SECJUR

WHITEPAPER
2026

NIS2 · GESUNDHEIT, KLINIK & MEDTECH

NIS2 im Gesundheitswesen: Sicherheit schützt Patienten.

Im Gesundheitswesen ist Informationssicherheit längst eine Frage der Patientensicherheit. Vernetzte Medizingeräte, digitale Patientenakten und die Telematikinfrastruktur verbinden alles miteinander, und ein Ransomware-Angriff kann eine Klinik in den Notbetrieb zwingen. Das NIS2-Umsetzungsgesetz erfasst die Branche, §75c SGB V verlangt den Stand der Technik, und für KRITIS-Häuser gilt der regelmäßige Nachweis. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen in IT und Medizintechnik liegen und wie ein ISMS entsteht, das den Betrieb nicht gefährdet.

NIS2 | ISO 27001 | KRITIS | B3S | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im Gesundheitswesen ist Sicherheit Patientensicherheit.

DAS WICHTIGSTE IN KÜRZE

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) ist am 6. Dezember 2025 in Kraft getreten und novelliert das BSI-Gesetz. Eine Übergangsfrist gibt es nicht. Der Sektor Gesundheitswesen gehört ausdrücklich zu den 18 erfassten Bereichen, häufig als besonders wichtige Einrichtung mit den strengsten Pflichten.

Für die Branche ist NIS2 dabei nur ein Baustein eines dichten Rahmens. §75c SGB V verpflichtet Krankenhäuser, angemessene Vorkehrungen nach dem Stand der Technik zu treffen, häufig nachgewiesen über den branchenspezifischen Sicherheitsstandard B3S oder ein ISMS nach ISO 27001. Hinzu kommen die KRITIS-Regulierung und der erhöhte Schutz von Gesundheitsdaten nach Art. 9 DSGVO. NIS2 fügt sich hier ein und verlangt Registrierung, Risikomanagement, Meldepflichten und eine haftende Leitung. Wer die Einstufung sauber dokumentiert, schafft Klarheit und schützt die Leitung im Zweifel vor Haftung. Für viele Häuser ist die Cyber-Regulierung damit vom IT-Randthema zur Vorstandsaufgabe geworden.

WARUM JETZT HANDELN

Der Pflichtenrahmen ist dicht, und die BSI-Registrierungsfrist endete am 31. Juli 2026. Wer betroffen und im Verzug ist, holt die Registrierung umgehend nach.

Zugleich ist die Bedrohungslage akut. Kliniken gehören zu den am häufigsten von Ransomware getroffenen Einrichtungen, weil der Druck zur schnellen Wiederherstellung dort am größten ist. Mehrere Häuser mussten nach Angriffen Operationen verschieben und sich von der Notfallversorgung abmelden. Ein Ausfall trifft hier nicht die Buchhaltung, sondern unmittelbar die Behandlung. Wer den Nachweis früh aufbaut, begegnet Aufsicht und Kostenträgern aus einer Position der Stärke. Ein Vorfall trifft zudem nicht nur die betroffene Klinik, sondern das Vertrauen einer ganzen Region.

EIN AUFBAU, MEHRERE PFLICHTEN

Die gute Nachricht: Ein ISMS nach ISO 27001 erfüllt §75c SGB V und deckt einen Großteil von NIS2 zugleich ab. Statt jede Vorschrift getrennt abzuarbeiten, entsteht ein gemeinsames Fundament, das Verwaltung, klinische Systeme und vernetzte Medizintechnik absichert und im Ernstfall den Betrieb aufrechterhält.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Medizintechnik, die Pflichten aus dem Gesetz und eine Roadmap, die im Klinikbetrieb funktioniert. So bleibt die knappe Kapazität bei der Versorgung, statt in Formularen zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht in der Einrichtung.

NIS2 IN KRAFT

06.12.2025

Das Gesundheitswesen zählt zu den erfassten Sektoren, häufig als besonders wichtige Einrichtung.

