollständig ausgeschöpft, und Anträge sind nicht mehr möglich. Das Programm wird wegen der Konsolidierung des Bundeshaushalts ab 2027 nicht fortgeführt.[414]

aws Digitalisierung vergibt Zuschüsse in einzelnen Calls, je nach Call bis zu 150.000 €. Derzeit ist kein Call offen. Der Call zur KI-Adoption schloss am 28. Februar 2025, ein weiterer Call ist nicht angekündigt.[25] Die aws bietet weiterhin ganzjährig Finanzierungen an:

- **aws erp-Kredit:** 10.000 € bis 37,5 Mio. €, bis zu 100 % der Projektkosten, mit fixem oder sprungfixem Zinssatz. Der Kredit muss vollständig durch eine Bank oder eine aws-Garantie besichert sein, und der Antrag muss vor Projektbeginn gestellt werden. Digitalisierung zählt zu den ausdrücklich genannten Förderzwecken.[26]
- **aws Garantie:** bis zu 80 % eines Kredits, mit einem aws-Obligo von höchstens 30 Mio. €.[27]

Das **FFG-Basisprogramm** ist in Österreich das wichtigste Förderinstrument für Produktentwicklung. Es ist themen- und größenoffen und nimmt 2026 jederzeit Anträge an.[313] Es fördert FuE-Projekte mit einer Kombination aus Zuschuss und Darlehen zu 1,75 % p. a. Die Gesamtförderquote beträgt 45 % für kleine Unternehmen (Zuschuss bis 28 %), 35 % für mittlere (bis 25 %) und 25 % für große (bis 19 %), mit bis zu 3 Mio. € je Projekt.[316] Das **Kleinprojekt** gewährt KMU einen Zuschuss von bis zu 88.500 € für Projekte bis 150.000 €.[318] Das Budget von **Projekt.Start 2026** für Machbarkeitsstudien war ausgeschöpft.[320] Das Programm schloss deshalb vorzeitig am 4. Mai 2026.[320] Das Sicherheitsforschungsprogramm **KIRAS** hat eine Ausschreibung vom 5. Oktober 2026 bis 26. Februar 2027 geöffnet, mit bis zu 2 Mio. € je Projekt. Sie zielt auf zivile Sicherheit und kritische Infrastruktur, nicht auf Produkt-Compliance.[317] Der DACH-Call 2026 der FFG fördert Verkehrsinfrastrukturforschung und kommt für Produkthersteller nicht in Frage.[314]

Die **Forschungsprämie** von 14 % der Forschungsaufwendungen gilt weiter. Der Antrag setzt ein jährliches Gutachten der FFG voraus.[315]

E.4 Schweiz: Innosuisse

Innosuisse fördert Unternehmen in ihrem Hauptinstrument nicht direkt. In einem **Innovationsprojekt mit Umsetzungspartner** finanziert sie den Schweizer Forschungspartner (Universität oder Fachhochschule). Das Unternehmen trägt 40 bis 60 % der gesamten Projektkosten, davon mindestens 5 % in bar.[223] Gesuche sind mindestens sechs Wochen vor den Sitzungen des Innovationsrats einzureichen. Innosuisse entscheidet innerhalb von sechs bis acht Wochen.[223] Das Instrument eignet sich für Vorhaben eines Schweizer Herstellers mit einer technischen Forschungsfrage, etwa einer sicheren Update-Architektur oder einem stromsparenden Tracker-Design, nicht für routinemäßige Compliance-Arbeit.

Der **Innovationsscheck** übernimmt 100 % der Kosten eines Forschungspartners bis 15.000 Franken. Unternehmen mit weniger als 250 Vollzeitstellen können ihn einmal alle zwei Jahre nutzen.[222] **Start-up-Innovationsprojekte** decken bis zu 70 % der direkten Kosten von Start-ups mit weniger als 50 Vollzeitstellen, die noch nicht am Markt sind.[224] Innosuisse plant keine Ausschreibung des **Swiss Accelerator**, der sich an bereits am Markt tätige KMU richtet. Schweizer Unternehmen können stattdessen seit dem 1. Januar 2025 vollberechtigt am EIC Accelerator teilnehmen.[225]

Das Entlastungspaket 2027 des Bundesrats sah vor, den Bundesbeitrag an Innosuisse 2027 um rund 10 % oder 32 Mio. Franken zu kürzen.[221, 348]

E.5 EU-Ausschreibungen mit CRA-Bezug

SECURE, ein vom Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) unterstütztes Projekt, reicht EU-Mittel an Kleinst-, kleine und mittlere Unternehmen im Geltungsbereich des CRA weiter.[353] Der zweite Aufruf ist vom 1. Oktober bis 11. Dezember 2026 offen und vergibt aus einem Budget von 11,5 Mio. € bis zu 30.000 € je Zuschuss bei 50 % Kofinanzierung.[353] Das Thema **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG** des Programms Digitales Europa fördert die Umsetzung der EU-Rechtsakte zur Cybersicherheit, darunter CRA, NIS-2, DSGVO, DORA und Cybersecurity Act. Es hat ein Budget von 20 Mio. € bei 50 % Förderquote und ist vom 1. September 2026 bis 14. Januar 2027 offen.[280] Ein weiteres Thema derselben Ausschreibung, **AI4SME**, stellt 20 Mio. € für die Cybersicherheit von KMU mit KI-Werkzeugen bereit, mit Förderquoten bis zu 75 % für KMU. Es nennt den CRA jedoch nicht.[279]

Die nationalen Koordinierungszentren bieten keine eigene Kaskadenförderung für den CRA an. Weder das deutsche NKCS noch das österreichische NCC-AT führen derzeit ein solches Programm.[281, 319] Die Europäischen Digitalen Innovationszentren bieten Unternehmen Dienstleistungen an. Die Kommission wählte im Oktober 2025 83 von ihnen für eine erneute Förderung aus.[152]

E.6 Überblick

Derzeit nehmen 24 der 41 Programme Anträge an (Tabelle 40).

PROGRAMM	LAND ODER BUNDES-LAND	INSTRUMENT	HÖHE	ANTRAGSBERECHTIGT	ANTRAGSFRIST	STATUS
KfW ERP-Digitalisierungs- und Innovationskredit (380, 390, 391)	Deutschland	Kredit	-	-	-	Geschlossen; seit 1. Juli 2025 ersetzt
KfW ERP-Förderkredit Digitalisierung (511, 512)	Deutschland	Kredit mit Zuschuss	Bis 7,5 Mio. € (Stufe 1) oder 25 Mio. €; Zuschuss 3 % oder 5 %, höchstens 200.000 €	Gruppenumsatz bis 500 Mio. €	Keine	Offen
KfW ERP-Förderkredit Innovation (513, 514)	Deutschland	Kredit mit Zuschuss	Wie 511, 512	Wie 511, 512	Keine	Offen
BAFA EEW Modul 3	Deutschland	Zuschuss	45 / 35 / 25 %	Alle Größen; nur eigener Betrieb	Keine angegeben	Offen; nicht für Produkte
Digital Jetzt	Deutschland	Zuschuss	-	-	31. Dez. 2023	Beendet
BMDS Digital-Tech-to-Product	Deutschland	Projektförderung	Bis 5 Mio. € je Vorhaben	Start-ups, KMU; Verbünde	Erster Aufruf 11. Okt. 2026	Zwischen zwei Aufrufen
BMDS InnoNT+	Deutschland	Zuschuss an Verbünde	Mindestens 60 Mio. € bis 2029	Verbünde für Anwendungszentren	13. Apr. / 6. Mai 2026 (Skizzen)	Erster Aufruf geschlossen
ZIM	Deutschland	Zuschuss	25-45 % (Einzelprojekt), 30-60 % (Kooperation); Kosten bis 690.000 €	KMU; weniger als 500 Beschäftigte (1.000 in Kooperation)	-	Antragsstopp seit 7. Juli 2026
Forschungszulage	Deutschland	Steuerliche Förderung	25 % (KMU 35 %) von bis zu 12 Mio. € jährlich	Alle Steuerpflichtigen	Nach Jahresende	Offen
L-Bank Digitalisierungsfinanzierung	Baden-Württemberg	Darlehen mit Tilgungszuschuss	10.000 € bis 5 Mio. € (größere Unternehmen 25 Mio. €); Zuschuss bis 5 %	KMU; Unternehmen bis 500 Mio. € Umsatz	Keine	Offen
Digitalisierungsprämie Plus	Baden-Württemberg	Zuschuss oder Darlehen	-	-	30. Juni 2025	Beendet

PROGRAMM	LAND ODER BUNDES-LAND	INSTRUMENT	HÖHE	ANTRAGSBERECHTIGT	ANTRAGSFRIST	STATUS
Digitalbonus.Bayern	Bayern	Zuschuss	Bis 7.500 € oder 30.000 €; bis 50 %	Kleine Unternehmen	31. Dez. 2027	Offen
Digitalprämie Berlin	Berlin	Zuschuss	-	-	31. Dez. 2023	Beendet
Hamburg Digital Check	Hamburg	Beratungszuschuss	Bis 50 %, höchstens 7.500 €	KMU	-	Offen
Hamburg-Kredit Digital	Hamburg	Darlehen mit Zuschuss	25.000 € bis 2,5 Mio. €; Zuschuss bis 12 %, höchstens 20.000 €	KMU	Längstens 31. Dez. 2028	Offen
DIGI-Zuschuss	Hessen	Zuschuss	Bis 50 %, höchstens 10.000 €	KMU; Vorhaben bis 50.000 €	Je Förderaufruf	Über Förderaufrufe
Distr@l	Hessen	Zuschuss	Bis 500.000 €; 50 % für KMU	KMU, Start-ups, Forschungseinrichtungen	-	Nicht veröffentlicht
Digitalbonus.Niedersachsen-innovativ	Niedersachsen	Zuschuss	-	-	31. Dez. 2025	Beendet
Mittelstand Innovativ & Digital (MID)	Nordrhein-Westfalen	Zuschuss	Bis 15.000 €; bis 48.000 € (Einstellung von Absolventen)	KMU	Digitale Prozesse ab 19. Okt. 2026	Offen; Losverfahren für zwei Module
DigiBoost	Rheinland-Pfalz	Zuschuss	-	-	-	Nicht mehr im Programmangebot der ISB
InnoTop	Rheinland-Pfalz	FuE-Zuschuss	Grundquote 25 % für experimentelle Entwicklung; höchstens 80 %	KMU; Unternehmen bis 499 Beschäftigte	-	Offen
IBI-EFRE	Rheinland-Pfalz	Investitionszuschuss	20 % (kleine) oder 10 % (mittlere); 50.000 € bis 5 Mio. €	KMU	-	Offen
Digi-D	Sachsen	Darlehen	30.000 bis 250.000 €	KMU	-	Offen

PROGRAMM	LAND ODER BUNDES-LAND	INSTRUMENT	HÖHE	ANTRAGSBERECHTIGT	ANTRAGSFRIST	STATUS
DKU	Schleswig-Holstein	Zuschuss	40 % von bis zu 20.000 € (Beratung) oder 200.000 € (Umsetzung)	Kleine Unternehmen (weniger als 50 Beschäftigte)	30. Juni 2027	Offen
Digitalbonus Thüringen	Thüringen	Zuschuss	-	-	-	Geschlossen; Mittel ausgeschöpft
KMU.DIGITAL 4.0	Österreich	Zuschuss	Bis 30 %, 6.000 € je Schiene	KMU	-	Geschlossen; ab 2027 keine Fortführung
aws Digitalisierung	Österreich	Zuschuss	Bis 150.000 € je Call	Unternehmen	Je Call	Kein offener Call
aws erp-Kredit	Österreich	Kredit	10.000 € bis 37,5 Mio. €	Voll besicherte Projekte	Laufend	Offen
aws Garantie	Österreich	Garantie	Bis 80 % eines Kredits; höchstens 30 Mio. €	-	Laufend	Offen
FFG-Basisprogramm	Österreich	Zuschuss und Darlehen	45 / 35 / 25 %; bis 3 Mio. €	Alle Größen	31. Dez. 2026	Offen
FFG Kleinprojekt	Österreich	Zuschuss	Bis 88.500 €	KMU	31. Dez. 2026	Offen
FFG Projekt.Start 2026	Österreich	Zuschuss	-	KMU, Start-ups	4. Mai 2026	Vorzeitig geschlossen; Budget ausgeschöpft
KIRAS	Österreich	Zuschuss	Bis 2 Mio. € je Projekt	Zivile Sicherheitsforschung	26. Feb. 2027	Offen; nicht für Produkt-Compliance
Forschungsprämie	Österreich	Steuerprämie	14 % der FuE-Aufwendungen	Alle Unternehmen	Nach Jahresende	Offen
Innosuisse-Innovationsprojekt	Schweiz	Förderung des Forschungspartners	Unternehmen trägt 40-60 %	Schweizer Forschungspartner	Sechs Wochen vor den Sitzungen des Innovationsrats	Offen
Innosuisse-Innovationsscheck	Schweiz	Gutschein	Bis 15.000 Franken	Weniger als 250 Vollzeitstellen	Laufend	Offen

