Whitepaper

EU-Regularien für medizinische Labore: Compliance-Wegweiser für die digitale Transformation

Von NIS-2, EU KI-Verordnung bis EHDS

Version 19.10.2025 (fortlaufend aktualisiert)

1. Executive Summary

Zwischen 2016 und 2025 wurden nicht weniger als acht fundamentale Verordnungen und Richtlinien verabschiedet, die jeden Aspekt des modernen Laborbetriebs berühren – von der Cybersicherheit über künstliche Intelligenz bis hin zum Datenschutz und zur Produkthaftung.

Diese regulatorische Welle ist keine zufällige Anhäufung von Vorschriften, sondern eine strategisch orchestrierte Antwort auf die digitale Transformation des Gesundheitswesens. Medizinische Labore, die einst als isolierte Analyseeinrichtungen fungierten, sind heute hochvernetzte, datengetriebene Zentren der modernen Diagnostik. Mit dieser Evolution gehen jedoch neue Risiken einher: Cyberangriffe können kritische Infrastrukturen lahmlegen, fehlerhafte KI-Algorithmen zu Fehldiagnosen führen, und Datenschutzverletzungen das Vertrauen in das gesamte Gesundheitssystem erschüttern.

Die Europäische Union hat auf diese Herausforderungen mit einem umfassenden regulatorischen Rahmenwerk reagiert, das gleichermaßen Schutz und Innovation fördern soll. Dabei zeigt sich ein klarer Trend: weg von nationalen Insellösungen hin zu einem harmonisierten europäischen Rechtsraum. EU-Verordnungen wie die IVDR, MDR, DSGVO und der AI Act gelten unmittelbar in allen Mitgliedstaaten und schaffen einheitliche Standards. Gleichzeitig geben Richtlinien wie die NIS-2 und die neue Produkthaftungsrichtlinie klare Ziele vor, lassen aber Raum für nationale Ausgestaltung.

Für Laborbetreiber bedeutet diese neue Realität eine fundamentale Neuausrichtung ihrer Compliance-Strategien. Die Zeit der reaktiven Anpassung ist vorbei; gefordert ist nun proaktives, systematisches Compliance-Management. Die persönliche Haftung der Geschäftsführung, wie sie die NIS-2-Richtlinie vorsieht, unterstreicht die Ernsthaftigkeit dieser Anforderungen. Gleichzeitig erweitert die neue Produkthaftungsrichtlinie den Haftungsrahmen: Software und KI werden explizit als Produkte definiert, Beweislastumkehrungen greifen bei komplexen Systemen, und Verjährungsfristen von bis zu 25 Jahren bei latenten Gesundheitsschäden schaffen langfristige Haftungsrisiken.

Die Implementierung dieser Regularien erfordert eine grundlegende Transformation der Laborорganisation, der technischen Infrastruktur und der Unternehmenskultur. ISO-Normen spielen dabei eine zentrale Rolle als Brücke zwischen abstrakten rechtlichen Anforderungen und konkreter praktischer Umsetzung. Standards wie ISO 27001 für Informationssicherheit, ISO 42001 für KI-Management oder ISO 13485 für Medizinprodukte-Qualitätsmanagement bieten bewährte Frameworks für die systematische Implementierung.

Die zeitliche Dimension verschärft den Handlungsdruck: Während einige Verordnungen wie die DSGVO bereits seit Jahren in Kraft sind, stehen andere kurz vor der Anwendung. Die KI-Verordnung wird ab Februar 2026 vollständig greifen, der Cyber Resilience Act ab Dezember 2027. Die NIS-2-Richtlinie hätte bereits im Oktober 2024 in nationales Recht umgesetzt sein sollen, die deutsche Umsetzung verzögert sich jedoch. Der European Health Data Space begann ab März 2025 schrittweise Realität zu werden.

Dieses Whitepaper bietet eine Orientierung in dieser komplexen regulatorischen Landschaft. Es analysiert die relevante Verordnung und Richtlinie, erklärt ihre Auswirkungen auf den Laborbetrieb und gibt konkrete Handlungsempfehlungen für die Umsetzung. Dabei wird deutlich: Die Einhaltung dieser Regularien ist keine Option, sondern eine zwingende Notwendigkeit – nicht nur aus rechtlicher Sicht, sondern auch als Grundlage für Qualität, Sicherheit und Vertrauen in der modernen Labordiagnostik.

2. Einleitung

Die Digitalisierung hat das Gesundheitswesen und insbesondere die medizinische Labordiagnostik in den letzten zwei Jahrzehnten transformiert. Was einst manuelle Prozesse mit Reagenzgläsern und Mikroskopen waren, ist heute ein hochautomatisierter, datengetriebener Workflow, der von komplexen Algorithmen, vernetzten Geräten und künstlicher Intelligenz geprägt ist. Mit dieser Transformation gehen jedoch auch neue Herausforderungen und Risiken einher. Cyberangriffe auf Gesundheitseinrichtungen haben in den letzten Jahren exponentiell zugenommen. Ransomware-Attacken legen ganze Krankenhäuser lahm, Datenlecks exponieren sensible Patientendaten, und manipulierte Laborergebnisse könnten theoretisch zu falschen Behandlungsentscheidungen führen.

Parallel dazu hat die Integration von künstlicher Intelligenz in diagnostische Prozesse neue ethische und rechtliche Fragen aufgeworfen. Wenn ein KI-Algorithmus eine Krebsdiagnose stellt oder übersieht – wer trägt die Verantwortung? Wie transparent müssen die Entscheidungsprozesse einer "Black Box" KI sein? Und wie stellen wir sicher, dass algorithmische Verzerrungen nicht zu systematischer Diskriminierung bestimmter Patientengruppen führen?

Die Europäische Union hat auf diese vielschichtigen Herausforderungen mit einem ambitionierten regulatorischen Programm reagiert. Ziel ist es, einen Rechtsrahmen zu schaffen, der Innovation fördert, gleichzeitig aber Sicherheit, Qualität und ethische Standards gewährleistet. Dieser Ansatz spiegelt die europäische Philosophie wider, Technologie in den Dienst des Menschen zu stellen und nicht umgekehrt. Die EU positioniert sich damit als globaler Vorreiter in der Regulierung digitaler Technologien im Gesundheitswesen.

Innerhalb weniger Jahre wurden Rechtsakte verabschiedet, die jeden Aspekt des digitalen Gesundheitswesens adressieren. Von der Datenschutz-Grundverordnung, die 2018 einen neuen globalen Standard für Datenschutz setzte, über die Medizinprodukte-Verordnungen MDR und IVDR, die die Qualitäts- und Sicherheitsanforderungen neu definierten, bis hin zur wegweisenden KI-Verordnung, dem weltweit ersten umfassenden Rechtsrahmen für künstliche Intelligenz.

Für medizinische Labore bedeutet diese, dass sie ihre gesamte Organisationsstruktur und Governance neu ausrichten müssen. Compliance ist nicht länger eine Nebentätigkeit der Rechts- oder Qualitätsabteilung, sondern wird zur strategischen Kernaufgabe der Unternehmensführung. Die in der NIS-2-Richtlinie verankerte persönliche Haftung der Geschäftsführung unterstreicht diese neue Realität nachdrücklich.

Dieses Whitepaper verfolgt das Ziel, medizinischen Laboren, ihren Betreibern, Qualitätsmanagern, IT-Verantwortlichen und Compliance-Beauftragten eine Orientierung in der komplexen regulatorischen Landschaft der EU zu bieten. Es soll als praktischer Leitfaden dienen, der nicht nur die rechtlichen Anforderungen erklärt, sondern auch konkrete Wege zur Umsetzung aufzeigt.

Ein weiterer Schwerpunkt ist die Identifikation von Synergien. Viele Anforderungen verschiedener Regularien überschneiden sich oder ergänzen sich gegenseitig. Ein gut implementiertes Informationssicherheitsmanagementsystem nach ISO 27001 erfüllt beispielsweise gleichzeitig Anforderungen der NIS-2-Richtlinie, der DSGVO und des Cyber Resilience Act. Diese Synergien zu erkennen und zu nutzen, ist essentiell für eine effiziente Compliance-Strategie.

Das Whitepaper adressiert verschiedene Zielgruppen: Geschäftsführer und Laborleiter erhalten einen strategischen Überblick und Entscheidungsgrundlagen, Compliance-Verantwortliche und Qualitätsmanager finden

detaillierte Anforderungsanalysen und Umsetzungshinweise, IT-Verantwortliche erhalten spezifische Informationen zu technischen Anforderungen, und Datenschutzbeauftragte finden Orientierung bei der Integration datenschutzrechtlicher Anforderungen.

Abschließend sei betont, dass dieses Whitepaper eine Momentaufnahme darstellt. Die regulatorische Landschaft ist in ständiger Bewegung. Neue Verordnungen werden erlassen, bestehende werden novelliert, Leitlinien werden veröffentlicht und Gerichtsentscheidungen prägen die Auslegung. Dennoch bietet dieses Whitepaper eine solide Grundlage für die Entwicklung einer zukunftsfähigen Compliance-Strategie. Es vermittelt nicht nur Wissen über aktuelle Anforderungen, sondern auch ein Verständnis für die zugrundeliegenden Prinzipien und Trends, die die regulatorische Entwicklung prägen werden.

3. Rechtlicher Rahmen der EU

3.1 Das europäische Rechtssystem

Die Rechtsetzung in der EU folgt einem Verfahren, das demokratische Legitimation, fachliche Expertise und die Interessen der Mitgliedstaaten ausbalanciert. Die Europäische Kommission hat das alleinige Initiativrecht für Gesetzgebung – ein Privileg, das ihre Rolle als "Hüterin der Verträge" unterstreicht. Gesetzesvorschläge der Kommission basieren in der Regel auf umfangreichen Konsultationen mit Stakeholdern, Folgenabschätzungen und wissenschaftlichen Gutachten. Gerade im Bereich der Gesundheitsregulierung spielen Expertengremien, wissenschaftliche Ausschüsse und Agenturen wie die Europäische Arzneimittel-Agentur (EMA) eine wichtige beratende Rolle.

Das ordentliche Gesetzgebungsverfahren, früher als Mitentscheidungsverfahren bekannt, ist der Standardweg für die meisten EU-Rechtsakte. Hier entscheiden das Europäische Parlament als direkt gewählte Vertretung der EU-Bürger und der Rat der Europäischen Union als Vertretung der Mitgliedstaaten gemeinsam. Dieses Verfahren kann sich über Monate oder sogar Jahre erstrecken und umfasst mehrere Lesungen, Trilog-Verhandlungen zwischen Parlament, Rat und Kommission sowie zahlreiche Kompromisse. Die Komplexität dieses Verfahrens erklärt, warum zwischen der ersten Ankündigung einer Regulierung und ihrem Inkrafttreten oft Jahre vergehen – eine Zeit, die Labore für die Vorbereitung nutzen sollten.

Die Hierarchie der EU-Rechtsakte ist klar strukturiert. An der Spitze stehen die Verträge (Primärrecht), gefolgt von allgemeinen Rechtsgrundsätzen und der Grundrechtecharta. Darunter folgt das Sekundärrecht mit Verordnungen, Richtlinien, Beschlüssen, Empfehlungen und Stellungnahmen. Für medizinische Labore sind primär Verordnungen und Richtlinien relevant, wobei die Wahl des Instruments praktische Auswirkungen hat. Ergänzt wird dieses formelle Recht durch sogenanntes "Soft Law" – Leitlinien, Mitteilungen, Empfehlungen und Standards, die zwar nicht rechtlich bindend sind, aber erheblichen faktischen Einfluss haben, insbesondere bei der Auslegung und praktischen Anwendung der formellen Rechtsakte.

3.2 EU-Verordnungen: Unmittelbare Geltung und einheitliche Anwendung

Eine EU-Verordnung (englisch: Regulation) ist das stärkste legislative Instrument der Europäischen Union. Artikel 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) definiert sie als "in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat". Die unmittelbare Geltung bedeutet, dass eine Verordnung ab ihrem Geltungsdatum automatisch Teil der nationalen Rechtsordnung wird, ohne dass ein nationaler Umsetzungsakt erforderlich wäre. Wenn beispielsweise die DSGVO am 25. Mai 2018 in Kraft trat, galten ihre Bestimmungen ab diesem

Tag in allen 27 Mitgliedstaaten, von Portugal bis Polen, von Schweden bis Malta. Für Labore bedeutet dies Rechtssicherheit und Planbarkeit – sie können sich auf den Verordnungstext verlassen und müssen nicht auf nationale Umsetzungsgesetze warten.

Die Verbindlichkeit in allen Teilen unterscheidet Verordnungen fundamental von Richtlinien. Mitgliedstaaten können nicht einzelne Artikel einer Verordnung umsetzen und andere ignorieren, sie können keine abweichenden nationalen Regelungen treffen (es sei denn, die Verordnung sieht explizit Öffnungsklauseln vor), und sie können die Anwendung nicht verzögern oder modifizieren. Diese Rigorosität mag zunächst als Einschränkung nationaler Souveränität erscheinen, ist aber essentiell für das Funktionieren des Binnenmarktes. Stellen Sie sich vor, jeder Mitgliedstaat hätte seine eigenen Datenschutzregeln für Gesundheitsdaten – der grenzüberschreitende Datenaustausch, wie er für moderne Labormedizin essentiell ist, wäre praktisch unmöglich.

Die einheitliche Anwendung wird durch den Europäischen Gerichtshof (EuGH) sichergestellt, der als oberste Instanz für die Auslegung des EU-Rechts fungiert. Seine Entscheidungen sind für alle nationalen Gerichte bindend. Dies schafft eine bemerkenswerte Rechtssicherheit: Ein Urteil des EuGH zur Auslegung der DSGVO gilt automatisch in allen Mitgliedstaaten. Für international tätige Laborkonzerne ist dies ein enormer Vorteil gegenüber einem Flickenteppich nationaler Regelungen.

