

■ **AI ACT UND MDR/IVDR -  
INTEGRATION STATT DOPPELBELASTUNG**

Wie MedTech-Unternehmen ein konformes QMS aufbauen und Compliance zum Wettbewerbsvorteil machen

Wir machen **DIGITALISIERUNG** – aber **SICHER!**

---

# Inhalt

<b>1. Executive Summary</b>	<b>3</b>
<b>2. Kernaussagen auf einen Blick</b>	<b>4</b>
<b>3. Doppelregulierung für SaMD: Was der AI Act konkret verändert</b>	<b>5</b>
3.1 Die neue Doppelregulierung: Was sich ändert	5
3.2 Die vier zentralen Herausforderungen für Hersteller	6
3.3 Was ein integriertes Compliance-System leisten muss	6
<b>4. Das Integrations-Framework: Drei Phasen zur AI-Act-Konformität</b>	<b>8</b>
4.1 Phase 1: Gap-Assessment	8
4.2 Phase 2: QMS-Erweiterung	8
4.3 Phase 3: Evidenz und Monitoring	9
<b>5. Integrierter Ansatz versus parallele Systeme</b>	<b>10</b>
<b>6. Umsetzung: Ein Handlungsrahmen für den Einstieg</b>	<b>10</b>
6.1 Quick Wins: Sofort umsetzbare Maßnahmen	10
6.2 Governance: Wer steuert die Integration?	11
6.3 Change Management: Die Organisation mitnehmen	11
<b>7. Typische Fallstricke und wie Sie sie vermeiden</b>	<b>12</b>
<b>8. Wirtschaftlichkeit und messbare Ergebnisse</b>	<b>12</b>
<b>9. Wie sepp.med Sie unterstützt</b>	<b>13</b>
<b>10. Häufig gestellte Fragen</b>	<b>14</b>
<b>11. Glossar</b>	<b>14</b>
<b>12. Quellenverzeichnis</b>	<b>15</b>



# 1. EXECUTIVE SUMMARY

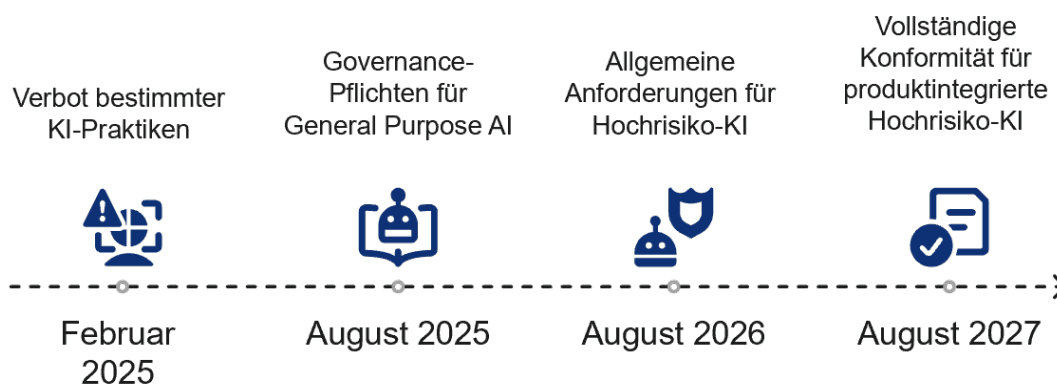
Hersteller von KI-basierter Software as a Medical Device (SaMD) stehen vor einer konkreten Herausforderung: Ab August 2026 gelten die Hochrisiko-Anforderungen des EU AI Act (Verordnung 2024/1689), und KI-basierte SaMD der Klassen IIa bis III werden in der Praxis häufig als Hochrisiko-KI nach Artikel 6 AI Act eingestuft. [1] Viele Unternehmen befürchten eine Verdoppelung des Compliance-Aufwands, doppelte Dokumentation und doppelte Audits.

Hinzu kommt der zeitliche Druck: Die verbleibende Zeit bis August 2026 ist für viele Hersteller bereits kritisch knapp. Wer die Integration der AI-Act-Anforderungen erst kurz vor dem Stichtag angeht, riskiert unnötige Projektverzögerungen, zusätzliche Audit-Schleifen und vermeidbare Nacharbeiten im Zertifizierungsprozess.

Die im Juni 2025 veröffentlichte MDCG 2025-6 Guidance der Medical Device Coordination Group (MDCG) und des Joint Artificial Intelligence Board (AIB) zeigt jedoch einen anderen Weg: Medical Device Regulation (MDR) / In Vitro Diagnostic Regulation (IVDR) und EU AI Act sind komplementäre Rechtsrahmen, die in ein integriertes Qualitätsmanagementsystem (QMS) zusammengeführt werden können und sollen. [2] Dieses Whitespace liefert ein konkretes Framework für diese Integration, ergänzt um eine erweiterte Evidenzstrategie, die klassische klinische Bewertung mit KI-spezifischen Anforderungen verbindet. Der Kern ist damit klar: Der EU AI Act erfordert kein zweites System, sondern ein intelligent erweitertes QMS, das die bestehenden Prozesse um KI-spezifische Anforderungen, Rollen und Nachweise ergänzt.

Wer heute integriert, gewinnt morgen Zeit, Audit-Sicherheit und Vertrauen. Aus regulatorischem Druck wird so ein Wettbewerbsvorteil: eine reibungslosere Zulassung, klinisches Vertrauen und effizientere Prozesse.

## Zeitplan für die AI Act-Konformität von SaMD



---

## 2. KERNAUSSAGEN AUF EINEN BLICK

- Fast alle KI-basierten SaMD (Klasse IIa bis III) werden in der Praxis als Hochrisiko-KI nach Artikel 6 AI Act eingestuft. [1]
- Die Stichtage August 2026 (allgemeine Hochrisiko-Anforderungen) und August 2027 (produktintegrierte Hochrisiko-KI nach Artikel 6 Absatz 1) sind nicht verhandelbar. [3]
- MDR/IVDR und AI Act sind komplementär, nicht konkurrierend. Die MDCG 2025-6 Guidance unterstützt explizit einen integrierten Ansatz. [2]
- Ein integriertes QMS nach ISO 13485 und ISO/IEC 42001 vermeidet Redundanzen und erhöht die Dokumentationseffizienz.
- Klinische Evidenz muss um eine vierte Ebene erweitert werden: Bias-Analysen und Real-World-Performance-Monitoring.
- Frühzeitige Integration schafft Audit-Sicherheit und verkürzt die Time-to-Market.
- Verzögerung riskiert Zulassungsstopps und den Verlust klinischen Vertrauens bei Kliniken und Patienten.
- Die fünf häufigsten Lücken betreffen Risikomanagement, Daten-Governance, Human Oversight, Logging und die frühzeitige Prüfung der zuständigen Benannten Stelle.