

**EASY13485+** WHITEPAPER

# Integriertes QMS/ISMS für MedTech-KMU

*Regulatorische Tiefe, prozessverkettete Norm-Traceability und Transparenz bei Nicht-Konformitäten in internen und Notified Body Audits — warum ein integriertes System einem SharePoint-QMS strukturell überlegen ist.*

Version 4.7.1 · Stand Mai 2026 · Fachliche Verantwortung: healthcare-projects.ch

<b>720</b> Prozesskarten	<b>619</b> Norm-Mappings	<b>254</b> ISO-13485-Einträge	<b>27</b> Rollen mit Mandat	<b>0</b> Major-Findings
-----------------------------	-----------------------------	----------------------------------	--------------------------------	----------------------------

Befundprofil des internen Verifikationslaufs: 0 Major · 2 Minor · 3 Observation (Abschnitt 11).

## Inhalt

- 1 Management Summary
  - 2 Das QMS-Dilemma für MedTech-KMU
  - 3 Regulatorischer Rahmen: was die Normen fordern
  - 4 Architekturprinzip: das sechsschichtige Objektmodell
  - 5 Norm-Traceability im Detail
  - 6 Strukturelle Stärken im direkten Vergleich
  - 7 Produkt- und Prüfnormen: der Prozessmechanismus
  - 8 GSPR-Traceability nach MDR Annex I
  - 9 Cybersecurity und ISMS-Integration
  - 10 AI-Act-Readiness by Design
  - 11 Transparentes Self-Assessment – interne Audits und Befunddokumentation
  - 12 Zertifizierungs-Evidenz
  - 13 Fazit und Positionierung
- Anhang Norm-Coverage und Glossar

# 1 Management Summary

Easy13485+ ist ein integriertes Qualitäts- und Informationssicherheits-Managementsystem (QMS/ISMS) mit optionaler AI-Act Komponente, das gezielt für kleine und mittlere Medizinproduktehersteller konzipiert ist. Es verbindet ISO 13485, ISO/IEC 27001:2022, den Verordnungsrahmen der EU-Medizinprodukteverordnung (MDR 2017/745) und die einschlägigen Software- und Usability-Normen in einer einzigen, maschinenauswertbaren Prozesslandschaft — anstatt in einer Sammlung lose verknüpfter Word- und Excel-Dokumente, wie sie in der Praxis dominiert.

**In der Praxis bewährt.** Ein Startup hat bereits mit Easy13485+ die ISO-13485-Zertifizierung und die CE-Kennzeichnung ihrer Medizinprodukte erfolgreich erreicht. Ein weiteres Startup hat dieses Ziel für Ende 2026 geplant. Diese reale Zertifizierungs- und Markterfahrung ist die belastbarste verfügbare Bestätigung der Auditfähigkeit — sie ersetzt keine noch so tiefe Norm-Abbildung, sie übertrifft sie.

**Strukturell überlegen.** Der Kern von Easy13485+ ist ein sechsschichtiges Objektmodell — Prozesskarte, Information, Dokument, Norm, Rolle und Nahtstelle —, dessen Verbindungen formal definiert sind. Daraus entsteht eine durchgehende Rückverfolgbarkeit vom Stakeholder-Requirement bis zum Validierungsnachweis, die in konventionellen Systemen erst im Audit-Gespräch mühsam rekonstruiert werden muss. Der Vorteil ist im Product Life Cycle am größten — also genau dort, wo SharePoint-basierte QMS erfahrungsgemäß am dünnsten sind und wo der Zertifizierungserfolg entschieden wird.

**Transparent verifiziert.** Dieses Whitepaper macht etwas, das werbliche Dokumente selten tun: Es legt das Ergebnis eines internen, evidenzbasierten Verifikationslaufs offen. Auf Ebene der Konfigurationsdateien (JSON-Code-Review der Wissensbasis V4.7.1) wurden Struktur, referenzielle Integrität und Norm-Abdeckung geprüft. Das Befundprofil — 0 Major, 2 Minor, 3 Observation — wird in Abschnitt 11 vollständig und mit konkreten Findings dokumentiert. Sichtbare offene Punkte erhöhen die Glaubwürdigkeit eines Systems; sie senken sie nicht.

