CERHA HEMPEL

Lieferkettensicherheit aus dem Blickwinkel der NIS 2 Richtlinie

Mag. Christoph Reiter

Marcus Lusar, LL.M., BSc.

18. Österreichischer IT-Rechtstag
Wien, 26. April 2024

NIS 2

Inkrafttreten und Umsetzung

- NIS 2 RL: am 16.12.2020 als Teil der neuen EU **Cybersicherheitsstrategie** von EU-Kommission vorgelegt
  - in Kraft seit 16. Jänner 2023
  - legt Maßnahmen fest, mit welchen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll
  - ersetzt die bisherigen Regeln der NIS 1 RL

- 21 Monate Umsetzungsfrist für Mitgliedstaaten
  - Anpassung des NISG sohin bis spätestens 17. Oktober 2024
  - aktuell Ministerialentwurf vom 3. April 2024 zum NISG 2024 vorliegend

NIS 2
Anwendungsbereich

- Anwendung primär nach vordefinierten Größenmerkmalen
  - alle **öffentlichen** & **privaten** Einrichtungen, die
    - als **mittlere Unternehmen** gelten oder die **Schwellenwerte** für mittlere Unternehmen **überschreiten** (vgl Art 2 des Anhangs der Empfehlung 2003/361/EG sowie § 25 NISG 2024);
    - ihre Dienste **in der EU erbringen** bzw. ihre Tätigkeiten dort **ausüben**; und
    - in einem wesentlichen oder wichtigen Wirtschaftssektor tätig sind (vgl Anhang I und Anhang II zur NIS 2 RL sowie § 24 NISG 2024 samt dessen Anlagen 1 und 2)
  - teils Anwendung unabhängig von Größenmerkmalen aufgrund besonders kritischen Tätigkeitsfeldes (zB Vertrauensdiensteanbieter, Betreiber öffentlicher Kommunikationsdienste udgl) (Art 2 Abs 2 NIS 2 RL sowie § 26 NISG 2024)
- Schwellenwerte für **mittlere Unternehmen**:
  - mindestens 50 Beschäftigte oder Jahresumsatz von mehr als 10 Mio Euro und Jahresbilanzsumme von mehr als 10 Mio Euro (Art 2 des Anhangs der Empfehlung 2003/361/EG sowie § 25 NISG 2024)
  - Einbeziehung der Kennzahlen verbundener Unternehmen und sog „Partnerunternehmen“ (Art 3 und 6 des Anhangs der Empfehlung 2003/361/EG sowie § 25 NISG 2024)
    - verbundene Unternehmen: Kontrolle (zB durch Mehrheit der Stimmrechte, beherrschenden Einfluss etc)
    - Partnerunternehmen: Beteiligung > 25% (aliquote Zurechnung der Kennzahlen)
      - vor- und nachgeschaltete Unternehmen relevant!

NIS 2

Wesentliche und wichtige Einrichtungen

- Unterscheidung zwischen **wesentlichen** und **wichtigen** Einrichtungen (Art 3 NIS 2 RL)
- **Wesentliche** Einrichtungen sind insb
  - **große Unternehmen** mit Tätigkeiten **in wesentlichen Sektoren** gem Anhang I NIS 2 RL bzw Anlage 1 NISG 2024
  - qualifizierte **Vertrauensdiensteanbieter** und **Domänennamenregister** der Domäne oberster Stufe sowie **DNS-Diensteanbieter** (jeweils unabhängig von ihrer Größe)
  - Anbieter **öffentlicher elektronischer Kommunikationsnetze** oder **öffentlich zugänglicher elektronischer Kommunikationsdienste** (soweit sie als mittlere Unternehmen gelten)
- **Wichtige** Einrichtungen sind Einrichtungen, die in den Anwendungsbereich der NIS 2 RL (des NISG 2024) fallen, aber keine wesentlichen Einrichtungen sind

- Pflichten zur Lieferkettensicherheit gelten **sowohl für wesentliche als auch wichtige** Einrichtungen

NIS 2

Pflicht zum Risikomanagement

- **Art 21 NIS 2 RL** : Die Mitgliedstaaten haben sicherzustellen, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die **Risiken** für die Sicherheit der Netz- und Informationssysteme (wie in Art 6 Z 1 NIS 2 RL definiert), die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, **zu beherrschen** und die **Auswirkungen** von Sicherheitsvorfällen **auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten**.