Allerdings bedeutet unmittelbare Geltung nicht, dass Verordnungen keine nationalen Begleitmaßnahmen erfordern. Viele Verordnungen enthalten Öffnungsklauseln oder Bereiche, in denen Mitgliedstaaten Präzisierungen vornehmen können oder müssen. Die DSGVO beispielsweise enthält über 70 solcher Öffnungsklauseln. So können Mitgliedstaaten die Altersgrenze für die Einwilligung von Kindern zwischen 13 und 16 Jahren festlegen oder spezifische Regelungen für die Verarbeitung von Gesundheitsdaten im öffentlichen Gesundheitswesen treffen. In Deutschland wurden diese Spielräume durch das Bundesdatenschutzgesetz (BDSG) und zahlreiche bereichsspezifische Gesetze ausgefüllt.

Ein weiterer wichtiger Aspekt von Verordnungen ist ihre horizontale Direktwirkung. Bürger und Unternehmen können sich direkt auf Verordnungen berufen, sowohl gegenüber staatlichen Stellen (vertikale Direktwirkung) als auch gegenüber anderen Privaten (horizontale Direktwirkung). Ein Patient kann sich beispielsweise direkt auf seine Rechte aus der DSGVO berufen, wenn ein Labor seine Auskunftsanfrage ignoriert. Diese Direktwirkung macht Verordnungen zu mächtigen Instrumenten des Verbraucherschutzes.

Die Durchsetzung von Verordnungen erfolgt auf mehreren Ebenen. Die Europäische Kommission überwacht die Anwendung und kann Vertragsverletzungsverfahren gegen Mitgliedstaaten einleiten, die Verordnungen nicht korrekt anwenden. Nationale Aufsichtsbehörden sind für die praktische Durchsetzung zuständig – bei der DSGVO sind dies die Datenschutzbehörden, bei der MDR die zuständigen Behörden für Medizinprodukte. Diese Behörden arbeiten zunehmend in europäischen Netzwerken zusammen, tauschen Informationen aus und koordinieren ihre Durchsetzungsmaßnahmen. Für Labore bedeutet dies, dass sie sich nicht auf unterschiedliche Durchsetzungspraktiken in verschiedenen Mitgliedstaaten verlassen können – die Harmonisierung betrifft auch die Aufsicht.

3.3 EU-Richtlinien: Ziele vorgeben, Wege offenlassen

EU-Richtlinien (englisch: Directives) repräsentieren einen anderen regulatorischen Ansatz, der Harmonisierung mit nationaler Flexibilität verbindet. Nach Artikel 288 AEUV ist eine Richtlinie "hinsichtlich des zu erreichenden

Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel". Dieser Ansatz reflektiert das Subsidiaritätsprinzip und respektiert die Vielfalt nationaler Rechtstraditionen und Verwaltungsstrukturen.

Der fundamentale Unterschied zu Verordnungen liegt in der Notwendigkeit der nationalen Umsetzung. Eine Richtlinie wird nicht automatisch Teil des nationalen Rechts, sondern muss durch nationale Gesetzgebungsakte transformiert werden. Dies gibt den Mitgliedstaaten erhebliche Gestaltungsspielräume. Sie können entscheiden, ob sie die Umsetzung durch ein einzelnes Gesetz oder mehrere Rechtsakte vornehmen, ob sie bestehende Gesetze anpassen oder neue schaffen, und wie sie die Richtlinienziele in ihr bestehendes Rechtssystem integrieren.

Die Umsetzungsfrist ist ein kritischer Aspekt von Richtlinien. Typischerweise haben Mitgliedstaaten 18 bis 24 Monate Zeit für die Umsetzung, bei besonders komplexen Materien auch länger. Diese Frist soll ausreichend Zeit für den nationalen Gesetzgebungsprozess bieten, einschließlich parlamentarischer Beratungen, Stakeholder-Konsultationen und gegebenenfalls verfassungsrechtlicher Prüfungen. Für Labore schafft dies eine gewisse Unsicherheit: Bis zur nationalen Umsetzung ist oft unklar, wie genau die Anforderungen aussehen werden. Andererseits bietet die Umsetzungsfrist auch eine Vorbereitungszeit, in der Labore sich auf kommende Anforderungen einstellen können.

Die Umsetzungstreue ist ein zentrales Prinzip des EU-Rechts. Mitgliedstaaten müssen die Ziele der Richtlinie vollständig und korrekt umsetzen. Sie dürfen weder hinter den Anforderungen zurückbleiben (Minderumsetzung) noch ohne Rechtfertigung darüber hinausgehen (Überschießende Umsetzung oder "Gold-Plating"). Die Kommission überwacht die Umsetzung akribisch und leitet bei Mängeln Vertragsverletzungsverfahren ein. Dennoch kommt es regelmäßig zu Umsetzungsdefiziten. Die NIS-2-Richtlinie beispielsweise sollte bis Oktober 2024 umgesetzt werden, doch viele Mitgliedstaaten, einschließlich Deutschlands, haben diese Frist verpasst.

Ein komplexes Phänomen ist die unmittelbare Wirkung von Richtlinien. Obwohl Richtlinien grundsätzlich der Umsetzung bedürfen, hat der EuGH unter bestimmten Bedingungen eine unmittelbare Wirkung anerkannt. Wenn eine Richtlinienbestimmung inhaltlich unbedingt und hinreichend bestimmt ist und die Umsetzungsfrist abgelaufen ist, können sich Bürger gegenüber dem Staat direkt auf die Richtlinie berufen (vertikale Direktwirkung). Dies ist besonders relevant, wenn Mitgliedstaaten die Umsetzung verzögern. Allerdings gilt dies nicht im Verhältnis zwischen Privaten (keine horizontale Direktwirkung) – ein wichtiger Unterschied zu Verordnungen.

Die richtlinienkonforme Auslegung ist ein weiteres wichtiges Prinzip. Nationale Gerichte sind verpflichtet, nationales Recht im Licht der Richtlinienziele auszulegen, auch wenn die Richtlinie noch nicht oder unvollständig umgesetzt wurde. Dies kann dazu führen, dass nationale Vorschriften anders interpretiert werden müssen als ursprünglich intendiert, um Konformität mit EU-Recht herzustellen.

Ein praktisches Beispiel für die Komplexität der Richtlinienumsetzung ist die NIS-2-Richtlinie. Sie gibt das Ziel vor, die Cybersicherheit kritischer Infrastrukturen zu erhöhen, lässt aber den Mitgliedstaaten Spielraum bei der Definition der betroffenen Einrichtungen, der konkreten Sicherheitsanforderungen und der Sanktionen. Deutschland plant die Umsetzung durch das NIS2UmsuCG, das deutlich über die Minimalanforderungen der Richtlinie hinausgeht und spezifische Sektorregeln für das Gesundheitswesen enthält. Frankreich hingegen verfolgt einen anderen Ansatz mit stärkerer Integration in bestehende Sicherheitsgesetze. Für ein international tätiges Labor bedeutet dies, dass es trotz der harmonisierenden Wirkung der

Richtlinie mit unterschiedlichen nationalen Anforderungen konfrontiert sein kann.

4. Übersicht über die Verordnungen und Richtlinien für medizinische Labore

Das regulatorische Gebäude, in dem sich medizinische Labore heute bewegen, ruht auf acht zentralen Säulen, die jeweils unterschiedliche, aber komplementäre Aspekte des Laborbetriebs adressieren. Diese Regularien sind nicht als isolierte Vorschriften zu verstehen, sondern als integrierte Komponenten eines umfassenden Regelwerks, das die Transformation des Gesundheitswesens im digitalen Zeitalter begleitet und gestaltet.

Die NIS-2-Richtlinie (Directive (EU) 2022/2555) bildet das Fundament der Cybersicherheit für kritische Infrastrukturen. Als Nachfolger der ursprünglichen NIS-Richtlinie erweitert sie den Anwendungsbereich und erfasst nun explizit medizinische Labore als Teil der kritischen Gesundheitsinfrastruktur. Mit ihren zehn Mindestmaßnahmen für Cybersicherheit, strikten Meldepflichten innerhalb von 24 Stunden und der Einführung persönlicher Haftung für die Geschäftsführung setzt sie neue Maßstäbe. Die deutsche Umsetzung durch das NIS2UmsuCG, ursprünglich für Oktober 2024 geplant, verzögert sich zwar, doch die Vorbereitungen sollten bereits jetzt mit Hochdruck laufen. Der Implementierung eines Information Security Management Systems nach dem B3S-Standard kommt dabei besondere Bedeutung zu. Weitere Informationen finden sich unter https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de und https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html.

Die neue Produkthaftungsrichtlinie (Directive (EU) 2024/2853) markiert einen Paradigmenwechsel im Haftungsrecht. Erstmals werden Software und künstliche Intelligenz explizit als haftungsrelevante Produkte definiert, was für Labore, die zunehmend auf softwarebasierte Diagnostik und KI-gestützte Analyseverfahren setzen, weitreichende Konsequenzen hat. Die Beweislastumkehr bei technischer Komplexität stellt Labore vor neue Herausforderungen: Sie müssen im Schadensfall nachweisen können, dass ihre Systeme einwandfrei funktioniert haben. Besonders ist die Ausweitung auf psychische Schäden und Datenverlust als ersatzfähige Schadensarten sowie die verlängerte Verjährungsfrist von 25 Jahren bei latenten Gesundheitsschäden. Die Umsetzung in nationales Recht muss bis Dezember 2026 erfolgen, was Laboren Zeit gibt, ihre Dokumentation zu verschärfen, Validierungsprozesse zu intensivieren und Haftpflichtversicherungen anzupassen. Details zur Richtlinie finden sich unter https://eur-lex.europa.eu/eli/dir/2024/2853/oj?eliuri=eli%3Adir%3A2024%3A2853%3Aoj&locale=de.

Die KI-Verordnung (Regulation (EU) 2024/1689) etabliert als weltweit erstes umfassendes Regelwerk für künstliche Intelligenz einen risikobasierten Ansatz, der KI-Systeme in vier Kategorien einteilt. Für medizinische Labore ist relevant, dass KI in der Diagnostik meist als Hochrisiko-KI klassifiziert wird, was umfassende Anforderungen nach sich zieht. Die CE-Kennzeichnung für KI-Systeme, strikte Transparenz- und Dokumentationspflichten sowie die Forderung nach menschlicher Aufsicht bei kritischen Entscheidungen prägen das neue Regelwerk. Ab Februar 2026 müssen Labore vollständige Compliance nachweisen können, was eine systematische Klassifizierung aller eingesetzten KI-Systeme, Konformitätsbewertungen und den Aufbau eines spezifischen Qualitätsmanagements für KI erfordert. Die Verordnung ist abrufbar unter https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=de.

Der Cyber Resilience Act (Regulation (EU) 2024/2847) richtet sich primär an Hersteller vernetzter Produkte, hat aber Auswirkungen auf Labore als Anwender. Die Verordnung fordert Cybersicherheit über den gesamten Produktlebenszyklus, wobei eine wichtige

Ausnahme für Medizinprodukte gilt, die bereits durch MDR und IVDR reguliert werden. Dennoch fallen viele in Laboren eingesetzte Systeme unter den CRA: Laborgeräte ohne Medizinprodukt-Status, Laborinformationssysteme, Middleware-Lösungen und allgemeine IT-Infrastruktur. Die Pflicht zur Software-Stückliste (SBOM) und das geforderte Schwachstellenmanagement werden die Beziehungen zwischen Laboren und ihren Lieferanten grundlegend verändern. Ab Dezember 2027 dürfen nur noch CRA-konforme Produkte eingesetzt werden. Die Verordnung findet sich unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847.

Die In-vitro-Diagnostika-Verordnung (Regulation (EU) 2017/746), kurz IVDR, hat die Landschaft der Labordiagnostik ebenfalls verändert. Mit der Einführung eines risikobasierten Klassifizierungssystems von A bis D und verschärften Anforderungen an klinische Evidenz und Leistungsbewertung setzt sie neue Standards. Für Labore besonders ist die strikte Regulierung von Laboratory Developed Tests (LDTs): Diese dürfen nur noch entwickelt und eingesetzt werden, wenn nachweislich kein gleichwertiges CE-zertifiziertes IVD auf dem Markt verfügbar ist. Die verstärkte Post-Market-Surveillance und das Unique Device Identifier-System für lückenlose Rückverfolgbarkeit erhöhen den administrativen Aufwand erheblich. Die Übergangsfristen erstrecken sich noch bis 2027/2028, doch die Zeit sollte intensiv für die Anpassung genutzt werden. Die konsolidierte Fassung ist verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02017R0746-20250110.

Die Medizinprodukte-Verordnung (Regulation (EU) 2017/745), die MDR, komplementiert die IVDR für alle nicht-IVD Medizinprodukte im Labor. Zentrifugen, Analysesoftware mit medizinischem Zweck und Point-of-Care-Testing-Geräte fallen in ihren Geltungsbereich. Die Klassifizierung in die Risikoklassen I, IIa, IIb und III bestimmt die regulatorischen Anforderungen. Besondere Aufmerksamkeit verdient Software als Medizinprodukt (SaMD), deren Klassifizierung oft komplex ist. Die EUDAMED-Datenbank wird künftig für Transparenz und Rückverfolgbarkeit sorgen. Labore müssen sowohl ihre Betreiberpflichten dokumentieren als auch bei Eigenherstellungen Herstellerpflichten erfüllen. Die Verordnung ist einsehbar unter https://eur-lex.europa.eu/eli/reg/2017/745/oj?locale=de.

Die Datenschutz-Grundverordnung (Regulation (EU) 2016/679), seit Mai 2018 in Kraft, bildet das Fundament des Datenschutzes im digitalen Zeitalter. Für medizinische Labore, die ausschließlich mit Gesundheitsdaten als besonderer Kategorie personenbezogener Daten arbeiten, gelten die strengsten Anforderungen. Die Rechtsgrundlagen für die Verarbeitung müssen sorgfältig geprüft werden, sei es Einwilligung, Behandlungsvertrag oder die Regelungen des §22 BDSG. Die Bestellung eines Datenschutzbeauftragten ist ab 20 Mitarbeitern, die regelmäßig mit Gesundheitsdaten arbeiten, verpflichtend. Technische und organisatorische Maßnahmen müssen dem Stand der Technik entsprechen, Verarbeitungsverzeichnisse akribisch geführt und Auftragsverarbeiterverträge sorgfältig gestaltet werden. Bei Verstößen drohen Bußgelder bis zu 4% des weltweiten Jahresumsatzes. Die DSGVO findet sich unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 .

