

NIS2 COMPLIANCE CHECKLIST FOR MANAGING DIRECTORS

ARE YOU MEETING YOUR PERSONAL OBLIGATIONS UNDER THE NIS2 DIRECTIVE?

1. SCOPE ASSESSMENT

- ☐ ☐ Determined whether your entity qualifies as essential or important under NIS2
- ☐ ☐ Assessed employee count (50+) and turnover (€10M+) thresholds
- ☐ ☐ Identified which of the 18 critical sectors apply

2. GOVERNANCE & BOARD ACCOUNTABILITY

- ☐ ☐ Board has formally acknowledged cybersecurity oversight responsibility
- ☐ ☐ Management body has approved the cybersecurity risk management framework
- ☐ ☐ Directors have completed mandatory cybersecurity training
- ☐ ☐ D&O insurance covers NIS2 personal liability exposure

3. RISK MANAGEMENT (ART. 21)

- ☐ ☐ Comprehensive risk analysis documented and current
- ☐ ☐ Technical and organisational security measures implemented
- ☐ ☐ Business continuity and crisis management plans in place
- ☐ ☐ Supply chain security requirements assessed and contractually addressed

4. INCIDENT REPORTING (ART. 23)

- ☐ ☐ 24-hour early warning process defined and tested
- ☐ ☐ 72-hour full incident report template prepared
- ☐ ☐ National competent authority contact details documented
- ☐ ☐ Internal escalation chain established and rehearsed

5. SUPPLY CHAIN

- ☐ ☐ Vendor cybersecurity risk inventory completed
- ☐ ☐ Existing contracts reviewed for NIS2-compliant security obligations
- ☐ ☐ New procurement templates include mandatory cybersecurity clauses
- ☐ ☐ Critical supplier audit programme established

6. DOCUMENTATION & EVIDENCE

- ☐ ☐ All measures documented in auditable form
- ☐ ☐ Board meeting minutes reflect cybersecurity governance decisions
- ☐ ☐ Training records maintained for all management body members
- ☐ ☐ Annual review cycle for cybersecurity posture established

NIS2-COMPLIANCE-CHECKLISTE FÜR GESCHÄFTSFÜHRER

ERFÜLLEN SIE IHRE PERSÖNLICHEN PFLICHTEN UNTER DER NIS2-RICHTLINIE?

1. ERFASSUNG DES ANWENDUNGSBEREICHS

- ☐ ☐ Festgestellt, ob Ihr Unternehmen als wesentlich oder wichtig unter NIS2 eingestuft wird
- ☐ ☐ Mitarbeiterzahl (50+) und Umsatz (€10M+) Schwellenwerte überprüft
- ☐ ☐ Identifiziert, welche der 18 kritischen Sektoren zutreffen

2. GOVERNANCE & GESCHÄFTSFÜHRERHAFTUNG

- ☐ ☐ Geschäftsführung hat formell die Cybersicherheitsverantwortung anerkannt
- ☐ ☐ Management hat das Cybersicherheits-Risikomanagement-Rahmenwerk genehmigt
- ☐ ☐ Geschäftsführer haben verbindliche Cybersicherheitsschulung absolviert
- ☐ ☐ D&O-Versicherung deckt persönliche NIS2-Haftungsrisiken ab

3. RISIKOMANAGEMENT (ART. 21)

- ☐ ☐ Umfassende Risikoanalyse dokumentiert und aktuell
- ☐ ☐ Technische und organisatorische Sicherheitsmaßnahmen implementiert
- ☐ ☐ Business-Continuity- und Krisenmanagementpläne vorhanden
- ☐ ☐ Supply-Chain-Sicherheitsanforderungen bewertet und vertraglich adressiert

4. INCIDENT REPORTING (ART. 23)

- ☐ ☐ 24-Stunden-Frühwarnungsprozess definiert und getestet
- ☐ ☐ 72-Stunden-Vollständige Incident-Report-Vorlage vorbereitet
- ☐ ☐ Kontaktdaten der Behörde dokumentiert
- ☐ ☐ Interne Eskalationskette etabliert und erprobt

5. LIEFERKETTE

- ☐ ☐ Cybersicherheits-Risikobestand der Lieferanten abgeschlossen
- ☐ ☐ Bestehende Verträge auf NIS2-konforme Sicherheitsverpflichtungen überprüft
- ☐ ☐ Neue Beschaffungsvorlagen enthalten verbindliche Cybersicherheitsklauseln
- ☐ ☐ Prüfprogramm für kritische Lieferanten etabliert

6. DOKUMENTATION & NACHWEISE

- ☐ ☐ Alle Maßnahmen in nachprüfbarer Form dokumentiert
- ☐ ☐ Geschäftsführungsprotokoll reflektiert Cybersicherheits-Governance-Entscheidungen
- ☐ ☐ Schulungsunterlagen für alle Geschäftsführer verwaltet
- ☐ ☐ Jährlicher Review-Zyklus der Cybersecurity-Lage etabliert