

GRATIS-CHECKLISTE · NIS2 · LUXEMBOURG

NIS2-Checkliste für Unternehmen in Luxemburg

In 10 Minuten wissen, wo Sie stehen: 12 Prüfpunkte zu Betroffenheit, Pflichten und Maßnahmen — zum Abhaken mit Ihrem Team.

Rechtsgrundlage	EU-Richtlinie 2022/2555 (NIS2), in Luxemburg umgesetzt durch das Gesetz vom 5. Mai 2026 über Maßnahmen für ein hohes Cybersicherheitsniveau.
Aufsicht	ILR (Institut Luxembourgeois de Régulation) für die meisten Sektoren · CSSF für den Finanzsektor.
Registrierung	Selbstregistrierung betroffener Einrichtungen über das ILR-Portal (guichet.ilr.lu).
Vorfallmeldung	Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen eines Monats — über die SERIMA-Plattform des ILR.
Sanktionen	Bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes für wesentliche Einrichtungen — und persönliche Verantwortung der Leitung.

So nutzen Sie diese Checkliste

Haken Sie jeden Punkt ab, den Ihr Unternehmen heute nachweisbar erfüllt. „Nachweisbar“ heißt: Es gibt ein Dokument, einen Prozess oder ein Protokoll — nicht nur ein gutes Gefühl.

Am Ende zählen Sie die Haken und lesen die Auswertung auf der letzten Seite.

A · Betroffenheit klären

☐

1. Sektor geprüft

Ihre Tätigkeit ist gegen Anhang I/II der NIS2-Richtlinie geprüft (u. a. Energie, Transport, Gesundheit, digitale Infrastruktur, verarbeitendes Gewerbe, Post, Abfall, Lebensmittel, Chemie).

☐

2. Größenschwelle geprüft

Sie wissen, ob Sie über der Schwelle liegen: ab 50 Mitarbeitenden oder mehr als 10 Mio. € Jahresumsatz bzw. Bilanzsumme (Ausnahmen: bestimmte kritische Dienste unabhängig von der Größe).

☐

3. Lieferkette geprüft

Sie haben geprüft, ob Kunden, die selbst unter NIS2 fallen, Sicherheitsanforderungen vertraglich an Sie weiterreichen — auch Nicht-Betroffene trifft NIS2 oft über die Lieferkette.

B · Governance & Pflichten

☐

4. Geschäftsleitung in der Verantwortung

Die Leitung hat die Cybersicherheits-Maßnahmen gebilligt, überwacht deren Umsetzung und ist selbst geschult — NIS2 sieht hier eine persönliche Verantwortung vor.

☐

5. Registrierung erledigt

Ihre Einrichtung ist als „wesentlich“ oder „wichtig“ beim ILR registriert (guichet.ilr.lu) bzw. bei der CSSF, falls Sie dem Finanzsektor angehören.

☐

6. Meldeprozess definiert

Es ist festgelegt, wer erhebliche Sicherheitsvorfälle wann und wie meldet: Frühwarnung binnen 24 h, Meldung binnen 72 h, Abschlussbericht binnen eines Monats (SERIMA-Plattform).

C · Technische & organisatorische Maßnahmen

☐

7. Risikoanalyse & Richtlinien

Eine dokumentierte Risikoanalyse und Sicherheitsrichtlinien existieren und werden regelmäßig auf Wirksamkeit geprüft.

☐

8. Backup & Notfallplan

Ein Backup-Konzept (z. B. nach der 3-2-1-1-0-Regel) mit getesteter Wiederherstellung sowie ein Plan für Betriebskontinuität und Krisenmanagement sind vorhanden.

☐

9. Zugriffe & Verschlüsselung

Multi-Faktor-Authentifizierung, ein sauberes Rechtekonzept und Verschlüsselung für sensible Daten und Kommunikation sind im Einsatz.

☐

10. Schwachstellen & Angriffserkennung

Patch-Management läuft systematisch, und Angriffe werden erkannt — durch Monitoring bzw. eine 24/7-Überwachung (SOC/XDR).

D · Mensch & Lieferkette☐**11. Awareness-Trainings**

Alle Mitarbeitenden werden regelmäßig zu Phishing und sicherem Verhalten geschult — mit Nachweis.

☐**12. Lieferantensicherheit geregelt**

Sicherheitsanforderungen an Ihre IT-Dienstleister und Lieferanten sind vertraglich festgehalten und werden überprüft.

Auswertung: Wo stehen Sie?

0–4 Haken	Hoher Handlungsbedarf. Die Grundpflichten sind noch nicht abgedeckt — bei Betroffenheit drohen Sanktionen und im Ernstfall lange Ausfälle. Starten Sie mit den Punkten 1–3 und 8.
5–9 Haken	Solide Basis, aber lückenhaft. Typische offene Punkte sind Meldeprozess, Registrierung und Angriffserkennung — genau die Punkte, die Prüfer zuerst sehen wollen.
10–12 Haken	Gut aufgestellt. Jetzt zählt Nachweisführung: Dokumentation, Restore-Protokolle und regelmäßige Überprüfung, damit Sie audit-fähig bleiben.

Nächster Schritt: kostenloser IT-Check (90 Minuten)

Sie erhalten eine schriftliche Bewertung Ihrer offenen Punkte aus dieser Checkliste — vor Ort oder remote, unverbindlich und auf Deutsch, Französisch oder Englisch.

Telefon: +352 20 60 12 44 · E-Mail: mail@local-it-partner.lu · Web: local-it-partner.lu

Stand: August 2026. Diese Checkliste ist eine Orientierungshilfe der Local-IT-Partner S.à r.l.-S und ersetzt keine Rechtsberatung. Maßgeblich sind die NIS2-Richtlinie (EU) 2022/2555, das luxemburgische Umsetzungsgesetz und die Vorgaben von ILR bzw. CSSF.