Der European Health Data Space (Regulation (EU) 2025/327), der ab März 2025 gilt, unterscheidet zwischen Primärnutzung für die Patientenversorgung und Sekundärnutzung für Forschung und Public Health. Ab März 2029 müssen Patientenkurzakten EU-weit zugänglich sein, ab März 2031 auch Laborergebnisse. Dies erfordert von Laboren eine fundamentale Transformation ihrer IT-Infrastruktur: Die Implementierung von HL7 FHIR und LOINC-Standards wird unumgänglich, Schnittstellen müssen vorbereitet und die Datenqualität auf ein neues Niveau gehoben werden. Die MyHealth@EU-Anbindung und ein funktionierendes Opt-Out-Management werden

zu kritischen Erfolgsfaktoren. Informationen finden sich unter https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng.

5. NIS-2-Richtlinie (EU) 2022/2555

Als direkte Nachfolgerin der ursprünglichen NIS-Richtlinie von 2016 erweitert NIS-2 nicht nur den Geltungsbereich erheblich, sondern führt auch grundlegend neue Konzepte ein, die speziell für medizinische Labore weitreichende Konsequenzen haben. Die Ransomware-Attacke auf das Universitätsklinikum Düsseldorf 2020, die zum ersten dokumentierten Todesfall durch einen Cyberangriff führte, unterstreicht die existenzielle Bedeutung robuster Cybersicherheit im Gesundheitswesen (https://tinyurl.com/ytv9ttkj)

Mit der expliziten Aufnahme des Gesundheitssektors in die Liste der 18 kritischen Sektoren macht die Richtlinie unmissverständlich klar, dass medizinische Labore als integraler Bestandteil der kritischen Gesundheitsinfrastruktur zu betrachten sind. Die Schwellenwerte für die Anwendbarkeit sind dabei bewusst niedrig angesetzt: Labore mit mehr als 50 Mitarbeitern oder einem Jahresumsatz über 10 Millionen Euro fallen automatisch in den Geltungsbereich. Doch selbst kleinere Einrichtungen können erfasst werden, wenn sie als einziger Anbieter in einer Region fungieren, ihre Dienste von besonderer Systemrelevanz sind oder sie Teil eines größeren Verbunds wie eines Medizinischen Versorgungszentrums sind.

Die zehn Mindestmaßnahmen, die Artikel 21 der Richtlinie definiert, bilden das Herzstück der neuen Anforderungen. Diese reichen von umfassenden Risikoanalysen und Sicherheitskonzepten über etablierte Incident-Response-Prozesse bis hin zu Business Continuity Management und Krisenmanagement. Besondere Bedeutung kommt der Sicherheit der Lieferkette zu – ein Aspekt, der in der Labormedizin angesichts der Vielzahl von Geräteherstellern, Software-Anbietern und Dienstleistern besonders komplex ist. Die Forderung nach Multi-Faktor-Authentifizierung für kritische Systeme mag technisch trivial erscheinen, stellt aber viele Labore vor praktische Herausforderungen, wenn beispielsweise Mitarbeiter mit Handschuhen arbeiten oder schneller Zugriff auf Notfallsysteme gewährleistet sein muss.

Innerhalb von nur 24 Stunden nach Kenntnisnahme eines signifikanten Vorfalls muss eine Frühwarnung an die zuständige Behörde erfolgen. Diese extrem kurze Frist erfordert definierte Prozesse und Verantwortlichkeiten, die rund um die Uhr funktionieren müssen. Nach 72 Stunden folgt eine detaillierte Vorfallsmeldung, und binnen eines Monats muss ein umfassender Abschlussbericht mit Lessons Learned vorgelegt werden.

Die vielleicht gravierendste Neuerung der NIS-2-Richtlinie ist die Einführung persönlicher Haftung für Leitungsorgane. Geschäftsführer und Vorstände können persönlich zur Verantwortung gezogen werden, wenn sie ihrer Aufsichtspflicht in Bezug auf Cybersicherheit nicht nachkommen. Diese Haftung ist nicht auf Extremfälle beschränkt, sondern greift bereits bei Vernachlässigung notwendiger Investitionen, Ignorieren von Audit-Ergebnissen oder unzureichender Reaktion auf bekannte Schwachstellen. Die Richtlinie fordert explizit, dass Führungskräfte Cybersicherheitsschulungen absolvieren müssen.

Die deutsche Umsetzung der Richtlinie durch das NIS2UmsuCG verzögert sich zwar gegenüber der ursprünglichen Frist vom 17. Oktober 2024, doch dies sollte Labore nicht zur Untätigkeit verleiten. Die Vorbereitung auf die kommenden Anforderungen benötigt erhebliche Zeit und Ressourcen. Die Implementierung eines Information Security Management Systems (ISMS) nach dem branchenspezifischen Sicherheitsstandard (B3S) für das Gesundheitswesen, wie unter

https://tinyurl.com/33ycx8e8 beschrieben, ist keine Angelegenheit von Wochen, sondern erfordert Monate systematischer Arbeit. Dies umfasst nicht nur die technische Implementierung von Sicherheitsmaßnahmen, sondern auch die Etablierung von Prozessen, die Schulung von Mitarbeitern und die Schaffung einer Sicherheitskultur.

Die praktische Umsetzung beginnt mit einer Bestandsaufnahme der aktuellen Sicherheitslage. Viele Labore unterschätzen die Komplexität ihrer IT-Landschaft erheblich. Neben dem offensichtlichen Laborinformationssystem existieren oft Dutzende von vernetzten Analysegeräten, Middleware-Lösungen, Schnittstellen zu Praxen und Krankenhäusern, Cloud-Dienste für Datenspeicherung und -analyse sowie eine Vielzahl von administrativen Systemen. Jedes dieser Systeme stellt potenzielle Angriffsvektoren dar und muss in die Sicherheitsbetrachtung einbezogen werden. Die geforderte Risikoanalyse muss dabei über reine IT-Risiken hinausgehen und die potenziellen Auswirkungen auf Patienten berücksichtigen: Was passiert, wenn kritische Testergebnisse verzögert werden? Welche Konsequenzen hätte die Manipulation von Laborwerten? Wie würde das Labor auf einen vollständigen Systemausfall reagieren?

Die 24-Stunden-Frist für die Frühwarnung bedeutet, dass auch außerhalb der regulären Arbeitszeiten – nachts, an Wochenenden und Feiertagen – qualifiziertes Personal verfügbar sein muss, das Sicherheitsvorfälle bewerten und Meldungen erstellen kann. Dies erfordert nicht nur Rufbereitschaftsdienste, sondern auch klare Eskalationswege und Entscheidungsbefugnisse. Die Koordination mit anderen Meldepflichten, etwa nach DSGVO oder MDR/IVDR, verkompliziert die Situation zusätzlich.

Die Sicherheit der Lieferkette erweist sich als besonders komplex. Ein modernes Labor arbeitet mit Dutzenden, wenn nicht Hunderten von Lieferanten und Dienstleistern zusammen. Von jedem dieser Partner gehen potenzielle Cyberrisiken aus. Die Bewertung und Überwachung all dieser Lieferanten übersteigt oft die Kapazitäten einzelner Labore. Hier wird Zusammenarbeit innerhalb der Branche essentiell: Gemeinsame Anforderungen an Lieferanten, geteilte Auditergebnisse und koordinierte Sicherheitsstandards können die Last für einzelne Labore reduzieren und gleichzeitig die Gesamtsicherheit erhöhen.

Neben den direkten Investitionen in Technologie und Personal drohen bei Verstößen Geldbußen von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes für wesentliche Einrichtungen. Die Erfahrungen mit der DSGVO zeigen, dass europäische Regulierungsbehörden bereit sind, empfindliche Strafen zu verhängen. Für Laborleiter bedeutet dies, dass Investitionen in Cybersicherheit nicht mehr als Kostenfaktor, sondern als existenzielle Notwendigkeit betrachtet werden müssen.

Trotz aller Herausforderungen bietet die NIS-2-Richtlinie auch Chancen. Labore, die die Anforderungen erfolgreich umsetzen, positionieren sich als vertrauenswürdige Partner im Gesundheitssystem. Robuste Cybersicherheit kann zum Wettbewerbsvorteil werden, insbesondere wenn Auftraggeber zunehmend Wert auf nachweisbare Sicherheitsstandards legen. Die erzwungene Professionalisierung der IT-Sicherheit führt zu resilienteren Systemen, die nicht nur gegen Cyberangriffe, sondern auch gegen andere Störungen besser gewappnet sind. Die verbesserte Dokumentation und die etablierten Prozesse erhöhen die operative Effizienz und reduzieren langfristig Risiken und Kosten.

Referenzen:

Richtlinientext: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de

Deutsche Umsetzung: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

B3S-Standard: https://tinyurl.com/33ycx8e8

6. Produkthaftungsrichtlinie (EU) 2024/2853

Die neue Produkthaftungsrichtlinie vom 28. November 2024 markiert einen Wendepunkt im europäischen Haftungsrecht und reflektiert die tiefgreifenden technologischen Veränderungen der letzten Jahrzehnte. Während die ursprüngliche Produkthaftungsrichtlinie von 1985 noch in einer Zeit entstand, als Software bestenfalls eine Randerscheinung war und künstliche Intelligenz ins Reich der Science-Fiction gehörte, trägt die neue Richtlinie der digitalen Realität des 21. Jahrhunderts Rechnung. Für medizinische Labore, die zunehmend auf softwarebasierte Diagnostik, algorithmische Auswertungen und KI-gestützte Analyseverfahren setzen, bedeutet diese Neuregelung eine fundamentale Erweiterung ihrer Haftungsrisiken.

Bislang bewegte sich Software in einer rechtlichen Grauzone, in der unklar war, ob und inwieweit Produkthaftungsregeln Anwendung finden. Die neue Richtlinie schafft hier Klarheit: Software ist ein Produkt wie jedes andere auch, und ihre Fehler können Haftungsansprüche auslösen. Für Labore bedeutet dies, dass praktisch jede eingesetzte Software – vom Laborinformationssystem über Schnittstellen-Software bis hin zu selbstentwickelten Auswertungstools – potenzielle Haftungsrisiken birgt. Besonders brisant wird dies bei Laboratory Developed Tests, die zunehmend Software-Komponenten enthalten, sei es für die Datenanalyse, die Interpretation von Ergebnissen oder die Qualitätskontrolle.

Traditionell musste der Geschädigte nachweisen, dass ein Produkt fehlerhaft war und dieser Fehler den Schaden verursacht hat. Bei komplexen technischen Systemen, insbesondere bei KI-basierten Lösungen, war dies oft praktisch unmöglich. Die neue Richtlinie kehrt diese Beweislast um: Wenn ein Produkt übermäßig technisch oder wissenschaftlich komplex ist, muss der Hersteller – oder im Fall von Eigenentwicklungen das Labor selbst – nachweisen, dass das System fehlerfrei funktioniert hat. Diese Umkehr greift auch, wenn das Labor die Offenlegung relevanter Beweise verweigert oder wenn eine offensichtliche Fehlfunktion vorliegt. Für Labore bedeutet dies eine Verschärfung der Dokumentations- und Nachweispflichten. Jeder Algorithmus, jede Softwareentscheidung, jede KI-basierte Analyse muss so dokumentiert werden, dass im Nachhinein die Fehlerfreiheit bewiesen werden kann.

Die Erweiterung der ersatzfähigen Schadensarten auf psychische Gesundheitsschäden und Datenverlust öffnet neue Dimensionen der Haftung. Ein fehlerhafter Laborbefund, der zu einer falschen Diagnose führt, kann nicht nur physische, sondern auch erhebliche psychische Schäden verursachen – man denke nur an eine fälschlich diagnostizierte schwere Erkrankung oder einen übersehenen Tumor. Der Verlust oder die Korruption von Patientendaten durch fehlerhafte Software kann ebenfalls zu Schadensersatzansprüchen führen, selbst wenn kein körperlicher Schaden entstanden ist.

Besonders bemerkenswert ist die Verlängerung der Verjährungsfrist auf 25 Jahre bei latenten Gesundheitsschäden. Diese außergewöhnlich lange Frist trägt der Tatsache Rechnung, dass sich manche Gesundheitsschäden erst nach Jahren oder Jahrzehnten manifestieren. Für Labore bedeutet dies, dass sie noch Jahrzehnte nach einer Analyse für fehlerhafte Ergebnisse haften können. Dies stellt nicht nur erhebliche Anforderungen an die Archivierung von Daten und Dokumentationen, sondern wirft auch Fragen zur langfristigen Verfügbarkeit von Beweismitteln auf. Wie kann ein Labor nach 20 Jahren noch nachweisen, dass eine bestimmte Software-Version korrekt funktioniert hat, wenn die Hersteller möglicherweise nicht mehr existieren und die technischen Systeme längst obsolet sind?

Die Discovery-Pflichten, die die neue Richtlinie einführt, orientieren sich am angloamerikanischen Rechtssystem und verpflichten Labore zur umfassenden

Offenlegung relevanter Informationen im Schadensfall. Dies umfasst nicht nur die offensichtlichen Dokumente wie Testprotokolle und Qualitätssicherungsunterlagen, sondern kann sich auch auf interne E-Mails, Entwicklungsdokumentation, Fehlerberichte und sogar Quellcode erstrecken. Die Verweigerung der Offenlegung kann zur Beweislastumkehr führen, was Labore in ein Dilemma bringt: Einerseits könnten offengelegte Informationen Schwachstellen aufzeigen, andererseits führt Verweigerung fast automatisch zur Haftung.

Die Umsetzungsfrist bis Dezember 2026 ist knapp bemessen. Labore müssen ihre gesamte Software-Landschaft inventarisieren und bewerten, von den großen Systemen bis zu den kleinen Hilfsprogrammen. Jede Software, die in irgendeiner Weise Einfluss auf Testergebnisse oder Patientendaten hat, muss hinsichtlich ihrer Haftungsrisiken evaluiert werden. Dies schließt explizit auch Software ein, die nicht als Medizinprodukt klassifiziert ist, aber dennoch im Laborprozess eingesetzt wird.