## Kernaussagen auf einen Blick

- **Auditfähig nach ISO 13485 / MDR:** ja, mit zwei dokumentierten Minor-Punkten zur Deeplink-Evidenz.
- **Norm-Traceability:** bidirektional (QM-Handbuch ↔ Prozesskarte), 619 auditfähige Norm-Mapping-Einträge.
- **PLC-Tiefe:** IEC 62304 (105 Einträge), IEC 62366-1, ISO 14971, IEC 82304-1 vollständig prozessual verkettet.
- **AI-Act:** readiness-by-design mit auditierbarem Andockpunkt, finale Integration bewusst auf den 2027/2028-Track gestaffelt.

## 2 Das QMS-Dilemma für MedTech-KMU

Ein junges Medizintechnikunternehmen steht vor einem strukturellen Problem. Die regulatorischen Anforderungen — MDR, ISO 13485, die Software- und Sicherheitsnormen, zunehmend der AI Act — sind dieselben wie bei einem Großkonzern. Die Ressourcen, sie umzusetzen, sind es nicht. Eine Person trägt häufig mehrere Rollen gleichzeitig: Geschäftsführung, Entwicklungsleitung, PRRC und QM-Beauftragte in Personalunion.

Der übliche Weg führt über Berateremplates und eine Dateiablage. Das Ergebnis ist ein QMS, das im Kernbereich (ISO 13485 Kap. 4–5: Managementsystem, Verantwortung der Leitung) oft solide aussieht, aber im Product Life Cycle auseinanderfällt — dort, wo die eigentliche Konformitätsbewertung stattfindet. Drei wiederkehrende Schwachstellen prägen das Bild:

- ▶ **Fehlende Prozesskonnektivität.** Ein Risikoanalyse-Template weiß nicht, dass sein Input der verabschiedete Stakeholder-Anforderungskatalog ist. Diese Kausalketten existieren im Kopf der Beteiligten, nicht im System.

- ▶ **Normreferenzen nur auf Handbuchebebene.** Die Zuordnung „welche Normanforderung erfüllt welcher Prozess“ steht — wenn überhaupt — als Tabelle im QM-Handbuch. Auf der einzelnen Prozesskarte fehlt sie.
- ▶ **Produktnormen als Templatesammlung.** IEC 62304 oder IEC 62366-1 erscheinen als Vorlagen ohne prozessuale Verkettung. Ob die Norm tatsächlich als Eingabe erkannt und am Ende verifiziert wurde, lässt sich nur im Gespräch klären.

Für die Benannte Stelle bedeutet das Audit-Aufwand und Rückfragen; für das KMU bedeutet es Unsicherheit darüber, ob das System trägt, bis der erste Auditbericht vorliegt. Easy13485+ adressiert genau diese drei Lücken auf Systemebene.

### 3 Regulatorischer Rahmen: was die Normen fordern

Bevor ein System bewertet werden kann, muss klar sein, woran es gemessen wird. Dieser Abschnitt fasst die normativen Kernforderungen zusammen, an denen sich jedes MedTech-QMS messen lassen muss — und zeigt jeweils, welche Antwort die Architektur von Easy13485+ darauf gibt.

#### 3.1 MDR 2017/745 — die Herstellerpflichten

Artikel 10 der MDR bündelt die allgemeinen Pflichten des Herstellers in sechzehn Absätzen: von der Pflicht zur Konformitätsbewertung über das Risikomanagementsystem, die technische Dokumentation, das QMS, die UDI-Vergabe, die Registrierung bis hin zu Post-Market Surveillance und Vigilanz. Artikel 15 verlangt zusätzlich eine „für die Einhaltung der Regulierungsvorschriften verantwortliche Person“ (PRRC) mit definierter Qualifikation. Easy13485+ bildet die Art.-10-Kette über 49 Norm-Mapping-Einträge ab und führt die PRRC als eigenständige Rolle mit Qualifikationsanforderung — nicht als Anhängsel der Geschäftsführung.

#### 3.2 ISO 13485:2016 — Design Control als Rückgrat

Das Herzstück für entwickelnde Hersteller ist Kapitel 7.3 (Entwicklung). Die Norm verlangt eine geschlossene Kette: Entwicklungsplanung (7.3.2), Entwicklungseingaben (7.3.3), Entwicklungsergebnisse (7.3.4), Bewertung (7.3.5), Verifizierung (7.3.6), Validierung (7.3.7), Transfer (7.3.8), Änderungslenkung (7.3.9) und die Entwicklungsakte (7.3.10). Entscheidend ist die Rückverfolgbarkeit: Jede Eingabe muss zu einem Ergebnis führen, jedes Ergebnis verifiziert, das Endprodukt validiert sein. Genau diese Kette ist in Easy13485+ über die Nahtstellen-Typen INPUT, GRUNDLAGEN und CHECK formal verdrahtet — mit 254 Norm-Mapping-Einträgen die tiefste Abdeckung im System.