- **All-hazards approach** = umfassender Ansatz für die Vorbereitung auf Notfälle, der das gesamte Ausmaß potentieller Beeinträchtigungen und Vorfälle bei der Planung von Reaktionskapazitäten und Maßnahmen zur Schadensbegrenzung berücksichtigt.
  - Betrifft die **gesamte IT-Infrastruktur** betroffener Einrichtungen

- umgesetzt in **§ 32 NISG 2024**

NIS 2

Pflicht zum Risikomanagement

- Vorbereitung auf "**alle Gefahren**", denen ein Unternehmen in Hinblick auf die Sicherheit und Funktionsfähigkeit seiner IT-Infrastruktur ausgesetzt ist
  - erfasst **interne und externe Bedrohungen** inklusive **höhere Gewalt** (zB Naturkatastrophen, Pandemien etc)
  - sowohl Gefahren für die IT-Infrastruktur selbst, als auch für deren „**physische Umwelt**“
- Umsetzung eines **Sicherheitsniveaus** der Netz- und Informationssysteme, das nach dem **Stand der Technik** dem bestehenden Risiko **angemessen** ist (Art 21 Abs 1 NIS 2 RL sowie § 32 Abs 2 NISG 2024)
  - **Verhältnismäßigkeitsprinzip** (Art 21 Abs 1 NIS 2 RL sowie § 32 Abs 3 NISG 2024):
    - Ausmaß der Risikoexposition der Einrichtung und Größe der Einrichtung
    - Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere (einschließlich gesellschaftlicher / wirtschaftlicher Auswirkungen)
    - Umsetzungskosten ergänzend zu berücksichtigen

NIS 2
Lieferkettensicherheit - Rechtliche Grundlagen

- Relevante Bestimmungen der NIS 2 RL

  - Art 21 Abs 2

  Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

  d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

  - Art 21 Abs 3

  Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d des vorliegenden Artikels die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.

  Die Mitgliedstaaten stellen ferner sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach jenem Buchstaben die Ergebnisse der gemäß Art 22 Abs 1 durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten berücksichtigen müssen.

NIS 2
Lieferkettensicherheit - Rechtliche Grundlagen

- Relevante Erläuterungen in der NIS 2 RL

- ErwGr 85

Besonders wichtig ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten, z. B. Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder Anbietern von verwalteten Sicherheitsdiensten und Softwareherstellern, betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden.

Die wesentlichen und wichtigen Einrichtungen sollten daher die Gesamtqualität und Widerstandsfähigkeit der Produkte und Dienste, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen.

Die wesentlichen und wichtigen Einrichtungen sollten insbesondere dazu angehalten werden, Risikomanagementmaßnahmen im Bereich der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten und Diensteanbietern einzubeziehen. Diese Einrichtungen könnten auch die Risiken berücksichtigen, die von Lieferanten und Dienstleistern anderer Ebenen ausgehen.

NIS 2

Lieferkettensicherheit - Rechtliche Grundlagen

- Nationale Umsetzungsbestimmungen im Ministerialentwurf des NISG 2024

  - **§ 32 Abs 1**

    Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen […] umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

  - **§ 32 Abs 2**

    Diese Risikomanagementmaßnahmen haben […]

    3. zur Sicherheit der Lieferketten

    a) die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse sowie

    b) die Ergebnisse der gemäß Art 22 Abs 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten, gebührend zu berücksichtigen.

