

Gilt NIS2 für Ihr Unternehmen?

Drei Prüfungen nach der rumänischen Dringlichkeitsverordnung (OUG) 155/2024 in ihrer geltenden konsolidierten Fassung. Entscheidend sind die im Anhang genannte Art der Einrichtung und ihre Tätigkeit, nicht nur die allgemeine Branchenbezeichnung.

1 Sind Sie in einem der 18 Sektoren tätig?

ANHANG 1 · SEKTOREN MIT HOHER KRITIKALITÄT

- ☐ Energie (Strom, Fernwärme und -kälte, Erdöl, Gas, Wasserstoff)
- ☐ Verkehr (Luft, Schiene, Wasser; Straßenverkehr: Straßenbehörden und Betreiber intelligenter Verkehrssysteme)
- ☐ Bankwesen (siehe DORA-Hinweis)
- ☐ Finanzmarktinfrastrukturen (siehe DORA-Hinweis)
- ☐ Gesundheit (Gesundheitsversorgung, Arzneimittelherstellung und -vertrieb, Apotheken)
- ☐ Trinkwasser
- ☐ Abwasser
- ☐ Digitale Infrastruktur (DNS, TLD, Cloud, Rechenzentren, elektronische Kommunikation, Vertrauensdienste)
- ☐ Verwaltete IKT-Dienste (einschließlich verwalteter Sicherheitsdienste)
- ☐ Zentrale öffentliche Verwaltung
- ☐ Weltraum

ANHANG 2 · SONSTIGE KRITISCHE SEKTOREN

- ☐ Post- und Kurierdienste
- ☐ Abfallbewirtschaftung (wenn dies die Haupttätigkeit ist)
- ☐ Chemische Stoffe (Herstellung, Produktion, Vertrieb)
- ☐ Lebensmittel (industrielle Herstellung und Verarbeitung, Großhandel)
- ☐ Verarbeitendes Gewerbe (Medizinprodukte, Elektronik und Optik, elektrische Ausrüstung, Maschinen, Fahrzeuge und sonstige Transportmittel)
- ☐ Digitale Anbieter (Online-Marktplätze, Suchmaschinen, soziale Netzwerke)
- ☐ Forschung

Grundlage: Anhänge 1 und 2 der OUG 155/2024

Straßenverkehr: Andere Tätigkeiten oder Umstände können eine Einbeziehung begründen. **DORA:** Für betroffene Finanzunternehmen gilt bei IKT-Risiken das besondere Sektorregime. Die Nennung in einem NIS2-Anhang bedeutet keine vollständige Kumulation gleicher Pflichten. Identifizierungs- und Registrierungspflichten werden gesondert geprüft.

2 Erfüllen Sie die gesetzlichen Größenkriterien?

Die Beschäftigtenzahl allein entscheidet nicht. Unter 50 Beschäftigte bedeutet keinen automatischen Ausschluss. Zu prüfen sind Schwellenwerte, Partner- und verbundene Unternehmen sowie größenunabhängig erfasste Kategorien.

- ☐ **Mittleres Unternehmen:** 50–249 Beschäftigte und Umsatz ≤ 50 Mio. EUR oder Vermögenswerte ≤ 43 Mio. EUR.
- ☐ **Großunternehmen:** oberhalb der Schwellen für mittlere Unternehmen.
- ☐ **Unabhängig von der Größe erfasst:** z. B. zentrale öffentliche Verwaltung, DNS-Dienste, TLD-Register und Vertrauensdienste. Die Liste ist nicht abschließend.

Grundlage: Art. 5–9, OUG 155/2024; Art. 4, Gesetz 346/2004

3 Haben Sie Kunden in diesen Sektoren?

- ☐ Wir liefern Produkte oder Dienstleistungen an Unternehmen in den Sektoren in Schritt 1 (IT, Software, Wartung, Logistik, Beratung oder jede Dienstleistung mit Zugriff auf ihre Systeme oder Daten)

Erfasste Einrichtungen müssen Sicherheitsrisiken ihrer direkten Lieferanten und Dienstleister steuern und können risikogerechte vertragliche Anforderungen stellen (Art. 11 und 13, OUG 155/2024).

SO LESEN SIE DAS ERGEBNIS

Sektor aus Anhang 1 und Großunternehmen;
zentrale öffentliche Verwaltung, DNS-Dienste,
TLD-Register, qualifizierte Vertrauensdienste

Sehr wahrscheinlich eine wesentliche Einrichtung
Art. 5

Sektor aus Anhang 1 und mittleres Unternehmen;
Sektor aus Anhang 2 und mittleres oder großes Unternehmen

Sehr wahrscheinlich eine wichtige Einrichtung
Ausnahmen: Manche Kategorien sind auch als mittlere Unternehmen oder größenunabhängig wesentlich, darunter Anbieter verwalteter Sicherheitsdienste (MSSP). Die endgültige Einstufung wird nach Art. 5–9 der OUG 155/2024 geprüft.

Nur Schritt 3 gilt

Auch wenn Sie selbst die Kriterien direkter Anwendbarkeit nicht erfüllen, können erfasste Kunden vertragliche Sicherheitsanforderungen stellen. Der Lieferantenstatus allein begründet keine NIS2-Anwendbarkeit.

Zeitplan der Pflichten

Die Fristen beginnen je Einrichtung mit unterschiedlichen Ereignissen. Klären Sie zuerst, an welcher Stelle dieses Ablaufs Sie stehen.