PROGRAMM	LAND ODER BUNDES-LAND	INSTRUMENT	HÖHE	ANTRAGSBERECHTIGT	ANTRAGSFRIST	STATUS
Innosuisse-Start-up-Innovationsprojekt	Schweiz	Zuschuss	Bis 70 % der direkten Kosten	Start-ups vor Markt-eintritt, weniger als 50 Vollzeitstellen	-	-
Swiss Accelerator	Schweiz	Zuschuss	-	KMU	-	Keine Ausschreibung geplant; stattdessen EIC Accelerator
SECURE, zweiter Auf-ruf	EU	Kaskadenförderung	Bis 30.000 € bei 50 %; Aufruf 11,5 Mio. €	Kleinst-, kleine und mittlere Unternehmen im Geltungsbereich des CRA	11. Dez. 2026	Offen
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG	EU	Zuschuss	Thema 20 Mio. €; 50 %	Alle Akteure	14. Jan. 2027	Offen
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME	EU	Zuschuss	Thema 20 Mio. €; bis 75 % für KMU	-	14. Jan. 2027	Offen; ohne CRA-Be-zug

Tabelle 40: Öffentliche Förderprogramme in DACH und der EU

Anmerkung: Kantonale Programme der Schweiz sind nicht enthalten. Quellen: [25, 26, 27, 29, 35, 57, 62, 66, 67, 68, 70, 71, 203, 204, 205, 222, 223, 224, 225, 226, 227, 228, 229, 236, 237, 238, 250, 251, 273, 279, 280, 282, 294, 315, 316, 317, 318, 320, 339, 353, 386, 387, 412, 414].

Über RUBINLAKE

Wir bauen vernetzte Produkte selbst, vom Funkprotokoll über Edge-Gateway und Cloud bis ins Warenwirtschaftssystem. Genau diese Systeme, ihre Pflichten, Kosten und Architektur untersucht dieser Bericht.

Wir bauen selbst, was wir empfehlen. Unsere Plattform RUBINLAKE.com für Vertrieb, Recruiting und Einkauf, ausgezeichnet mit dem German Innovation Award 2025, verbindet Daten aus amtlichen Registern und von Unternehmenswebsites mit Echtzeit-Signalen und eigenen KI-Agenten. Mit ihr erfassen wir die Märkte, über die wir schreiben.

RUBINLAKE wurde 2021 in Frankfurt am Main gegründet und arbeitet als Unternehmen für Beratung und Engineering in den Bereichen Daten, KI und vernetzte Produkte, vor allem für Gerätehersteller und Netzbetreiber. Mehr unter rubinlake.com.

Prämiert für exzellente Leistungen und Arbeitsbedingungen



Haftungsausschluss

Dieser Bericht dient ausschließlich der allgemeinen Information. Er ist keine Rechts-, Steuer- oder Anlageberatung und ersetzt keine fachliche Beratung im Einzelfall. Wir haben die Inhalte mit großer Sorgfalt erstellt, übernehmen aber keine Gewähr für ihre Richtigkeit, Vollständigkeit und Aktualität. Die Angaben geben den Stand zum Zeitpunkt der Veröffentlichung wieder. Prognosen, Modellrechnungen und Schätzungen beruhen auf Annahmen und können von der tatsächlichen Entwicklung abweichen. Entscheidungen auf Grundlage dieses Berichts treffen Leserinnen und Leser in eigener Verantwortung. Die RUBINLAKE GmbH haftet nicht für Schäden aus der Nutzung dieses Berichts, soweit diese nicht auf Vorsatz oder grober Fahrlässigkeit beruhen und das Gesetz keine zwingende Haftung vorsieht. Für die Inhalte zitierter Quellen und verlinkter Websites sind allein deren Herausgeber und Betreiber verantwortlich. Auf diese Inhalte hat die RUBINLAKE GmbH keinen Einfluss.

Genannte Marken, Produkt- und Firmennamen gehören ihren jeweiligen Inhabern. Die gesetzlichen Bestimmungen gelten für sie auch dann, wenn sie ohne Markenzeichen erscheinen. © RUBINLAKE GmbH, Bettinastraße 62, 60325 Frankfurt am Main, Amtsgericht Frankfurt am Main, HRB 97948. Alle Rechte vorbehalten. Zitate sind mit Quellenangabe zulässig. Die Vervielfältigung oder Weitergabe von Texten, Daten und Grafiken aus diesem Bericht zu geschäftlichen Zwecken oder zur Verwendung auf anderen Websites bedarf der vorherigen Zustimmung der RUBINLAKE GmbH. Anfragen richten Sie bitte an contact@rubinlake.com.

Quellen

Stand: 15. Oktober 2026. An diesem Tag haben wir alle Online-Quellen zuletzt abgerufen.

[1] 1NCE. (2025). *1NCE raises 60 million USD in new funding*. https://www.1nce.com/en-eu/resources/news-insights/press-releases/1nce-raises-60-million-usd-in-new-funding

[2] 1NCE. (2026). *1NCE Connect pricing*. https://www.1nce.com/en-eu/1nce-connect/pricing

[3] 1NCE. (2026). *1NCE Connect: IoT Lifetime Flat and 500 MB data volume*. https://www.1nce.com/en-eu/1nce-connect

[4] 1NCE. (2026). *1NCE in a nutshell*. https://www.1nce.com/en-eu/about/1nce-in-a-nutshell

[5] 3GPP. (2023). *A glimpse into RedCap NR devices*. https://www.3gpp.org/technologies/nr-redcap-glimpse

[6] A1 Digital. (2026). *2G network sunset announcement*. https://www.a1.digital/news/2g-network-sunset-announcement/

[7] A1 Digital. (2026). *A1 Digital*. https://www.a1.digital/

[8] Abeeway. (2026). *Abeeway Compact Tracker*. https://www.abeeway.com/compact-tracker/

[9] achelos GmbH. (2026). *achelos GmbH*. https://www.achelos.de/en/

[10] Adolf Würth GmbH & Co. KG. (2026). *W-CONNECT tag with Bluetooth function (art. no. 5703000100)*. https://eshop.wuerth.de/W-CONNECT-tag-with-Bluetooth-function-TAG-W-CONNECT-WCT-BT-/5703000100.sku/en/US/EUR

[11] Advent International. (2025). *Advent completes acquisition of u-blox*. https://www.adventinternational.com/news/advent-completes-acquisition-of-u-blox/

[12] Akkodis. (2026). *Akkodis*. https://www.akkodis.com/

[13] ALTEN. (2026). *2025 annual results*. https://echanges.dila.gouv.fr/OPENDATA/AMF/ECO/2026/02/FCECO081021_20260224.pdf

[14] Amazon Web Services. (2025). *AWS IoT Analytics end of support*. https://docs.aws.amazon.com/iotanalytics/latest/userguide/iotanalytics-end-of-support.html

[15] Amazon Web Services. (2026). *AWS IoT Core pricing, EU (Frankfurt), price list file of 3 October 2026*. https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AWSIoT/current/eu-central-1/index.json

[16] Amazon Web Services. (2026). *AWS IoT Device Management pricing*. https://aws.amazon.com/iot-device-management/pricing/

[17] Amazon Web Services. (2026). *AWS IoT Events end of support*. https://docs.aws.amazon.com/iotevents/latest/developerguide/iotevents-end-of-support.html

[18] Amazon Web Services. (2026). *AWS IoT FleetWise*. https://aws.amazon.com/iot-fleetwise/

[19] Amazon Web Services. (2026). *AWS Private CA pricing*. https://aws.amazon.com/private-ca/pricing/

[20] Amazon Web Services. (2026). *FreeRTOS over-the-air updates*. https://docs.aws.amazon.com/freertos/latest/userguide/freertos-ota-dev.html

[21] Amazon Web Services. (2026). *Provisioning devices that don't have device certificates using fleet provisioning*. https://docs.aws.amazon.com/iot/latest/developerguide/provision-wo-cert.html

[22] Apple. (2026). *AirTag: Preis und technische Daten*. https://www.apple.com/de/shop/buy-airtag/airtag

[23] Arviem. (2026). *Arviem cargo monitoring as a service*. https://arviem.com/

[24] Austria Wirtschaftsservice. (2024). *KMU.DIGITAL 4.0: Förderrichtlinien Umsetzung*. https://www.kmudigital.at/inhalte/kmudigital-4.0-foerderrichtlinien-umsetzung.pdf

[25] Austria Wirtschaftsservice. (2026). *aws Digitalisierung*. https://www.aws.at/aws-digitalisierung/

[26] Austria Wirtschaftsservice. (2026). *aws erp-Kredit*. https://www.aws.at/aws-erp-kredit/

[27] Austria Wirtschaftsservice. (2026). *aws Garantie*. https://www.aws.at/aws-garantie/

[28] balena. (2026). *balena pricing*. https://www.balena.io/pricing

[29] Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie. (2026). *Digitalbonus.Bayern: Förderprogramm*. https://www.digitalbonus.bayern/foerderprogramm/

[30] Berg Insight. (2025). *Fleet Management in Europe, 20th edition: press summary*. https://telematik-markt.de/sites/default/files/news/attachments/bi-fm20-ps.pdf

[31] Berg Insight. (2025). *Smart Labels in Logistics, 1st edition: press summary*. https://media.berginsight.com/2025/03/13103757/bi-smartlabels1-ps.pdf

[32] Berg Insight. (2025). *Trailer and Cargo Container Tracking, 12th edition: press summary*. https://media.berginsight.com/2025/01/08162415/bi-container12-ps.pdf

[33] Berg Insight. (2025). *Trailer and Cargo Container Tracking, 13th edition*. https://media.berginsight.com/2025/12/13211620/bi-container13-ps.pdf

[34] Bertrandt AG. (2026). *Press release: first quarter 2025/2026*. https://www.bertrandt.com/fileadmin/files/files/00_Unternehmen/03_Presse/Pressemitteilungen/2026/2026-02-12_press_release_q1_2025-2026_bertrandt.pdf

[35] Bescheinigungsstelle Forschungszulage. (2025). *Steuerliches Investitionssofortprogramm: Änderungen bei der Forschungszulage*. https://www.bescheinigung-forschungszulage.de/steuerliches-investitionssofortprogramm

[36] Bitkom e.V. (2026). *Cyber Resilience Act: Nur 3 von 10 Unternehmen sind vorbereitet*. https://www.bitkom.org/Presse/Presseinformation/Cyber-Resilience-Act-3-von-10-Unternehmen-vorbereitet

[37] Bitkom e.V. (2026). *Industrie 4.0 - Wie digital ist Deutschlands Industrie? (Präsentation 2026)*. https://www.bitkom.org/sites/main/files/2026-04/bitkom-praesentation-industrie-4-0-wie-digital-ist-deutschlands-industrie-2026.pdf

[38] Black Duck Software. (2024). *Introducing Black Duck Software: the leader in application security has a new name*. https://news.blackduck.com/2024-10-01-Introducing-Black-Duck-Software-The-Leader-in-Application-Security-Has-a-New-Name

[39] Black Duck Software. (2025). *STMicroelectronics integrates Black Duck SCA and Coverity for automated SBOM generation*. https://news.blackduck.com/2025-03-06-STMicroelectronics-Integrates-Black-Duck-SCA-and-Coverity-for-Automated-SBOM-Generation-and-Enhanced-Software-Security

[40] Black Duck Software. (2026). *Company*. https://www.blackduck.com/company.html

[41] Bluetooth SIG. (2017). *Bluetooth pairing part 4: LE Secure Connections*. https://www.bluetooth.com/blog/bluetooth-pairing-part-4/

[42] Bluetooth SIG. (2024). *Bluetooth Channel Sounding*. https://www.bluetooth.com/press/bluetooth-channel-sounding/