Die Intensivierung der Validierung wird zu einer der wichtigsten Aufgaben. Jede Software, jeder Algorithmus, jede KI-Anwendung muss nicht nur initial validiert, sondern kontinuierlich überwacht und revalidiert werden. Die Validierung muss dabei über die reine Funktionalität hinausgehen und auch Aspekte wie Robustheit, Fehlertoleranz und Verhalten in Grenzfällen umfassen. Besonders herausfordernd ist dies bei KI-Systemen, deren Verhalten sich durch kontinuierliches Lernen verändern kann. Die Dokumentationsanforderungen erreichen eine neue Dimension. Bei einer KI-basierten Bildanalyse in der Pathologie muss beispielsweise dokumentiert werden, welche Merkmale das System erkannt hat, wie diese gewichtet wurden und wie die finale Entscheidung zustande kam. Diese Anforderung steht in Spannung zur oft zitierten "Black Box"-Natur vieler KI-Systeme und wird die Auswahl und Entwicklung von KI-Lösungen beeinflussen. Explainable AI, also erklärbare künstliche Intelligenz, wird von einem akademischen Konzept zur rechtlichen Notwendigkeit.

Regressvereinbarungen mit Herstellern gewinnen an Bedeutung. Wenn ein Laborbefund aufgrund eines Softwarefehlers des LIS-Anbieters fehlerhaft ist, wer haftet dann? Die neue Richtlinie macht klar, dass zunächst das Labor als direkter Vertragspartner des Patienten haftet, aber Regress beim Softwarehersteller nehmen kann. Diese Regressmöglichkeiten müssen vertraglich sauber geregelt werden, was angesichts der Marktmacht großer Softwareanbieter oft schwierig ist. Labore sollten bei Neuverträgen oder Vertragsverlängerungen auf angemessene Haftungsregelungen bestehen und notfalls bereit sein, den Anbieter zu wechseln.

Die neue Produkthaftungsrichtlinie ist mehr als eine regulatorische Pflichtübung – sie ist ein Katalysator für die Professionalisierung der digitalen Labormedizin. Labore, die diese Herausforderung annehmen und meistern, werden nicht nur rechtlich abgesichert sein, sondern sich auch als qualitätsbewusste, verantwortungsvolle Partner im Gesundheitssystem positionieren.

Referenzen:

Richtlinientext: https://eur-lex.europa.eu/eli/dir/2024/2853/oj?eliuri=eli%3Adir%3A2024%3A2853%3Aoj&locale=de

Deutsche Umsetzung: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2025_Produkthaftung.html

7. KI-Verordnung (EU) 2024/1689

Als weltweit erstes umfassendes Regelwerk für künstliche Intelligenz setzt die KI-Verordnung globale Standards und wird, ähnlich wie die DSGVO im Datenschutz, voraussichtlich internationale Strahlkraft entwickeln. Für medizinische Labore, die sich inmitten einer KI-getriebenen Revolution befinden, markiert diese Verordnung den Übergang von einem unregulierten Experimentierfeld zu einem

strukturierten, aber dennoch innovationsoffenen Rahmen.

Der risikobasierte Ansatz der Verordnung teilt KI-Systeme in vier Kategorien ein, wobei die Anforderungen proportional zum Risikopotenzial steigen. Systeme mit unannehmbarem Risiko, wie Social Scoring oder unterschwellige Manipulation, sind vollständig verboten. Hochrisiko-KI-Systeme, zu denen die meisten medizinischen Anwendungen gehören, unterliegen strengen Anforderungen. Systeme mit begrenztem Risiko müssen Transparenzpflichten erfüllen, während Systeme mit minimalem Risiko weitgehend unreguliert bleiben. Diese Abstufung ermöglicht es, Innovation in unkritischen Bereichen zu fördern, während gleichzeitig strenge Sicherheitsvorkehrungen dort greifen, wo Gesundheit und Leben auf dem Spiel stehen.

Für medizinische Labore ist die Einordnung ihrer KI-Systeme in die Hochrisiko-Kategorie praktisch unvermeidlich. Die Verordnung definiert explizit KI-Systeme, die als Sicherheitskomponenten von Medizinprodukten dienen oder selbst Medizinprodukte sind, als Hochrisiko-Systeme. Darüber hinaus fallen KI-Systeme, die für die Triage von Patienten, die Diagnosestellung oder Behandlungsentscheidungen eingesetzt werden, eindeutig in diese Kategorie. In der Labormedizin betrifft dies ein breites Spektrum von Anwendungen: Bildanalysesysteme in der digitalen Pathologie, die Krebszellen in Gewebeproben identifizieren, Algorithmen zur Mustererkennung in komplexen Laborwertkonstellationen, prädiktive Modelle zur Früherkennung von Sepsis oder anderen kritischen Zuständen, KI-gestützte Qualitätskontrollsysteme, die Präanalytikfehler erkennen, und automatisierte Befundungssysteme, die Laborergebnisse interpretieren und klinische Empfehlungen generieren.

Die CE-Kennzeichnung für KI-Systeme wird zur neuen Normalität. Ähnlich wie bei Medizinprodukten müssen Hochrisiko-KI-Systeme eine Konformitätsbewertung durchlaufen, bevor sie in Verkehr gebracht oder in Betrieb genommen werden dürfen. Diese Bewertung umfasst die Prüfung der technischen Dokumentation, die Validierung der Trainings-, Validierungs- und Testdaten, die Überprüfung der Risikomanagementmaßnahmen sowie die Bewertung der Genauigkeit, Robustheit und Cybersicherheit des Systems. Für Labore bedeutet dies, dass sie nicht nur beim Einkauf von KI-Systemen auf die CE-Kennzeichnung achten müssen, sondern auch bei Eigenentwicklungen oder Anpassungen bestehender Systeme möglicherweise selbst als Anbieter im Sinne der Verordnung agieren und entsprechende Pflichten erfüllen müssen.

Die Anforderung an menschliche Aufsicht ist ein zentrales Prinzip der Verordnung und reflektiert die Überzeugung, dass bei kritischen Entscheidungen der Mensch die letzte Verantwortung tragen muss. KI-Systeme müssen so konzipiert sein, dass sie von natürlichen Personen wirksam beaufsichtigt werden können. Dies bedeutet konkret, dass die Nutzer die Fähigkeiten und Grenzen des Systems verstehen müssen, die Ausgaben des Systems interpretieren und bewerten können, in der Lage sein müssen, das System zu übersteuern oder zu stoppen, und die Entscheidung haben, die Systemausgabe in einem bestimmten Kontext nicht zu verwenden.

Die technische Dokumentation muss eine vollständige Beschreibung des Systems enthalten, einschließlich seiner Zweckbestimmung, der verwendeten Algorithmen, der Trainings-, Validierungs- und Testdaten, der Leistungsmetriken und der Risikomanagementmaßnahmen. Besonders herausfordernd ist die Forderung nach Erklärbarkeit: Nutzer müssen verstehen können, wie das System zu seinen Ergebnissen kommt. Bei komplexen Deep-Learning-Modellen, die oft als "Black Boxes" operieren, stellt dies eine erhebliche technische und konzeptuelle Herausforderung dar. Die Dokumentation muss kontinuierlich aktualisiert werden und über die

gesamte Lebensdauer des Systems verfügbar bleiben.

Die zeitliche Staffelung der Anwendbarkeit gibt Laboren die Möglichkeit einer strukturierten Vorbereitung. Die Verbote für unannehmbares Risiko gelten ab Februar 2025, Regelungen für General-Purpose-AI-Modelle ab August 2025, und die vollständige Anwendbarkeit für Hochrisiko-Systeme tritt im August 2026 in Kraft. Diese Übergangsfristen sollten jedoch nicht zur Untätigkeit verleiten, denn die Komplexität der Anforderungen erfordert eine frühzeitige und systematische Herangehensweise.

Der erste Schritt zur Compliance ist eine umfassende Bestandsaufnahme aller im Labor eingesetzten oder geplanten KI-Systeme. Viele Labore sind überrascht, wie viele ihrer Systeme KI-Komponenten enthalten – oft versteckt in scheinbar konventioneller Software. Moderne Laborgeräte nutzen zunehmend Machine-Learning-Algorithmen für die Kalibrierung, Qualitätskontrolle oder Mustererkennung. Bildgebende Systeme verwenden neuronale Netze für die Bildverbesserung oder automatische Anomalieerkennung. Selbst Laborinformationssysteme integrieren zunehmend KI für die Prozessoptimierung oder prädiktive Wartung. Jedes dieser Systeme muss identifiziert, klassifiziert und hinsichtlich seiner Compliance-Anforderungen bewertet werden.

Die Klassifizierung der Systeme nach Risikokategorien erfordert eine sorgfältige Analyse ihrer Zweckbestimmung und potenziellen Auswirkungen. Ein KI-System zur Optimierung der Laborlogistik mag als Niedrigrisiko-System gelten, während dasselbe System, wenn es für die Priorisierung von Notfallproben verwendet wird, möglicherweise als Hochrisiko einzustufen ist. Die Grenzziehung ist nicht immer eindeutig, und im Zweifelsfall empfiehlt sich eine konservative Einschätzung. Die Dokumentation dieser Klassifizierungsentscheidungen ist essentiell, da sie möglicherweise gegenüber Aufsichtsbehörden gerechtfertigt werden muss.

Das Qualitätsmanagementsystem des Labors muss erweitert werden, um die spezifischen Anforderungen der KI-Verordnung zu integrieren. Dies umfasst Prozesse für die Bewertung und Beschaffung von KI-Systemen, die kontinuierliche Überwachung ihrer Leistung und Sicherheit, das Management von Trainingsdaten und Modell-Updates, die Dokumentation aller relevanten Entscheidungen und Vorfälle sowie die Schulung und Kompetenzerhaltung der Mitarbeiter. Das bestehende QM-System nach ISO 15189 oder ISO 13485 bietet eine gute Grundlage, muss aber um KI-spezifische Elemente erweitert werden.

Die Zusammenarbeit mit KI-Anbietern muss neu strukturiert werden. Labore müssen von ihren Lieferanten umfassende Compliance-Nachweise einfordern, einschließlich der CE-Kennzeichnung, der technischen Dokumentation, der Konformitätserklärung und regelmäßiger Updates zur Systemleistung. Verträge müssen klare Regelungen zur Verantwortungsverteilung, zu Updates und Patches, zur Datennutzung und zum Support enthalten. Besonders wichtig sind Regelungen für den Fall von Systemfehlern oder Compliance-Verstößen.

Die Schulung der Mitarbeiter wird zur kritischen Erfolgskomponente. Die Verordnung fordert, dass Nutzer von Hochrisiko-KI-Systemen über ausreichende KI-Kompetenz verfügen müssen. Dies geht weit über die reine Bedienungsschulung hinaus und umfasst das Verständnis der Funktionsweise von KI-Systemen, ihrer Stärken und Schwächen, die Fähigkeit zur kritischen Bewertung von KI-Ausgaben, das Erkennen von Anomalien und Fehlfunktionen sowie ethische und rechtliche Aspekte des KI-Einsatzes. Für viele Labormitarbeiter bedeutet dies eine erhebliche Weiterqualifizierung, die Zeit und Ressourcen erfordert.

Die Einrichtung einer KI-Governance-Struktur wird für größere Labore unumgänglich. Ein KI-Verantwortlicher oder ein KI-Komitee sollte die Oversight-Funktion übernehmen und

sicherstellen, dass alle regulatorischen Anforderungen erfüllt werden, neue KI-Systeme angemessen bewertet werden, Risiken kontinuierlich überwacht und gemanagt werden, ethische Aspekte berücksichtigt werden und die Organisation aus Erfahrungen lernt und sich kontinuierlich verbessert.

Die Integration mit anderen Regularien erfordert besondere Aufmerksamkeit. KI-Systeme, die als Medizinprodukte klassifiziert sind, müssen sowohl die Anforderungen der KI-Verordnung als auch der MDR oder IVDR erfüllen. Die Datenschutzaspekte müssen mit der DSGVO harmonisiert werden. Cybersicherheitsanforderungen überschneiden sich mit NIS-2 und dem Cyber Resilience Act. Diese Mehrfachregulierung macht einen integrierten Compliance-Ansatz unumgänglich.

Referenzen:

Verordnungstext: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=de

KI-Compliance Checker: https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/

8. Cyber Resilience Act (EU) 2024/2847

Während bisherige Regularien primär sektorspezifisch agierten, etabliert der CRA erstmals horizontale Cybersicherheitsanforderungen, die branchen- und produktübergreifend gelten. Für medizinische Labore erscheint die Relevanz auf den ersten Blick begrenzt, da Medizinprodukte explizit vom Anwendungsbereich ausgenommen sind, sofern sie bereits durch MDR oder IVDR reguliert werden. Doch diese scheinbare Ausnahme täuscht über die tatsächliche Tragweite der Verordnung hinweg. Die moderne Laborinfrastruktur besteht aus einem komplexen Ökosystem digitaler Produkte, von denen viele nicht als Medizinprodukte klassifiziert sind und somit voll unter den CRA fallen.

Die Philosophie des CRA basiert auf der Erkenntnis, dass die Sicherheit digitaler Infrastrukturen nur so stark ist wie ihr schwächstes Glied. Ein hochsicheres Laborinformationssystem nützt wenig, wenn es über unsichere Middleware mit vulnerablen Peripheriegeräten kommuniziert oder wenn die zugrundeliegende Netzwerkinfrastruktur kompromittiert werden kann. Der CRA adressiert genau diese Schwachstellen, indem er Cybersicherheit als inhärente Produkteigenschaft definiert, die über den gesamten Produktlebenszyklus gewährleistet werden muss. Diese Lebenszyklusbetrachtung geht weit über die bisherige Praxis hinaus, bei der Sicherheit oft als nachträgliche Ergänzung behandelt wurde.

