

Zehn Treiber für Compliance-Management-Systeme und betroffene Unternehmen

Hinweis: Ein **Compliance-System** wird in verschiedenen Rechtsbereichen **nicht immer ausdrücklich als „CMS“** verlangt, aber über **konkrete Organisations-, Sorgfalts- und Dokumentationspflichten** **faktisch** gefordert.

Beispielsunternehmen:

A	Maschinenbau-Export GmbH, 180 Mitarbeiter, Export von Maschinen mit Steuerungssoftware	D	FinTechZahlungsdienste GmbH, 70 Beschäftigte, reguliertes Zahlungsinstitut	G	Steuerberatungs- und Wirtschaftsprüfungskanzlei PartG mbH, 55 Beschäftigte
B	Cloud-Managed-Service GmbH, 95 Beschäftigte, SaaS, Hosting, IT-Betrieb, KI-Modul	E	Schreinerei & Innenausbau GmbH, 85 Beschäftigte, mittelgroßer Handwerksbetrieb	H	Onlinehändler – E-Commerce GmbH, 60 Beschäftigte, eigener Webshop, Marktplatzvertrieb
C	Diagnostiklabor-Pflegeverbund gGmbH, 230 Beschäftigte, Gesundheitsdaten	F	Lebensmittelhersteller & Großhandels GmbH, 85 Beschäftigte, internationale Lieferanten	I	Architekturbüro GmbH, 55 Beschäftigte; öffentliche und private Auftraggeber

✓	anwendbar	△	Nur risikoabhängig anwendbar	✗	Nicht anwendbar / regelmäßig kein Schwerpunkt
---	-----------	---	------------------------------	---	---

Nr.	Themenbereich	Rechtsquelle	Warum braucht es ein Compliance-System oder faktische Regelungen?	A Maschinenbau	B Cloud	C Gesundheit	D FinTech	E Handwerk	F Lebensmittel	G StB/WP	H online	I Architekt
1	Steuer / Tax Compliance	AO; insbes. § 153 AO	Steuerliche Pflichten müssen richtig, fristgerecht und nachweisbar erfüllt werden; Fehler müssen erkannt und berichtigt werden; IKS als relevantes Indiz bei der Abgrenzung von Fehlern zu vorsätzlichem Verhalten	✓ USt, Zoll, Verrechnungspreise	✓ USt, digitale Leistungen, Lizenzumsätze	✓ USt, Lohnsteuer Gemeinnützigkeitsthemen	✓ USt, komplexe Transaktions- und Steuerdaten	✓ USt, Lohnsteuer, Bau-/Montageleistungen,	✓ USt	✓ Besonders hoch: eigene Pflichten plus Beratung fremder Steuerpflichtiger	✓ USt, grenzüberschreitender Warenverkauf	✓ USt, Projektabrechnungen, Subunternehmer
2	Geldwäsche / AML-VO	Aktuell: §§ 4-6 GwG Künftig Art. 9ff. AML-VO	Risikomanagement, Risikoanalyse, interne Sicherungsmaßnahmen; mit ausdrücklich geforderten internen Strategien, Verfahren, und Kontrollen	△ bei Hochrisikogeschäften, Export-/Sanktionsnähe	△ bei Zahlungsabwicklung nur mittelbar; sonst eher KYC ggü Geschäftskunden	✗ idR kein GwG-Verpflichteter	✓ Kernpflicht als Finanzunternehmen	✗ idR kein Kernbereich; nur bei ungewöhnlichen Barzahlungen, Immobiliennähe	△ bei Bargeschäften/Handel nur je nach Ausgestaltung	✓ Verpflichteter nach GwG	△ kein klassischer GwG_Verpflichteter; nur bei ungewöhnlichen Zahlungsströmen	△ kein typischer GwG_Verpflichteter; relevant bei Immobiliennähe, ungewöhnlichen Investorenstrukturen
3	Datenschutz / DSGVO	Art. 24-35 DSGVO	technische und organisatorische Maßnahmen, Verzeichnis, Sicherheit, Datenschutzfolgeabschätzung, Meldeprozesse	✓ Beschäftigten-, Kunden- und Lieferantendaten	✓ Kernrisiko: Kundendaten, Cloud, Auftragsverarbeitung	✓ Bes. hoch: Gesundheitsdaten	✓ Finanz- und Identitätsdaten	✓ Beschäftigten, Kunden- und Lieferantendaten	✓ Beschäftigten, Kunden- und Lieferantendaten	✓ Beschäftigten, Kunden- und Steuerdaten	✓ Kunden-, Lieferantendaten, Tracking, Webanalyse	✓ Beschäftigten, Kunden- und Lieferantendaten
4	Hinweisgeberschutz / Whistleblowing	§§12 HinSchG	Pflicht zur Einrichtung interner Meldestellen und Meldekanäle	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte	✓ Über 50 Beschäftigte