[43] Bosch. (2026). *Bosch Asset Tracking: Sense I, Sensoren und All-in-One-Gateways*. https://assettracking.bosch.io/de/

[44] Bosch Global Software Technologies GmbH. (2026). *Bosch IoT Suite*. https://bosch-iot-suite.com/

[45] Bundesamt für Cybersicherheit (BACS). (2025). *Der Bundesrat will die Cyberresilienz von digitalen Produkten stärken*. https://www.bacs.admin.ch/de/newnsb/QHVUxTqE5DMteBjfCqLlM

[46] Bundesamt für Energie BFE. (2025). *Energiestrategie 2050: Monitoring-Bericht 2025 (ausführliche Fassung)*. https://pubdb.bfe.admin.ch/de/publication/download/12426

[47] Bundesamt für Kommunikation BAKOM. (2025). *3G and 2G shutdown*. https://www.bakom.admin.ch/en/3g-and-2g-shutdown

[48] Bundesamt für Kommunikation BAKOM. (2025). *Statistical observatory: the telecommunications sector in figures*. https://www.bakom.admin.ch/en/statistical-observatory

[49] Bundesamt für Sicherheit in der Informationstechnik. (2023). *FAQ: Anwendungsbereich der BSI TR-03109-5 (Kommunikationsadapter)*. https://bsi.bund.de/DE/Service-Navi/FAQ/TR-03109-5/faq_03109-5_node.html

[50] Bundesamt für Sicherheit in der Informationstechnik. (2025). *BSI TR-03183-2: Cyber Resilience Requirements for Manufacturers and Products, Part 2: Software Bill of Materials, Version 2.1.0*. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

[51] Bundesamt für Sicherheit in der Informationstechnik. (2026). *Certification report BSI-DSZ-CC-1277-2026, Infineon OPTIGA TPM SLB9672*. https://sec-certs.org/cc/ad5e2081def39258/

[52] Bundesamt für Sicherheit in der Informationstechnik. (2026). *CSAF provider metadata of CERT-Bund*. https://wid.cert-bund.de/.well-known/csaf/provider-metadata.json

[53] Bundesamt für Sicherheit in der Informationstechnik. (2026). *Das Smart-Meter-Gateway: Cyber-Sicherheit für die Digitalisierung der Energiewende*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf

[54] Bundesamt für Sicherheit in der Informationstechnik. (2026). *Technische Richtlinie BSI TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte (Teil 1 v1.0.0, Teil 2 SBOM v2.1.0, Teil 3 v1.0.0, Teil H v1.1.0)*. https://www.bsi.bund.de/dok/TR-03183

[55] Bundesamt für Statistik (BFS). (2025). *Institutionelle Einheiten und Beschäftigte nach Jahr, Kanton, Wirtschaftsart und Beobachtungseinheit (px-x-0602010000_105)*. https://www.pxweb.bfs.admin.ch/pxweb/de/px-x-0602010000_105/px-x-0602010000_105.px/

[56] Bundesamt für Statistik (BFS). (2026). *Marktwirtschaftliche Unternehmen nach Wirtschaftsabteilungen und Grössenklasse (T 6.2.1.1), STATENT 2011-2024*. https://dam-api.bfs.admin.ch/hub/api/dam/assets/36734571/master

[57] Bundesamt für Wirtschaft und Ausfuhrkontrolle. (2026). *Bundesförderung für Energie- und Ressourceneffizienz in der Wirtschaft, Modul 3: MSR, Sensorik und Energiemanagement-Software*. https://www.bafa.de/DE/Energie/Energieeffizienz/Energieeffizienz_und_Prozesswaerme/Modul3_Energiemanagementsysteme/modul3_energiemanagementsysteme_node.html

[58] Bundesdruckerei Gruppe GmbH. (2025). *Lagebericht 2024*. https://www.bundesdruckerei.de/files/dokumente/pdf/bdr_Lagebericht_2024_DE_barrierefrei.pdf

[59] Bundeskanzleramt Österreich. (2026). *Fragen und Antworten zur Cyberresilienz-Verordnung (CRA)*. https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/cyberresilienz-verordnung-cra/fragen-und-antworten-zu-cra.html

[60] Bundesministerium der Justiz. (2025). *§ 45 Messstellenbetriebsgesetz: Rollout targets*. https://www.gesetze-im-internet.de/messbg/__45.html

[61] Bundesministerium der Justiz. (2026). *§ 14a Energiewirtschaftsgesetz: Netzorientierte Steuerung von steuerbaren Netzanschlüssen und steuerbaren Verbrauchseinrichtungen*. https://www.gesetze-im-internet.de/enwg_2005/__14a.html

[62] Bundesministerium der Justiz. (2026). *Forschungszulagengesetz (FZulG) vom 14. Dezember 2019 (BGBl. I S. 2763), zuletzt geändert durch Artikel 3 des Gesetzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 363)*. https://www.gesetze-im-internet.de/fzulg/

[63] Bundesministerium der Justiz. (2026). *Krankenhausentgeltgesetz (KHEntgG), § 5 Vereinbarung und Abrechnung von Zu- und Abschlägen*. https://www.gesetze-im-internet.de/khentgg/__5.html

[64] Bundesministerium der Justiz. (2026). *Krankenhausstrukturfonds-Verordnung (KHSFV), § 19 Förderungsfähige Vorhaben*. https://www.gesetze-im-internet.de/khsfv/__19.html

[65] Bundesministerium der Verteidigung. (2026). *Verteidigungshaushalt*. https://www.bmvg.de/de/themen/verteidigungshaushalt

[66] Bundesministerium für Digitales und Staatsmodernisierung. (2026). *Förderprogramm „Digital-Tech-to-Product“*. https://bmds.bund.de/en/themen/digitalpolitik/foerderprogramm-digital-tech-to-product

[67] Bundesministerium für Digitales und Staatsmodernisierung. (2026). *Mehr als 60 Millionen Euro für smarte Konnektivität*. https://bmds.bund.de/aktuelles/pressemitteilungen/detail/mehr-als-60-millionen-euro-fuer-smarte-konnektivitaet

[68] Bundesministerium für Digitales und Staatsmodernisierung. (2026). *Neues Förderprogramm für digitale Technologien und Souveränität*. https://bmds.bund.de/aktuelles/pressemitteilungen/detail/neues-foerderprogramm-fuer-digitale-technologien-und-souveraenitaet

[69] Bundesministerium für Gesundheit. (2026). *Krankenhauszukunftsgesetz*. https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz

[70] Bundesministerium für Wirtschaft und Energie. (2026). *Digital Jetzt: Investitionszuschüsse für den Mittelstand*. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Dossier/digital-jetzt.html

[71] Bundesministerium für Wirtschaft und Klimaschutz. (2024). *Förderrichtlinie Zentrales Innovationsprogramm Mittelstand vom 28. November 2024, BAnz AT 11.12.2024 B1*. https://www.bundesanzeiger.de/pub/publication/H4hLAtOVVOn1N7yG6vR/content/H4hLAtOVVOn1N7yG6vR/BAnz%20AT%2011.12.2024%20B1.pdf?inline=

[72] Bundesnetzagentur. (2020). *Entscheidung der Präsidentenkammer vom 16. November 2020 über die Vergabe von Frequenzen im Bereich 450 MHz für den drahtlosen Netzzugang (Vergabe- und Ausschreibungsregeln), BK1-20/001*. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/450MHZ/Praesidentenkammerentscheidung450MHz.pdf?__blob=publicationFile&v=2

[73] Bundesnetzagentur. (2021). *Erfolgreiche Bewerbung der 450connect GmbH*. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20210309_450Mhz.html

[74] Bundesnetzagentur. (2023). *Festlegung BK6-22-300, Anlage 1: Netzorientierte Steuerung steuerbarer Verbrauchseinrichtungen*. https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-300/Beschluss/BK6-22-300_Beschluss_Anlage1.pdf

[75] Bundesnetzagentur. (2025). *Übersicht der Zuteilungsinhaber für Frequenzzuteilungen für lokale Frequenznutzungen im Frequenzbereich 3.700-3.800 MHz*. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/LokaleNetze/Zuteilungsinhaber3,7GHz.pdf

[76] Bundesnetzagentur. (2025). *Übersicht der Zuteilungsinhaber für lokale Frequenznutzungen im Frequenzbereich 24,25-27,5 GHz*. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/LokaleNetze/Zuteilungsinhaber26GHz.pdf

[77] Bundesnetzagentur. (2026). *2G-Abschaltung*. https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Breitband/2GAbschaltung/start.html

[78] Bundesnetzagentur. (2026). *Jahresbericht Telekommunikation 2025*. https://data.bundesnetzagentur.de/Bundesnetzagentur/SharedDocs/Mediathek/Jahresberichte/JB2025TK.pdf

[79] Bundesnetzagentur. (2026). *Pressemitteilung zu Netzentgelten nach § 14a EnWG*. https://bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2026/20260528_14a.html

[80] Bundesnetzagentur. (2026). *Regionale und lokale Netze*. https://www.bundesnetzagentur.de/lokalesbreitband

[81] Bundesverband der Deutschen Heizungsindustrie (BDH). (2026). *Absatz Heizungen 2025 in Deutschland: Marktentwicklung Wärmemarkt 2025*. https://www.bdh-industrie.de/fileadmin/user_upload/Downloads/PresseMeldungen/Absatzzahlen_Heizungen_Deutschland_2025.pdf

[82] CEN and CENELEC. (2026). *CEN and CENELEC Work Programme 2026: Digital society*. https://wp2026.cencenelec.eu/sectors-list/digital-society/