FÜR KRANKENHÄUSER

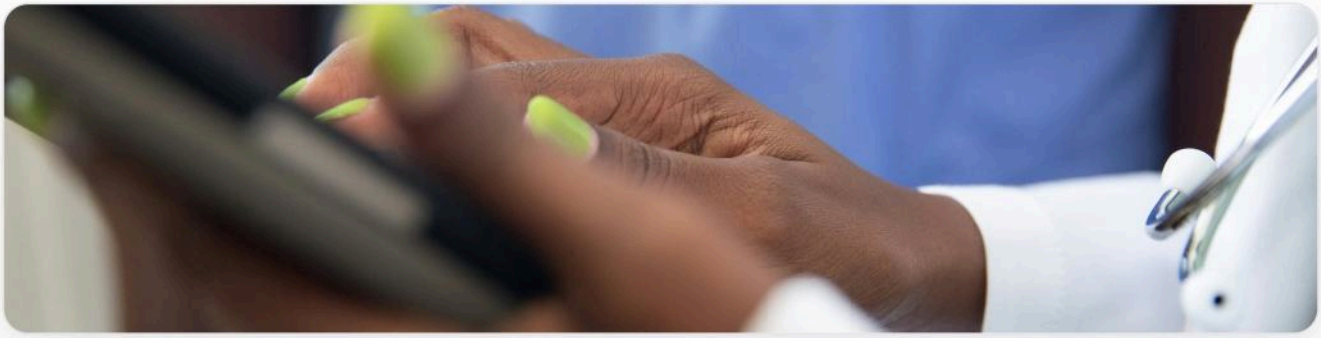
§75c SGB V

Vorkehrungen nach dem Stand der Technik, nachgewiesen über B3S oder ISO 27001.

BUSSGELD

10 Mio €

Bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen.



BRANCHENKONTEXT

Die Versorgung hängt am Netz und an den Daten.

Moderne Medizin ist digital. Patientenakten, Diagnostik, Medizingeräte und die Telematikinfrastruktur sind eng vernetzt, und ein Ausfall trifft unmittelbar die Versorgung. Genau deshalb ist das Gesundheitswesen reguliert wie kaum eine Branche und zugleich ein bevorzugtes Ziel.

Fällt das Klinik-IT-System aus, geht es nicht um Daten, *sondern um Behandlung.*

EINE DURCHDIGITALISIERTE VERSORGUNG

Krankenhausinformationssysteme, elektronische Patientenakte, Labor- und Radiologiesysteme, vernetzte Medizingeräte und die Telematikinfrastruktur bilden eine durchgehende digitale Kette. Befunde, Medikation und Vitaldaten fließen in Echtzeit zwischen Stationen, Praxen und Diensten.

Diese Vernetzung verbessert die Versorgung und vergrößert die Angriffsfläche zugleich. Wo IT und Medizintechnik aufeinandertreffen, entstehen die kritischen Punkte, und sie betreffen nicht nur Daten, sondern den Behandlungsbetrieb selbst. Schon ein Blick auf die Übergänge zwischen KIS und Medizintechnik zeigt, wo die dringendsten Lücken liegen.

EIN DICHTER PFLICHTENRAHMEN

Das Gesundheitswesen ist mehrfach reguliert. §75c SGB V verlangt von Krankenhäusern Vorkehrungen nach dem Stand der Technik, üblicherweise über den B3S Krankenhaus oder ein ISMS nachgewiesen. Häuser ab den KRITIS-Schwellen müssen regelmäßig Nachweise erbringen, und NIS2 erweitert den Kreis der erfassten Einrichtungen deutlich.

Hinzu kommt der Datenschutz: Gesundheitsdaten sind nach Art. 9 DSGVO eine besondere Kategorie mit erhöhten Anforderungen. Ein ISMS bündelt diese Pflichten in einem System, statt sie einzeln zu verwalten. Ein gemeinsames ISMS spart die Doppelarbeit, die getrennte Nachweise sonst erzeugen.

KLINIKEN IM VISIER

Krankenhäuser zählen zu den häufigsten Ransomware-Zielen. Angreifer wissen, dass eine Klinik nicht tagelang stillstehen kann, und erhöhen so den Druck zur Zahlung. Mehrere Häuser mussten nach Angriffen Operationen verschieben und sich von der Notfallversorgung abmelden.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als Daten: um Behandlungsfähigkeit, Patientensicherheit und am Ende Menschenleben. Ein Ausfall der Systeme kann Diagnosen verzögern und Eingriffe gefährden.