Die Abgrenzung zwischen Medizinprodukten und anderen digitalen Produkten im Labor erweist sich in der Praxis als komplex und oft unklar. Laborinformationssysteme ohne diagnostische Funktionen, reine Datenmanagementsysteme und Workflow-Optimierungstools fallen unter den CRA. Middleware-Lösungen, die Daten zwischen verschiedenen Systemen transferieren, aber keine medizinische Zweckbestimmung haben, sind ebenfalls betroffen. Allgemeine IT-Infrastruktur wie Server, Netzwerkkomponenten, Firewalls und Backup-Systeme unterliegen vollständig dem CRA. Laborgeräte, die keine CE-Kennzeichnung als Medizinprodukt tragen – beispielsweise Kühlschränke mit IoT-Sensoren, Klimaüberwachungssysteme oder Zugangskontrollsysteme – müssen CRA-konform sein. Selbst Software-Tools für administrative Aufgaben, Qualitätsmanagement oder Dokumentation fallen in den Geltungsbereich. Diese breite Erfassung bedeutet, dass praktisch jedes Labor eine Vielzahl von CRA-relevanten Produkten einsetzt.

Die Software Bill of Materials (SBOM) stellt eine der Anforderungen des CRA dar. Hersteller müssen eine vollständige, maschinenlesbare Auflistung aller Softwarekomponenten ihrer Produkte bereitstellen, einschließlich aller verwendeten Open-Source-Bibliotheken,

Frameworks und Abhängigkeiten. Für Labore eröffnet dies völlig neue Möglichkeiten des Schwachstellenmanagements. Wenn eine kritische Sicherheitslücke in einer weit verbreiteten Softwarekomponente entdeckt wird – wie beispielsweise die Log4j-Schwachstelle 2021 – können Labore anhand der SBOMs sofort identifizieren, welche ihrer Systeme betroffen sind. Diese Transparenz war bisher unmöglich, da Hersteller die Zusammensetzung ihrer Software als Geschäftsgeheimnis behandelten. Die SBOM-Pflicht transformiert das Schwachstellenmanagement von einem reaktiven Ratespiel zu einem proaktiven, datengesteuerten Prozess.

Das Schwachstellenmanagement über den gesamten Produktlebenszyklus ist eine weitere zentrale Säule des CRA. Hersteller sind verpflichtet, ihre Produkte kontinuierlich auf Schwachstellen zu überwachen, zeitnah Sicherheitsupdates bereitzustellen und diese Updates für mindestens fünf Jahre nach Markteinführung – oder für die erwartete Produktlebensdauer, je nachdem was länger ist – zu gewährleisten. Für Labore bedeutet dies eine fundamentale Verbesserung ihrer Sicherheitslage. Bisher war es üblich, dass Hersteller den Support für ältere Produkte einstellten und Labore mit unsicheren, aber funktionsfähigen Systemen zurückließen. Der CRA macht dieser Praxis ein Ende und zwingt Hersteller zu langfristigem Sicherheitssupport.

Die CE-Kennzeichnung wird um eine Cybersicherheitsdimension erweitert. Produkte mit digitalen Elementen müssen künftig nicht nur funktionale und sicherheitstechnische Anforderungen erfüllen, sondern auch umfassende Cybersicherheitsanforderungen nachweisen. Die Konformitätsbewertung umfasst dabei die Überprüfung der Secure-by-Design-Prinzipien, die Validierung der Schwachstellenmanagement-Prozesse, die Bewertung der Updatefähigkeit und -sicherheit sowie die Prüfung der Dokumentation und Nutzerinformationen. Für Labore wird die CE-Kennzeichnung damit zu einem verlässlichen Indikator für Cybersicherheit, der Kaufentscheidungen erheblich vereinfacht.

Die Inventarisierung der Nicht-Medizinprodukt-IT stellt für viele Labore die erste Herausforderung dar. Eine vollständige Erfassung aller digitalen Produkte, die nicht unter MDR oder IVDR fallen, offenbart oft überraschende Lücken. Viele Labore haben keine vollständige Übersicht über ihre Software-Landschaft, insbesondere bei Tools, die von einzelnen Abteilungen eigenständig beschafft wurden. Diese Schatten-IT muss identifiziert und in das Compliance-Management integriert werden. Die Kategorisierung nach CRA-Relevanz erfordert dabei oft juristische Expertise, da die Abgrenzung zu Medizinprodukten nicht immer eindeutig ist.

Die Lieferantenbewertung muss um CRA-Compliance-Kriterien erweitert werden. Labore müssen von ihren Lieferanten nicht nur Konformitätserklärungen einfordern, sondern auch konkrete Nachweise über Sicherheitsmaßnahmen, Update-Prozesse und Support-Zusagen. Die Verhandlungsmacht gegenüber großen Herstellern ist oft begrenzt, weshalb sich Labore zu Einkaufsgemeinschaften zusammenschließen sollten, um gemeinsame Standards durchzusetzen. Besonders kritisch ist die Situation bei Bestandslieferanten, deren Produkte möglicherweise nicht CRA-konform sind und auch nicht nachgerüstet werden können. Hier müssen rechtzeitig Alternativen evaluiert und Migrationspläne entwickelt werden.

Die Integration der SBOM in das Schwachstellenmanagement erfordert neue Prozesse und möglicherweise neue Tools. Labore müssen in der Lage sein, SBOMs zu empfangen, zu speichern und auszuwerten. Automatisierte Vulnerability-Scanner, die SBOMs gegen aktuelle Schwachstellendatenbanken abgleichen, werden zur Notwendigkeit. Die schiere Menge an Informationen – ein einzelnes Produkt kann Hunderte von Komponenten enthalten – macht

manuelle Prozesse unmöglich. Die Herausforderung besteht darin, aus der Informationsflut die wirklich kritischen Schwachstellen zu identifizieren und priorisiert zu adressieren.

Der CRA verpflichtet Hersteller zur Bereitstellung von Sicherheitsupdates, aber die Installation und Validierung bleibt Aufgabe der Anwender. Für Labore bedeutet dies, dass sie robuste Prozesse für die Bewertung, Testung und Deployment von Updates etablieren müssen. Die Herausforderung besteht darin, die Balance zwischen schneller Sicherheitsreaktion und der Aufrechterhaltung validierter Zustände zu finden. Automatische Updates, wie sie in der Consumer-IT üblich sind, sind in der regulierten Laborumgebung oft nicht möglich. Stattdessen müssen kontrollierte Update-Prozesse etabliert werden, die sowohl Sicherheitsanforderungen als auch Qualitätsanforderungen genügen.

Die IT-Abteilung, die traditionell für allgemeine IT-Infrastruktur zuständig ist, muss enger mit der Medizintechnik-Abteilung zusammenarbeiten, die für Medizinprodukte verantwortlich ist. Die Einkaufsabteilung muss neue Bewertungskriterien in ihre Prozesse integrieren. Das Qualitätsmanagement muss seine Systeme um CRA-relevante Aspekte erweitern. Diese organisatorische Herausforderung wird oft unterschätzt, ist aber kritisch for erfolgreiche Compliance.

Die Budgetplanung muss die CRA-Anforderungen berücksichtigen. CRA-konforme Produkte werden tendenziell teurer sein als ihre unsicheren Vorgänger, da die Hersteller die Kosten für Sicherheitsentwicklung und langfristigen Support einpreisen müssen. Zusätzlich entstehen Kosten für neue Tools zum Schwachstellenmanagement, möglicherweise zusätzliches Personal für Security-Aufgaben und Schulungen für bestehendes Personal. Diese Kosten müssen frühzeitig eingeplant werden, um Budgetengpässe zu vermeiden.

Die Cybersicherheitsanforderungen des CRA ergänzen die organisatorischen Anforderungen der NIS-2-Richtlinie perfekt. Während NIS-2 fordert, dass Labore angemessene Sicherheitsmaßnahmen implementieren, stellt der CRA sicher, dass die eingesetzten Produkte diese Maßnahmen unterstützen. Die Dokumentationsanforderungen des CRA harmonieren mit den Nachweispflichten der DSGVO. Die Update-Verpflichtungen unterstützen die kontinuierlichen Sicherheitsanforderungen der KI-Verordnung.

Referenzen:

Verordnungstext: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847

IEC 62443 Standards (Harmonisierung für CRA): https://webstore.iec.ch/publication/7030

9. In-vitro-Diagnostika-Verordnung (EU) 2017/746

Die In-vitro-Diagnostika-Verordnung trat am 26. Mai 2022 nach einer fünfjährigen Übergangsphase vollständig in Kraft. Als Ablösung der über zwei Jahrzehnte alten IVD-Richtlinie 98/79/EG bringt die IVDR nicht nur inkrementelle Verbesserungen, sondern einen Paradigmenwechsel in der Art und Weise, wie diagnostische Tests reguliert, überwacht und eingesetzt werden.

Der Wechsel von einem listenbasierten zu einem risikobasierten Klassifizierungssystem stellt die offensichtlichste, aber keineswegs einzige Neuerung dar. Das neue System mit seinen vier Risikoklassen A bis D orientiert sich an international anerkannten Prinzipien und berücksichtigt dabei den vorgesehenen Verwendungszweck, die Bedeutung der Information für die Diagnose, die Auswirkungen eines falschen Ergebnisses auf den Einzelnen und die öffentliche Gesundheit sowie die Neuartigkeit der Technologie. Diese nuancierte Herangehensweise ersetzt die starre Listenkategorisierung und ermöglicht eine flexible Anpassung an technologische Innovationen. Klasse A umfasst Produkte mit dem niedrigsten Risiko wie Laborgeräte ohne

kritische Messfunktion, während Klasse D Hochrisikoprodukte wie HIV- oder Hepatitis-Tests einschließt. Die überwiegende Mehrheit diagnostischer Tests fällt in die Klassen B und C, was deutlich strengere Anforderungen als unter der alten Direktive bedeutet.

Die Ausweitung der Rolle Benannter Stellen transformiert die Marktüberwachungslandschaft. Während unter der alten Direktive nur etwa 20% der IVDs eine Bewertung durch Benannte Stellen benötigten, sind es unter der IVDR etwa 85%. Diese Verschiebung hat zu einem Flaschenhals geführt, da die Kapazitäten der Benannten Stellen nicht mit dem explosionsartig gestiegenen Bedarf Schritt halten konnten. Die Konsequenzen sind: verlängerte Zeiträume für Marktzulassungen, erhöhte Kosten für Konformitätsbewertungen und in einigen Fällen das Verschwinden von Nischenprodukten vom Markt, deren Hersteller die regulatorischen Hürden nicht bewältigen können oder wollen.

Die Anforderungen an klinische Evidenz und Leistungsbewertung haben eine neue Qualitätsdimension erreicht. Die IVDR fordert wissenschaftliche Validität des Analyten, analytische Leistung einschließlich Richtigkeit, Präzision, Spezifität, Sensitivität, Nachweis- und Quantifizierungsgrenze sowie klinische Leistung mit diagnostischer Sensitivität, diagnostischer Spezifität, positivem und negativem prädiktiven Wert. Diese Evidenz muss nicht nur bei der Marktzulassung vorliegen, sondern kontinuierlich über den gesamten Produktlebenszyklus aktualisiert und verbessert werden. Für Labore bedeutet dies, dass sie bei der Auswahl von IVDs nicht mehr nur auf die CE-Kennzeichnung vertrauen können, sondern die zugrundeliegende Evidenz kritisch bewerten müssen.

Artikel 5 Absatz 5 der IVDR erlaubt die Eigenherstellung und Verwendung von Tests nur unter extrem restriktiven Bedingungen. Das Labor muss nachweisen, dass kein gleichwertiges CE-gekennzeichnetes Produkt auf dem Markt verfügbar ist – eine Nachweispflicht, die angesichts des breiten Angebots kommerzieller Tests oft schwer zu erfüllen ist. Die Tests dürfen ausschließlich in derselben Gesundheitseinrichtung verwendet werden, ein Transfer zu anderen Einrichtungen, selbst innerhalb desselben Konzerns, ist untersagt. Die allgemeinen Sicherheits- und Leistungsanforderungen des Anhangs I müssen erfüllt werden, was umfassende Dokumentation, Validierung und Qualitätssicherung erfordert. Das Labor muss ein Qualitätsmanagementsystem implementieren, das den Anforderungen entspricht, und eine öffentlich zugängliche Erklärung über die Verwendung des Tests abgeben. Diese Beschränkungen haben dazu geführt, dass viele Labore ihre LDT-Programme drastisch reduzieren oder ganz einstellen mussten.

Das Unique Device Identification System: Jedes Produkt erhält eine eindeutige UDI, die in der europäischen EUDAMED-Datenbank registriert wird. Diese digitale Kennzeichnung ermöglicht eine lückenlose Rückverfolgung vom Hersteller bis zum Endanwender und erleichtert die Marktüberwachung, Vigilanz und Post-Market-Surveillance erheblich. Für Labore bedeutet das UDI-System zunächst zusätzlichen administrativen Aufwand bei der Warenwirtschaft und Dokumentation, langfristig jedoch verbesserte Transparenz und Sicherheit.

Die strategische Neuausrichtung der Testportfolios ist für viele Labore unumgänglich geworden. Die Einschränkung von LDTs zwingt zur kritischen Evaluation: Welche Eigenentwicklungen sind wirklich unverzichtbar und rechtfertigen den enormen regulatorischen Aufwand? Welche können durch kommerzielle CE-IVDs ersetzt werden? Die Antworten auf diese Fragen haben weitreichende Konsequenzen für die Positionierung des Labors im Markt. Speziallabore, die sich durch innovative Eigenentwicklungen differenziert haben, müssen neue Wege finden, ihren Wettbewerbsvorteil zu erhalten. Einige wählen den Weg, selbst Hersteller im Sinne der IVDR zu werden und ihre Tests als CE-gekennzeichnete

Produkte anzubieten – ein Schritt, der erhebliche Investitionen und fundamentale organisatorische Veränderungen erfordert.

Das Qualitätsmanagementsystem muss grundlegend überarbeitet und erweitert werden. Die IVDR-Anforderungen gehen weit über die traditionellen Qualitätsstandards wie ISO 15189 hinaus. Besonders die Anforderungen an die Post-Market-Surveillance und Vigilanz stellen neue Herausforderungen dar. Labore müssen systematisch die Leistung aller eingesetzten IVDs überwachen, Vorkommnisse dokumentieren und melden sowie an Korrekturmaßnahmen der Hersteller mitwirken. Dies erfordert neue Prozesse, Verantwortlichkeiten und oft auch IT-Systeme zur Erfassung und Auswertung der relevanten Daten.