[83] CEN-CENELEC JTC 13. (2023). *EN 17927:2023 Security Evaluation Standard for IoT Platforms (SESIP)*. https://iteh.es/catalog/standards/cen/e545f156-f87b-4463-a711-9483b31a202d/en-17927-2023
[84] CEPT ECC. (2001). *ERC Decision (01)04 on non-specific short range devices*. https://docdb.cept.org/download/2369
[85] Council of the European Union. (2026). *Amending Protocol to the Agreement between the European Community and the Swiss Confederation on mutual recognition in relation to Conformity Assessment (Council document 10572/25, 11 February 2026; signed 2 March 2026, BBl 2026 619)*. https://data.consilium.europa.eu/doc/document/ST-10572-2025-INIT/en/pdf
[86] Cumulocity. (2025). *A new chapter for Cumulocity: building an AIoT powerhouse*. https://community.cumulocity.com/t/a-new-chapter-for-cumulocity-building-an-aiot-powerhouse/13692
[87] Cumulocity. (2026). *Cumulocity named a Visionary in the inaugural Gartner Magic Quadrant for Global Industrial AIoT Platforms*. https://www.cumulocity.com/press-releases/cumulocity-named-a-visionary-in-the-inaugural-gartner-magic-quadrant-for-global-industrial-aiot-platforms/
[88] Cumulocity GmbH. (2026). *Imprint*. https://cumulocity.com/docs/legal-notices/imprint/
[89] Cybeats Technologies. (2026). *Cybeats and Keysight partner to OEM Cybeats SBOM platform*. https://www.cybeats.com/news/cybeats-and-keysight-partner-to-oem-cybeats-sbom-platform-for-software-supply-chain-security
[90] Cybellum. (2026). *About Cybellum*. https://cybellum.com/about/
[91] Cybellum. (2026). *Contact us: Where to find us*. https://cybellum.com/contact/
[92] Decklar. (2026). *Roambee is now Decklar*. https://www.decklar.com/
[93] Deutsche Energie-Agentur (dena). (2025). *Factsheet CLS-Einheit*. https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2025/FS_CLS-Einheit.pdf
[94] Deutsche Telekom. (2020). *Deutsche Telekom launches LTE-M in Germany*. https://www.telekom.com/en/newsroom/latest-updates/media-information/2020/7/deutsche-telekom-launches-lte-m-in-germany
[95] Deutsche Telekom. (2025). *Nur bei der Telekom: Die neue Apple Watch funkt mit 5G*. https://www.telekom.com/de/newsroom/aktuelles/medieninformationen/2025/09/nur-bei-der-telekom-die-neue-apple-watch-funkt-mit-5g
[96] Deutsche Telekom. (2026). *IoT and M2M data plans: IoT Business Classic, LPWA and Data Best*. https://iot.telekom.com/en/iot-connectivity/iot-data-plans
[97] Deutsche Telekom. (2026). *IoT SIM cards: IoT Business Classic*. https://iot.telekom.com/en/iot-connectivity/iot-sim-cards
[98] Deutsche Telekom AG. (2026). *Annual Report 2025*. https://report.telekom.com/annual-report-2025/_assets/downloads/entire-dtag-ar25.pdf
[99] Deutsche Telekom IoT. (2026). *Deutsche Telekom IoT*. https://iot.telekom.com/en
[100] Deutscher Bundestag. (2026). *Gesetzentwurf der Bundesregierung zur Durchführung der Verordnung (EU) 2024/2847 (Cyber Resilience Act), Drucksache 21/6134*. https://dserver.bundestag.de/btd/21/061/2106134.pdf
[101] deutsche-startups.de. (2024). *Inspirierende Startups aus Düsseldorf*. https://www.deutsche-startups.de/2024/03/04/inspirierende-startups-aus-duesseldorf/
[102] Device Insight GmbH. (2026). *Über Device Insight*. https://device-insight.com/device-insight/
[103] DigiCert. (2024). *DigiCert completes acquisition of Vercara*. https://goldengatecap.com/digicert-completes-acquisition-of-vercara-acquisition-furthers-digicerts-position-as-a-leader-in-digital-trust/
[104] DigiCert. (2025). *DigiCert acquires Valimail*. https://www.digicert.com/news/digicert-acquires-valimail-global-leader-in-email-authentication
[105] DigiCert. (2026). *DigiCert Device Trust Manager*. https://www.digicert.com/device-trust-manager
[106] DigiKey. (2026). *Espressif ESP32-C6-WROOM-1-N8*. https://www.digikey.com/en/products/result?keywords=ESP32-C6-WROOM-1-N8
[107] DigiKey. (2026). *Infineon SLB9672VU20FW1523XTMA1*. https://www.digikey.com/en/products/result?keywords=SLB9672VU20FW1523XTMA1
[108] DigiKey. (2026). *Microchip ATECC608B-MAHDA-S and ATECC608B-TNGTLSS-B*. https://www.digikey.com/en/products/result?keywords=ATECC608B
[109] DigiKey. (2026). *Murata LBAA0QB1SJ-296 (Type 1SJ)*. https://www.digikey.com/en/products/result?keywords=LBAA0QB1SJ-296
[110] DigiKey. (2026). *Nordic Semiconductor NRF54L15-QFAA-R*. https://www.digikey.com/en/products/detail/nordic-semiconductor-asa/NRF54L15-QFAA-R/24773448
[111] DigiKey. (2026). *Nordic Semiconductor NRF9151-LACA-R7*. https://www.digikey.com/en/products/result?keywords=NRF9151-LACA-R7
[112] DigiKey. (2026). *NXP SE050C2HQ1/Z01SDZ*. https://www.digikey.com/en/products/result?keywords=SE050C2HQ1
[113] DigiKey. (2026). *Quectel EG915UEUAB-N05-SNNSA*. https://www.digikey.com/en/products/detail/quectel/EG915UEUAB-N05-SNNSA/21272504
[114] DigiKey. (2026). *STMicroelectronics STSAFA110DFSPL02*. https://www.digikey.com/en/products/result?keywords=STSAFA110

[115] DigiKey. (2026). *u-blox MAX-M10S-00B*. https://www.digikey.com/en/products/result?keywords=MAX-M10S-00B
[116] Digital Matter. (2026). *Oyster3: battery-powered GPS tracker*. https://www.digitalmatter.com/devices/oyster3/
[117] DIN. (2026). *EN IEC 62443-4-2:2019/prAA, amendment for citation under the CRA*. https://www.dinmedia.de/de/norm-entwurf/din-en-iec-62443-4-2-a1/
[118] Dragos. (2026). *Dragos acquires NetRise and runZero*. https://www.dragos.com/blog/dragos-acquires-netrise-runzero-xot-platform
[119] Eclipse Foundation. (2026). *Eclipse hawkBit*. https://projects.eclipse.org/projects/iot.hawkbit
[120] Ecma International. (2025). *ECMA-424: CycloneDX Bill of Materials Specification, 2nd edition*. https://ecma-international.org/publications-and-standards/standards/ecma-424/
[121] E-Control. (2026). *TOR Stromerzeugungsanlagen: Anschluss und Parallelbetrieb von Stromerzeugungsanlagen des Typs A und von Kleinsterzeugungsanlagen, Version 1.4*. https://www.e-control.at/documents/1785851/1811582/TOR+Stromerzeugungsanlagen+Typ+A+Version+1.4+(7).pdf/093752f5-e220-0731-b8a8-bfa85ccb7287?t=1780897058735
[122] EDAG Engineering Group AG. (2026). *EDAG Group: market uncertainty and delayed awarding of projects shape FY 2025*. https://live.deutsche-boerse.com/news/EQS-News-EDAG-Group-Market-uncertainty-and-delayed-awarding-of-projects-shape-FY-2025--Strategic-measures-accelerated-to-restore-sustainable-growth-and-competitiveness-bc5ff7b3-8c89-47a0-b416-f1bf55f3fcb9
[123] EEBus Initiative. (2024). *FAQs § 14a*. https://www.eebus.org/wp-content/uploads/2024/04/FAQs-%C2%A7-14a.pdf
[124] Eidgenössisches Departement für auswärtige Angelegenheiten (EDA). (2026). *Paket Schweiz-EU (Bilaterale III)*. https://www.europa.eda.admin.ch/de/paket-schweiz-eu
[125] Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF. (2025). *Totalrevision der Verordnung über die Sicherheit von Maschinen (MaschV): Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*. https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2025/44/cons_1/doc_3/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2025-44-cons_1-doc_3-de-pdf-a.pdf
[126] emnify. (2022). *emnify raises 50 million Series B*. https://www.emnify.com/blog/emnify-raises-50-million-series-b
[127] emnify. (2026). *emnify announces leadership transition*. https://www.emnify.com/blog/pr-emnify-announces-leadership-transition
[128] emnify. (2026). *emnify appoints Sacha Herrmann as CFO and Christian Friis as CRO*. https://www.emnify.com/blog/emnify-appoints-sacha-herrmann-cfo-christian-friis-cro
[129] emnify. (2026). *emnify introduces SGP.32 eSIM*. https://www.emnify.com/blog/emnify-introduces-sgp.32-esim
[130] emnify. (2026). *emnify named a Visionary in the 2026 Gartner Magic Quadrant for Managed IoT Connectivity Services, Worldwide*. https://www.emnify.com/blog/emnify-named-a-visionary-in-the-2026-gartner-magic-quadrant-for-managed-iot-connectivity-services-worldwide
[131] emteria GmbH. (2026). *emteria pricing*. https://emteria.com/pricing
[132] Energie-Control Austria (E-Control). (2025). *Bericht zur Einführung von intelligenten Messgeräten in Österreich 2025, Berichtsjahr 2024*. https://www.e-control.at/documents/1785851/1811582/20251020-Monitoringbericht-SM-2025.pdf/4ce4b22f-8149-5162-770a-83f132511199
[133] ENISA. (2026). *The CRA Single Reporting Platform is launched*. https://www.enisa.europa.eu/news/the-cra-single-reporting-platform-is-launched
[134] Ericsson. (2026). *Ericsson Mobility Report, June 2026: IoT connections outlook*. https://www.ericsson.com/en/mobility-report/dataforecasts/iot-connections-outlook
[135] ETSI. (2024). *ETSI EN 303 645 V3.1.3 (2024-09): Cyber Security for Consumer Internet of Things: Baseline Requirements*. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
[136] ETSI. (2026). *ETSI launches approval process for 17 European Standards supporting the Cyber Resilience Act*. https://www.etsi.org/newsroom/press-releases/etsi-launches-approval-process-for-17-european-standards-supporting-the-cyber-resilience-act/
[137] European Central Bank. (2026). *Euro foreign exchange reference rates, 15 October 2026*. https://www.ecb.europa.eu/stats/eurofxref/eurofxref-daily.xml
[138] European Commission. (2003). *Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises*. https://eur-lex.europa.eu/eli/reco/2003/361/oj
[139] European Commission. (2021). *Commission Implementing Regulation (EU) 2021/1228 amending Implementing Regulation (EU) 2016/799 as regards the requirements for smart tachographs (version 2)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1228
[140] European Commission. (2021). *Impact assessment accompanying Commission Delegated Regulation (EU) 2022/30 (Radio Equipment Directive, Article 3(3)(d), (e) and (f)), SWD(2021) 302 final*. https://publications.europa.eu/resource/cellar/bc0a31a7-38a0-11ec-8daf-01aa75ed71a1.0001.02/DOC_1
[141] European Commission. (2022). *Commission Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU (RED) with regard to cybersecurity*. https://eur-lex.europa.eu/eli/reg_del/2022/30/oj

[142] European Commission. (2022). *Executive summary of the impact assessment report, SWD(2022) 283 final*. https://ec.europa.eu/newsroom/dae/redirection/document/89553

[143] European Commission. (2022). *Impact assessment report accompanying the proposal for a Data Act, SWD(2022) 34 final*. https://publications.europa.eu/resource/cellar/490c2d61-961f-11ec-b4e4-01aa75ed71a1.0001.02/DOC_1

[144] European Commission. (2022). *Impact assessment report accompanying the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements, SWD(2022) 282 final*. https://ec.europa.eu/newsroom/dae/redirection/document/89545

[145] European Commission. (2023). *Commission Delegated Regulation (EU) 2023/2444 amending Delegated Regulation (EU) 2022/30 as regards the date of application*. https://eur-lex.europa.eu/eli/reg_del/2023/2444/oj

[146] European Commission. (2024). *Commission Delegated Regulation (EU) 2024/1180 amending Regulation (EU) 2015/758 as regards the standards relating to eCall*. https://eur-lex.europa.eu/eli/reg_del/2024/1180/oj

[147] European Commission. (2025). *Annexes to the Commission Implementing Decision on a standardisation request to CEN, Cenelec and ETSI as regards products with digital elements in support of Regulation (EU) 2024/2847, C(2025) 618 final, 3 February 2025 (M/606)*. https://ec.europa.eu/transparency/documents-register/api/files/C(2025)618_1/de00000001069729

[148] European Commission. (2025). *Commission Implementing Decision (EU) 2025/138 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards for cybersecurity of radio equipment*. http://data.europa.eu/eli/dec_impl/2025/138/oj

[149] European Commission. (2025). *Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847*. https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj

[150] European Commission. (2025). *Commission Notice C/2025/214: guidelines on Article 11 of Regulation (EU) 2023/1542*. https://eur-lex.europa.eu/eli/C/2025/214/oj/eng

[151] European Commission. (2025). *Cyber Resilience Act: standardisation*. https://digital-strategy.ec.europa.eu/en/policies/cra-standardisation

[152] European Commission. (2025). *European Digital Innovation Hubs*. https://digital-strategy.ec.europa.eu/en/activities/edihs

[153] European Commission. (2025). *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final*. http://publications.europa.eu/resource/cellar/ebf17714-c56e-11f0-8da2-01aa75ed71a1.0001.02/DOC_1

[154] European Commission. (2026). *Commission Delegated Regulation (EU) 2026/339 of 16 February 2026 repealing Delegated Regulation (EU) 2022/30 (OJ L, 2026/339, 29.4.2026)*. https://eur-lex.europa.eu/eli/reg_del/2026/339/oj

[155] European Commission. (2026). *Commission Implementing Decision (EU) 2026/2015 of 4 September 2026 amending and repealing Implementing Decision (EU) 2023/1586 as regards harmonised standards for machinery drafted in support of Directive 2006/42/EC*. https://eur-lex.europa.eu/eli/dec_impl/2026/2015/oj

[156] European Commission. (2026). *Cyber Resilience Act - Reporting obligations (last update 11 September 2026)*. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

[157] European Commission. (2026). *Cyber Resilience Act: conformity assessment*. https://digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment

[158] European Commission. (2026). *Frequently asked questions on the Data Act, version 1.4*. https://ec.europa.eu/newsroom/dae/redirection/document/108144

[159] European Commission. (2026). *Harmonised standards: Machinery (MD)*. https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/harmonised-standards/machinery-md_en

[160] European Commission. (2026). *NANDO: notified bodies under Directive 2014/53/EU (RED) and Regulation (EU) 2023/1230 (Machinery)*. https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