FRIST	PFLICHT	FRISTBEGINN UND ANFORDERUNGEN	GRUNDLAGE
30 Tage	Meldung zur Registrierung	Einreichung innerhalb von 30 Tagen nach dem Tag, an dem das Unternehmen den geltenden Bestimmungen unterliegt.	Art. 18(2)
30 Tage	Benennung der sicherheitsverantwortlichen Person	Von der Benachrichtigung über die Registrierungsentscheidung, vorbehaltlich der Bedingungen für die Rolle und die Unternehmenskategorie: Ein IT-Support-Vertrag stellt an sich nicht die satzungsmäßige Bestellung dar.	Art. 14(3)–(4)
60 Tage	Einreichung der Risikoniveaubewertung	Für Unternehmen, die diesem Verfahren unterliegen: ab der Zustellung der Registrierungsentscheidung; das sich daraus ergebende Sicherheitsniveau unterscheidet sich vom rechtlichen Status eines wichtigen oder wesentlichen Unternehmens.	Art. 18(6)
60 Tage	Erste Selbstbewertung des Reifegrads	Erstellung und Einreichung innerhalb der gesetzlichen Frist von 60 Tagen nach Vorlage der Risikobewertung.	Art. 18(7)
30 Tage	Einreichung des Maßnahmenplans	Wesentliche Unternehmen legen den Plan innerhalb von 30 Tagen nach der Selbstbewertung vor; dies ist die Frist für die Vorlage des Plans, nicht für den Abschluss aller Abhilfemaßnahmen.	Art. 12(5)
Jährlich	Regelmäßige Selbstbewertung	Jährlich durchgeführt, vom Management gebilligt und im Rahmen des geltenden Verfahrens eingereicht.	Art. 12(4)
24 h · 72 h	Meldung eines erheblichen Sicherheitsvorfalls	Frühwarnung binnen 24 Stunden und Vorfallmeldung binnen 72 Stunden ab Kenntnis. Abschlussbericht binnen eines Monats nach der Vorfallmeldung; für laufende Vorfälle gelten Sonderregeln. Zwischenbericht auf Verlangen der Behörde; besondere Frist für Vertrauensdiensteanbieter.	Art. 15(7)–(8)

MEHR ALS FORMALITÄTEN

Mehr als nur die Registrierung

Registrierung und Selbstbewertung ersetzen nicht die Umsetzung: Risikomanagement, Zugriffs- und Systemsicherheit, Vorfallmanagement, Betriebsfortführung, Datensicherung, Lieferantensicherheit, Schulung und Wirksamkeitsprüfung der Kontrollen.

Grundlage: Art. 11 und 13, OUG 155/2024

FÜR DIE LEITUNGSBESPRECHUNG

Fünf Fragen an die Leitung

- ☐ Wissen wir schriftlich, ob wir ein wesentliches Unternehmen, ein wichtiges Unternehmen oder nur ein Lieferant sind?
- ☐ Haben wir die Registrierungsmitteilung eingereicht und die Registrierungsentscheidung erhalten?
- ☐ Wer ist für die Sicherheit verantwortlich und wem berichten sie?
- ☐ Können wir die Umsetzung unserer Richtlinien belegen?
- ☐ Weiß jemand, was in den ersten 24 Stunden nach einem Vorfall zu tun ist?

ART. 60 OUG 155/2024

Was das Gesetz vorsieht

- **Verwaltungsverstöße:** Für bestimmte Verstöße, auch gegen Registrierungspflichten, gelten die Sanktionen nach Artikel 60. Die Obergrenze richtet sich nach Verstoß und Unternehmenskategorie.
- **Höchstbetrag:** Bei erfassten Verstößen gilt der höhere Wert aus Festbetrag und gesetzlichem Anteil am weltweiten Gesamtjahresumsatz des Vorjahres: 7 Mio. EUR oder 1,4 % für wichtige Einrichtungen; 10 Mio. EUR oder 2 % für wesentliche Einrichtungen. Die Geldbuße wird nach dem Gesetz festgesetzt.
- **Die Leitung** billigt und überwacht die Maßnahmen und muss Schulungspflichten erfüllen. Sie haftet unter den gesetzlichen Voraussetzungen für Pflichtverletzungen (Art. 14).

WICHTIG

Die Selbstbewertung umfasst Dokumentation und tatsächliche Umsetzung. Für bestimmte digitale Anbieter und verwaltete Dienste ist auch die Durchführungsverordnung (EU) 2024/2690 zu prüfen.

Benötigen Sie eine begründete Anwendbarkeitsprüfung?

Clarified IT erstellt Ihre Anwendbarkeitsbewertung mit begründetem Ergebnis, Pflichten und vorläufigem Zeitplan.

it.clarified.ro/nis2

office@clarified.ro · +40 774 456 127

Quellen: OUG 155/2024, genehmigt mit Änderungen und Ergänzungen durch das Gesetz 124/2025, in seiner geltenden konsolidierten Form; Richtlinie (EU) 2022/2555; Verordnung (EU) 2022/2554 (DORA); Gesetz 346/2004. Diese Checkliste ist informativ: Sie bietet eine Anleitung auf der Grundlage verfügbarer Informationen und ersetzt nicht die Bewertung der spezifischen Situation oder der Entscheidung oder der Befugnisse der Behörde.