Ja, es gibt 13 Regelwerke.
Nein, das ist kein Grund zur Lähmung.
Hierauf musst du achten.

Mit den richtigen Maßnahmen bist du auf der sicheren Seite.

DSGVO	BDSG	EU AI Act
NIS2	BetrVG	AGG
DORA	GwG	GoBD
UrhG	TDDDG	Produkthaftung
Art. 13/14		

DSGVO / GDPR

Was tun?

AVV mit jedem KI-Anbieter abschließen, der personenbezogene Daten verarbeitet. DSFA durchführen. Automatisierte Entscheidungen (Art. 22) auf Rechtsgrundlage prüfen und Betroffenenrechte sicherstellen.

Typischer Verstoß

Unzulässige KI-Profilbildung; fehlende DSFA; automatisierte Entscheidungen ohne Rechtsgrundlage (Art. 22); unzureichende Einwilligung; Datenweitergabe an KI-Anbieter ohne AVV.

Max. Sanktion: **bis 20 Mio. €**

oder 4 % des weltweiten Jahresumsatzes (höherer Wert) — plus Schadensersatz und Abmahnungen

BDSG

Was tun?

DSB-Pflicht prüfen. Betriebsvereinbarung vor Einführung jedes Monitoring-Tools abschließen. Videoüberwachungskonzept rechtlich absichern.

Typischer Verstoß

Fehlende Betriebsvereinbarung bei Mitarbeiterüberwachungs-Software; unzulässige KI-Videoüberwachung; kein Datenschutzbeauftragter trotz Pflicht (ab 20 Personen mit Datenzugriff).

Max. Sanktion: **bis 50.000 €**

direkt (§ 43 BDSG) — schwere Verstöße laufen über DSGVO-Sanktionen bis 20 Mio. €

DSGVO Art. 13/14

Transparenzpflichten

Was tun?

Datenschutzerklärung um einen KI-Abschnitt ergänzen: welche Systeme eingesetzt werden, zu welchem Zweck, ob automatisierte Entscheidungen stattfinden.

Typischer Verstoß

Keine Information über KI-gestützte Entscheidungen; fehlende Angaben zu automatisierter Verarbeitung in der Datenschutzerklärung.

Max. Sanktion: **bis 20 Mio. €**

Teil der DSGVO-Sanktionen — Verwarnungen und Abmahnungen durch Verbraucherverbände

EU AI Act

Was tun?

KI-Inventar anlegen und nach Risikoklasse (verboten / Hochrisiko / minimal) klassifizieren. Hochrisiko-Systeme (z. B. HR-Screening) dokumentieren, testen und mit menschlicher Aufsicht flankieren.

Typischer Verstoß

Einsatz verbotener KI-Praktiken (Social Scoring, manipulative Systeme); fehlende Konformitätsbewertung; keine Dokumentation/Logs; fehlende menschliche Aufsicht bei Hochrisiko-KI.

Max. Sanktion: **bis 35 Mio. €**

oder 7 % Umsatz (verbotene Praktiken) — sonstige Verstöße: 15 Mio. € / 3 % — HR-KI: Frist bis Dez. 2027

Produkthaftung (EU)

Was tun?

Outputs und Entscheidungspfade dokumentieren. Menschliche Prüfung bei kritischen Ausgaben verpflichtend machen. Haftungsausschlüsse mit Rechtsanwalt prüfen. Versicherungsschutz bewerten.

Typischer Verstoß

KI-System verursacht Schaden durch fehlerhafte Ausgabe; kein Haftungsausschluss vereinbart; fehlende Dokumentation der Entscheidungspfade für Beweiszwecke.

Max. Sanktion: **Unbegrenzt**

zivilrechtlich — Beweislastumkehr bei Hochrisiko-KI: Hersteller muss Fehlerfreiheit nachweisen

UrhG / DSM-RL

Urheberrecht

Was tun?

KI-Output vor Veröffentlichung auf Ähnlichkeit prüfen. Nutzungsbedingungen des Anbieters zu Trainingsdaten kennen und dokumentieren. KI-generierte Inhalte kennzeichnen.

Typischer Verstoß

KI-Training mit urheberrechtl. geschütztem Material ohne Opt-out-Prüfung; KI-Output verletzt Originalwerke; fehlende Kennzeichnung KI-generierter Inhalte.

Max. Sanktion: **3× Lizenzbetrag**

+ Abmahnkosten (§ 97 UrhG) — keine feste Obergrenze; einstw. Verfügungen und Vernichtung rechtswidriger Kopien möglich

BetrVG

Betriebsverfassungsgesetz

Was tun?

Betriebsrat vor der Pilotphase einbinden — informell, bevor der formelle Prozess startet. Betriebsvereinbarung als Rahmen abschließen. Das schafft Akzeptanz und Rechtssicherheit.

Typischer Verstoß

Einführung von KI-Überwachungs- oder Bewertungssystemen ohne Betriebsratsbeteiligung; automatisierte Leistungsbeurteilung; KI-Personalauswahl ohne Mitbestimmung.