[161] European Commission. (2026). *NANDO: Regulation (EU) 2024/2847 (Cyber Resilience Act), notifications and notifying authorities*. https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/notifying-authorities?filter=legislationId:167953

[162] European Commission. (2026). *NANDO: SGS FIMKO OY, NB 0598, notification under Directive 2014/53/EU (notification 1024166) and Regulation (EU) 2023/1230 (notification 1024508)*. https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/notifications/1024166

[163] European Commission, DG MOVE. (2025). *Stronger and more unified enforcement of EU rules in international road transport with the smart tachograph*. https://transport.ec.europa.eu/news-events/news/stronger-and-more-unified-enforcement-eu-rules-international-road-transport-smart-tachograph-2025-08-19_en

[164] European Labour Authority. (2026). *Driving and rest rules and compulsory tachographs apply to light commercial vehicles in cross-border transport*. https://www.ela.europa.eu/en/news/driving-and-rest-rules-and-compulsory-tachographs-apply-light-commercial-vehicles-cross-border

[165] European Parliament and Council. (2019). *Regulation (EU) 2019/1020 on market surveillance and compliance of products*. https://eur-lex.europa.eu/eli/reg/2019/1020/oj

[166] European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[167] European Parliament and Council. (2023). *Corrigendum to Regulation (EU) 2023/1230 on machinery (OJ L 169, 4.7.2023, p. 35): application dates corrected to 20 January 2027 and 20 January 2024*. https://eur-lex.europa.eu/eli/reg/2023/1230/corrigendum/2023-07-04/oj

[168] European Parliament and Council. (2023). *Regulation (EU) 2023/1230 on machinery (Machinery Regulation)*. https://eur-lex.europa.eu/eli/reg/2023/1230/oj

[169] European Parliament and Council. (2023). *Regulation (EU) 2023/1542 concerning batteries and waste batteries (battery passport)*. https://eur-lex.europa.eu/eli/reg/2023/1542/oj

[170] European Parliament and Council. (2023). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[171] European Parliament and Council. (2024). *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[172] European Parliament and Council of the European Union. (2020). *Regulation (EU) 2020/1054 amending Regulation (EC) No 561/2006 and Regulation (EU) No 165/2014 (Mobility Package I: driving times and tachographs)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020R1054

[173] European Parliament and Council of the European Union. (2024). *Regulation (EU) No 165/2014 on tachographs in road transport, consolidated text of 31 December 2024*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014R0165-20241231

[174] European Parliament, Legislative Observatory. (2026). *Procedure file 2025/0360(COD): Simplification of the digital legislative framework, Digital Omnibus (Omnibus VII)*. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/0360(COD)

[175] Eurostat. (2026). *Enterprise statistics by size class and NACE Rev. 2 activity (from 2021 onwards), dataset sbs_sc_ovw*. https://ec.europa.eu/eurostat/databrowser/view/sbs_sc_ovw/default/table

[176] EUSPA. (2025). *From testing to operations: Galileo OSNMA service now available to users*. https://www.euspa.europa.eu/newsroom-events/news/testing-operations-galileo-osnma-service-now-available-users

[177] Exein. (2025). *Exein raises €100M to accelerate its global expansion*. https://exein.io/blog/exein-raises-100m-funding-to-accelerate-its-global-expansion

[178] Exein. (2025). *Exein raises €70M Series C to secure IoT devices*. https://exein.io/blog/exein-raises-70m-series-c-to-secure-iot-devices

[179] Exein. (2026). *Exein partners with Deutsche Telekom IoT*. https://exein.io/blog/exein-partners-with-deutsche-telekom-iot-to-secure-the-next-generation-of-connected-devices

[180] Exein. (2026). *Exein raises $270M at $1.7bn valuation*. https://exein.io/blog/exein-raises-270m-at-1-7bn-valuation-to-build-the-security-layer-for-physical-ai

[181] Fachverband der Elektro- und Elektronikindustrie (FEEI). (2026). *Zahlen, Daten, Fakten 2026: Die Elektro- und Elektronikindustrie in Österreich*. https://www.feei.at/wp-content/uploads/2026/07/feei-zahlen-daten-fakten-folder-2026.pdf

[182] Fachverband Metalltechnische Industrie (FMTI). (2026). *Jahreszahlen MTI 2025 (vorläufig)*. https://www.metalltechnischeindustrie.at/fileadmin/content/Dokumente/Zahlen_Daten_Fakten/Metalltechnische_Industrie_Jahr_2025vorl.pdf

[183] FERCHAU GmbH. (2026). *Wer wir sind*. https://www.ferchau.com/de/de/ueber-uns/wer-wir-sind

[184] Finite State. (2024). *Finite State acquires MergeBase*. https://finitestate.io/news/finite-state-acquires-mergebase-to-form-a-powerhouse-in-application-security

[185] Finite State. (2024). *Finite State raises $20 million growth round*. https://finitestate.io/news/finite-state-raises-20-million-growth-round

[186] firmenauto. (2026). *Würth: Vernetzter Transporter erkennt Werkzeug*. https://www.firmenauto.de/fahrzeuge/transporter/wuerth-w-connect-vernetzte-fahrzeugeinrichtung-iaa-transportation-2026/

[187] FOSSA. (2024). *FOSSA acquires StackShare*. https://fossa.com/blog/fossa-acquires-stackshare-enhance-developer-tools-management-security/

[188] FOSSA. (2025). *FOSSA acquires EdgeBit*. https://fossa.com/blog/fossa-acquires-edgebit/

[189] FOSSA. (2026). *FOSSA pricing*. https://fossa.com/pricing/

[190] Fraunhofer-Institut für System- und Innovationsforschung ISI. (2020). *Digitale Plattformen im Verarbeitenden Gewerbe (Mitteilungen aus der ISI-Erhebung Modernisierung der Produktion, Nr. 77)*. https://www.isi.fraunhofer.de/content/dam/isi/dokumente/modernisierung-produktion/erhebung2018/PI_77_B2B_Plattformoekonomie.pdf

[191] Giesecke+Devrient. (2026). *Facts and figures*. https://www.gi-de.com/en/about-us/company/facts

[192] Ginzinger electronic systems GmbH. (2026). *Connectivity & Security*. https://www.ginzinger.com/en/technologies/connectivity-security/

[193] Ginzinger electronic systems GmbH. (2026). *Über uns*. https://www.ginzinger.com/de/ginzinger-als-partner-wie-laeuft-ein-projekt-mit-uns-ab/ueber-uns/
[194] GlobalPlatform. (2025). *PSA Certified now available with GlobalPlatform's SESIP evaluation methodology*. https://globalplatform.org/psa-certified-now-available-with-globalplatforms-sesip-evaluation-methodology/
[195] GlobalSign. (2026). *IoT Identity Platform*. https://www.globalsign.com/en/internet-of-things/iot-identity-platform
[196] GMO GlobalSign Holdings. (2026). *GMO GlobalSign Holdings: company summary and financial highlights*. https://www.gmogshd.com/english/aboutus/summary/
[197] Golioth. (2023). *Golioth raises $4.6M seed round*. https://blog.golioth.io/may-2023-golioth-seed-round/
[198] Golioth. (2026). *Golioth is now a part of Canonical*. https://blog.golioth.io/golioth-is-now-a-part-of-canonical/
[199] Golioth. (2026). *Golioth pricing*. https://golioth.io/pricing
[200] Golioth. (2026). *Zephyr 26.04 LTS: up to 15 years of support with Golioth OTA built in*. https://blog.golioth.io/zephyr-26-04-lts-up-to-15-years-of-support-with-golioth-ota-built-in/
[201] Google. (2023). *python-iot: Cloud IoT Core client library (archived)*. https://github.com/googleapis/python-iot
[202] GSMA. (2026). *SGP.32 eSIM IoT Technical Specification*. https://www.gsma.com/solutions-and-impact/technologies/esim/esim-specification/
[203] Hamburgische Investitions- und Förderbank. (2026). *Hamburg Digital Check*. https://www.ifbhh.de/foerderprogramm/hamburg-digital-check
[204] Hamburgische Investitions- und Förderbank. (2026). *Hamburg-Kredit Digital: Produktinformation, gültig ab 15. April 2026*. https://www.ifbhh.de/resource/blob/1568/8d055a13d38153a13f01b83c3338db77/produktinformation-hamburg-kredit-digital-data.pdf
[205] Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen. (2026). *Merkblatt zum Förderprogramm Zuschuss zu Digitalisierungsmaßnahmen (DIGI-Zuschuss), Stand 10.04.2026*. https://www.wibank.de/resource/blob/wibank/464736/8c4d12698c41d88849d95ae7efa14f08/download-merkblatt-digitalisierungsmassnahmen-data.pdf
[206] Hilti. (2026). *Hilti Group 2025 business result*. https://www.hilti.group/content/hilti/CP/XX/en/company/media-relations/media-releases/2025-business-result.html
[207] Hilti Deutschland. (2026). *ON!Track Asset Management*. https://www.hilti.de/content/hilti/E3/DE/de/services/tool-services/on-track.html
[208] IEC. (2018). *IEC 62443-4-1:2018 Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements*. https://webstore.iec.ch/en/publication/33615
[209] IEC. (2019). *IEC 62443-4-2:2019 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components*. https://webstore.iec.ch/en/publication/34421
[210] IEC. (2023). *IEC 63278-1:2023 Asset Administration Shell for industrial applications, Part 1: Asset Administration Shell structure*. https://webstore.iec.ch/en/publication/65628
[211] IEC. (2025). *IEC 62541-1:2025 OPC Unified Architecture, Part 1: Overview and concepts*. https://webstore.iec.ch/en/publication/81513
[212] IETF. (2013). *RFC 7030: Enrollment over Secure Transport*. https://www.rfc-editor.org/info/rfc7030
[213] IETF. (2021). *RFC 8995: Bootstrapping Remote Secure Key Infrastructure (BRSKI)*. https://www.rfc-editor.org/info/rfc8995
[214] IETF. (2021). *RFC 9019: A Firmware Update Architecture for Internet of Things*. https://www.rfc-editor.org/rfc/rfc9019
[215] IETF. (2022). *RFC 9124: A Manifest Information Model for Firmware Updates in Internet of Things Devices*. https://www.rfc-editor.org/rfc/rfc9124
[216] Industrial Digital Twin Association. (2026). *AAS specifications, Release 26-01*. https://industrialdigitaltwin.org/en/content-hub/aasspecifications
[217] Infineon Technologies. (2026). *OPTIGA Trust M*. https://www.infineon.com/OPTIGA-Trust-M
[218] Infineon Technologies. (2026). *OPTIGA Trust M Express*. https://infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-trust/optiga-trust-m-express
[219] Infineon Technologies AG. (2025). *Annual Report 2025*. https://www.infineon.com/row/public/documents/corporate/investors/annual-reports/2025/2025-annual-report-v01-00-en.pdf
[220] ingenieur.de. (2026). *CRA-Meldepflicht: wann die Frist beginnt*. https://www.ingenieur.de/technik/fachbereiche/ittk/cra-meldepflicht-wann-die-frist-beginnt/
[221] Innosuisse. (2025). *Auswirkungen des Entlastungspakets 2027 auf Innosuisse*. https://www.innosuisse.admin.ch/de/auswirkungen-entlastungspaket
[222] Innosuisse. (2026). *Innovation cheque*. https://www.innosuisse.admin.ch/en/innovation-cheque
[223] Innosuisse. (2026). *Innovation project with implementation partner*. https://www.innosuisse.admin.ch/en/innovation-project-with-implementation-partner
[224] Innosuisse. (2026). *Start-up innovation projects*. https://www.innosuisse.admin.ch/en/start-up-innovation-projects
[225] Innosuisse. (2026). *Swiss Accelerator innovation projects*. https://www.innosuisse.admin.ch/en/swiss-accelerator-innovation-projects

[226] Investitions- und Strukturbank Rheinland-Pfalz. (2026). *358 Einzelbetriebliches Innovations- und Technologieförderungsprogramm (InnoTop) im Rahmen des EFRE 2021-2027*. https://isb.rlp.de/foerderung/358.html

[227] Investitions- und Strukturbank Rheinland-Pfalz. (2026). *Landesförderprogramm im Rahmen des EFRE 2021-2027 "Implementierung betrieblicher Innovationen" (IBI-EFRE)*. https://isb.rlp.de/foerderung/361

[228] Investitions- und Strukturbank Rheinland-Pfalz. (2026). *Wirtschaft: Innovation und Digitalisierung, Programmübersicht*. https://isb.rlp.de/wirtschaft/innovation-digitalisierung.html

