NIS-2 Checkliste für Einrichtungen im Gesundheitswesen

(Krankenhäuser, Kliniken, große Pflegeeinrichtungen und Arztpraxen)

Übersicht:

Diese Checkliste fasst die wichtigsten Anforderungen der NIS-2-Richtlinie zusammen, einschließlich Schulungspflichten für die Geschäftsleitung und aller weiteren Pflichten mit Fristen und Priorisierung.

Priorisierung:

1) Registrierung & Meldepflichten (BSI),

2) Risikomanagement & Notfallpläne,

3) Schulungen & Dokumentation.

Schulungspflicht der Geschäftsleitung im Gesundheitswesen

Aspekt	**Details**
Wer ist betroffen?	Geschäftsleitung von ‚wichtigen' und ‚besonders wichtigen Einrichtungen' (z.B. Krankenhäuser, Kliniken, große Pflegeeinrichtungen und Arztpraxen)
Rechtsgrundlage	§ 38 Abs. 3 BSIG-E, NIS-2 EU RL
Intervall	Alle 2-3 Jahre (bei erhöhtem Risiko z.B. mit KI kürzer)
Dauer	Ca. 4 Stunden pro Schulungskomplex gesamt (auch in 2-3 Teilen)
Inhalte	Erkennung & Bewertung von Cyberrisiken; Verständnis von Risikomanagementmaßnahmen; Auswirkungen auf Versorgungsprozesse
Ziel	Strategisches Verständnis, **keine technischen Details**
Nachweis	Dokumentation der Teilnahme für Schulungen, Audits und Haftungsabsicherung
Haftung	Persönliche Haftung der Geschäftsleitung bei Pflichtverletzung
Sanktionen	Bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes

MCSS CONSULTING Systems & Services

NiS-2 AKADEMIE

Gesamtübersicht aller NIS-2-Pflichten

Pflicht	Frist / Intervall	Details
Registrierung beim BSI	Unmittelbar nach Inkrafttreten (Januar 2026)	Alle betroffenen Unternehmen müssen sich registrieren
Meldung Sicherheitsvorfälle	24h Erstmeldung, 72h Upd.,1 Monat Abschluss	Meldung erheblicher Vorfälle an das BSI
Risikomanagement	Kontinuierlich (z.B. alle 6 Monate)	Risikoanalyse, technische, organisatorische und rechtliche Maßnahmen
Business Continuity	Regelmäßig testen	Notfall- und Wiederherstellungspläne
Lieferkettensicherheit	Kontinuierlich (z.B. alle 6 Monate)	Prüfung externer Dienstleister und Zulieferer
Schulung Geschäftsleitung	Alle 2 bis 3 Jahre (mindestens)	Strategisches Verständnis für Cyberrisiken, Dauer ca. 4 Stunden
Mitarbeiterschulungen	Regelmäßig (einmal jährlich)	Awareness-Trainings für alle relevanten Mitarbeiter
Dokumentation & Nachweis	Fortlaufend	Vollständige IT-Dokumentation für Audits und Behörden
Haftung & Sanktionen	Bei Verstoß	Bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes
Empfehlung (KAS)	kontinuierlich	Konsolidiertes Assistenz-system: ISMS, DMS, QMS & KIMS

Literaturnachweise:

NIS-2 Gesetz im Gesundheitswesen (Rechtssicherheit für Geschäftsführung und Führungskräfte SPRINGER Verlag ISBN 978-3-662-70937-5, Autoren: Claudia Wente-Waedlich, Rainer Waedlich)

Handbuch Klinisches Risikomanagement (Digitalisierung und innovatives Cyber- und IT-Risikomanagement SPRINGER Verlag ISBN 978-3-662-67564-9, Autoren Rainer Waedlich, Timo Baumann (Kapitel 42))