Sicherheit ist hier unmittelbar Teil der Versorgungsqualität. Ein belastbarer Nachweis schützt deshalb nicht nur vor Bußgeldern, sondern die Handlungsfähigkeit der Einrichtung im Ernstfall. Gerade kommunale Häuser tragen hier Verantwortung für die Versorgung einer ganzen Region.

HERAUSFORDERUNGEN

Warum NIS2 im Gesundheitswesen besonders fordert.

Die Anforderungen gelten unabhängig von der Branche, der Aufwand ist es nicht. Sechs Eigenheiten des Gesundheitswesens machen die Umsetzung anspruchsvoller als anderswo, und für jede gibt es einen pragmatischen Umgang.

VERNETZTE MEDIZINGERÄTE

Vom Beatmungsgerät bis zum MRT sind Medizingeräte heute vernetzt, haben aber lange Lebenszyklen und laufen oft auf veralteten Betriebssystemen. Hersteller schränken Updates ein, und ein Gerät lässt sich nicht im laufenden Betrieb neu starten. Die Risikoanalyse muss diese Geräte einbeziehen, ohne ihre Verfügbarkeit zu gefährden. Netzsegmentierung und strenge Zugänge schützen, wo ein Patch nicht möglich ist. Ein eigenes Gerätenetz, klar vom übrigen Betrieb getrennt, hält den Schaden im Ernstfall lokal.

VERFÜGBARKEIT RETTET LEBEN

In der Büro-IT steht oft Vertraulichkeit zuerst. In der Klinik ist Verfügbarkeit überlebenswichtig, denn Systeme müssen rund um die Uhr laufen. Eine Sicherheitsmaßnahme, die ein klinisches System destabilisiert, ist keine Option. Maßnahmen müssen schützen, ohne den Betrieb zu stören. Wiederanlaufpläne, Redundanzen und ein geübter Notbetrieb sind hier besonders wichtig. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf spürbar.

HÖCHSTES SCHUTZNIVEAU FÜR DATEN

Gesundheitsdaten sind nach Art. 9 DSGVO besonders geschützt. Ein Abfluss ist nicht nur ein Vertrauensbruch, sondern kann hohe Bußgelder und Erpressung nach sich ziehen. Verschlüsselung, strenge Zugriffskontrolle und Protokollierung sind hier nicht optional, sondern Grundlage jeder Prüfung. Wer weiß, wo die sensibelsten Daten liegen, kann sie zuerst und am stärksten schützen.

SCHICHTBETRIEB UND FLUKTUATION

Kliniken arbeiten im Schichtbetrieb mit vielen Beschäftigten, Wechseldiensten und externem Personal. Zugänge müssen schnell vergeben und ebenso schnell wieder entzogen werden. Sauberes On- und Offboarding und rollenbasierte Rechte sind eine Daueraufgabe. Ein automatisierter Entzug beim Austritt verhindert, dass Berechtigungen liegen bleiben.

BUDGET- UND PERSONALDRUCK

Das Gesundheitswesen arbeitet unter Kosten- und Personaldruck, eigene Sicherheitsfunktionen sind selten üppig besetzt. NIS2 verlangt aber Struktur und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen hier den Unterschied.

MEDTECH ALS ZULIEFERER

Auch Hersteller von Medizinprodukten und IT-Dienstleister der Branche werden erfasst, direkt über NIS2 oder über die Lieferkette ihrer Klinikkunden. Wer Kliniken beliefert, muss die eigene Sicherheit zunehmend nachweisen, und ein ISMS liefert genau diesen Beleg. Wer den Nachweis früh vorlegt, bleibt für Kliniken ein bevorzugter Partner.

BEDROHUNGSLAGE & RISIKEN

Wo das Gesundheitswesen konkret angreifbar ist.