[229] Investitionsbank Berlin. (2026). *Digitalprämie Berlin*. https://www.ibb.de/de/foerderprogramme/digitalpraemie-berlin.html

[230] JFrog. (2021). *JFrog to acquire Vdoo*. https://jfrog.com/blog/jfrog-to-acquire-vdoo/

[231] Keyfactor. (2025). *Keyfactor acquires InfoSec Global and CipherInsights*. https://www.keyfactor.com/press-releases/keyfactor-acquires-infosec-global-and-cipherinsights/

[232] Keyfactor. (2026). *EJBCA Enterprise*. https://www.keyfactor.com/products/ejbca-enterprise/

[233] Keyfactor. (2026). *Keyfactor announces $1B strategic growth investment led by Summit Partners*. https://www.keyfactor.com/press-releases/keyfactor-announces-1b-strategic-growth-investment-led-by-summit-partners-to-expand-leadership-in-securing-the-ai-and-post-quantum-enterprise/

[234] Keyfactor. (2026). *Keyfactor exceeds $200 million in ARR*. https://www.keyfactor.com/press-releases/keyfactor-exceeds-200-million-in-arr-as-global-demand-for-digital-trust-infrastructure-accelerates/

[235] KfW. (2025). *New ERP promotional loans for innovation and digitalisation*. https://www.kfw.de/About-KfW/Newsroom/Latest-News/Pressemitteilungen-Details_855872.html

[236] KfW. (2026). *ERP-Digitalisierungs- und Innovationskredit (380, 390, 391)*. https://www.kfw.de/inlandsfoerderung/Unternehmen/Innovation/F%C3%B6rderprodukte/ERP-Digitalisierungs-und-Innovationskredit-(380-390-391)/

[237] KfW. (2026). *ERP-Förderkredit Digitalisierung (511, 512)*. https://www.kfw.de/inlandsfoerderung/Unternehmen/Innovation-und-Digitalisierung/F%C3%B6rderprodukte/ERP-F%C3%B6rderkredit-Digitalisierung-(511-512)/

[238] KfW. (2026). *ERP-Förderkredit Innovation (513, 514)*. https://www.kfw.de/inlandsfoerderung/Unternehmen/Innovation-und-Digitalisierung/F%C3%B6rderprodukte/ERP-F%C3%B6rderkredit-Innovation-(513-514)/

[239] KfW. (2026). *Konditionenübersicht für Endkreditnehmer in den Förderprogrammen der KfW: ERP-Förderkredit Digitalisierung (511, 512) und Innovation (513, 514)*. https://www.kfw-formularsammlung.de/KonditionenanzeigerINet/KonditionenAnzeiger

[240] Kizy. (2026). *www.kizy.com*. https://www.kizy.com/

[241] Kontron. (2026). *KontronOS: secure operating system for edge devices*. https://www.kontron.com/en/products-solutions/susietec/kontronos-secure-operating-system-for-edge-devices

[242] Kontron AG. (2026). *Kontron AG significantly expands profitability, record operating cash flow*. https://www.kontron.com/en/media/news/kontron-ag-significantly-expands-profitability-record-operating-cashflow?eqs=259108011

[243] Kontron AG. (2026). *Kontron AG: all conditions of the mandatory tender offer of Ennoconn Corporation are met*. https://www.kontron.com/en/media/news/kontron-ag-all-conditions-of-the-mandatory-tender-offer-of-ennoconn-corporation-are-met-settlement-will-take-place-shortly?eqs=1035566611

[244] Kudelski Group. (2024). *Kudelski Group closes sale of SKIDATA to ASSA ABLOY*. https://www.nagra.com/kudelski-group-closes-sale-skidata-assa-abloy

[245] Kudelski Group. (2024). *Silicon Labs and Kudelski IoT partner to accelerate Matter device certification*. https://www.nagra.com/silicon-labs-and-kudelski-iot-partner-accelerate-matter-device-certification

[246] Kudelski Group. (2026). *Kudelski Group 2025 annual results*. https://www.nagra.com/2025-annual-results

[247] Kudelski Group. (2026). *Kudelski Group 2026 half-year results*. https://www.nagra.com/2026-half-year-results

[248] Kudelski Group. (2026). *Report on non-financial matters 2025*. https://www.nagra.com/sites/default/files/2026-03/Report_on_Nonfinancial_Matters_2025_A3.pdf

[249] Kurrant. (2025). *IoT platform Cumulocity reclaims independence*. https://www.kurrant.com/kurrantly-news/iot-platform-cumulocity-reclaims-independence/

[250] L-Bank. (2025). *Digitalisierungsprämie Plus - Zuschussvariante*. https://www.l-bank.de/produkte/finanzhilfen/digiplus-zuschuss.html

[251] L-Bank. (2026). *Digitalisierungsfinanzierung*. https://www.l-bank.de/produkte/wirtschaftsfoerderung/digitalisierungsfinanzierung.html

[252] LG Electronics. (2021). *LG to acquire majority stake in Cybellum*. https://www.lg.com/global/mobility/media-center/press-release/20210923-company-lg-cybellum-vehicle-solution-provider

[253] Linux Foundation SPDX. (2024). *SPDX overview and release history*. https://spdx.dev/about/overview/

[254] LoRa Alliance. (2021). *LoRaWAN approved as ITU-T Recommendation Y.4480*. https://lora-alliance.org/?p=219640

[255] LoRa Alliance. (2026). *Netze BW: largest LoRaWAN deployment in Germany*. https://lora-alliance.org/?p=598

[256] Magenta Telekom. (2024). *Entgeltbestimmungen IoT-Tarife (IoT Tarif 5, IoT Tarif 10)*. https://www.rtr.at/files/staging/tk_agb/147B1AE9E933B9D5C1258B790031F35C_RAGB_344_2024.pdf

[257] Marvell Technology. (2025). *Marvell completes sale of its Automotive Ethernet business to Infineon Technologies*. https://www.sec.gov/Archives/edgar/data/1835632/000119312525180425/d96358dex991.htm
[258] MCUboot project. (2026). *MCUboot documentation*. https://docs.mcuboot.com/
[259] Memfault. (2023). *Memfault raises $24 million in Series B funding*. https://memfault.com/news/memfault-raises-24-million-in-series-b-funding-supercharge-iot-reliability-platform/
[260] Memfault. (2026). *Memfault pricing*. https://memfault.com/pricing/
[261] Microchip Technology. (2020). *Microchip TA100 automotive secure element*. https://www.microchip.com/en-us/product/TA100
[262] Microchip Technology. (2026). *Annual report on Form 10-K for the fiscal year ended 31 March 2026*. https://www.sec.gov/Archives/edgar/data/827054/000082705426000016/mchp-20260331.htm
[263] Microchip Technology. (2026). *Trust Platform for the CryptoAuthentication family: Trust&GO, TrustFLEX, TrustCUSTOM*. https://onlinedocs.microchip.com/oxy/GUID-5C346303-A9CB-4341-B67F-4354AB92FE04-en-US-3/GUID-67185155-9838-416B-8F46-33923D075394.html
[264] Microsoft. (2026). *Azure IoT Central is evolving: what you need to know*. https://techcommunity.microsoft.com/blog/iotblog/azure-iot-central-is-evolving-what-you-need-to-know/4554570
[265] Microsoft. (2026). *Azure IoT Edge: lifecycle*. https://learn.microsoft.com/en-us/lifecycle/products/azure-iot-edge
[266] Microsoft. (2026). *Azure IoT Hub and Device Update for IoT Hub retail prices*. https://azure.microsoft.com/en-us/pricing/details/iot-hub/
[267] Microsoft. (2026). *Device Update for IoT Hub*. https://learn.microsoft.com/en-us/azure/iot-hub-device-update/understand-device-update
[268] Microsoft. (2026). *What is Azure IoT Hub Device Provisioning Service?* https://learn.microsoft.com/en-us/azure/iot-dps/about-iot-dps
[269] Microsoft. (2026). *What is Azure IoT Operations?* https://learn.microsoft.com/en-us/azure/iot-operations/overview-iot-operations
[270] Milwaukee Tool. (2026). *ONE-KEY: tool and equipment management*. https://onekey.milwaukeetool.com/
[271] Minew Technologies. (2026). *Minew Store: asset tracker category (E8, MTB07, MTB04, LTB01-G)*. https://www.minewstore.com/product-category/asset-tracker
[272] Minew Technologies. (2026). *UWB technology: MBM01 and MBS02 location beacons*. https://www.minew.com/uwb-technology/
[273] Ministerium für Wirtschaft, Verkehr, Arbeit, Technologie und Tourismus des Landes Schleswig-Holstein. (2026). *Richtlinie des Landes Schleswig-Holstein zur Förderung von Digitalisierungsmaßnahmen in kleinen Unternehmen (DKU), Bekanntmachung vom 5. März 2026, Amtsblatt für Schleswig-Holstein Nr. 2026/190 vom 5. Juni 2026*. https://verkuendungsportal.schleswig-holstein.de/home/amtsblatt/ab_veroeffentlichungen/2026/06_2026/2026-190.pdf?__blob=publicationFile&v=1
[274] Myriota. (2026). *Myriota enquiries: satellite data plans*. https://myriota.com/enquiries
[275] Myriota. (2026). *Myriota: HyperPulse, UltraLite, AssetHawk*. https://myriota.com/
[276] National Institute of Standards and Technology. (2023). *Cryptographic Module Validation Program, certificate 4421: Microchip Trust Anchor TA100*. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4421
[277] National Institute of Standards and Technology. (2026). *Cryptographic Module Validation Program, certificate 5371: Microchip Trust Anchor TA101*. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5371
[278] National Institute of Standards and Technology. (2026). *FIPS 140-3 Transition Effort*. https://csrc.nist.gov/projects/fips-140-3-transition-effort
[279] Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung. (2026). *DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME*. https://nkcs.bund.de/de/foerderprogramme/DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME
[280] Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung. (2026). *DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG*. https://nkcs.bund.de/de/foerderprogramme/DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG
[281] Nationales Koordinierungszentrum für Cybersicherheit (NKCS). (2026). *Förderprogramme: Aktuelle Ausschreibungen*. https://www.nkcs.bund.de/de/foerderprogramme
[282] NBank. (2026). *Digitalbonus.Niedersachsen-innovativ (ausgelaufen)*. https://www.nbank.de/F%C3%B6rderprogramme/Ausgelaufene-F%C3%B6rderungen/Digitalbonus.Niedersachsen-innovativ-(ausgelaufen).html
[283] Netzwoche. (2024). *Zühlke wächst weiter*. https://www.netzwoche.ch/news/2024-04-24/zuehlke-waechst-weiter
[284] Nordic Semiconductor. (2024). *nRF9151 Product Specification v1.0*. https://mm.digikey.com/Volume0/opasdata/d220001/medias/docus/6470/NRF9151-DK.pdf
[285] Nordic Semiconductor. (2025). *Nordic launches full device observability and OTA capabilities via nRF Cloud by Memfault*. https://www.nordicsemi.com/Nordic-news/2025/09/Nordic-launches-full-device-observability-and-OTA-capabilities-via-nRF-Cloud-by-Memfault