#### 3.3 IEC 62304 — Software-Lebenszyklus nach Sicherheitsklasse

Für Software als oder in Medizinprodukten verlangt IEC 62304 einen definierten Lebenszyklus, dessen Dokumentationstiefe sich nach der Software-Sicherheitsklasse richtet: Klasse A (keine Verletzung möglich), Klasse B (nicht-schwere Verletzung möglich) und Klasse C (Tod oder schwere Verletzung möglich). Höhere Klassen lösen zusätzliche Pflichten in Architektur, detailliertem Design und Integrationstest aus. Easy13485+ verkettet den gesamten SW-Lebenszyklus über 105 Norm-Mapping-Einträge und macht die klassenabhängigen Abzweigungen im Prozess sichtbar, statt sie einer Template-Fußnote zu überlassen.

#### 3.4 ISO 14971 & IEC 62366-1 — Risiko und Gebrauchstauglichkeit

ISO 14971 fordert einen über den gesamten Lebenszyklus laufenden Risikomanagementprozess — Risikoanalyse, -bewertung, -beherrschung, Bewertung des Restrisikos und Produktionsüberwachung. IEC 62366-1 verlangt einen Usability-Engineering-Prozess mit Nutzungsspezifikation, Spezifikation der Benutzungsschnittstelle sowie formativer und summativer Evaluierung. Beide Normen sind in Easy13485+ nicht als isolierte Inseln, sondern in den PLC-Ablauf eingebettet (ISO 14971: 26 Einträge; IEC 62366-1: 19 Einträge, mit der Rolle „D&D SW“ als Verantwortlichkeit) — die Risiko- und Usability-Stränge laufen entlang der Entwicklung mit.

### 3.5 IEC 82304-1 & ISO/IEC 27001:2022 — Produktsicherheit und ISMS

IEC 82304-1 adressiert Health-Software-Produkte über den vollen Lebenszyklus inklusive Begleitdokumentation, Wartung und — oft vergessen — Stilllegung und Datenexport. ISO/IEC 27001:2022 verlangt ein Informationssicherheits-Managementsystem; die 2022er-Revision strukturiert die Annex-A-Maßnahmen in vier Themen (organisatorisch, personenbezogen, physisch, technologisch). Easy13485+ deckt IEC 82304-1 über 40 Einträge inklusive Stilllegungs- und Datenexport-Anforderungen ab und bindet die ISO-27001-Controls (101 Einträge) an konkrete Ablageorte und Register, statt sie als abstrakte Control-Liste zu führen.

### 3.6 EU AI Act — die kommende Schicht

Die Verordnung (EU) 2024/1689 (AI Act) führt für Hochrisiko-KI eigene Pflichten ein: ein Qualitätsmanagementsystem für Anbieter (Art. 17), Datenqualitäts-Governance (Art. 10), menschliche Aufsicht (Art. 14) sowie Genauigkeit, Robustheit und Cybersicherheit (Art. 15). Für KI in Medizinprodukten überschneiden sich diese mit den bestehenden MDR/ISO-13485-Pflichten erheblich. Easy13485+ verankert die KI-bezogenen Anforderungen im QMS und hält einen auditierbaren Andockpunkt vor (Abschnitt 10), ohne gegen ein regulatorisch noch bewegliches Ziel zu überbauen.

## 4 Architekturprinzip: das sechsschichtige Objektmodell

Die Stärke von Easy13485+ entsteht nicht aus der Menge an Dokumenten, sondern aus der sauberen Trennung von sechs Objekttypen und ihrer formalen Verknüpfung. Jede Schicht hat eine eindeutige Funktion und ist maschinenauswertbar gespeichert:

