Cybersicherheit in Rumänien: Neue Pflichten für Unternehmen

von *Sonia Benga*, *Avocat (Rechtsanwältin RO)*

Die Dringlichkeitsverordnung 155/2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netzen und Informationssystemen im zivilen nationalen Cyberspace („**DVO 155**“) wurde am Ende des letzten Jahres verabschiedet und ist am 31. Dezember in Kraft getreten. Grundlagen sind in unserem letzten Bericht einsehbar:

https://stalfort.ro/wp-content/uploads/2025/03/NIS-2_in_Rumaenien_umgesetzt_erweiterte_Pflichten_zu_Cyber-und_Informationssicherheit.pdf

Sechs Monate später wurde das Gesetz 124/2025 zur Genehmigung der DVO 155 („**Gesetz**“) verabschiedet. Dieses genehmigt die DVO 155 und ändert sie zugleich teilweise. Zentrale Aspekte der DVO wurden konkretisiert, verschärft oder erweitert, unklare Vorschriften verbessert.

Das Gesetz, das am 10 Juli,2025 in Kraft getreten ist, müssen viele in Rumänien tätige Unternehmen berücksichtigen, da die aktuellen Änderungen für sie praxisrelevant sind.

Erweiterung und Klärung des Anwendungsbereichs

Vielleicht eine der wichtigsten Änderungen, die das Gesetz mit sich bringt, besteht in der Erweiterung des Anwendungsbereichs der DVO 155 durch Aufnahme bestimmter Einrichtungen im Bereich der öffentlichen Gesundheit und der Lebensmittel in die als kritisch eingestuften Einrichtungen.

Anhang 1 zur DVO, der die als kritisch eingestuften Einrichtungen aufzählt, wird um diejenigen Einrichtungen, die

- Inhaber einer Arzneimittelvertriebserlaubnis sind;
- Groß- und Einzelhandel mit pharmazeutischen und medizinischen Erzeugnissen betreiben (4646 und 4773 gemäß CAEN Rev 3.),

erweitert;

Darüber hinaus wird nun klargestellt, dass Unternehmen, die mit der Herstellung, der Verarbeitung und/ **oder** dem Vertrieb von Lebensmitteln befasst sind, grundsätzlich von der DVO 155 erfasst werden.

Diese Klarstellungen sind für Unternehmen, die bisher noch unsicher waren, ob sie vom Gesetz betroffen sind oder nicht, bedeutsam. Dies betrifft z.B. mittlere und große Unternehmen, die sich mit dem Vertrieb von Lebensmitteln beschäftigen. Gab es bislang Argumente dafür, dass diese Tätigkeit nicht unter die DVO fiel, sofern sie nicht zusammen mit Produktions- und Verarbeitungstätigkeiten ausgeübt wurde, fällt diese Argumentation künftig weg.

Fristenregelungen und Benennung eines NIS-Verantwortlichen

Gemäß der DVO 155 war es für betroffene Unternehmen bereits zuvor notwendig, eine verantwortliche Person für die Sicherheit von Netz- und Informationssystemen zu benennen. Allerdings legte Sie keinen konkreten Zeitraum fest, innerhalb dessen wesentliche und

wichtige Einrichtungen diese Person ernennen mussten. Das Gesetz setzt nun feste Grenzen; die Benennung der verantwortlichen Person muss innerhalb von 30 Tagen nach Zugang des Beschlusses des DNSC-Direktors über die Eintragung in das Register erfolgen.

Eine weitere Änderung betrifft Fristen für die Umsetzung von Maßnahmen zur Behebung von bei Kontrollen festgestellten Mängeln. Bislang sah die DVO nur vor, dass Einrichtungen 15 Tage nach Erhalt einer Aufforderung einen Maßnahmenplan zu erstellen haben, der eigene Fristen für die Umsetzung setzt. Die neue Fassung enthält nun die Verpflichtung, diese selbst gesetzten Fristen auch einzuhalten, und binnen 5 Tagen nach deren Ablauf Nachweise für die Umsetzung einzureichen.

Klarstellungen zu Sicherheitsvorfällen

Da die DVO 155 hinsichtlich der Definition des Begriffs „*bedeutendes Ereignis*“ unklar formuliert war, regelt das Gesetz dies nun eindeutig. So gilt ein Ereignis oder dessen Auswirkung dann als bedeutend, wenn es

- **entweder** schwerwiegende Betriebsstörungen der Dienstleistungen oder finanzielle Verluste für das betreffende Unternehmen verursacht hat oder verursachen kann;
- **oder** andere natürliche oder juristische Personen mit Verursachung erheblicher materieller oder immaterieller Schäden beeinträchtigt hat oder beeinträchtigen kann.

In Erwartung neuer Vorschriften

Sekundäre Rechtsvorschriften zur Umsetzung des DVO 155 sind noch erforderlich. Dazu gehören Kriterien und Methoden für die Risikobewertung, Regeln für die Meldung von Vorfällen, Anforderungen an die Benachrichtigung und Informationsübermittlung, Maßnahmen für das Risikomanagement und Rechtsvorschriften für die Organisation der Arbeit von Cybersicherheitseinrichtungen.

Seit dem 30. April wurden eine Reihe von Verordnungsentwürfen veröffentlicht, in denen die Kriterien und Methoden im Einzelnen aufgeführt sind. Bislang sind diese Verordnungen jedoch noch im Entwurfsstadium und wurden nicht angenommen, obwohl die öffentliche Konsultation abgeschlossen ist.

Fazit

Obwohl die Sekundärgesetzgebung zur Cybersicherheit noch aussteht, bringt das Gesetz 124 einige notwendige und willkommene Klarstellungen. Durch die Kombination seiner Bestimmungen mit den von der DNSC veröffentlichten Verordnungsentwürfen können sich Unternehmen besser auf ihre Verpflichtungen in diesem Bereich vorbereiten.

Kontakt und weitere Informationen:

Stalfort
Legal. Tax. Audit.
25 Jahre

STALFORT Legal. Tax. Audit.
Bukarest – Bistrița – Sibiu

Büro Bukarest:
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
www.stalfort.ro