Die Risiken sind selten abstrakt. Sie hängen an vernetzter Medizintechnik, an höchst sensiblen Daten und an einer Versorgung, die keinen Stillstand verträgt. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE ZWINGT IN DEN NOTBETRIEB

Der gefährlichste Ernstfall. Werden Krankenhausinformationssystem und klinische Systeme verschlüsselt, fällt die Einrichtung auf Stift und Papier zurück, Operationen werden verschoben und die Notaufnahme meldet sich ab. Hier geht es unmittelbar um Patientensicherheit. Getestete Backups, Segmentierung und ein eingeübter Notfallplan entscheiden, wie schnell der Betrieb zurückkehrt. Wer den Notbetrieb regelmäßig übt, verliert im Ernstfall keine Zeit mit Grundsatzfragen. Ein aktueller Notfallplan legt vorab fest, wer was entscheidet.

2 · KOMPROMITTIERTE MEDIZINGERÄTE

Vernetzte, schlecht gepatchte Geräte sind ein Einfallstor und im schlimmsten Fall selbst manipulierbar. Ein verändertes Gerät oder ein über das Medizingerätenetz verbreiteter Angriff gefährdet Diagnose und Therapie. Strikte Trennung der Gerätenetze und überwachte Zugänge sind hier zentral und schützen zugleich Patient und Betrieb. Ein Inventar aller vernetzten Geräte ist die Grundlage, um Schwachstellen überhaupt zu erkennen. Wo ein Patch fehlt, kompensiert die Netztrennung.

3 · DIEBSTAHL VON PATIENTENDATEN

Gesundheitsdaten sind auf dem Schwarzmarkt besonders wertvoll und für Erpressung geeignet. Ein Abfluss von Diagnosen, Befunden und Stammdaten ist ein schwerer DSGVO-Vorfall nach Art. 9 mit hohem Bußgeldrisiko. Verschlüsselung und strenge Zugriffskontrolle schützen diesen Datenschatz, eine Protokollierung macht Zugriffe nachvollziehbar. Auffällige Massenzugriffe fallen nur auf, wenn sie protokolliert und ausgewertet werden.

4 · ANGRIFFE ÜBER DIE LIEFERKETTE

Gerätehersteller, Wartungsdienste und IT-Dienstleister mit Fernzugängen sind ein beliebter Umweg ins Kliniknetz. Ein kompromittierter Partner oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung nach §30 und abgesicherte Fernwartung begrenzen dieses Risiko. Ein aktuelles Verzeichnis aller Wartungszugänge macht die Kette überhaupt erst überblickbar. Feste Zeitfenster und eine Mehrfaktor-Anmeldung begrenzen, was über einen Fernzugang möglich ist.

5 · INSIDER UND OFFENE ZUGÄNGE

Im Schichtbetrieb mit hoher Fluktuation bleiben Zugänge ausscheidender oder externer Kräfte leicht offen, Rechte häufen sich an. Ein vergessenes Konto wird zum Risiko. Rollenbasierte Rechte, sauberes Offboarding und Protokollierung schließen diese Lücke. Ein fester Rhythmus zur Rechteprüfung räumt verwaiste Konten zuverlässig aus. Eine lückenlose Protokollierung macht ungewöhnliche Zugriffe früh sichtbar.

REGULATORISCHE PFLICHTEN

Was NIS2 und §75c SGB V konkret verlangen.

NIS2 steht im Gesundheitswesen neben §75c SGB V, dem B3S Krankenhaus, der KRITIS-Regulierung und Art. 9 DSGVO. Fünf Bausteine muss jede betroffene Einrichtung kennen: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Der Sektor Gesundheitswesen umfasst Kliniken, große Gesundheitsdienstleister, Labore und Hersteller kritischer Medizinprodukte, häufig als besonders wichtige Einrichtungen. Maßgeblich sind Funktion und Größe, nicht das Selbstbild. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal. Für Krankenhäuser tritt der Nachweis nach §75c SGB V hinzu, für KRITIS-Häuser der regelmäßige Nachweis gegenüber dem BSI. Im Zweifel schafft eine kurze, dokumentierte Einstufung Klarheit für die Leitung.

§30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Multifaktor-Authentifizierung. Vernetzte Medizintechnik gehört ausdrücklich dazu. Wer bereits ein ISMS nach ISO 27001 oder den B3S betreibt, bringt vieles mit und setzt NIS2 als Erweiterung um, nicht als zweites Projekt. Entscheidend ist, dass jede Maßnahme nicht nur existiert, sondern nachweisbar gelebt und regelmäßig überprüft wird.