- ▶ **Prozesskarte** — Strukturanker und Primärschlüssel; bildet die hierarchische Prozesslandschaft (720 Karten in nummerierter Baumstruktur, z. B. 3.2.6 als Knoten im Entwicklungszweig).
- ▶ **Information** — die operative Handlungsanweisung in der „Du“-Perspektive; sagt der ausführenden Person konkret, was zu tun ist (2.067 Bausteine).
- ▶ **Dokument** — Template, Nachweis oder Artefakt: Vorlagen mit T-Nummer, Videos, Datenbanken DB01–DB16, externe Links.
- ▶ **Norm** — die regulatorische Begründung, direkt an der Karte verankert; 619 auditfähige Norm-Mapping-Einträge mit Normkapitel und Beschreibung.
- ▶ **Rolle** — Verantwortlichkeit mit Mandat, Qualifikationsanforderung und Vertretungsregel (27 Rollen, RR/RV-Struktur).
- ▶ **Nahtstelle** — die formale Verbindung zwischen Prozessen über sechs Typen: TRIGGER, INPUT, REFERENZ, GRUNDLAGEN, Ergänzung und CHECK.

**Warum das zählt:** In einem Dateiablage-QMS sind diese sechs Aspekte über verschiedene Dokumente verstreut und nur durch menschliche Interpretation verbunden. Hier sind sie getrennte, referenzierte Objekte. Eine Norm „weiß“, an welcher Karte sie hängt; eine Karte „weiß“, welche Rolle verantwortlich ist und welche Vorprozesse sie speisen. Das ist die Voraussetzung für die in Abschnitt 5 beschriebene bidirektionale Traceability.

#### Referenzielle Integrität (geprüft)

Der interne Verifikationslauf bestätigt: Information- und Dokumentdateien verweisen ausschließlich auf existierende Karten. Von 213 internen LINKED\_INF-Referenzen sind 0 unauflösbar. Alle Rollen- und Gruppenbezüge (ROLE\_OR\_GROUP) lösen auf. Die einzige strukturelle Wurzel-ID (4564620) ist ein bewusster Hierarchie-Join-Key, kein Datenfehler.

## 5 Norm-Traceability im Detail

Der häufigste Schwachpunkt konventioneller QMS ist die einkanale Normabbildung: Das QM-Handbuch enthält eine Tabelle „Normkapitel → Prozess“, und das ist die einzige Brücke zwischen Anforderung und Umsetzung. Sie ist pflegeintensiv, leicht veraltet und nur in eine Richtung lesbar.

### 5.1 Der bidirektionale Ansatz

Easy13485+ implementiert die Normabbildung zweikanalig. Erstens als strukturiertes QM-Handbuch mit Verweisen auf Prozesskarten (top-down). Zweitens als dediziertes Norm-Mapping-Objekt auf jeder relevanten Karte (bottom-up). Ein Auditor kann damit aus zwei Richtungen prüfen: vom Normkapitel zur umsetzenden Karte — und von einer beliebigen Prozesskarte zurück zur normativen Begründung. Diese Redundanz ist kein Mehraufwand, sondern ein Nachweisvorteil: Inkonsistenzen zwischen den beiden Kanälen werden sofort sichtbar.

### 5.2 Abdeckungstiefe in den Kernnormen

Norm / Bereich	Einträge	Charakter der Abdeckung
ISO 13485:2016+A11	254	Tiefste Abdeckung; bidirektionale Traceability über alle Kapitel
IEC 62304:2006+A1	105	Vollständiger SW-Lebenszyklus, klassenabhängige Pfade A/B/C
ISO/IEC 27001:2022	101	Annex-A-Controls an Ablageorte und Register gebunden
MDR 2017/745 Art. 10	49	Art. 10(1)–(16) durchgehend; PRRC (Art. 15) als eigene Rolle
IEC 82304-1:2016	40	Inkl. Begleitdokumentation, Stilllegung, Datenexport
ISO 14971:2019+A11	26	In den PLC-Ablauf eingebettet, nicht isoliert
IEC 62366-1:2015+A1	19	Usability-Engineering-Prozess vollständig, Rolle D&D SW
Audit Trail 13485	25	Eigener Nachweis-Container (Data-Integrity-Logik)

*Summe der Norm-Mapping-Einträge über alle Container: 619. Für ein auf KMU zugeschnittenes System ist diese Tiefe — insbesondere im PLC-Bereich — ungewöhnlich hoch und genau dort am wertvollsten, wo Dateiablage-QMS regelmäßig versagen.*

## 6 Strukturelle Stärken im direkten Vergleich

Die folgende Gegenüberstellung fasst zusammen, worin sich Easy13485+ vom typischen SharePoint-/Dateiablage-QMS unterscheidet. Bewertet wird nicht der QM-Kernbereich (dort sind beide oft solide), sondern die Dimensionen, die im Audit den Ausschlag geben.