- Sohin weitestgehend **wortgleiche** Umsetzung der Richtlinienbestimmungen

NIS 2

Lieferkettensicherheit - Rechtliche Grundlagen

- Relevante Erläuterungen im Ministerialentwurf des NISG 2024

  - zu § 32 Abs 2 Z 3 NISG 2024

  ➢ im Wesentlichen wortgleich zu ErwGr 85 NIS 2 RL, mit folgender inhaltlicher Ergänzung:

Beispielsweise hat eine wesentliche oder wichtige Einrichtung Risiken und Abhängigkeiten, die sich aus den Beziehungen zu einem unmittelbaren Diensteanbieter ergeben, zu identifizieren, zu bewerten und entsprechend zu behandeln, aber auch bei der Auswahl von neuen Lieferanten oder Anbietern oder bei vertraglichen Vereinbarungen generell die zuvor genannten Aspekte zu berücksichtigen.

NIS 2

Lieferkettensicherheit – Wesentliche Eckpunkte

- gültig für **wesentliche** und **wichtige** Einrichtungen
- Absicherung der Cybersicherheit im Verhältnis zu **direkten Lieferanten** und **Diensteanbietern**
  - **Risikobewertung** unter Berücksichtigung von…
    - **Gesamtqualität** und **Widerstandsfähigkeit** der Produkte und Dienste der Lieferanten
    - **Risikomanagementmaßnahmen** und vorhandenen **Cybersicherheitsverfahren der** Lieferanten (einschließlich sicherer Entwicklungsprozesse)
  - Angemessene Absicherung der bestehenden Risiken in **vertraglichen Vereinbarungen** mit den Lieferanten
    - **Problematik:** Nur die jeweilige wesentliche oder wichtige Einrichtung wird verpflichtet, nicht aber die Lieferanten selbst

NIS 2

Vertragliche Vereinbarungen zur Lieferkettensicherheit

- Einbindung des Lieferanten in das unternehmenseigene Risikomanagementsystem
  - zB Secure Coding Standards, Zugangssteuerung zu kritischen Systemen (remote und on-site), Passwortsicherheit, Identitätsfeststellung und -verfikation von Mitarbeitern, Richtlinien für die Erfassung, Eskalation und Lösung von Incidents, relevante Kommunikationskanäle und -abläufe usw
    - erforderlicher Grad der Einbindung im Lichte des Verhältnismäßigkeitsgrundsatzes **einzelfallbezogen** zu bestimmen
    - Ausmaß der Risikoexposition, Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere (einschließlich gesellschaftlicher / wirtschaftlicher Auswirkungen) etc
- Betrifft sowohl **Dauerschuldverhältnisse** als auch **Zielschuldverhältnisse**
  - Umgang mit Sicherheitslücken bei **bereits erfüllten** Zielschuldverhältnissen?
    - Gewährleistung, SLAs
    - ggf. Notwendigkeit zur Neuinvestition bzw zum Austausch betroffener Software / Dienste
- Ergänzend:
  - Führung eines vollständigen und jederzeit aktuellen Lieferanten- und Assetverzeichnisses
    - welche Dienste (Assets) werden von welchem Lieferanten bereitgestellt?
    - Kritikalität der jeweiligen Assets; Bewertungsdokumentation
    - Einrichtung von Prozessen zur Anpassung der Verzeichnisse

NIS 2

Lieferkettensicherheit – Umgang mit neuen Vertragsverhältnissen

- angemessene vertragliche Absicherung der bestehenden Risiken
  - gemeinsame Evaluierung der relevanten Parameter bereits im Stadium der Vertragsverhandlungen
  - Implementierung geeigneter Maßnahmen, zB Definition spezifischer Richtlinien, Maßnahmen und Pflichten als **Anlagen** zum Vertrag
  - nach Möglichkeit zudem:
    - Vereinbarung vertraglicher **Auskunfts-, Informations- und Mitwirkungspflichten** des Lieferanten für die Zeit nach Vertragsabschluss
    - spezifische **Auditrechte** zugunsten der wesentlichen / wichtigen Einrichtung (inklusive konkreter Prüfungsintervalle und definierter Prüfnachweise und -ziele)
  - Ausdehnung auch auf **nachgelagerte** Ebenen der Lieferkette?
    - ErwGr 85 der NIS 2 RL als Grundlage
    - allerdings nicht rechtsverbindlich
- **Verhältnismäßigkeitsprinzip** zu beachten
  - Maßnahmen abhängig von Kritikalität der Leistung, Risikoexposition, Größe und Wichtigkeit des Lieferanten