§32 · MELDEFRISTEN

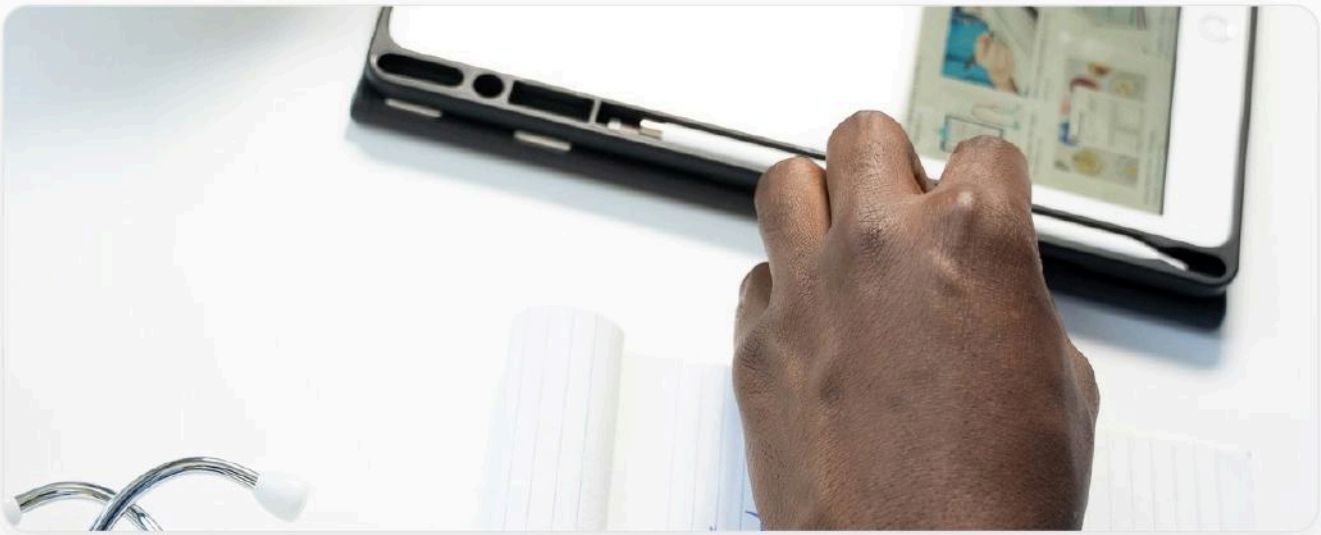
Bei einem erheblichen Sicherheitsvorfall gilt eine gestufte Meldepflicht an das BSI: Frühwarnung binnen 24 Stunden, Meldung mit erster Bewertung binnen 72 Stunden, Abschlussbericht binnen eines Monats. Steht die Versorgung still, zählt jede Stunde, und die Uhr läuft ab Kenntnis. Nur ein vorab geübter Prozess hält diese Fristen. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im Ernstfall wertvolle Minuten.

§38 · LEITUNG HAFTET PERSÖNLICH

Die Geschäftsführung muss die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Die Verantwortung ist nicht delegierbar, auch nicht an den externen IT-Dienstleister. Gerade unter Budgetdruck ist der sichtbare Rückhalt der Leitung entscheidend. Das dokumentierte Engagement ist im Ernstfall zugleich ein Nachweis gelebter Sorgfalt. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil dieser Pflicht.

§65 · SANKTIONEN UND VERHÄLTNISMÄSSIGKEIT

Verstöße kosten bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen. Hinzu treten Anordnungen der Aufsicht. Zugleich gilt die Verhältnismäßigkeit: geschuldet ist ein Schutzniveau, das zu Größe und Risiko passt. Ein dokumentierter, gelebter Prozess ist im Prüffall die beste Verteidigung. Wer Lücken kennt und plant, wird selbst bei einem Vorfall milder bewertet als eine untätige Einrichtung.



UMSETZUNG IN DER PRAXIS

In sechs Schritten mit Augenmaß NIS2-konform.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Strukturen, statt bei null zu beginnen. Realistisch führt der Weg je nach Reife und Gerätelandschaft in einigen Monaten zu einem auditbereiten Stand.