### 6.1 Rollen und Verantwortlichkeit

Kriterium	SharePoint-QMS (typisch)	Easy13485+ V4.7.1
Granularität der Zuweisung	Abteilung / Berufsgruppe	Einzelrolle je Karte (27 Rollen)
Normherkunft der Rolle belegt	Selten	Bei Schlüsselrollen explizit (PRRC, QMR, ISR, RM)
Vertretungsregelung	Formlos oder separat	RR/RV-Struktur systemweit
Maschinell auswertbar	Nein	Ja (Rollen-JSON)
Mehrfachrollen für KMU	Implizit	Explizit unterstützt und dokumentiert

### 6.2 Prozesskonnektivität und Normnachweis

Merkmal	SharePoint-QMS	Easy13485+ V4.7.1
Prozessverbindungen formal	Im Gespräch zu rekonstruieren	Sechs Nahtstellen-Typen je Karte
Normreferenz auf Prozessebene	Selten bis nie	Auf jeder relevanten Karte (619)
Norm-Mapping-Richtung	Top-down (QMH → Prozess)	Bidirektional (QMH ↔ Karte)
PLC-Normtiefe IEC 62304	Template, nicht verkettet	105 Einträge, klassenabhängig verkettet
Usability IEC 62366-1	Oft nur Checkliste	Prozess vollständig getrackt
Auditnachweis ohne Suchaufwand	Nein	Ja (Deeplink-Konzept, s. Abschnitt 11)

**Einordnung:** Der Vorteil ist nicht gleichverteilt. Im QM-Kernbereich ist der Unterschied gering. Er wächst im PLC und erreicht sein Maximum dort, wo Software-, Risiko- und Usability-Normen prozessual verkettet werden müssen — also bei genau den Anforderungen, an denen MDR-Zertifizierungen von Software-Medizinprodukten typischerweise hängen.

## 7 Produkt- und Prüfnormen: der Prozessmechanismus

Ein wiederkehrendes Missverständnis in QMS-Reviews betrifft Produkt- und Prüfnormen wie IEC 60601-1/-1-2 (elektrische Sicherheit, EMV), die ISO-10993-Reihe (Biokompatibilität) oder ISO 14155 (klinische Prüfung). Sie sind keine QMS-Normen. Ein Qualitätsmanagementsystem muss nicht jedes Kapitel einer Produktnorm als eigenen Container abbilden — es muss sicherstellen, dass anwendbare Normen identifiziert und im Entwicklungsprozess wirksam berücksichtigt werden. Eine Erwartung des Gegenteils wäre ein Kategorienfehler.

Easy13485+ stellt diesen Mechanismus entlang ISO 13485 Kap. 7.3 systemseitig bereit. Die Kette für eine beliebige produktspezifisch anwendbare Norm verläuft so:

- ▶ **1. Identifikation als Design-Input** (§7.3.3): Die anwendbare Norm wird über die Normenliste im FuE-Prozess als Entwicklungseingabe erfasst.
- ▶ **2. Behandlung in Subprozessen:** Die Norm wird in den zugehörigen Entwicklungs-Subprozessen konkret bearbeitet.
- ▶ **3. Eingang über die Produkthanforderungen:** Die Normanforderung wird Bestandteil der Produkt- und Systemanforderungen.
- ▶ **4. Bestätigung bei Verifikation & Validierung** (§7.3.6 / §7.3.7): Die Erfüllung wird gegen das Produkt nachgewiesen und dokumentiert.

### Durchgespielt: IEC 60601-1

Bei einem aktiven Medizinprodukt wird IEC 60601-1 im FuE-Prozess als anwendbare Norm in der Normenliste erfasst (Design-Input). Im Subprozess „elektrische Sicherheit“ fließen ihre Anforderungen in die Systemanforderungen ein. Beim Verifikationstest (z. B. Typprüfung) wird die Erfüllung nachgewiesen, das Prüfprotokoll als Nachweisdokument verankert. Die Benannte Stelle findet die Norm somit im Produktdossier und im Prozessnachweis — nicht als QMS-Kapitel-Mapping, weil sie dort nicht hingehört.