NIS 2

Lieferkettensicherheit – Umgang mit neuen Vertragsverhältnissen

Vorschlag einer Musterklausel zugunsten des Leistungsempfängers

Unbeschadet der Bestimmungen dieser Vereinbarung hat der Auftragnehmer im Rahmen der Erbringung der von ihm geschuldeten Dienste und Leistungen die Informationssicherheitsrichtlinien des Auftraggebers (wie diesem Vertrag als Anlage ./X beigefügt) einzuhalten und sicherzustellen, dass die vom Auftragnehmer für die Erbringung seiner Dienste und Leistungen eingesetzten Arbeitnehmer und genehmigten Subunternehmer diese Richtlinien ebenfalls einhalten.

Der Auftraggeber ist jederzeit berechtigt, die betreffenden Anweisungen, Richtlinien und Pflichten einseitig anzupassen und insbesondere zu erweitern, sofern und soweit dies notwendig ist, um die dem Auftraggeber obliegenden, gesetzlichen Vorschriften auf Basis der geltenden und/oder künftigen NIS-Gesetzgebung der Europäischen Union und/oder deren Mitgliedsstaaten, insbesondere der Richtlinie (EU) 2022/2555 (NIS 2 Richtlinie) und deren Umsetzung in nationales Recht, vollumfänglich zu entsprechen.

Der Auftraggeber kann auf dieser Grundlage insbesondere die Einhaltung zusätzlicher Regeln und Vorkehrungen vom Auftragnehmer verlangen, soweit dies dazu dient, die im Rahmen der NIS 2 Richtlinie oder sonstigen NIS 2 Gesetzgebung erforderliche Absicherung der Lieferkette des Auftraggebers sicherzustellen.

NIS 2

Lieferkettensicherheit – Umgang mit bestehenden Vertragsverhältnissen

- NIS 2 beschränkt sich nicht allein auf nach ihrem Inkrafttreten abgeschlossene Verträge
  - auch bestehende Vertragsverhältnisse sind in die Risikobeurteilung einzubeziehen
  - Notwendigkeit der Anpassung bestehender Vertragsverhältnisse

➢ **Problematik:** Häufig keine vertraglichen Regeln hierfür vorgesehen

➢ Zentrale Fragen:

- **Informationspflichten** des Lieferanten?
- **einseitige** Vertragsanpassung möglich?
- **Verhandlungspflicht** des Lieferanten über Vertragsanpassungen?
- Sonstige Optionen zur (faktischen) **Risikosteuerung?**
- **Beendigung** bestehender Verträge möglich? **Beendigungspflicht**?

NIS 2

Informationspflichten des Lieferanten?

- Evaluierung bestehender Risikoexposition erfordert Mitwirkung des Vertragspartners
  - Erteilung von Informationen bzw. Gewährung von Einsicht in bestehende Abläufe
    - vertragliche **Nebenleistungspflicht**?
      - Informationspflicht als (idR **inäquivalente**) Nebenpflicht aus dem Vertragsverhältnis
      - als Handlungspflicht **nicht** gerichtlich durchsetzbar; allerdings **Schadenersatz** bei schuldhafter Verletzung
      - auch **ao Kündigungsrecht / Rücktritt** bei Verletzung?
        - grds nur, wenn Vertrauenserschütterung hinreichend **schwerwiegend**
        - bei Verweigerung notwendiger Informationen zur Risikobeurteilung uE argumentierbar