Ein ISMS erfüllt §75c SGB V und einen Großteil von NIS2 zugleich. *Ein Aufbau, mehrere Pflichten.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Feststellen, ob die Einrichtung unter NIS2, §75c SGB V oder KRITIS fällt, und den Scope auf die versorgungskritischen Bereiche schneiden: KIS, klinische Systeme, Medizintechniknetze und zugehörige IT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und für die Nachweise gegenüber der Aufsicht.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. Der sichtbare Rückhalt der Leitung ist gerade im Klinikbetrieb entscheidend. Registrierung und Kontaktstellen für das BSI gehören ebenfalls in diesen Schritt.

3 · RISIKEN IN IT UND MEDIZINTECHNIK

Assets erfassen, von der Verwaltung über das KIS bis zu den vernetzten Geräten. Risiken gemeinsam für IT und Medizintechnik bewerten, Verfügbarkeit und Datenschutz besonders gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

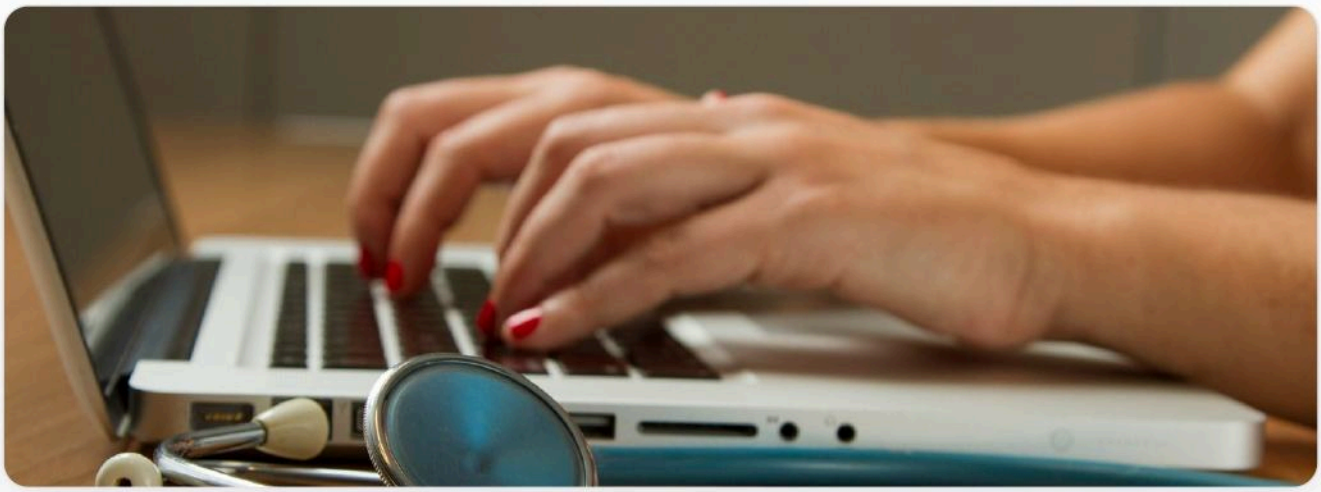
Mit den wirksamsten Hebeln beginnen: Netzsegmentierung der Gerätenetze, Backup, Zugriffskontrolle und abgesicherte Fernwartung. Jede Maßnahme so festhalten, dass sie im Audit und vor der Aufsicht Bestand hat. In der Medizintechnik gilt: schützen, ohne die Verfügbarkeit zu gefährden. Zentrale Vorgaben verhindern, dass jede Station eigene Wege geht.

5 · MELDE- UND NOTBETRIEBSPROZESSE

Die 24-Stunden-Meldekette an das BSI einrichten, Zuständigkeiten klären und den Notbetrieb testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen und die Versorgung. Eine Übung pro Jahr zeigt, wo der Ablauf zwischen Stationen und IT noch hakt.