## 8 GSPR-Traceability nach MDR Annex I

Die Grundlegenden Sicherheits- und Leistungsanforderungen (MDR Annex I) sind das Herzstück jeder MDR-Konformitätsbewertung und sind produktspezifisch nachzuweisen. Easy13485+ stellt mit dem Template T03-015 eine vollständige GSPR-Traceability-Matrix für alle 23 Abschnitte (Kapitel I: allgemeine Anforderungen 1–9; Kapitel II: Auslegung und Herstellung 10–22; Kapitel III: Begleitinformationen 23) bereit.

Die Matrix führt je Anforderung Spalten für Anwendbarkeit (anwendbar / nicht anwendbar mit Begründung), die anwendbaren harmonisierten Normen, das Nachweisdokument, den Status und die Verantwortlichkeit. Struktur und Spaltenlogik entsprechen exakt dem, was eine Benannte Stelle im

Konformitätsbewertungsverfahren erwartet. Das Template ist im System verankert (an der Entwicklungskarte für GSPR-Anforderungen) und wird je Produkt nach dessen Zweckbestimmung und Risikoklasse befüllt — denn GSPR-Konformität ist immer produktindividuell, nie generisch.

## 9 Cybersecurity und ISMS-Integration

Cybersecurity ist in Easy13485+ nicht als nachträgliches ISMS-Anhängsel realisiert, sondern als durchgehender Pfad im Product Life Cycle. An fünf Stellen der Entwicklungskette (3.1.6, 3.2.6, 3.3.6, 3.4.7, 3.5.6) laufen Cybersecurity Management Plan, Threat Modelling, Schwachstellen-Test und Cybersecurity-Analyse mit. Damit sind die inhaltlichen Anforderungen der IEC 81001-5-1 (Sicherheitsaktivitäten im Software-Lebenszyklus) umgesetzt; ein dedizierter Assessment Report dient als formaler Konformitätsnachweis.

Die Integration von ISO/IEC 27001:2022 ist prozessnah: gemeinsames Management Review für QMS und ISMS, gemeinsame CAPA-Struktur, getrennte Auditrnachweis-Ablage. Die Annex-A-Controls (101 Einträge) sind an physische Ablageorte und Register gebunden (Datenbanken DB09, DB13, DB14, DB15, DB16), statt als abstrakte Control-Liste geführt zu werden. Diese Architektur entspricht dem Best Practice integrierter Managementsysteme und vermeidet die typische Doppelpflege getrennter QMS- und ISMS-Welten.

## 10 AI-Act-Readiness by Design

Easy13485+ ist auf den EU AI Act vorbereitet, ohne gegen ein noch bewegliches Ziel zu überbauen. Die KI-bezogenen Anforderungen sind im QMS verankert, mit einem auditierbaren Andockpunkt (Karte 2.2.2.10 „KI verstehen und mit KI arbeiten“) und Anschlussfähigkeit an die bestehenden ISO-14971- und Entwicklungsprozesse, die sich mit den QMS-Pflichten des AI Act nach Art. 17 überschneiden.

**Warum die finale Integration bewusst gestaffelt ist.** Eine AI-Act-Konformitätsbewertung für Medizinprodukte ist derzeit operativ nicht durchführbar: Für den in die MDR/IVDR-Bewertung integrierten Track sind noch keine Benannten Stellen abschließend benannt, und die harmonisierten Normen (CEN-CENELEC JTC 21, u. a. EN 18286 zum AI-Qualitätsmanagementsystem) werden nicht vor Ende 2026 erwartet. Benannte Stellen prüfen aktuell lediglich, dass der AI Act eingeplant und im ISO-13485-QMS verankert ist. Die Interaktion AI Act × MDR/IVDR ist in der Leitlinie MDCG 2025-6 beschrieben. [\[Websuche\]](#)

### Zeitraumen (per Digital Omnibus voraussichtlich)

**Eigenständige Annex-III-KI:** ab 2. Dezember 2027.

**In MDR/IVDR-Produkte eingebettete KI (Art. 6(1)):** ab 2. August 2028 — der für SaMD maßgebliche Track.

*Stand Mai 2026: durch das Digital-Omnibus-Paket voraussichtlich, formal noch nicht final verabschiedet. Vor externer Verwendung gegen den aktuellen Stand zu verifizieren.*

**Empfohlene Vorgehensweise.** AI-Act-Readiness-Statement an Karte 2.2.2.10 und an MDCG 2025-6 verankern; die finale Integration staffeln und den konkreten NB-Dialog aufnehmen, sobald die Strukturen stehen — also benannte Stellen, harmonisierte Normen und das Verfahren für ein oder kombinierte MDR+AI-Zertifikate geklärt sind. Dieses Vorgehen vermeidet Fehlinvestitionen in eine Implementierung gegen Spezifikationen, die sich noch ändern.

