NIS 2 RL:

Bereits 2016 wurden mit der Richtlinie zur Sicherheit von Netz- und Informationssystemen (EU 2016/1148; NIS) erstmals Maßnahmen für ein gemeinsames Cybersicherheitsniveau in der Europäischen Union vorgestellt. Nach deren Überarbeitung, Ausweitung und Anpassung an sektorspezifische Rechtsvorschriften im Rahmen der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 (NIS 2 RL) sind die enthaltenen Risikomanagementmaßnahmen und Meldepflichten nunmehr bis spätestens 17. Oktober 2024 in nationales Recht umzusetzen.

Erfasst werden fortan sowohl öffentliche als auch private Einrichtungen, sofern diese Einrichtungen als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten, ihre Dienste in der EU erbringen oder ihre Tätigkeiten dort ausüben und in einem der in Anhang I oder Anhang II zur NIS 2 RL genannten Wirtschaftszweige tätig sind. Die relevanten Schwellenwerte für mittlere Unternehmen werden wie folgt festgelegt: weniger als 250 Mitarbeiter und Jahresumsatz von unter 50 Mio. Euro oder eine Bilanzsumme von höchstens 43 Mio. EUR.

Die Richtlinie differenziert außerdem zwischen wesentlichen Einrichtungen, somit Unternehmen, welche die genannten Schwellenwerte für mittlere Unternehmen überschreiten oder von den Mitgliedstaaten gesondert als wesentlich bzw. kritisch eingestuft werden (bspw. Unternehmen im Bereich Energie, Verkehr, Gesundheit, Finanzdienstleistungen und digitale Infrastruktur) und sonstigen wichtigen Einrichtungen (bspw. Online-Marktplätze oder Suchmaschinen, ebenso aber etwa Unternehmen mit Tätigkeit im Bereich der Produktion, Verarbeitung und des Vertriebs von Lebensmitteln sowie Forschungseinrichtungen). Abhängig von der Kategorisierung eines Unternehmens als wesentliche oder wichtige Einrichtung kommen teils differenzierte Pflichten- und Sanktionsregime zur Anwendung.

Wesentliche Bestimmungen:

Die für wesentliche und wichtige Einrichtungen zentralsten Pflichten sind in Art 21 ff NIS 2 RL festgelegt. Eingeführt wird zunächst eine Verpflichtung der Leitungsorgane wesentlicher und wichtiger Einrichtungen, an Schulungen teilzunehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit zu erwerben. Die Leitungsorgane haben überdies sicherzustellen, dass derartige Schulungen den Mitarbeitern ihres Unternehmens regelmäßig angeboten werden. Bei Verletzung ihrer betreffenden Pflichten können die jeweiligen Leitungsorgane persönlich zur Haftung herangezogen werden.

Weiters werden wesentliche und wichtige Einrichtungen dazu verpflichtet, geeignete und verhältnismäßige Maßnahmen zu ergreifen, um die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern. Dies umfasst insbesondere eine Verpflichtung zur Absicherung der Lieferkette gegenüber unmittelbaren Vertragspartnern. Die NIS 2 RL verlangt daher von betroffenen Unternehmen, mit ihren jeweiligen direkten Lieferanten geeignete Maßnahmen zu treffen, um die Cybersicherheit ihrer IT-Einrichtungen zu gewährleisten. Direkte Lieferanten sind zur Umsetzung und Einhaltung angemessener Sicherheitsmaßnahmen sowie ggf. weiters auch dazu zu verhalten, die Einhaltung derartiger

Maßnahmen auf vorgelagerten Ebenen der Lieferkette (*i.e.* durch eigene Sublieferanten) sicherzustellen.

Überdies müssen betroffene Unternehmen alle erheblichen Sicherheitsvorfälle melden, die sich in Bezug auf ihre IT-Infrastruktur ereignen. Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder zu bewältigen, so können die zuständigen staatlichen Stellen entsprechende Veröffentlichungen vornehmen.

Auswirkungen und Maßnahmen:

Die Auswirkungen der NIS 2 RL auf erfasste Unternehmen sind teils gravierend, da die Bewertung potentieller Risiken für Netzwerk- und Informationssysteme, der Auf- bzw. Ausbau entsprechender technischer und organisatorischer Prozesse sowie die Schulung des Personals erhebliche Kosten verursachen und möglicherweise umfassende Änderungen an bereits bestehenden Prozessen und Systemen erforderlich machen. Behörden können Vor-Ort-Kontrollen, gezielte Sicherheitsprüfungen und Sicherheitsscans durchführen sowie Informationen, Daten und Dokumente bzw. einen Nachweis für die Umsetzung der Cybersicherheitskonzepte von erfassten Unternehmen anfordern.

Mögliche Sanktionen bei Nichteinhaltung der Vorgaben der NIS 2 RL umfassen insbesondere die Erteilung verbindlicher behördlicher Anweisungen, die öffentliche Bekanntmachung von Verstößen sowie die Verhängung von Geldbußen, wobei für wesentliche Einrichtungen mindestens EUR 10 Mio. oder 2% des gesamten weltweiten, im vorangegangenen Geschäftsjahr getätigten Umsatzes und für wichtige Einrichtungen mindestens EUR 7 Mio. oder 1,4% des gesamten weltweiten, im vorangegangenen Geschäftsjahr getätigten Umsatzes vorgesehen sind.

Nicht zuletzt aber die Verpflichtung zur Absicherung der Lieferkette gegenüber unmittelbaren Vertragspartnern stellt betroffene Unternehmen vor erhebliche Herausforderungen, indem sie sie zur Evaluierung bestehender Vertragsbeziehungen und deren Anpassung an die geänderten, strengen Vorschriften zwingt.

Auch wenn die Umsetzung der NIS 2 RL zweifelsfrei eine bedeutende Entwicklung in den Bemühungen der EU zur Verbesserung der Sicherheit von digitalen Infrastrukturen und Diensten darstellt, sollten erfasste Unternehmen daher frühzeitig die sie treffenden Verpflichtungen evaluieren sowie die zu deren Einhaltung notwendigen Schritte planen, um potentiell schwerwiegende Haftungsfolgen zu vermeiden.