6 · PRÜFEN, NACHWEISEN, VERBESSERN

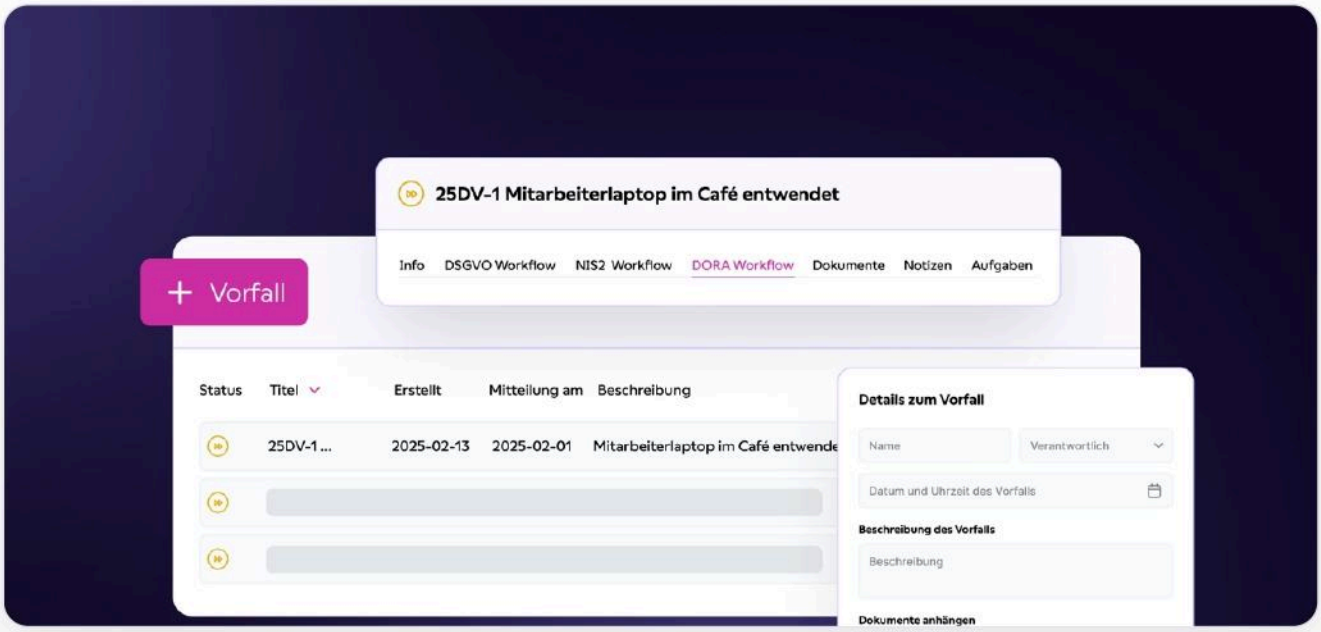
Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Diese Schleife deckt sich mit den wiederkehrenden Nachweisen nach §75c SGB V und KRITIS. Wer sie einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen.



WIE SECJUR ES EINFACH MACHT

Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt Gesundheitseinrichtungen durch NIS2 und §75c SGB V zugleich: Risiken in IT und Medizintechnik, Maßnahmen, Meldeprozess und Nachweise an einem Ort, mehrere Frameworks parallel. Statt monatelanger Beratung arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



IT und Medizintechnik

Eine Risikoanalyse, die Verwaltung, klinische Systeme und vernetzte Geräte zusammen denkt, mit Vorlagen, die den Klinikbetrieb kennen.

Vorfall & Notbetrieb

Strukturiertes Incident-Management mit der 24-Stunden-Meldekette an das BSI, inklusive Fristenverfolgung (24h / 72h / 1 Monat) und geübtem Notbetrieb.

Mehrere Pflichten

NIS2, §75c SGB V, B3S und ISO 27001 laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt mehrfach.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie legen den Geltungsbereich fest, das DCO führt durch jede Anforderung, und wo eine Expertin nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereiter Nachweis in Wochen statt in Quartalen, ohne dass die Versorgung stehen bleibt.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets in IT und Medizintechnik sowie bestehende Maßnahmen ab und leitet daraus die offenen Punkte ab. Jeder Schritt ist mit einer Vorlage hinterlegt, sodass niemand vor einem leeren Blatt sitzt.