Nr.	Themenbereich	Rechtsquelle	Warum braucht es ein Compliance-System oder faktische Regelungen?	A Maschinenbau	B Cloud	C Gesundheit	D FinTech	E Handwerk	F Lebensmittel	G StB/WP	H online	I Architekt
5	Lieferkette / Menschenrechte	§§4-10 LkSG	Risikomanagement, Risikoanalyse, Präventions- und Abhilfemaßnahmen, Beschwerdeverfahren	△ indirekt: Lieferant für größere Kunden	△ indirekt: Lieferant für größere Kunden	△ indirekt: Beschaffung, Pflege-/ Medizinprodukte	△ Dienstleister großer Finanzunternehmen	△ indirekt über Holzlieferketten, Kundenanforderungen	✓ Besonders relevant: Agrar-/ Rohstofflieferketten, Verpackung, Logistik	✗ eher gering; evtl., wenn Kanzlei Dienstleister größerer Mandanten	△ indirekt über Kunden, Banken oder Marktplätze	△ indirekt über Anforderungen von Auftraggebern
6	IT-Sicherheit/NIS-2	Art. 20 + 21 NIS-2-Richtlinie	Leitungsverantwortung und Cybersicherheits-Risikomanagementmaßnahmen	△ vernetzte Maschinen	✓ Typischer NIS2-Treiber	✓ Gesundheitssektor und sensible Systeme	✓ Finanzsektor, zusätzlich DORA	✗ idR keine unmittelbaren NIS2-Pflichten	△ Produktion/Logistik: direkte NIS2-Pflichten nur bei Sektor-/Größenschwelle	△ Berufsgheimnisträger mit hohem Schutzbedarf; idR nicht NIS2	✓ Webshop, Zahlungsprozesse; NIS2 nicht direkt, aber IT-Sicherheit hoch; nur bei Sektor-/Größenschwellen	△ relevant, aber nicht NIS2 direkt
7	Cyber Resilience Act	CRA VO (EU) 2024/2847	Security-by-Design (bei Entwicklung Sicherheitsanforderungen beachten), Schwachstellen über den Produktlebenszyklus managen; Meldepflichten bei Vorfällen	✓ Maschinen mit digitaler Steuerung/Software	✓ Softwareprodukte/SaaS – mindestens Security-prozesse	△ nur bei eigener Software/ Medizinprodukten	△ nur bei eigenen Apps /FinTech Software	△ nicht einschlägig, Ausn: Produkte mit digitalen Elementen (smart Home)	△ bei importierten smarten Geräten, Produktlinien	✗ idR nicht einschlägig	△ nur einschlägig, wenn eigene Apps, smarte Produkte etc. vertrieben werden	✗ idR nicht einschlägig
8	KI-Compliance / EU AI Act	Art. 9+17 EU AI Act	Risikomanagementsystem und Qualitätsmanagementsystem für Hochrisiko-KI	△ nur bei KI-gestützter Maschinensteuerung/Qualitätsprüfung	✓ KI-Modul als Produkt oder HR-Entscheidungssystem	△ nur bei KI in Diagnostik Personalplanung, ggf. hochsensibel	△ Betrugsprävention, Kredit- und Zahlungsrisiko, abhängig von Nutzung	△ nur bei KI in HR-Tools oder bei Kundenbewertung	△ nur bei KI in Produktionsplanung/	△ nur bei KI in HR-Tools, Beratung, Prüfung	△ nur bei KI in Marketing und in HR	△ Einsatz von KI für Ausschreibungen, HR
9	Antikorruption, Exportkontrolle / Sanktionen	§§ 30, 130 OWiG EU-Sanktionsverordnungen	Korruptionsstraftatbestände im StGB; Pflicht, betriebsbezogene Pflichtverletzungen durch angemessene Organisation zu verhindern) faktische Pflicht zu Screenings-, Genehmigungs- und Kontrollprozessen	✓ Sehr relevant; Auslands-geschäft	△ Geschäftspartner-/Sanktions-screening	△ Beschaffung, Spenden, Kooperationen	✓ Finanzsanktionen, Fraud, Geschäftspartnerprüfung	△ bei öffentlichen Aufträgen, Vergaben, Subunternehmer	△ Lieferanten, Großkunden, öffentliche Abnehmer	✓ Mandantenan-nahme, Unabhängigkeit, Geldwäs-che	△ Sanktionslistenprüfung bei internationalen Kunden/Lieferanten	✓ Bes. bei öffentlichen Aufträgen, Subunternehmer
10	Arbeitsrecht / HR-Compliance	Arbeitsschutzrecht, Arbeitszeitrecht, künftig: EU-Entgelttransparenzrichtlinie	faktisch: HR-System, das Diskriminierung, Arbeitsschutz-, Arbeitszeit- und Vergütungsrisiken systematisch adressiert)	✓ Alle Arbeitgeberpflichten, Schicht-/Montage-einsätze	✓ Alle Arbeitgeberpflichten, Remote Work, Arbeitszeit	✓ Alle Arbeitgeberpflichten, Schichtdienst, Arbeitsschutz, Gleichbehandlung	✓ Alle Arbeitgeberpflichten, reguliertes HR, Vergütung	✓ Alle Arbeitgeberpflichten, Baustelle / Arbeitsschutz	✓ Alle Arbeitgeberpflichten, Schichtarbeit	✓ Alle Arbeitgeberpflichten	✓ Alle Arbeitgeberpflichten, Lager, Versand, Schicht	✓ Alle Arbeitgeberpflichten, Projektarbeit, Baustellen