KI-PFLICHTEN-KOMPASS

fuer BaFin-regulierte Organisationen im DACH-Raum

REGULATORISCHE TIMELINE

* Aktuell gesetzlich bindend. ** Digital Omnibus in Trilogue (Stand: April 2026). *** Beide Co-Legislatoren stuetzen feste Backstop-Deadline 2. Dez 2027 (Annex III).

PFLICHTEN-MATRIX: WAS GILT FUER IHR INSTITUT?

Pflicht	Normstelle	Gilt ab	Relevanz Finanzsektor	M365-Hebel
AI Literacy	EU AI Act Art. 4	**Feb 2025 (BEREITS IN KRAFT)**	Alle Provider und Deployer; gilt unabhaengig von Risikostufe	SharePoint + Forms (Quiz + Teilnehmerliste)
Verbotene Praktiken	EU AI Act Art. 5	**Feb 2025 (BEREITS IN KRAFT)**	Social Scoring, manipulative Techniken, Emotionserkennung am Arbeitsplatz	Defender for Cloud Apps (Shadow AI Discovery)
Risikoklassi-fikation	EU AI Act Art. 6, Annex III	Aug 2026 / Dez 2027*	Kreditwuerdigkeit, Versiche-rungs-Scoring = High-Risk; Copilot Standard != High-Risk	AI-Inventar (SharePoint Lists)
Deployer-Pflichten	EU AI Act Art. 26	Aug 2026 / Dez 2027*	NUR fuer High-Risk-Systeme; Human Oversight, Monitoring, Input Data Governance	Purview Audit Logs, DSPM for AI
Transparenz	EU AI Act Art. 50	Aug 2026	Kennzeichnung KI-generierter Inhalte; Information bei Interaktion mit KI-System	Copilot-Hinweistexte, UI-Kennzeichnung
ICT Risk Management	DORA Art. 5-13	**Jan 2025 (BEREITS IN KRAFT)**	KI als ICT-Asset identifizieren, schuetzen, ueberwachen; Incident Management	Purview, Entra ID, Defender, SAM
Third-Party Risk	DORA Art. 28-30	**Jan 2025 (BEREITS IN KRAFT)**	Microsoft als KI-Provider bewerten; Register of Information fuehren	Provider-Checkliste, Vertragspruefung
AI-Strategie & Governance	BaFin-Guidance Kap. Strategie	**Jan 2026 (BENCHMARK)**	Management-genehmigte KI-Strategie; Einbettung in ICT-Risikoframework	Operating Model, RICI, Stage-Gate

* Digital Omnibus (in Trilogue): Backstop-Deadline 2. Dez 2027 fuer Annex-III-Systeme. Bis zur formalen Adoption gilt der 2. Aug 2026.

STRAFRAHMEN EU AI ACT (Art. 99)

Verbotene Praktiken: bis 35 Mio. EUR / 7% Umsatz | Sonstige Pflichtverstoesse: bis 15 Mio. EUR / 3% Umsatz | Fehlerhafte Angaben: bis 7,5 Mio. EUR / 1% Umsatz

Massgeblich ist jeweils der hoehere Betrag. Strafen fuer GPAI-Provider gelten ab Aug 2026. Quelle: Reg. (EU) 2024/1689, Art. 99 Abs. 3-5.

Reemento GmbH | Mustafa Pakir | AI-Governance-Architekt | kontakt@reemento.de

5 FINDINGS, DIE WIR IN JEDEM M365-TENANT FINDEN

Anonymisierte, typische Befunde aus M365-Governance-Assessments. Diese Muster treten branchenuebergreifend auf.

01 KRITISCH — Oversharing: Copilot exponiert HR- und Finanzdaten

DSPM for AI zeigt: Copilot hat Zugriff auf SharePoint-Sites mit Gehalts-, Personal- und Vorstandsdaten. Berechtigungen sind ueber 'Everyone except external users' vergeben. Bei aktivem Copilot koennen alle lizenzierten Nutzer diese Daten ueber Prompts abrufen.