Labore müssen nicht nur die vom Hersteller angegebene Leistung verifizieren, sondern auch sicherstellen, dass die Tests unter den spezifischen Bedingungen ihres Labors die geforderte Leistung erbringen. Dies umfasst die Berücksichtigung präanalytischer Faktoren, die Evaluation von Matrixeffekten, die Etablierung laborspezifischer Referenzbereiche und die kontinuierliche Überwachung der Testleistung im Routinebetrieb.

Die Marktkonsolidierung als Folge der IVDR zeichnet sich bereits ab. Kleinere Hersteller, die die regulatorischen Anforderungen nicht stemmen können, verschwinden vom Markt oder werden übernommen. Das Angebot an Nischenprodukten für seltene Erkrankungen schrumpft, da die Zulassungskosten in keinem Verhältnis zum Marktpotenzial stehen. Für Labore bedeutet dies eine Reduktion der Auswahlmöglichkeiten und potenzielle Versorgungslücken. Gleichzeitig eröffnen sich Chancen für Labore, die bereit sind, in die Entwicklung und Zulassung eigener CE-gekennzeichneter Tests zu investieren.

Die langfristigen Auswirkungen der IVDR auf Innovation und Patientenversorgung sind noch nicht vollständig absehbar. Einerseits führen die hohen regulatorischen Hürden zu einer Verlangsamung der Innovation und einer Reduktion der Testvielfalt. Andererseits gewährleistet die IVDR ein bisher unerreichtes Niveau an Qualität und Sicherheit diagnostischer Tests. Labore müssen in diesem Spannungsfeld ihren Weg finden, zwischen regulatorischer Compliance und innovativer Patientenversorgung.

Referenzen:

Konsolidierte Fassung der IVDR: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02017R0746-20250110

Ursprüngliche Verordnung: https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32017R0746

10. Medizinprodukte-Verordnung (EU) 2017/745

Die Medizinprodukte-Verordnung, die seit dem 26. Mai 2021 vollständig anwendbar ist, wird in der Labormedizin oft als sekundär gegenüber der IVDR wahrgenommen. Während die IVDR zweifellos die primäre Regulierung für diagnostische Tests darstellt, erfasst die MDR eine Vielzahl von Produkten und Systemen, die für den Laborbetrieb unverzichtbar sind. Die Grenzziehung zwischen MDR und IVDR ist dabei keineswegs immer eindeutig, und viele Produkte bewegen sich in regulatorischen Grauzonen, die sorgfältige Analyse und oft auch juristische Expertise erfordern.

Die MDR-relevanten Produkte im Labor sind vielfältiger als gemeinhin angenommen. Zentrifugen, die für die Probenvorbereitung unverzichtbar sind, fallen unter die MDR, sofern sie eine medizinische Zweckbestimmung haben. Die Unterscheidung zwischen einer Labor-Zentrifuge mit und ohne medizinische Zweckbestimmung mag akademisch erscheinen, hat aber erhebliche regulatorische Konsequenzen. Analysegeräte, die keine In-vitro-Diagnostika im Sinne der IVDR sind, aber dennoch medizinische Informationen

generieren, unterliegen der MDR. Point-of-Care-Testing-Geräte befinden sich oft an der Schnittstelle zwischen MDR und IVDR, wobei das Gerät selbst unter die MDR und die verwendeten Reagenzien unter die IVDR fallen können. Diese regulatorische Zweiteilung eines funktional integrierten Systems schafft Komplexität in Beschaffung, Validierung und Betrieb.

Software als Medizinprodukt (Software as a Medical Device, SaMD) umfasst ein breites Spektrum von Anwendungen, die in Laboren eingesetzt werden. Bildanalysesoftware für die digitale Pathologie, die über reine Visualisierung hinausgeht und diagnostische Interpretationen liefert, fällt unter die MDR. Entscheidungsunterstützungssysteme, die Laborwerte interpretieren und klinische Empfehlungen generieren, sind eindeutig Medizinprodukte der Klasse IIa oder höher. Workflow-Management-Systeme können als Medizinprodukte klassifiziert werden, wenn sie kritische Entscheidungen über Probenpriorisierung oder Testauswahl treffen. Die Klassifizierung von Software nach Regel 11 der MDR, die speziell für Software-Medizinprodukte entwickelt wurde, führt oft zu höheren Risikoklassen als unter der alten Medizinprodukterichtlinie, mit entsprechend strengeren Anforderungen.

Die EUDAMED-Datenbank, obwohl ihre vollständige Implementierung sich verzögert hat, wird die Transparenz und Rückverfolgbarkeit von Medizinprodukten verbessern. Sobald vollständig funktionsfähig, wird EUDAMED eine zentrale Informationsquelle für alle in der EU verkehrsfähigen Medizinprodukte darstellen. Für Labore bedeutet dies verbesserten Zugang zu Produktinformationen, Sicherheitsdaten und Konformitätsnachweisen. Die UDI-Integration ermöglicht eine nahtlose Rückverfolgung von Produkten über die gesamte Lieferkette. Die Vigilanz-Komponente von EUDAMED wird die Meldung und Verfolgung von Vorkommnissen vereinfachen und beschleunigen. Gleichzeitig entstehen neue Verpflichtungen für Labore als professionelle Anwender, die zur aktiven Teilnahme am Vigilanzsystem verpflichtet sind.

Die verschärften klinischen Bewertungsanforderungen der MDR haben direkte Auswirkungen auf die Produktverfügbarkeit und -kosten. Hersteller müssen umfassende klinische Daten vorlegen, die die Sicherheit und Leistung ihrer Produkte über den gesamten Lebenszyklus belegen.

Die Abgrenzung zwischen Eigenherstellung und Anwendung ist unter der MDR komplexer geworden. Wenn ein Labor ein Medizinprodukt modifiziert oder mehrere Produkte zu einem System kombiniert, kann es selbst zum Hersteller werden mit allen damit verbundenen regulatorischen Verpflichtungen. Die Integration verschiedener Laborgeräte zu einem automatisierten System, die Modifikation von Software für spezifische Laboranforderungen oder die Entwicklung eigener Schnittstellen zwischen Geräten können das Labor in die Herstellerrolle bringen. Die Kriterien für die Eigenherstellung nach Artikel 5 Absatz 5 der MDR sind streng und erfordern, ähnlich wie bei der IVDR, den Nachweis, dass kein geeignetes Produkt auf dem Markt verfügbar ist, sowie die Einhaltung der relevanten allgemeinen Sicherheits- und Leistungsanforderungen.

Das Management von Software-Updates stellt eine besondere Herausforderung dar, die die Schnittstelle zwischen regulatorischen Anforderungen und praktischer IT-Sicherheit betrifft. Software-Updates können die Klassifizierung eines Medizinprodukts ändern, neue Risiken einführen oder die validierte Konfiguration beeinträchtigen. Labore müssen einen strukturierten Change-Management-Prozess implementieren, der regulatorische Bewertung, Risikobewertung, Validierungsplanung und Dokumentation umfasst. Die Balance zwischen der Notwendigkeit zeitnaher Sicherheitsupdates und der Aufrechterhaltung des validierten Zustands erfordert sorgfältige Planung und oft einen gestaffelten Ansatz, bei dem kritische

Sicherheitsupdates priorisiert und funktionale Updates gebündelt werden.

Die Zusammenarbeit zwischen verschiedenen Abteilungen wird unter der MDR wichtiger denn je. Die traditionelle Trennung zwischen Labormedizin und Medizintechnik verschwimmt zunehmend. IT-Abteilungen müssen in regulatorische Prozesse einbezogen werden, wenn Software als Medizinprodukt eingesetzt wird. Die Beschaffung muss regulatorische Kriterien in ihre Prozesse integrieren. Das Facility Management muss die besonderen Anforderungen für die Umgebungsbedingungen von Medizinprodukten berücksichtigen.

Die langfristige Perspektive zeigt, dass die MDR, trotz aller aktuellen Herausforderungen, zu einer Professionalisierung und Qualitätssteigerung in der Labormedizin führen wird. Die strengeren Anforderungen eliminieren unsichere und unzureichend validierte Produkte vom Markt. Die verbesserte Transparenz durch EUDAMED und UDI erhöht die Patientensicherheit. Die systematische Post-Market-Surveillance führt zu kontinuierlicher Verbesserung der Produkte. Labore, die die MDR-Transformation erfolgreich meistern, werden mit robusten Prozessen, qualifizierten Mitarbeitern und sicheren Produkten für die Zukunft gerüstet sein.

Referenzen:

MDR Verordnungstext: https://eur-lex.europa.eu/eli/reg/2017/745/oj?locale=de

EUDAMED Datenbank: https://ec.europa.eu/tools/eudamed

Medical Device Coordination Group Dokumente: https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en

11. Datenschutz-Grundverordnung (EU) 2016/679

Die Datenschutz-Grundverordnung, die seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten gilt, hat das Datenschutzrecht revolutioniert und dabei besonders tiefgreifende Auswirkungen auf den Gesundheitssektor entfaltet. Jede Blutprobe, jeder Laborwert, jeder Befund enthält Gesundheitsdaten, die nach Artikel 9 der DSGVO als besondere Kategorie personenbezogener Daten den höchsten Schutzstandard genießen.

Die Verarbeitung von Gesundheitsdaten ist grundsätzlich verboten und nur unter engen Ausnahmetatbeständen zulässig. Diese scheinbar prohibitive Grundhaltung zwingt Labore zu einer fundamentalen Auseinandersetzung mit der Rechtsgrundlage jeder einzelnen Datenverarbeitung. Die Einwilligung nach Artikel 9 Absatz 2 lit. a DSGVO mag als offensichtliche Rechtsgrundlage erscheinen, erweist sich in der Praxis jedoch als komplex und oft unpraktikabel. Eine wirksame Einwilligung muss freiwillig, informiert, spezifisch und unmissverständlich sein – Kriterien, die im medizinischen Kontext, wo Patienten oft in Abhängigkeitsverhältnissen stehen und die Tragweite der Datenverarbeitung kaum überblicken können, schwer zu erfüllen sind. Die Alternative des Behandlungsvertrags in Verbindung mit §22 BDSG bietet eine solidere Grundlage, beschränkt die Verarbeitung aber auf den unmittelbaren Behandlungskontext. Für Forschungszwecke, Qualitätssicherung oder sekundäre Nutzungen müssen separate Rechtsgrundlagen gefunden werden, was zu einem komplexen Geflecht unterschiedlicher Legitimationen für verschiedene Verarbeitungszwecke führt.

Das Prinzip der Zweckbindung kollidiert fundamental mit der Realität moderner Labormedizin, in der Daten mehrfach und für verschiedene Zwecke genutzt werden. Eine Blutprobe wird für die angeforderten Tests verwendet, die Ergebnisse fließen in die Patientenbehandlung ein, werden für die interne Qualitätskontrolle ausgewertet, dienen der externen Qualitätssicherung, werden für die Abrechnung benötigt und sollen idealerweise auch für Forschung und Entwicklung nutzbar sein. Jede dieser Nutzungen erfordert eine eigene Rechtfertigung, und die Grenzen

zwischen kompatiblen und inkompatiblen Zweckänderungen sind oft unscharf. Die DSGVO erlaubt zwar privilegierte Zweckänderungen für wissenschaftliche Forschungszwecke, aber die praktische Umsetzung erfordert sorgfältige Dokumentation und oft zusätzliche Schutzmaßnahmen wie Pseudonymisierung oder Anonymisierung.

Die Betroffenenrechte nach Kapitel III der DSGVO stellen Labore vor operative Herausforderungen, die weit über die technische Implementierung hinausgehen. Das Auskunftsrecht nach Artikel 15 konfrontiert Labore mit der Frage, wie umfassend die Auskunft sein muss und wie medizinische Daten laienverständlich aufbereitet werden können. Das Recht auf Berichtigung nach Artikel 16 wirft bei Laborwerten fundamentale Fragen auf: Können objektive Messwerte "berichtigt" werden? Wie geht man mit nachträglichen Korrekturen um, ohne die Integrität der medizinischen Dokumentation zu gefährden? Das Recht auf Löschung nach Artikel 17 kollidiert mit gesetzlichen Aufbewahrungspflichten, die für medizinische Unterlagen oft 10, 30 oder sogar unbegrenzte Jahre betragen. Das Recht auf Datenportabilität nach Artikel 20 erfordert die Bereitstellung von Daten in einem strukturierten, maschinenlesbaren Format – eine Herausforderung für Labore mit heterogenen IT-Systemen und proprietären Datenformaten.

Die technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO müssen dem hohen Schutzbedarf von Gesundheitsdaten Rechnung tragen. Die Pseudonymisierung, von der DSGVO als Schutzmaßnahme privilegiert, erweist sich in der Laborpraxis als komplex, da die Zuordnung von Proben zu Patienten für die medizinische Versorgung essentiell ist. Die Verschlüsselung muss sowohl ruhende Daten in Datenbanken und Archiven als auch Daten in Übertragung zwischen Systemen und zu externen Empfängern schützen. Zugriffskontrollen müssen granular gestaltet sein und dem Prinzip der minimalen Rechtevergabe folgen, was in der Praxis oft mit der Notwendigkeit schneller Verfügbarkeit in Notfällen kollidiert. Die physische Sicherheit von Proben und Dokumenten erfordert besondere Aufmerksamkeit, da ein Datenschutzverstoß nicht nur digital, sondern auch durch unsachgemäße Entsorgung oder ungesicherte Lagerung erfolgen kann.

Die Rolle des Datenschutzbeauftragten nach Artikel 37 DSGVO ist für Labore nicht optional, sondern verpflichtend, sobald die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Datenkategorien besteht – was für jedes medizinische Labor zutrifft. Der Datenschutzbeauftragte muss nicht nur über juristische Expertise verfügen, sondern auch die Besonderheiten der Labormedizin verstehen, um praxisgerechte Lösungen entwickeln zu können. Die Position zwischen Beratung und Überwachung, zwischen Unterstützung der Geschäftsführung und Unabhängigkeit, zwischen interner Rolle and externer Ansprechpartner für Behörden und Betroffene erfordert diplomatisches Geschick und fachliche Autorität.