Max. Sanktion: **Einführungsstopp**

per einstw. Verfügung + bis 10.000 € (§ 121 BetrVG) — Unwirksamkeit von Maßnahmen, zurück auf Null

AGG

Allg. Gleichbehandlungsgesetz

Was tun?

Bias-Audit vor Go-live durchführen. Geschützte Merkmale aus Inputdaten ausschließen. Entscheidungen des Algorithmus regelmäßig auf Diskriminierungsmuster prüfen.

Typischer Verstoß

Algorithmische Diskriminierung bei Bewerbung, Kreditvergabe oder Kündigung aufgrund Alter, Geschlecht, Herkunft — auch ohne Absicht, durch Bias in Trainingsdaten.

Max. Sanktion: **bis 3 Monatsgehälter**

je Betroffenem (§ 15 AGG) — kein festes Bußgeldlimit; Sammelklagen möglich

GwG / AML

Geldwäschegesetz

Was tun?

KI-Modelle für Transaktionsmonitoring regelmäßig validieren und dokumentieren. Meldeprozess zur FIU automatisieren und testen. KYC-Ergebnisse revisionssicher speichern.

Typischer Verstoß

KI-Transaktionsmonitoring fehlerhaft konfiguriert; keine Meldung von Verdachtsmomenten an die FIU; unzureichende KYC-Prozesse im automatisierten Onboarding.

Max. Sanktion: **bis 5 Mio. €**

oder 10 % Jahresumsatz (§ 56 GwG) — Entzug der Geschäftserlaubnis; strafrechtliche Verfolgung (§ 261 StGB) möglich

HGB / AO / GoBD

Buchführung & Datenzugriff

Was tun?

Verfahrensdokumentation für alle KI-gestützten Buchungsprozesse anlegen. Archivierungskonzept mit Steuerberater abstimmen. GoBD-Konformität des KI-Buchhaltungstools prüfen.

Typischer Verstoß

KI-generierte Buchungen ohne Nachvollziehbarkeit; fehlende Verfahrensdokumentation; unzureichende Archivierung (Pflicht: 10 Jahre) — Finanzamt kann Prüfung nicht durchführen.

Max. Sanktion: **Steuerschätzung**

+ Zinsen und bis 25.000 € (AO) — Betriebsprüfungsrisiko erhöht; § 283b StGB bei Vorsatz

DORA

Finanzsektor — ab Jan. 2025

Was tun?

IKT-Drittanbieter-Register führen und Verträge auf DORA-Konformität prüfen. Incident-Response-Plan mit Meldekette (inkl. Fristen) definieren und regelmäßig testen.

Typischer Verstoß

Unzureichendes IKT-Risikomanagement; fehlende Resilienz-Tests; keine Meldung schwerer IKT-Vorfälle; mangelnde Überwachung von KI-Cloud-Anbietern.

Max. Sanktion: **1 % Tagesumsatz**

täglich für die Dauer des Verstoßes — kumuliert schnell; gilt für Finanzunternehmen ab Jan. 2025

NIS2 / BSIG-Novelle

Was tun?

Zuerst prüfen: Greift NIS2 überhaupt (Sektorzugehörigkeit, Größe)? Dann: 24-h-Meldekette definieren, Incident-Response-Plan erstellen, Geschäftsleitung schulen.

Typischer Verstoß

Keine Risikoanalyse und Sicherheitskonzepte; fehlende Meldung von Cyberangriffen (24-h/72-h-Frist); unzureichende Supply-Chain-Sicherheit; kein Incident-Response-Plan.

Max. Sanktion: **bis 10 Mio. €**

oder 2 % Jahresumsatz — persönliche Organverantwortung der Geschäftsleitung (§ 38 BSIG) möglich

TDDDG / ePrivacy

ehem. TTDSG

Was tun?

Consent Management Platform einsetzen. Tracking-Skripte erst nach gültiger Einwilligung laden — technisch sicherstellen, nicht nur im Banner. Web-Scraping rechtlich prüfen.

Typischer Verstoß

Tracking-KI, Cookies oder Fingerprinting ohne gültige Einwilligung; automatisierte Nutzerprofile ohne Opt-in; illegales Web-Scraping für KI-Training.

Max. Sanktion: **bis 300.000 €**

(§ 28 TDDDG) — DSGVO-Bußgelder kumulativ möglich; Abmahnungen durch Wettbewerber und Verbraucherverbände

Anpacken — mit Augenmaß, nicht mit Angst.

1. **KI-Inventar anlegen**
   Welche Tools verarbeiten Personendaten?

2. **AVV prüfen & abschließen**
   Mit jedem KI-Anbieter, der Daten verarbeitet

3. **Datenschutzerklärung updaten**
   KI-Einsatz und automatisierte Verarbeitung benennen

4. **Betriebsrat früh einbinden**
   Informell, bevor der formelle Prozess startet

5. **DSFA & Fachanwalt**
   Bei HR, Finance oder grenzüberschreitendem Einsatz

Welche Frage brennt dir auf den Nägeln? Schreib sie in die Kommentare.

Speichere dieses Karussell — damit du's griffbereit hast.