Regulatorische Referenz: DORA Art. 9 (Schutz) | BaFin-Guidance Kap. Cybersecurity | DSGVO Art. 5 Abs. 1 lit. f
M365-Control: Restricted Content Discovery, Sensitivity Labels, Named Groups statt EEEU

02 KRITISCH — Shadow AI: Unkontrollierte KI-Nutzung ohne Inventar

Defender for Cloud Apps Discovery identifiziert 15-40 KI-/GenAI-Dienste, die ohne Freigabe genutzt werden. Kein AI-Inventar vorhanden, keine Risikoklassifikation, keine Verantwortlichkeitszuweisung. Art. 4 AI Literacy-Pflicht wird nicht erfuellt.

Regulatorische Referenz: EU AI Act Art. 4 (Literacy), Art. 6 (Klassifikation) | DORA Art. 8 (Asset-ID) | BaFin-Guidance Kap. Lifecycle
M365-Control: Defender Cloud App Discovery, AI-Inventar (SharePoint Lists), Conditional Access

03 HOCH — Keine AI-Literacy-Nachweise trotz geltender Pflicht

Art. 4 EU AI Act verpflichtet seit Februar 2025 alle Provider und Deployer, ein ausreichendes AI-Kompetenzniveau sicherzustellen. In der Praxis fehlen rollenbasierte Schulungen, Teilnehmerlisten und auditfaehige Nachweise vollstaendig.

Regulatorische Referenz: EU AI Act Art. 4 (gilt seit 2. Feb 2025) | BaFin-Guidance Kap. Kompetenz / Interdisziplinaritaet
M365-Control: SharePoint-basiertes Schulungskonzept, MS Forms Quiz, Teilnehmerliste mit Refresh-Logik

04 HOCH — KI nicht im DORA-Risikoframework verankert

KI-Systeme (inkl. Copilot, ChatGPT, SaaS-KI) sind nicht als ICT-Assets identifiziert und klassifiziert. Kein Bezug zu DORA Art. 5-6 Governance, kein Incident-Pfad fuer KI-bezogene Vorfaelle, keine Third-Party-Bewertung von Microsoft als KI-Provider.

Regulatorische Referenz: DORA Art. 5-6 (Governance), Art. 8 (Asset-ID), Art. 28-30 (Third-Party) | BaFin-Guidance Kap. Strategie
M365-Control: AI-Inventar mit DORA-Kritikalitaet, Provider-Checkliste, Incident-Playbook

05 MITTEL — DLP- und Label-Luecken vor Copilot-Rollout

Sensitivity Labels sind nicht oder nur teilweise ausgerollt. DLP-Policies decken KI-spezifische Szenarien nicht ab. Ohne Labels behandelt Copilot alle Inhalte gleich - kein Unterschied zwischen 'kann geteilt werden' und 'darf nicht geteilt werden'.

Regulatorische Referenz: DORA Art. 9 (Schutz) | EU AI Act Art. 26 Abs. 4 (Input Data Governance, bei High-Risk)
M365-Control: Purview Information Protection, DLP-Policies mit KI-Kontext, SAM Site Access Review

Wollen Sie wissen, welche dieser Findings bei Ihnen zutreffen?

Copilot Governance Quick Scan | 3-5 Tage | ab 3.500 EUR

Top-10 Findings mit regulatorischer Einordnung + 30/60/90-Remediation-Backlog. Keine Rechtsberatung, keine Schreibzugriffe.

QUELLENBASIS

EU AI Act: Reg. (EU) 2024/1689 | digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
DORA: Reg. (EU) 2022/2554 | eur-lex.europa.eu/eli/reg/2022/2554/oj
BaFin-Orientierungshilfe IKT-Risiken bei KI (Jan 2026) | bafin.de
Digital Omnibus on AI: COM(2025) 836 | In Trilogue seit 26. Maerz 2026, pol. Agreement erw. 28. April 2026