Die Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten nach Artikel 30 DSGVO entwickelt sich für Labore zu einer Mammutaufgabe. Jeder Verarbeitungsvorgang muss erfasst werden, von der Probenannahme über die Analyse bis zur Befundübermittlung und Archivierung. Die Komplexität entsteht durch die Vielzahl der Beteiligten: einweisende Ärzte, kooperierende Labore, Geräte hersteller mit Fernwartungszugang, IT-Dienstleister, Entsorgungs unternehmen für Proben und Dokumente – alle sind in irgendeiner Form in die Datenverarbeitung involviert. Die Dokumentation muss dabei nicht nur den Ist-Zustand abbilden, sondern kontinuierlich aktualisiert werden, wenn neue Tests eingeführt, Prozesse geändert oder Dienstleister gewechselt werden.

Die Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO ist für viele Verarbeitungen in Laboren obligatorisch, da die umfangreiche Verarbeitung besonderer Datenkategorien ein

hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Die systematische Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Bewertung der Risiken für Betroffene und die Darstellung der geplanten Abhilfemaßnahmen erfordern interdisziplinäre Zusammenarbeit zwischen Datenschutzexperten, IT-Sicherheitsspezialisten und Labormedizinern.

Die Meldung von Datenschutzverletzungen nach Artikel 33 und 34 DSGVO innerhalb von 72 Stunden stellt Labore vor ähnliche Herausforderungen wie die NIS-2-Meldepflichten, jedoch mit anderem Fokus. Während NIS-2 auf Cybersicherheitsvorfälle abzielt, umfasst die DSGVO jede Verletzung des Schutzes personenbezogener Daten, einschließlich versehentlicher Offenlegungen, Fehlversendungen oder unsachgemäßer Entsorgung.

Die Sanktionspraxis der Datenschutzbehörden zeigt, dass die theoretischen Maximalbußgelder von bis zu 4% des weltweiten Jahresumsatzes oder 20 Millionen Euro keine leere Drohung sind. Beispiele wie die Bußgelder gegen Krankenhäuser und Gesundheitsdienstleister demonstrieren, dass Aufsichtsbehörden bereit sind, auch im Gesundheitssektor empfindliche Strafen zu verhängen. Die Enforcement Tracker Datenbank (https://www.enforcementtracker.com/) dokumentiert eine steigende Zahl von Sanktionen im Gesundheitsbereich. Typische Verstöße umfassen unzureichende technische und organisatorische Maßnahmen, fehlerhafte Rechtsgrundlagen für die Verarbeitung, Verletzungen von Betroffenenrechten und verspätete oder unterlassene Meldungen von Datenschutzverletzungen.

Die Integration der DSGVO-Anforderungen mit anderen Regularien erfordert sorgfältige Koordination. Die Transparenzanforderungen der DSGVO können mit der ärztlichen Schweigepflicht kollidieren. Die Löschpflichten der DSGVO stehen im Spannungsverhältnis zu den Aufbewahrungspflichten aus MDR und IVDR. Die Datenminimierung der DSGVO konfligiert mit den umfassenden Dokumentationsanforderungen der GxP-Regularien. Die Pseudonymisierung für Forschungszwecke muss mit den Anforderungen klinischer Studien harmonisiert werden. Diese Konflikte erfordern oft kreative Lösungen und intensive Abstimmung mit verschiedenen Stakeholdern.

Referenzen:

DSGVO Verordnungstext: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

Bundesdatenschutzgesetz (BDSG): https://www.gesetze-im-internet.de/bdsg_2018/

Enforcement Tracker: https://www.enforcementtracker.com/

12. European Health Data Space (EU) 2025/327

Der European Health Data Space, dessen Verordnung im Januar 2025 verabschiedet wurde und ab dem 26. März 2025 gilt, repräsentiert die ambitionierteste Vision der Europäischen Union für die digitale Transformation des Gesundheitswesens. Diese Verordnung ist der Architektenentwurf für ein neues Gesundheitsdatenökosystem, das nationale Grenzen überwindet, Datensilos aufbricht und die Vision einer wirklich integrierten europäischen Gesundheitsversorgung Realität werden lässt. Für medizinische Labore, deren Kerntätigkeit in der Generierung, Verarbeitung und Bereitstellung diagnostischer Daten besteht, markiert der EHDS einen Wendepunkt von historischer Tragweite. Laborergebnisse werden nicht mehr isolierte Datenpunkte sein, sondern integrale Bestandteile eines paneuropäischen Gesundheitsdatennetzes, das die Art und Weise, wie Medizin praktiziert, Forschung betrieben und Gesundheitspolitik gestaltet wird, fundamental verändern wird.

Die duale Struktur des EHDS mit Primär- und Sekundärnutzung von Gesundheitsdaten reflektiert die zweifache Zielsetzung der Initiative. Die Primärnutzung fokussiert auf die direkte Patientenversorgung und gibt Bürgern erstmals echte Kontrolle über ihre Gesundheitsdaten. Patienten erhalten das Recht, ihre Gesundheitsdaten europaweit zu nutzen, unabhängig davon, wo diese generiert wurden. Ein deutscher Patient, der im Spanienurlaub erkrankt, soll Zugriff auf seine vollständigen Laborwerte aus Deutschland haben. Ein polnischer Arbeitnehmer, der nach Frankreich zieht, soll seine medizinische Historie nahtlos mitnehmen können. Diese Vision erfordert nicht nur technische Interoperabilität, sondern auch semantische Harmonisierung – Laborwerte müssen nicht nur übertragen, sondern auch verstanden und korrekt interpretiert werden können, unabhängig von nationalen Unterschieden in Einheiten, Referenzbereichen oder Terminologien.

Die Sekundärnutzung öffnet Gesundheitsdaten für Forschung, Innovation, Politik gestaltung und Public Health, allerdings unter strikten Datenschutz- und Sicherheitsvorkehrungen. Der EHDS schafft einen Mechanismus, durch den Forscher Zugang zu pseudonymisierten oder anonymisierten Daten aus ganz Europa erhalten können, ohne dass Patienten ihre Privatsphäre opfern müssen. Für Labore bedeutet dies, dass ihre Daten zu einer wertvollen Ressource für medizinischen Fortschritt werden, gleichzeitig aber auch neue Verantwortlichkeiten für Datenqualität und -governance entstehen.

Ab März 2029 müssen Patientenkurzakten EU-weit austauschbar sein – ein Meilenstein, der bereits erhebliche Vorbereitungen erfordert. Diese Kurzakten enthalten essenzielle medizinische Informationen, einschließlich wichtiger Laborwerte wie Blutgruppe, Allergiemarker oder chronische Erkrankungsparameter. Ab März 2031 folgt die vollständige Integration von Laborergebnissen in das System. Diese zweijährige Verzögerung erkennt die besondere Komplexität der Labormedizin an, mit ihren Tausenden verschiedener Tests, unterschiedlichen Analysemethoden und der Notwendigkeit präziser Interpretation.

Die technologische Grundlage des EHDS basiert auf HL7 FHIR (Fast Healthcare Interoperability Resources) als primärem Standard für den Datenaustausch. FHIR repräsentiert einen Paradigmenwechsel von dokumentenzentrierten zu datenzentrierten Austauschformaten. Anstatt PDF-Berichte zu versenden, werden strukturierte, maschinenlesbare Datensätze ausgetauscht, die automatisch verarbeitet, analysiert und in verschiedene Systeme integriert werden können.

LOINC (Logical Observation Identifiers Names and Codes) wird zum universellen Vokabular für Laborobservationen. Dieses standardisierte Codierungssystem, entwickelt vom Regenstrief Institute, umfasst über 90.000 Begriffe für Labortests und klinische Beobachtungen. Die Adoption von LOINC bedeutet für deutsche Labore eine erhebliche Umstellung, da traditionell andere Codierungssysteme verwendet wurden. Jeder Test muss auf LOINC gemappt werden, was bei Standard tests relativ einfach, bei spezialisierten oder neu entwickelten Tests jedoch komplex sein kann. Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) bietet Unterstützung durch die Bereitstellung von LOINC und RELMA-Tools (https://www.bfarm.de/DE/Kodiersysteme/Terminologien/LOINC-UCUM/LOINC-und-RELMA/_node.html), doch die praktische Implementierung bleibt eine Herausforderung für jedes Labor.

Die MyHealth@EU-Initiative, erreichbar unter https://www.gesundheit.gv.at/service/my-health-eu.html, bildet die operative Infrastruktur für den grenzüberschreitenden Datenaustausch. Diese Initiative, die bereits vor dem EHDS begann, wird nun zur zentralen Plattform ausgebaut. Für Labore bedeutet die Anbindung an MyHealth@EU nicht nur technische Integration, sondern auch die

Teilnahme an einem komplexen Governance-System mit nationalen Kontaktpunkten, Qualitätsstandards und Audit-Mechanismen. Die Anbindung ist nicht optional – sie wird zur Voraussetzung für die Teilnahme am europäischen Gesundheitsmarkt.

Das Opt-Out-Management stellt eine besondere Herausforderung dar, die die Balance zwischen individuellen Rechten und kollektivem Nutzen reflektiert. Während die Primärnutzung auf der Prämisse basiert, dass Patienten ihre eigenen Daten kontrollieren, sieht die Sekundärnutzung ein Opt-Out-Modell vor: Daten werden standardmäßig für Forschung und Public Health verfügbar gemacht, es sei denn, der Patient widerspricht aktiv. Labore müssen robuste Systeme implementieren, die diese Opt-Out-Entscheidungen verwalten, respektieren und über verschiedene Verwendungskontexte hinweg durchsetzen. Die Komplexität entsteht durch die Granularität: Patienten könnten der Nutzung für kommerzielle Forschung widersprechen, aber öffentliche Gesundheitsforschung erlauben, oder bestimmte Datenkategorien ausschließen, während andere freigegeben werden.

Die Forschungsperspektive eröffnet völlig neue Möglichkeiten. Durch den EHDS erhalten Forscher Zugang zu Daten von 450 Millionen EU-Bürgern – ein Datenschatz von unschätzbarem Wert für die medizinische Forschung. Für Labore ergeben sich Chancen zur Teilnahme an paneuropäischen Forschungsprojekten, zur Validierung neuer Biomarker an großen Populationen und zur Entwicklung KI-basierter Diagnostik mit ausreichenden Trainingsdaten. Gleichzeitig können Labore selbst von aggregierten Daten profitieren, um ihre eigenen Referenzbereiche zu optimieren, seltene Muster zu erkennen oder Qualitätsbenchmarks zu etablieren.

Die kulturelle Transformation darf nicht unterschätzt werden. Der EHDS erfordert einen Mentalitätswandel von Daten als Eigentum zu Daten als gemeinsame Ressource. Labore müssen ihre Rolle neu definieren: von isolierten Dienstleistern zu Knotenpunkten in einem vernetzten Ökosystem. Die Bereitschaft zur Datenteilung, zur Standardisierung und zur Zusammenarbeit über traditionelle Grenzen hinweg wird zum Erfolgsfaktor.

Referenzen:

EHDS Verordnungstext: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

HL7 FHIR: https://www.hl7.org/fhir/

LOINC/RELMA (BfArM): https://www.bfarm.de/DE/Kodiersysteme/Terminologien/LOINC-UCUM/LOINC-und-RELMA/_node.html

MyHealth@EU: https://www.gesundheit.gv.at/service/my-health-eu.html

13. ISO-Normen als Brücke zwischen Regulierung und Praxis

ISO-Normen fungieren als unverzichtbare Brücke zwischen den abstrakten Anforderungen europäischer Verordnungen und Richtlinien und ihrer praktischen Umsetzung im Laboralltag. Diese internationalen Standards übersetzen das "Was" der Gesetzgebung in das "Wie" der Implementierung und bieten bewährte Praktiken, die über Jahrzehnte entwickelt und kontinuierlich verfeinert wurden. Für medizinische Labore sind sie nicht nur Hilfsmittel zur Compliance, sondern essenzielle Werkzeuge zur Demonstration der Sorgfaltspflicht und zur Erlangung von Rechtssicherheit.

13.1 Normen für die NIS-2-Richtlinie und Cybersicherheit

Die Implementierung der NIS-2-Anforderungen wird durch die ISO/IEC 27000-Familie unterstützt, die den globalen Standard für Informationssicherheit darstellt. Die ISO/IEC 27001:2022 definiert die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) und ist die einzige zertifizierbare Norm dieser Familie. Die aktuelle Version von 2022

bringt wichtige Neuerungen, insbesondere in Bezug auf Cloud-Sicherheit und Bedrohungsintelligenz, wobei die Übergangsfrist für Organisationen mit Zertifizierungen nach der alten Version bis zum 31. Oktober 2025 läuft. Die ISO/IEC 27002:2022 ergänzt dies als umfassender Leitfaden mit 93 Sicherheitsmaßnahmen in vier Kategorien: organisatorisch, personell, physisch und technisch. Diese Maßnahmensammlung bietet konkrete Handlungsanweisungen für die Umsetzung der abstrakten NIS-2-Anforderungen.

Das Risikomanagement für Informationssicherheit wird durch ISO/IEC 27005:2022 strukturiert, die einen systematischen Ansatz zur Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken bietet. Für das Management von Sicherheitsvorfällen, eine zentrale Anforderung der NIS-2-Richtlinie, bietet ISO/IEC 27035-1:2023 einen strukturierten Rahmen, der von der Vorbereitung über die Erkennung und Bewertung bis zur Reaktion und Nachbereitung alle Phasen abdeckt. Die ISO 22301:2019 für Business Continuity Management ergänzt diese technischen Standards um organisatorische Resilienz und stellt sicher, dass Labore auch bei schwerwiegenden Störungen ihre kritischen Funktionen aufrechterhalten können.

Für Labore, die Cloud-Dienste nutzen – und das sind heute praktisch alle – bietet ISO/IEC 27017:2015 spezifische Sicherheitskontrollen für Cloud-Services, die sowohl für Cloud-Anbieter als auch Cloud-Nutzer relevant sind. Die ISO/IEC 27019:2024 adressiert spezifisch die Informationssicherheit in der Energieversorgung und ist für Labore relevant, die als Teil der kritischen Infrastruktur eingestuft werden. Die ISO/IEC 27701:2019 schließlich schlägt die Brücke zwischen Informationssicherheit und Datenschutz als Privacy Information Management System und hilft bei der gleichzeitigen Erfüllung von NIS-2 und DSGVO-Anforderungen.