[286] Nordic Semiconductor. (2025). *Nordic Semiconductor acquires Memfault, launches the first complete chip-to-cloud platform*. https://www.nordicsemi.com/Nordic-news/2025/06/Nordic-Semiconductor-acquires-Memfault
[287] Nordic Semiconductor. (2026). *nRF Cloud Location Services*. https://docs.nrfcloud.com/docs/platform/location-services
[288] Nordic Semiconductor. (2026). *nRF9151*. https://www.nordicsemi.com/Products/nRF9151
[289] Northern.tech. (2024). *Northern.tech integrates Mender over-the-air updates with NVIDIA Jetson Platform Services*. https://www.prnewswire.com/news-releases/northerntech-accelerates-ai-iot-products-integrating-mender-over-the-air-ota-updates-with-nvidia-jetson-platform-services-jps-302229660.html
[290] Northern.tech. (2026). *About Northern.tech*. https://northern.tech/about-us
[291] Northern.tech. (2026). *Mender by Northern.tech extends over-the-air update management to microcontrollers (MCUs)*. https://www.prnewswire.com/news-releases/mender-by-northerntech-extends-industry-leading-ota-update-management-to-microcontrollers-mcus-302769349.html
[292] Northern.tech. (2026). *Mender pricing*. https://mender.io/pricing
[293] Noser Group. (2026). *Noser Group*. https://www.noser.com/firma/noser-group/
[294] NRW.BANK. (2026). *Mittelstand Innovativ & Digital (MID)*. https://www.nrwbank.de/mid
[295] NXP Semiconductors. (2024). *Protecting the Edge at scale with NXP Security Solutions*. https://www.nxp.com/docs/en/training-presentation/NXP-Security-Solutions-Protecting-the-Edge-at-scale-Technology-Six-Pack.pdf
[296] NXP Semiconductors. (2026). *EdgeLock 2GO service platform*. https://www.nxp.com/products/security-and-authentication/authentication/edgelock-2go:EDGELOCK-2GO
[297] NXP Semiconductors. (2026). *EdgeLock SE050 Plug and Trust secure element family*. https://www.nxp.com/products/SE050
[298] NXP Semiconductors. (2026). *EdgeLock SE051 Plug and Trust secure element*. https://www.nxp.com/products/SE051
[299] NXP Semiconductors N.V. (2026). *Annual report on Form 10-K for the fiscal year ended 31 December 2025*. https://www.sec.gov/Archives/edgar/data/1413447/000141344726000008/nxpi-20251231.htm
[300] o2 Telefónica. (2025). *Mobilfunk über Satelliten: Startschuss für den ersten o2 Business Satellite IoT Tarif*. https://hilfe.o2online.de/o2-news-3/mobilfunk-ueber-satelliten-startschuss-fuer-den-ersten-o2-business-satellite-lot-tarif-649729
[301] OASIS. (2019). *MQTT Version 5.0*. https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html
[302] OASIS. (2022). *Common Security Advisory Framework Version 2.0*. https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
[303] OASIS. (2026). *Common Security Advisory Framework Version 2.1, Committee Specification Draft 03*. https://docs.oasis-open.org/csaf/csaf/v2.1/csaf-v2.1.html
[304] ONEKEY GmbH. (2024). *ESCRYPT CycurRISK meets ONEKEY: a joint solution for effective vulnerability management in software-defined vehicles*. https://www.onekey.com/press-release/escrypt-cycurrisk-meets-onekey-a-joint-solution-for-effective-vulnerability-management-in-software-defined-vehicles
[305] ONEKEY GmbH. (2026). *About ONEKEY*. https://www.onekey.com/about-us
[306] ONEKEY GmbH. (2026). *Imprint*. https://www.onekey.com/imprint
[307] ONEKEY GmbH. (2026). *IoT & OT Cybersecurity Report 2026*. https://www.onekey.com/resource/onekey-iot-ot-cybersecurity-report-2026
[308] ONEKEY GmbH. (2026). *ONEKEY product cybersecurity and compliance platform*. https://www.onekey.com/
[309] Onomondo. (2026). *Onomondo announces majority investment from Aspirity Partners*. https://onomondo.com/blog/onomondo-announces-majority-investment-from-aspirity-partners-to-scale-global-iot/
[310] Onomondo. (2026). *Onomondo pricing*. https://onomondo.com/pricing/
[311] Onomondo, & Berg Insight. (2025). *Asset Tracking in Transport and Logistics (analyst report by Berg Insight)*. https://iot-now.com/app/uploads/2025/10/BergInsight-AssetTrackingReport.pdf
[312] OPC Foundation. (2025). *OPC 10000-14: OPC UA Part 14 PubSub, v1.05.06*. https://reference.opcfoundation.org/Core/Part14/v105/docs/7.3.4
[313] Österreichische Forschungsförderungsgesellschaft. (2026). *Basisprogramm 2026*. https://www.ffg.at/ausschreibung/basisprogramm-2026
[314] Österreichische Forschungsförderungsgesellschaft. (2026). *DACH Cooperation on Transportation Infrastructure Research: Call for Proposals 2026*. https://www.ffg.at/en/dach-call2026
[315] Österreichische Forschungsförderungsgesellschaft. (2026). *Forschungsprämie*. https://www.ffg.at/forschungspraemie
[316] Österreichische Forschungsförderungsgesellschaft. (2026). *General Programme (Basisprogramm)*. https://www.ffg.at/en/programme/general-programme
[317] Österreichische Forschungsförderungsgesellschaft. (2026). *KIRAS Sicherheitsforschung*. https://www.ffg.at/kiras
[318] Österreichische Forschungsförderungsgesellschaft. (2026). *Kleinprojekt*. https://www.ffg.at/kleinprojekt

[319] Österreichische Forschungsförderungsgesellschaft. (2026). *NCC-AT: Nationales Koordinierungszentrum für Cybersicherheit*. https://www.ffg.at/europa/ncc
[320] Österreichische Forschungsförderungsgesellschaft. (2026). *Projekt.Start*. https://www.ffg.at/projektstart
[321] OWASP Foundation. (2026). *OWASP Dependency-Track*. https://owasp.org/www-project-dependency-track/
[322] PAJ GPS. (2026). *PAJ GPS: GPS-Tracker und Abo-Preise*. https://www.paj-gps.de/
[323] Parlament Österreich. (2025). *Nationalrat: Elektrizitätswirtschaftsgesetz erhält mit Zustimmung der Grünen notwendige Verfassungsmehrheit (PK Nr. 1179)*. https://www.parlament.gv.at/aktuelles/pk/jahr_2025/pk1179
[324] Plattner, G. (2021). *Baustellendiebstahl in Österreich*. Kuratorium für Verkehrssicherheit (KFV). https://web.archive.org/web/20241010195437/https://www.kfv.at/wp-content/uploads/2022/04/Langbericht-Baustellendiebstahl_HP_04.pdf
[325] PSA Certified. (2026). *Getting certified: security levels*. https://www.psacertified.org/getting-certified/
[326] PSA Certified. (2026). *PSA Certified products database*. https://products.psacertified.org/
[327] PTC. (2026). *PTC third fiscal quarter 2026 results*. https://s27.q4cdn.com/610238322/files/doc_earnings/2026/q3/earnings-result/Q32026_PTC_Earnings-release.pdf
[328] PTC Inc. (2025). *Annual Report on Form 10-K for the fiscal year ended September 30, 2025*. https://www.sec.gov/Archives/edgar/data/857005/000119312525291326/ptc-20250930.htm
[329] Publications Office of the European Union. (2026). *TED: Tenders Electronic Daily, notice search*. https://ted.europa.eu/
[330] PwC Deutschland. (2026). *Product Security Survey 2026: Digital vernetzt, aber auch sicher?* https://www.pwc.de/de/cyber-security/product-cyber-security/pwc-product-security-survey-2026.html
[331] PwC Deutschland. (2026). *Trotz Meldepflichten: Nur 3 % der deutschen Industrieunternehmen sind vollständig auf EU Cyber Resilience Act vorbereitet*. https://www.pwc.de/de/pressemitteilungen/2026/nur-3-prozent-der-deutschen-industrieunternehmen-sind-vollstaendig-auf-eu-cyber-resilience-act-vorbereitet.html
[332] querdenker engineering GmbH. (2026). *qdCloud: overview*. https://querdenkerengineering.de/en/products/qd-cloud/overview
[333] RAKwireless. (2026). *RAK2270 Sticker Tracker*. https://store.rakwireless.com/products/rak2270-rak-sticker-tracker
[334] Republik Österreich, Rechtsinformationssystem des Bundes (RIS). (2025). *Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026), BGBl. I Nr. 94/2025*. https://ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273913/NOR40273913.pdf
[335] Republik Österreich, Rechtsinformationssystem des Bundes (RIS). (2026). *Elektrizitätswirtschaftsgesetz (ElWG), BGBl. I Nr. 91/2025, Fassung vom 15.10.2026*. https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013066
[336] Robert Bosch Power Tools GmbH. (2026). *PRO GCY 42 Bluetooth-Modul (1 600 A01 6NH)*. https://www.bosch-professional.com/de/de/products/gcy-42-1600A016NH
[337] Rundfunk und Telekom Regulierungs-GmbH (RTR). (2024). *RTR Telekom Monitor Jahresbericht 2023*. https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/m/tm/RTR_Telekom_Monitor_Jahresbericht-2023.pdf
[338] Rundfunk und Telekom Regulierungs-GmbH (RTR). (2026). *RTR Telekom Monitor Jahresbericht 2025*. https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/m/tm/RTR_Telekom_Monitor_Jahresbericht-2025_ua.pdf
[339] Sächsische Aufbaubank. (2026). *Digitalisierungsdarlehen (Digi-D)*. https://www.sab.sachsen.de/digitalisierungsdarlehen-digi-d-
[340] Saft. (2026). *LS 17500 primary lithium-thionyl chloride A-size cell, data sheet*. https://saft4u.saft.com/en/download_file/6fbdd60f-bba6-4f67-81a0-85ce1b412664/English
[341] Saft. (2026). *LS 33600 primary lithium-thionyl chloride D-size cell, data sheet*. https://saft4u.saft.com/en/download_file/5241def1-8668-4a68-9d2e-820bd3c68589/English
[342] Schweizerische Bundeskanzlei. (2026). *Vernehmlassung: Totalrevision der Maschinenverordnung (MaschV), Projekt 2025/44 (Frist 19. Dezember 2025)*. https://www.fedlex.admin.ch/eli/dl/proj/2025/44/cons_1/de
[343] Schweizerische Eidgenossenschaft. (2026). *Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen, SR 0.946.526.81, Fassung vom 22. Dezember 2017*. https://www.fedlex.admin.ch/eli/cc/2002/276/de
[344] Schweizerische Eidgenossenschaft. (2026). *Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz, StromVG), SR 734.7, Stand 13. August 2026*. https://www.fedlex.admin.ch/eli/cc/2007/418/de
[345] Schweizerische Eidgenossenschaft. (2026). *Stromversorgungsverordnung (StromVV), SR 734.71, Stand 1. Juli 2026*. https://www.fedlex.admin.ch/eli/cc/2008/226/de
[346] Schweizerische Eidgenossenschaft. (2026). *Verordnung des BAKOM vom 26. Mai 2016 über Fernmeldeanlagen (VFAV), SR 784.101.21, Stand am 1. Januar 2026*. https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2016/307/20260101/de/pdf-a/fedlex-data-admin-ch-eli-cc-2016-307-20260101-de-pdf-a.pdf

[347] Schweizerische Eidgenossenschaft. (2026). *Verordnung vom 2. April 2008 über die Sicherheit von Maschinen (Maschinenverordnung, MaschV), SR 819.14, Fassung vom 20. Januar 2024*. https://www.fedlex.admin.ch/eli/cc/2008/263/de

[348] Schweizerischer Bundesrat. (2025). *Botschaft zum Entlastungspaket 2027 für den Bundeshaushalt (EP 27), Ziffer 3.7: Kürzung des Bundesbeitrags für Innosuisse*. https://www.efd.admin.ch/dam/de/sd-web/RNU8WrkGOw4d/botschaft-entlastungspaket-2027-de.pdf

[349] Schweizerischer Bundesrat. (2025). *Faktenblatt Technische Handelshemmnisse (MRA), 13.06.2025*. https://www.europa.eda.admin.ch/dam/de/sd-web/5ux6SWfoouHr/005%20Faktenblatt%20Technische%20Handelshemmnisse%20(MRA)%20(DE).pdf

[350] Schweizerischer Bundesrat. (2025). *Maschinen: Erhalt des erleichterten Zugangs zum EU-Binnenmarkt (Eröffnung der Vernehmlassung zur revidierten Maschinenverordnung, 19. September 2025)*. https://www.admin.ch/de/newnsb/Vw47o_OIAjefyvEdNuC0o

[351] Schweizerischer Bundesrat. (2026). *Bundesrat will neues Cybersicherheitsgesetz schaffen*. https://www.estv.admin.ch/de/newnsb/zX9oNK8tuI-Z

[352] Sectigo. (2025). *Sectigo acquires Entrust public certificate business*. https://www.sectigo.com/resource-library/sectigo-acquires-entrust-public-certificate-business

[353] SECURE project consortium. (2026). *SECURE: Second Open Call for micro, small and medium-sized enterprises under the scope of the Cyber Resilience Act*. https://www.secure4sme.eu/

[354] Seeed Studio. (2026). *SenseCAP Card Tracker T1000-A*. https://www.seeedstudio.com/SenseCAP-Card-Tracker-T1000-A-p-5697.html