Wo es schnell gehen muss, arbeitet das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar. Der Fortschritt bleibt jederzeit sichtbar, für die IT ebenso wie für die Leitung.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, §75c SGB V, der B3S und ISO 27001 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Für eine Einrichtung heißt das weniger Doppelarbeit. Der NIS2-Nachweis und die Zertifizierung nach ISO 27001 entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist die Einrichtung für die nächste Prüfung nach §75c SGB V oder das nächste KRITIS-Audit vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Schutz der Versorgung.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Kliniken, Gesundheitsdienstleister, MedTech-Unternehmen und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Gesundheitswesen:

Der Medizinische Dienst Nordrhein baut mit SECJUR ein ISMS nach ISO 27001 für alle acht Standorte auf und ist damit *zugleich optimal auf NIS2 vorbereitet.*

Medizinischer Dienst Nordrhein
ISO 27001 & NIS2 · 1.500 Mitarbeitende, 8 Standorte

REFERENZEN AUS GESUNDHEIT, PFLEGE UND MEDTECH

VIDEOCLINIC · St. Bernhard Hospital · HOMECARE · Medizinischer Dienst Nordrhein · AllDent Zahnzentrum · URSAPHARM

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

ZEITERSPARNIS
50%
Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN
60+
Native API-Anbindungen, von Microsoft 365 bis GitHub.

STANDARDS
10+
Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM GESUNDHEITSEINRICHTUNGEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und der Branchentiefe. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die IT und Medizintechnik gemeinsam denken. Das Team bleibt bei der Versorgung, das ISMS entsteht parallel.

Nachweise wachsen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass Leitung, IT und Medizintechnik an einer Quelle arbeiten statt an verstreuten Tabellen.

Weil dieselbe Struktur auch §75c SGB V und die NIS2-Pflichten bedient, deckt ein Projekt mehrere Anforderungen zugleich ab. Das senkt den Aufwand und macht den Fortschritt jederzeit sichtbar, für die Leitung wie für die Aufsicht.

Und die Plattform denkt in der Realität eines Versorgungsbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und schützt, ohne den klinischen Betrieb zu stören.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat und der Nachweis nach §75c SGB V, sondern eine Einrichtung, die ihre Risiken kennt und im Ernstfall handlungsfähig bleibt. Genau das schützt die Versorgung und die Patienten.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Betriebsvorteil. Audits verlieren ihren Schrecken, Störungen werden schneller beherrscht, und Verwaltung wie Medizintechnik ziehen an einem Strang.

Weil das DCO die Nachweise laufend aktuell hält, bleibt die Einrichtung auch nach dem Audit auskunftsfähig, gegenüber Aufsicht, Partnern und der eigenen Geschäftsführung. Informationssicherheit wird damit zur Routine statt zum Projekt.

So wird aus einer Pflicht ein dauerhafter Schutz von Behandlung, Daten und Vertrauen, der mit jedem vernetzten Gerät und jeder digitalen Akte an Bedeutung gewinnt.

SECJUR

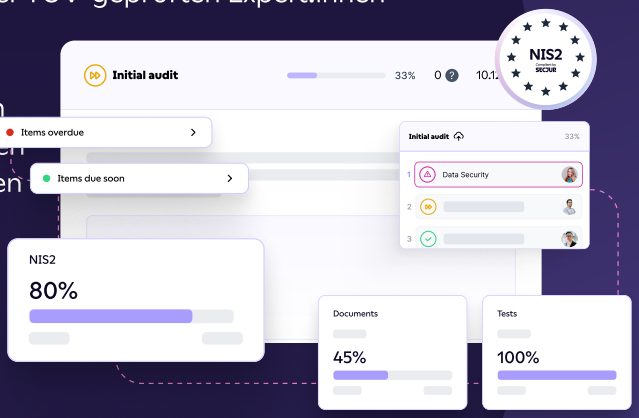
Mit SECJUR zu 100 % NIS2-Compliance

Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.



Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**

Mit SECJUR zur automatisierten Compliance

"Als Einrichtung im Gesundheitswesen mussten wir NIS2 verlässlich und prüfungssicher umsetzen. Mit SECJUR haben wir Risikoanalyse, Dokumentation und Behördennachweise zentral abgebildet, ohne unser Tagesgeschäft auszubremsen."

Anonym

Leitung IT-Sicherheit, Gesundheitswesen

VIDEOCLINIC GSK EvoCare. St. Bernhard HOSPITAL HOMECARE viluavitartis

www.secjur.com