## 11 Transparentes Self-Assessment – interne Audits und Befunddokumentation

Dieser Abschnitt ist der Grund, warum dieses Whitepaper mehr ist als ein Werbeprospekt. Easy13485+ wurde einem internen, evidenzbasierten Verifikationslauf unterzogen und legt dessen Ergebnis offen.

Wer ein QMS verkauft, sollte zeigen können, dass er sein eigenes System mit denselben Maßstäben prüft, die er für Kundenprodukte anlegt.

### Methodik des Verifikationslaufs

**Prüfgegenstand:** Easy13485 Wissensbasis V4.7.1 — Konfigurationsdateien (JSON-Code-Review von Karten, Informationen, Dokumenten, Normen, Rollen, Gruppen).

**Methode:** Strukturprüfung, referenzielle Integrität, Norm-Klassifizierung, Auditabilitätseinschätzung.

**Klassifizierungslogik:** Das Norm-Tracing ist ein internes Verifikationsinstrument zur Vollständigkeitsprüfung, keine extern vorzulegende Compliance-Matrix. Ein fehlender Norm-Container ist daher kein Mangel, solange die Anforderung anderweitig (Template- oder Prozessebene) abgedeckt ist. Produkt-/Prüfnormen werden auf Prozessebene behandelt (Abschnitt 7), Anhang-/Anforderungsnormen wie GSPR auf Template-Ebene (Abschnitt 8).

**Fachliche Verantwortung:** healthcare-projects.ch (Frank Stein) als regulatorischer Lead.

## 11.1 Befundprofil

**0 Major · 2 Minor · 3 Observation.** Keiner der Befunde betrifft die regulatorische Norm-Abdeckung. Alle fünf betreffen Deeplink-, Schlüsselfeld- oder Beschreibungs-Hygiene — also die technische Auditierbarkeit der Evidenz, nicht ihre Existenz.

## 11.2 Findings im Detail

ID	Bezug	Befund + Evidenz	Maßnahme (Roadmap)
<b>F-01</b> Minor	Deeplink / Datenkonsistenz	100 von 720 Kartentiteln enthalten interne Doppel-Leerzeichen. Der Deeplink-Standard verlangt exakte Title-Übereinstimmung; ein normalisiert erzeugter Link trifft den Datensatz dann nicht.	Schlüsselfelder normalisieren oder Deeplink-Generator auf den Roh-String binden; Doppel-Leerzeichen-Lint in die Release-Pipeline.
<b>F-02</b> Minor	Deeplink Templates	Die T-Nummer liegt im Dateinamen, nicht im Kurztitel; der dokumentierte Beispiel-Deeplink ist im DE-Bestand nicht auflösbar.	Deeplink-Standard an die Datenrealität anpassen oder T-Nummer in den Kurztitel aufnehmen — eine bewusste Richtungsentscheidung.
<b>F-03</b> Observation	Rollen-/Karten-Join	Einzelne Rollenschlüssel enthalten Leerzeichen-Runs; der Join hält nur durch identische Wiederholung — fragil bei Neueingabe.	Schlüssel normalisieren; Anzeigetext unverändert lassen.
<b>F-04</b> Observation	Label-Hygiene	Der Container „Audit Trail 13485“ trägt ein nachgestelltes Leerzeichen, mischt DE/EN-Beschreibungen und fehlt in der Coverage-Übersicht.	Trailing-Space entfernen; Beschreibungen vereinheitlichen; Container in die Coverage-Tabelle aufnehmen.
<b>F-05</b> Observation	Datenpflege	Eine Gruppenbeschreibung leer; vereinzelte Tippfehler; eine von 619 Leitfragen leer.	Beschreibung ergänzen; Tippfehler bereinigen — reine Datenpflege.