[355] Semtech. (2025). *LoRa Cloud is sunsetting on July 31st 2025*. https://www.semtech.com/loracloud-shutdown

[356] Sensolus. (2026). *About Sensolus*. https://www.sensolus.com/about-us/

[357] Sensolus. (2026). *Sensolus pricing*. https://www.sensolus.com/pricing/

[358] Sensolus. (2026). *Track 1115 smart tracker*. https://www.sensolus.com/hardware/battery-powered-smart-trackers/track-1115/

[359] Serma Safety & Security. (2026). *Cybersecurity guidance for the RED directive*. https://www.serma-safety-security.com/en/cybersecurity/cybersecurity-guidance-for-red-directive/

[360] SGS Brightsight. (2026). *CRA notified body services*. https://www.brightsight.com/cra-notified-body-services

[361] Siemens. (2026). *Insights Hub: FAQ*. https://www.siemens.com/en-us/products/insights-hub/resources/faq/

[362] Skylo Technologies, & o2 Telefónica. (2025). *Mobile communications via satellite: o2 Business launches first tariff for satellite IoT*. https://www.skylo.tech/newsroom/mobile-communications-via-satellite-o2-business-launches-first-tariff-for-satellite-iot

[363] Snyk. (2026). *Snyk plans and pricing*. https://snyk.io/plans/

[364] Staatssekretariat für Wirtschaft SECO. (2026). *Bezeichnung technischer Normen für Maschinen gestützt auf das Bundesgesetz über die Produktesicherheit und die Maschinenverordnung, 9. Oktober 2026 (BBl 2026 2698)*. https://www.fedlex.admin.ch/eli/fga/2026/2698/de

[365] Staatssekretariat für Wirtschaft SECO. (2026). *MRA Schweiz - EU: Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen*. https://www.seco.admin.ch/de/mra-schweiz-eu

[366] Statistisches Bundesamt (Destatis). (2019). *Kostenstruktur der Unternehmen des Verarbeitenden Gewerbes sowie des Bergbaus und der Gewinnung von Steinen und Erden 2017 (Fachserie 4 Reihe 4.3)*. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Industrie-Verarbeitendes-Gewerbe/Publikationen/Downloads-Struktur/kostenstruktur-2040430177004.pdf?__blob=publicationFile

[367] Statistisches Bundesamt (Destatis). (2025). *Statistischer Bericht - Kostenstrukturerhebung im Verarbeitenden Gewerbe sowie im Bergbau und der Gewinnung von Steinen und Erden - 2023 (Tabelle 42251-01: Rechtliche Einheiten nach Wirtschaftszweigen und Beschäftigtengrößenklassen)*. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Industrie-Verarbeitendes-Gewerbe/Publikationen/Downloads-Struktur/statistischer-bericht-kostenstruktur-2040430237005.html

[368] STMicroelectronics. (2026). *STSAFE-A110 authentication, state-of-the-art security for peripherals and IoT devices*. https://www.st.com/en/secure-mcus/stsafe-a110.html

[369] STMicroelectronics N.V. (2026). *Annual report on Form 20-F for 2025*. https://www.sec.gov/Archives/edgar/data/932787/000093278726000009/stm-20251231.htm

[370] Sunrise. (2022). *Accès facile à l'Internet des objets avec Sunrise Business (IoT Starter Services)*. https://mailing-ircockpit.eqs.com/crm-mailing/f4b46288-e4c1-1015-a68b-b34b05d60f5f/bb85010d-c5fc-4f87-8b67-9b1ff9e0d7ee/8c1ad055-6241-4728-89df-2551d18a0ff3/20220630_PR_IoT_Sunrise+Business_FR.pdf

[371] Swiss Medtech. (2026). *Medtech-Branchenstudie 2026: Zahlen und Fakten im Überblick*. https://www.swiss-medtech.ch/sites/default/files/2026-09/2026_SMTI_Faktenblatt_DE.pdf

[372] Swissbit. (2026). *Company*. https://www.swissbit.com/en/company/

[373] Swisscom. (2025). *Abschaltung 3G*. https://www.swisscom.ch/de/about/news/2025/12/16-abschaltung-3g.html

[374] Swisscom. (2026). *Annual Report 2025*. https://reports.swisscom.ch/short/2025/en/report-pdf

[375] Swisscom. (2026). *IoT connectivity*. https://www.swisscom.ch/en/business/enterprise/offer/iot/iot-connectivity.html

[376] Swisscom. (2026). *IoT Webshop: CMP Mobile and CMP LPN*. https://www.swisscom.ch/de/business/enterprise/angebot/iot/iot-connectivity/iot-webshop.html
[377] Swissmem. (2026). *Aktuelle Lage der Schweizer Tech-Industrie Q2/2026 (Branchenkennzahlen)*. https://www.swissmem.ch/fileadmin/user_upload/Swissmem/Medienarbeit/Branchenzahlen/2026_Q2/D/Swissmem_Tech-Industrie_Branchenkennzahlen_Q2_2026.pdf
[378] Swissmem. (2026). *Die Tech-Industrie zwischen Stagnation und Lichtblicken*. https://www.swissmem.ch/de/mediencorner/medienmitteilungen/die-tech-industrie-zwischen-stagnation-und-lichtblicken.html
[379] TelcoTitans. (2024). *Vodafone to close German IoT biz grandcentrix*. https://www.telcotitans.com/vodafonewatch/vodafone-to-close-german-iot-biz-grandcentrix-report/8725.article
[380] Telefónica Deutschland Holding AG. (2026). *Annual Report 2025*. https://www.telefonica.de/file/public/826/ANNUAL-REPORT-2025-EN-Telefonica-Deutschland-Holding-AG.pdf
[381] Telefónica Germany. (2026). *o2 Business Easy IoT*. https://easyiot.telefonica.de/
[382] Teltonika Telematics. (2026). *TAT141 asset tracker*. https://teltonika-gps.com/products/trackers/assets-workforce/tat141
[383] Thales. (2025). *AT&T and Thales collaborate to revolutionize IoT deployments with new eSIM solution*. https://www.thalesgroup.com/en/news-centre/press-releases/att-and-thales-collaborate-revolutionize-iot-deployments-new-esim
[384] Thales. (2026). *Full-year results 2025: slideshow*. https://www.thalesgroup.com/sites/default/files/press_release/documents/Thales%20-%20FY%202025%20-%20Slideshow%20-%20%2003%20March%202026_1.pdf
[385] The Things Industries. (2026). *The Things Stack Cloud plans*. https://www.thethingsindustries.com/stack/plans/
[386] Thüringer Aufbaubank. (2026). *Digitalbonus Thüringen*. https://www.aufbaubank.de/Foerderprogramme/Digitalbonus-Thueringen
[387] Thüringer Ministerium für Wirtschaft, Landwirtschaft und Ländlichen Raum. (2026). *Befristeter Antragsstopp für das Zentrale Innovationsprogramm Mittelstand (ZIM). Dringlichkeitsanfrage des Abgeordneten Dr. Augsten (BSW) und Antwort, Drucksache 8/4021 vom 30. Juli 2026*. https://parldok.thueringer-landtag.de/ParlDok/dokument/108588
[388] Tive. (2026). *Tive caps record-setting first half of 2026 with $100 million ARR milestone and $20 million funding round*. https://www.tive.com/press-release/tive-caps-record-setting-first-half-of-2026-with-100-million-arr-milestone-20-million-funding-round
[389] Tive. (2026). *Tive real-time trackers: Solo 5G, Solo Lite, Solo Pro*. https://www.tive.com/products/real-time-trackers
[390] Trackunit. (2025). *Trackunit announces closing of investment*. https://trackunit.com/press/trackunit-announces-closing-of-investment/
[391] Trackunit. (2026). *Trackunit hardware: Raw, Pass, Spot, Kin, Beam*. https://trackunit.com/
[392] Trackunit. (2026). *Trackunit pricing*. https://trackunit.com/pricing/
[393] Transferstelle Cybersicherheit im Mittelstand. (2026). *Transferstelle Cybersicherheit im Mittelstand*. https://transferstelle-cybersicherheit.de/
[394] Trusted Computing Group. (2024). *TPM 2.0 Library, Family 2.0, Level 00, Revision 01.83*. https://trustedcomputinggroup.org/resource/tpm-library-specification/
[395] Trusted Firmware. (2026). *Trusted Firmware-M documentation*. https://trustedfirmware-m.readthedocs.io/
[396] TÜV Informationstechnik GmbH. (2026). *Cyber Resilience Act*. https://www.tuvit.de/en/topics/regulations/cyber-resilience-act/
[397] u-blox. (2026). *MAX-M10S data sheet UBX-20035208 R08*. https://content.u-blox.com/sites/default/files/MAX-M10S_DataSheet_UBX-20035208.pdf
[398] umati / VDMA. (2026). *About umati*. https://umati.org/about/
[399] Utimaco. (2025). *INVISION and PINOVA acquire Utimaco's lawful interception business*. https://utimaco.com/news/press-releases/invision-and-pinova-acquire-utimacos-lawful-interception-business
[400] Utimaco. (2025). *Keyfactor strengthens partnership with Utimaco to redefine PKI deployment*. https://utimaco.com/news/press-releases/keyfactor-strengthens-partnership-utimaco-redefine-pki-deployment
[401] Utimaco. (2026). *Company*. https://utimaco.com/company
[402] VDE. (2022). *VDE-AR-E 2829-6-1:2022-12 Energy management in the smart home, use cases*. https://vde-verlag.de/standards/0800840/vde-ar-e-2829-6-1-anwendungsregel-2022-12.html
[403] VDE FNN. (2025). *Neues erweitertes Lastenheft Steuerbox 1.5*. https://www.vde.com/de/fnn/aktuelles/neues-erweitertes-lastenheft-steuerbox-1-5-
[404] VDMA. (2018). *Maschinenbau in Zahl und Bild 2018*. https://www.messe.de/apollo/hannover_messe_2020/obs/Binary/A1004789/1004789_02146924.pdf
[405] VDMA. (2020). *Maschinenbau in Zahl und Bild 2020*. https://www.vdma.eu/documents/34570/0/MbauinZuB2020.pdf
[406] VDMA. (2026). *Maschinenbau in Zahl & Bild*. https://www.vdma.eu/de/maschinenbau-zahl-bild

[407] VerkehrsRundschau. (2025). *Dataforce-Studie: Telematiknutzung bei Transportern steigt*. https://www.verkehrsrundschau.de/nachrichten/nfz-fuhrpark/dataforce-studie-telematiknutzung-bei-transportern-steigt-3617775
[408] Vodafone Deutschland. (2020). *Vodafone aktiviert bundesweit das Netz für Mensch und Maschine*. https://unternehmen.vodafone.de/newsroom/vodafone-aktiviert-bundesweit-das-netz-fuer-mensch-und-maschine
[409] Vodafone Group. (2026). *Annual Report 2026*. https://reports.investors.vodafone.com/view/500231330/
[410] Wavestone and ICF and CEPS and CARSA. (2021). *Study on the need of cybersecurity requirements for ICT products, No. 2020-0715, final study report*. https://ec.europa.eu/newsroom/dae/redirection/document/82006
[411] Wi-Fi Alliance. (2026). *WPA3 deployment options*. https://www.wi-fi.org/system/files/WPA3_Deployment_Options_Highlights_202602.pdf
[412] Wirtschafts- und Infrastrukturbank Hessen. (2026). *Distr@l: Digitalisierung stärken, Transfer leben*. https://www.wibank.de/distral
[413] Wirtschaftskammer Österreich. (2026). *Abschaltung 2G- und 3G-Netz in Österreich*. https://www.wko.at/sicherheitsanlagentechnik/abschaltung-2g-und-3g-netz-in-oesterreich
[414] Wirtschaftskammer Österreich. (2026). *KMU.DIGITAL*. https://www.kmudigital.at/
[415] Zühlke Group. (2026). *Facts and figures*. https://www.zuehlke.com/en/about-us/facts-figures
[416] ZVEI e.V. (2026). *Elektro- und Digitalindustrie stabil ins Jahr gestartet*. https://www.zvei.org/presse-medien/pressebereich/elektro-und-digitalindustrie-stabil-ins-jahr-gestartet
[417] ZVEI e.V. (2026). *ZVEI: Elektro- und Digitalindustrie 2026 wieder mit Wachstum*. https://www.zvei.org/presse-medien/pressebereich/zvei-elektro-und-digitalindustrie-2026-wieder-mit-wachstum