

Zwölf ausgewählte regulatorische Treiber für Compliance Management-Systeme (Stand: 30.06.2026)

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

Nr.	Themenbereich		Rechtsquelle/Konkrete Compliance-Anforderung	Geltungsbeginn	Typischer Verstoß (Beispiele)	Rechtsfolgen
1	Steuer / Tax Compliance	AO; insbes. § 153 AO	insbesondere steuerliche Erklärungs-, Aufzeichnungs- und Berichtigungspflichten § 153 AO; BMF-AEAO zu § 153 AO mit Hinweis auf innerbetriebliches Kontrollsystem als Indiz gegen Vorsatz/Leichtfertigkeit	Laufend, BMF-Hinweis seit 2016	- Fehlerhafte USt-Voranmeldungen, - Unvollständige Steuererklärungen, - Verspätete Berichtigung erkannter Fehler	- Steuernachzahlung - Zinsen - Säumniszuschläge - Bußgeld - Steuerstrafverfahren - Organhaftung
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	GwG: bereits aktuell geltend Neue AML-VO: ab 10.07.2027	- Fehlende KYC-Prüfung („Know Your Customer“) - Keine PEP-Prüfung - Unzureichendes Transaktionsmonitoring - Verspätete Verdachtsmeldung	- Bußgelder - Aufsichtsrechtliche Maßnahmen - Sonderprüfungen - Strafrechtliche Risiken
3	Datenschutz /DSGVO	Art. 24-35 DSGVO	technische und organisatorische Maßnahmen, Verzeichnis, Sicherheit, Datenschutzfolgeabschätzung, Meldeprozesse	DSGVO anwendbar seit 25.05.2018	- Verarbeitung ohne Rechtsgrundlage - Datenpanne ohne Meldung - Fehlende Löschprozesse - Unzureichende Auftragsverarbeitung	- Bußgelder - Schadensersatz - Untersagungsverfügungen - Reputationsschäden
4	Hinweisgeberschutz / Whistleblowing	§§12 HinSchG	Pflicht zur Einrichtung interner Meldestellen und Meldekanäle	ab 02.07.2023: ab 250 Beschäftigte ab 17.12.2023: ab 50 Beschäftigte	- Keine interne Meldestelle - Verletzung der Vertraulichkeit - Repressalien gegen Hinweisgeber - Fehlende Rückmeldung	- Bußgeld - Arbeitsrechtliche Ansprüche - Reputationsschäden - Eskalation an externe Stellen
5	Lieferkette/Menschenrechte	§§4-10 LkSG	Risikomanagement, Risikoanalyse, Präventions- und Abhilfemaßnahmen, Beschwerdeverfahren	ab 01.01.2023: ab 3.000 Beschäftigten ab 01.01.2024: ab 1.000 Beschäftigten	- Keine Risikoanalyse - Fehlendes Beschwerdeverfahren - Keine Abhilfe trotz bekannter Menschenrechtsverletzungen	- Bußgelder - Behördliche Anordnungen - Ausschluss von öffentlichen Aufträgen - Reputationsstellen
6	IT-Sicherheit/NIS-2	Art. 20 + 21 NIS-2-Richtlinie	Leitungsverantwortung und Cybersicherheits-Risikomanagementmaßnahmen	ab 06.12.2025	- Kein Incident-Response-Prozess (=Verfahren zum Erkennen und Bewältigen von Cybersicherheitsvorfällen) - Fehlende Risikoanalyse - Unzureichende Lieferkettensicherheit - Verspätete Meldung	- Bußgelder - Aufsichtsrechtliche Maßnahmen - Betriebsunterbrechungen
7	KRITIS/BSIG	§8a BSIG	KRITIS-Betreiber müssen angemessene organisatorische und technische Vorkehrungen nach Stand der Technik treffen und nachweisen	Seit 2015/2016 Fortlaufende Weiterentwicklung durch IT-Sicherheitsgesetze	- Fehlender Stand-der-Technik-Nachweis - Unzureichendes Notfallmanagement - Mangelhafte Sicherheitskonzepte	- BSI-Anordnungen - Bußgelder - Nachweispflichten - Versorgungs- und Betriebsrisiken

Nr.	Themenbereich		Rechtsquelle/Konkrete Compliance-Anforderung	Geltungsbeginn	Typischer Verstoß (Beispiele)	Rechtsfolgen
8	Cyber Resilience Act	CRA VO (EU) 2024/2847	Security-by-Design (bei Entwicklung Sicherheitsanforderungen beachten), Schwachstellen über den Produktlebenszyklus managen; Meldepflichten bei Vorfällen	Meldepflichten ab 11.09.2026 Hauptpflichten ab: 11.09.2027	• Produkt mit bekannten Schwachstellen • Fehlende Sicherheitsupdates • Kein Produktlebenszykluskontrollsystem	• Marktüberwachung • Produktrückruf • Vertriebsverbot • Bußgelder
9	KI-Compliance/ EU AI Act	Art. 9+17 EU AI Act	Risikomanagementsystem und Qualitätsmanagementsystem für Hochrisiko-KI	Verbote bestimmter KI-Praktiken seit 02.02.2025 Zentrale Pflichten grundsätzlich ab 02.08.2026	• Hochrisiko-KI ohne Risikomanagement • Fehlende Datengovernance • Keine menschliche Aufsicht	• Hohe Bußgelder • Marktverbote • Rücknahme- oder Korrekturpflichten • Haftungsrisiken
10	Antikorruption	§§ 30, 130 OWiG	Korruptionsstraftatbestände im StGB; Pflicht, betriebsbezogene Pflichtverletzungen durch angemessene Organisation zu verhindern)	Laufend	• Bestechung im Vertrieb • Scheinberaterverträge • Unzulässige Geschenke und Einladungen	• Strafverfahren gegen Personen • Unternehmensgeldbußen • Vermögensabschöpfung • Reputationsschäden •
11	Exportkontrolle/Sanktionen	EU-Sanktionsverordnungen	faktische Pflicht zu Screenings-, Genehmigungs- und Kontrollprozessen	Laufend; besonders verschärft seit 2022 durch Russland-Sanktionen	• Lieferung an sanktionierte Personen • Export genehmigungspflichtiger Güter ohne Genehmigung • Umgehungsgeschäfte	• Straf- und Bußgeldrisiken • Einziehung • Lieferstopp • Verlust von Genehmigungen • Reputationsschäden •
12	Arbeitsrecht / HR-Compliance	Arbeitsschutzrecht, Arbeitszeitrecht, künftig: EU-Entgelttransparenzrichtlinie	faktisch: HR-System, das Diskriminierung, Arbeitsschutz-, Arbeitszeit- und Vergütungsrisiken systematisch adressiert)	Bestehende HR-Pflichten: laufend EU-EntgelttransparenzRL: ab 07.06.2026	• Diskriminierende Vergütung • Arbeitszeitverstöße • Unzulässige Beschäftigtendatenverarbeitung	• Schadensersatz • Entschädigung • Bußgelder • Arbeitsgerichtliche Verfahren