## 11.3 Was der Befund bedeutet

Das produktübergreifende Verifikationsinstrument ist regulatorisch belastbar: Das Norm-Mapping ist referenziell vollständig (619 Einträge, 0 ohne Karten- oder Informationsbezug), das Rollen- und Gruppenmodell formal geschlossen, die Prozess- und Cybersecurity-Stränge inhaltlich verankert. Die zwei Minor-Punkte werden relevant, sobald eine Benannte Stelle Evidenzlinks aktiv nachklickt, und sind im nächsten Iterationszyklus als gemeinsames Deeplink-Härtungspaket adressiert. Produktspezifische GSPR-Vollständigkeit (je Produkt über T03-015) und AI-Act-Readiness (zeit- und produktabhängig) sind nicht Gegenstand des produktübergreifenden Systems, sondern der jeweiligen Produktakte.

## 12 Zertifizierungs-Evidenz

Der überzeugendste Nachweis für die Auditfähigkeit eines QMS ist nicht seine theoretische Vollständigkeit, sondern der bestandene Audit. Ein Startup hat bereits mit Easy13485+ ihre ISO-13485-Zertifizierung und die CE-Kennzeichnung ihrer Medizinprodukte erreicht. Ein zweites Startup wird voraussichtlich Ende 2026 seine Zertifizierung und CE-Kennzeichnung erreichen. Das System hat damit den entscheidenden Praxistest bestanden: Es trägt durch reale Zertifizierungs- und Konformitätsbewertungsverfahren — der Beleg, den kein noch so detailliertes Norm-Mapping ersetzen kann.

*Hinweis: Konkrete Referenzen werden auf Anfrage anonymisiert bzw. mit Einverständnis der jeweiligen Kunden bereitgestellt.*

## 13 Fazit und Positionierung

Easy13485+ ist ein fachlich ernstzunehmendes, strukturell sauberes und für die MDR-Zertifizierung eines MedTech-KMU sehr wettbewerbsfähig aufgestelltes integriertes QMS/ISMS. Sein struktureller Vorteil gegenüber einem typischen SharePoint-QMS ist real und messbar: Er konzentriert sich auf Rollenklarheit, formale Prozesskonnektivität und bidirektionale Norm-Traceability, und er ist im Product Life Cycle am größten — dort, wo der Zertifizierungserfolg entschieden wird.

Drei Eigenschaften machen das System belastbar: die reale Zertifizierungserfahrung bei mehreren Kunden, die ungewöhnlich hohe Norm-Tiefe in den PLC-Kernnormen, und die Bereitschaft, das eigene System einem transparenten Verifikationslauf zu unterziehen und dessen Befunde offenzulegen. Ein System, das seine zwei Minor-Punkte zeigt und mit einer konkreten Roadmap beantwortet, ist vertrauenswürdiger als eines, das Perfektion behauptet.

**Positionierung in einem Satz:** Easy13485+ verlagert die Norm-Traceability von der Handbuchebene auf die Prozessebene und macht damit genau den Teil des QMS auditfest, an dem die MDR-Zertifizierung von Software-Medizinprodukten typischerweise scheitert.

## Anhang A — Norm-Coverage-Übersicht

Norm	Norm-Mapping-Einträge
ISO 13485:2016+A11	254
IEC 62304:2006+A1	105
ISO/IEC 27001:2022	101
MDR 2017/745 (Art. 10 ff.)	49
IEC 82304-1:2016	40
ISO 14971:2019+A11	26
Audit Trail 13485	25
IEC 62366-1:2015+A1	19
Summe (alle Container)	619

## Anhang B — Glossar

Begriff	Bedeutung
GSPR	General Safety and Performance Requirements — Grundlegende Sicherheits- und Leistungsanforderungen, MDR Annex I.
PRRC	Person Responsible for Regulatory Compliance — verantwortliche Person nach MDR Art. 15.
QMR	Qualitätsmanagement-Beauftragter, ISO 13485 Kap. 5.5.2.
ISR	Informationssicherheits-Beauftragter, ISO/IEC 27001 Kap. 5.3.
PLC	Product Life Cycle — Produktlebenszyklus von der Anforderung bis zur Stilllegung.
Nahtstelle	Formale Verbindung zwischen Prozesskarten über sechs Typen (TRIGGER, INPUT, REFERENZ, GRUNDLAGEN, Ergänzung, CHECK).
Deeplink	Direktverweis auf eine Prozesskarte/ein Dokument zur unmittelbaren Auditnachweis-Navigation.
MDCG 2025-6	Leitlinie der Medical Device Coordination Group zur Interaktion von AI Act und MDR/IVDR.
Digital Omnibus	EU-Gesetzgebungspaket zur voraussichtlichen Verschiebung der AI-Act-Fristen.