13.2 Standards für den Cyber Resilience Act

Die Umsetzung des Cyber Resilience Act wird durch die IEC 62443-Serie unterstützt, die bis 2026/27 als harmonisierte europäische Norm (hEN) anerkannt werden soll. Diese Normenfamilie, ursprünglich für industrielle Automatisierungssysteme entwickelt, hat sich zum de-facto Standard für Cybersicherheit in vernetzten Systemen entwickelt. Die IEC 62443-4-1:2018 definiert einen sicheren Produktentwicklungsprozess und wird durch das Amendment 11:2026 spezifisch an CRA-Anforderungen angepasst. Die IEC 62443-4-2:2019 legt technische Sicherheitsanforderungen für Komponenten fest und erhält ebenfalls 2026 ein Amendment zur CRA-Harmonisierung. Die IEC 62443-3-3 definiert Systemsicherheitsanforderungen und Sicherheitsstufen, die Laboren helfen, angemessene Schutzmaßnahmen zu definieren.

Für die Evaluierung und Zertifizierung von IT-Sicherheit bietet ISO/IEC 15408:2022, bekannt als Common Criteria, einen international anerkannten Rahmen, der die Basis für die europäische EUCC-Zertifizierung bildet. Die ISO/IEC 27034-Serie zur Application Security wird für Labore relevant, die eigene Software entwickeln oder anpassen. Die Management von Schwachstellen, eine Kernforderung des CRA, wird durch ISO/IEC 29147:2018 für Vulnerability Disclosure und ISO/IEC 30111:2019 für Vulnerability Handling Processes strukturiert. Die ETSI EN 303 645 schließlich definiert Basissicherheitsanforderungen für Consumer IoT-Geräte, die auch in Laborumgebungen zunehmend eingesetzt werden.

13.3 Normen für MDR und IVDR

Die Medizinprodukte-Regularien werden durch eine etablierte Familie von Normen unterstützt, allen voran die ISO 13485:2016, die als harmonisierte Norm das Qualitätsmanagementsystem für Medizinprodukte definiert. Diese Norm ist die Grundlage für praktisch alle anderen

medizintechnischen Standards und ihre Einhaltung ist de facto obligatorisch für die CE-Kennzeichnung. Die ISO 14971:2019 für Risikomanagement ist ebenfalls harmonisiert und definiert einen systematischen Prozess zur Identifikation, Bewertung und Kontrolle von Risiken über den gesamten Produktlebenszyklus.

Die IEC 62304:2025, deren zweite Edition im Entwurf vorliegt, adressiert spezifisch den Software-Lebenszyklus für Medizinprodukte und wird angesichts der zunehmenden Digitalisierung immer wichtiger. Die IEC 62366-1:2015+A1:2020 für Gebrauchstauglichkeit (Usability Engineering) stellt sicher, dass Medizinprodukte sicher und effektiv bedient werden können. Die umfangreiche ISO 10993-Serie zur biologischen Beurteilung von Medizinprodukten ist für Labore relevant, die mit Probenmaterial in Kontakt kommende Produkte einsetzen. Die IEC 60601-1:2005+A1:2012+A2:2020 definiert Sicherheitsanforderungen für elektrische medizinische Geräte, während die IEC 82304-1:2016 spezifisch Gesundheitssoftware adressiert.

13.4 Standards für die KI-Verordnung

Die Regulierung künstlicher Intelligenz wird durch eine neue Generation von Standards unterstützt, angeführt von der ISO/IEC 42001:2023, der weltweit ersten zertifizierbaren Norm für KI-Managementsysteme (AIMS). Diese Norm definiert Anforderungen an die Governance, das Risikomanagement und die kontinuierliche Verbesserung von KI-Systemen. Die ISO/IEC 42005:2025, die im Mai 2025 veröffentlicht werden soll, bietet einen strukturierten Rahmen für KI-Folgenabschätzungen. Die ISO/IEC 42006:2025, geplant für Juli 2025, legt Anforderungen an Zertifizierungsstellen fest und wird die Grundlage für die Konformitätsbewertung von KI-Systemen bilden.

Für das technische Verständnis und die Implementierung von KI bietet ISO/IEC 23053:2022 ein umfassendes Framework für KI-Systeme mit Machine Learning. Das KI-spezifische Risikomanagement wird durch ISO/IEC 23894:2023 strukturiert, die auf die besonderen Herausforderungen von KI-Systemen eingeht. Die ISO/IEC 42009 zur KI-Governance befindet sich noch in Entwicklung, wird aber wichtige Leitlinien für die organisatorische Einbettung von KI liefern. Für die technische Robustheit neuronaler Netze bieten ISO/IEC 24029-1 und -2 Bewertungsmethoden, während ISO/IEC 25059 ein Qualitätsmodell speziell für KI-Systeme definiert.

13.5 Normen für DSGVO und EHDS

Die Datenschutzanforderungen werden durch ISO/IEC 27701:2019 als Privacy Information Management System unterstützt, das als Erweiterung zur ISO 27001 konzipiert ist und die gleichzeitige Zertifizierung für Informationssicherheit und Datenschutz ermöglicht. Das ISO/IEC 29100:2024 Privacy Framework bietet eine umfassende Grundlage für Datenschutz in IT-Systemen mit der neuesten Aktualisierung von 2024. Die ISO/IEC 29134:2023 strukturiert Datenschutz-Folgenabschätzungen und bietet praktische Werkzeuge für diese DSGVO-Anforderung. Cloud-spezifischer Datenschutz wird durch ISO/IEC 27018:2019 adressiert, während die ISO/IEC 27560-Serie zu Privacy by Design sich noch in Entwicklung befindet, aber wichtige Impulse für die Systemgestaltung liefern wird. Die ISO/IEC 25237:2017 schließlich definiert Standards für Pseudonymisierung, eine Schlüsseltechnik für datenschutzkonforme Datenverarbeitung.

13.6 Laborspezifische Normen

Über die regulatorisch getriebenen Standards hinaus gibt es spezifische Normen für medizinische Labore, die als Grundlage für Qualität und Kompetenz dienen. Die ISO 15189:2022 für medizinische Laboratorien ist der Goldstandard für Laborqualität und -kompetenz und wird international als

Akkreditierungsgrundlage anerkannt. Diese Norm integriert Qualitätsmanagement und technische Kompetenzanforderungen und bildet oft die Basis für die Erfüllung verschiedener regulatorischer Anforderungen. Ergänzend bietet die ISO 22870:2016 spezifische Anforderungen für Point-of-Care-Testing, einem wachsenden Bereich der Labormedizin. Die ISO 35001:2019 für Biolaboratorien adressiert spezifische Risikomanagementaspekte im Umgang mit biologischen Materialien.

13.7 Strategische Empfehlungen für den Einstieg

Die Vielzahl der Standards kann überwältigend wirken, weshalb eine strategische Priorisierung essentiell ist. Für Labore, die mit der Standardisierung beginnen, empfiehlt sich folgender Ansatz: Für die NIS-2-Compliance sollte mit ISO 27001:2022 begonnen werden, da diese die Basis für ein umfassendes Informationssicherheitsmanagement bildet. KI-Anbieter sollten sich frühzeitig mit ISO 42001 auseinandersetzen und die ISO 42006 für die kommende Zertifizierungsvorbereitung im Blick behalten. Der KI-Compliance Checker unter https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/ bietet eine erste Orientierung. Produkthersteller, die unter den CRA fallen, sollten prioritär IEC 62443-4-1 für sichere Entwicklungsprozesse implementieren. Für Medizintechnik bleiben die harmonisierten Normen ISO 13485 und ISO 14971 unverzichtbar.

Die Implementierung dieser Standards sollte nicht als isolierte Compliance-Übung verstanden werden, sondern als integrierter Ansatz zur Organisationsentwicklung. Viele Normen überschneiden sich in ihren Anforderungen und können synergetisch implementiert werden. Ein integriertes Managementsystem, das ISO 27001, ISO 13485 und ISO 15189 kombiniert, vermeidet Redundanzen und schafft Effizienz. Die Investition in Standardkonformität zahlt sich nicht nur durch regulatorische Compliance aus, sondern auch durch verbesserte Prozesse, reduzierte Risiken und gesteigertes Vertrauen von Kunden und Partnern.

14. Von der Compliance-Last zur strategischen Chance

Die regulatorische Landschaft für medizinische Labore hat sich in den vergangenen Jahren gewandelt und wird sich in den kommenden Jahren weiter verdichten. Die in diesem Whitepaper dargestellten acht Kernregularien – von der NIS-2-Richtlinie über die KI-Verordnung bis zum European Health Data Space – repräsentieren nicht isolierte Anforderungen, sondern Facetten einer umfassenden Transformation des Gesundheitswesens im digitalen Zeitalter. Diese Transformation ist unumkehrbar und alternativlos. Labore, die versuchen, sich dieser Entwicklung zu entziehen oder sie zu ignorieren, werden nicht nur rechtliche Konsequenzen tragen, sondern auch ihre Wettbewerbsfähigkeit und letztendlich ihre Existenz gefährden.

Die schiere Komplexität der regulatorischen Anforderungen kann lähmend wirken. Cybersicherheit nach NIS-2, erweiterte Produkthaftung für Software und KI, strenge Anforderungen an künstliche Intelligenz, umfassende Medizinprodukteregulierung, rigoroser Datenschutz und die Vision eines vernetzten europäischen Gesundheitsdatenraums – jede einzelne dieser Regularien würde für sich genommen bereits erhebliche Ressourcen und Aufmerksamkeit erfordern. In ihrer Gesamtheit erscheinen sie manchmal als unüberwindbare Hürde. Doch diese Perspektive greift zu kurz und verkennt die inhärenten Chancen dieser Entwicklung.

Die neuen Regularien sind nicht willkürliche bürokratische Hürden, sondern reflektieren reale Risiken und Herausforderungen der digitalisierten Medizin. Cyberangriffe auf Gesundheitseinrichtungen sind keine theoretische Bedrohung, sondern tägliche Realität. KI-Systeme treffen zunehmend diagnostische Entscheidungen mit weitreichenden Konsequenzen für Patienten.

Die Qualität und Sicherheit von In-vitro-Diagnostika kann über Leben und Tod entscheiden. Der Schutz sensibler Gesundheitsdaten ist nicht nur rechtliche Pflicht, sondern ethische Verantwortung. Die Regularien zwingen Labore, diese Risiken systematisch zu adressieren und dabei Standards zu erreichen, die dem Stand der Technik und der Kritikalität ihrer Funktion angemessen sind.

Der Schlüssel zum Erfolg liegt in einem integrierten, strategischen Ansatz zur Compliance. Anstatt jede Regulierung isoliert zu betrachten, sollten Labore die Synergien erkennen und nutzen. Ein robustes Informationssicherheitsmanagementsystem nach ISO 27001 erfüllt nicht nur NIS-2-Anforderungen, sondern unterstützt auch DSGVO-Compliance, Cyber Resilience Act-Konformität und die Sicherheitsaspekte der KI-Verordnung. Ein umfassendes Qualitätsmanagementsystem integriert MDR/IVDR-Anforderungen mit den Qualitätsaspekten des EHDS und der Produkthaftungsrichtlinie. Die Dokumentation für eine Regulierung kann oft für andere genutzt werden. Investitionen in Technologie und Prozesse amortisieren sich über multiple Compliance-Anforderungen.

Die zeitliche Dimension erfordert sofortiges Handeln, aber auch langfristige Planung. Während einige Regularien bereits vollständig in Kraft sind, gewähren andere noch Übergangsfristen. Diese Zeit sollte nicht als Gnadenfrist missverstanden werden, sondern als Opportunity Window für systematische Vorbereitung. Die Implementierung umfassender Compliance-Systeme benötigt Zeit – oft Jahre für vollständige Transformation. Labore, die jetzt beginnen, werden rechtzeitig bereit sein. Labore, die zögern, werden in Zeitnot geraten und zu kostspieligen Schnellschüssen gezwungen sein.

Die internationalen Standards (ISO-Normen) übersetzen abstrakte regulatorische Anforderungen in konkrete, praxiserprobte Handlungsanweisungen. Sie repräsentieren das kollektive Wissen der globalen Expertengemeinschaft und bieten einen strukturierten Weg zur Compliance.

Die Transformation der regulatorischen Landschaft ist eine Chance zur Neupositionierung. Labore, die Compliance nicht als notwendiges Übel, sondern als Differenzierungsmerkmal verstehen und kommunizieren, können sich im Markt abheben. Nachweisbare Exzellenz in Cybersicherheit, Datenschutz und Qualität wird zum Wettbewerbsvorteil. Die Fähigkeit, neue Technologien wie KI compliant einzusetzen, eröffnet Innovationsmöglichkeiten. Die Integration in den European Health Data Space erschließt neue Märkte und Kooperationsmöglichkeiten.

Die Zukunft der Labormedizin wird von denjenigen gestaltet, die die regulatorische Transformation nicht als Hindernis, sondern als Katalysator für Evolution verstehen. Die Regularien zwingen zu Professionalisierung, Standardisierung und Qualität – Eigenschaften, die ohnehin für nachhaltigen Erfolg essentiell sind. Sie fördern Transparenz und Verantwortlichkeit – Werte, die das Vertrauen von Patienten und Partnern stärken. Sie treiben Innovation in sichere und ethische Bahnen – eine Notwendigkeit für die Akzeptanz neuer Technologien.

Der Weg zur regulatorischen Exzellenz ist zweifellos anspruchsvoll. Er erfordert Investitionen, nicht nur finanziell, sondern auch in Form von Zeit, Aufmerksamkeit und organisatorischem Wandel. Er verlangt neue Kompetenzen, interdisziplinäre Zusammenarbeit und kontinuierliches Lernen. Er zwingt zu manchmal schmerzhaften Entscheidungen über Prioritäten und Ressourcenallokation. Doch dieser Weg ist alternativlos. Die Frage ist nicht, ob Labore diesen Weg gehen müssen, sondern wie sie ihn gestalten – reaktiv und widerwillig oder proaktiv und gestaltend.