NIS 2

Informationspflichten - Mangelnde Kooperation des Lieferanten

- Verharren der wesentlichen / wichtigen Einrichtung in einer nicht hinreichend beurteilbaren Risikolage uE im Lichte der gesetzlichen Regeln **nicht** vertretbar
  - Pflicht zur Evaluierung verfügbarer Alternativanbieter oder Ergreifung sonstiger Risikominderungsmaßnahmen mit hinreichender Erfolgsaussicht (falls denkbar)
  - Verhältnismäßigkeitsgrundsatz zu beachten
    - uE **keine** automatische Pflicht zur Vertragsbeendigung
    - insbesondere Übergangsphasen denkbar (aber: Kündigungsvorbehalt zu empfehlen, ansonsten konkludenter Verzicht)
    - stets **einzelfallbezogene** Abwägung und Beurteilung
    - sorgsame **Dokumentation** aller Entscheidungsgrundlagen und Maßnahmen empfehlenswert

NIS 2

Einseitige Anpassung bestehender Verträge?

- Vertragsanpassung?
  - Vertragsanpassung wegen List, Drohung oder *laesio enormis* in aller Regel nicht denkbar
  - Irrtumsanpassung gemäß § 871 f ABGB?
    - falsche oder mangelhafte Vorstellung von der Wirklichkeit
    - wesentlicher (Geschäfts-)Irrtum?
      - Irrtum über künftige Entwicklung der Rechtslage ist idR bloßer **Motivirrtum**
    - zudem fraglich, ob Vertrauensschutzbedürfnis des Vertragspartners fehlt
      - keine Veranlassung, kein Auffallenmüssen, keine rechtzeitige Aufklärung iSd *res integra* Lehre
      - eventuell gemeinsamer Irrtum? Nach wie vor **strittig**!

  - uE eher **keine** einseitige Vertragsanpassung wegen Irrtums möglich
    - überdies: praktisches Problem der Determinierung des Inhalts der Vertragsanpassung anhand des hypothetischen Parteiwillens

NIS 2

Einseitige Anpassung bestehender Verträge?

- Anpassung wegen Änderung der Geschäftsgrundlage?
  - Persistenz der Rechtslage als „*Geschäftsgrundlage*“ denkbar?
  - nur dann, wenn der Bestand eines Gesetzes zur Geschäftsgrundlage gemacht wurde oder Vertrag auf dem Bestand eines bestimmten Gesetzes aufbaut (OGH 8 Ob 60/70)
  - Änderung der Gesetzeslage im Übrigen grds nicht beachtlich (OGH 4 Ob 151/21s)

- uE daher regelmäßig **keine** einseitige Vertragsanpassung infolge Wegfalls bzw. Änderung der Geschäftsgrundlage möglich
- Institut des Wegfalls der Geschäftsgrundlage zudem subsidiär
  - Verhältnis zur außerordentlichen Kündigung strittig; hA gibt der ao Kündigung „relativen“ Vorrang, also nur bei Vertragsbeendigung
  - Anpassung wäre demnach möglich, wenn die Voraussetzungen vorliegen und die Vertragsänderung dem Vertragspartner zumutbar ist

NIS 2
Verhandlungspflicht des Lieferanten?

- Ergänzende Vetragsauslegung
  - hypothetischer Parteiwille kann eine Pflicht zur Verhandlung und Abstimmung erforderlicher Maßnahmen und Richtlinien nach Treu und Glauben ergeben
    - idR **inäquivalente Nebenleistungspflicht** (vertragliche Schutzpflicht)
  - als Handlungspflicht **nicht** gerichtlich durchsetzbar; aber: **Schadenersatz** bei Verletzung
    - allerdings nur, wenn der Aufwand des Lieferanten hieraus im Verhältnis zum Interesse der wesentlichen bzw. wichtigen Einrichtung bloß eine **untergeordnete** Rolle spielt
    - uE wohl regelmäßig argumentierbar, da die wesentliche bzw wichtige Einrichtung ohne Vereinbarung adäquater Risikomanagementmaßnahmen erheblichen Haftungsrisiken ausgesetzt ist
      - Pflicht des Lieferanten jedenfalls dann, wenn **angemessene Entschädigung** angeboten wird?
    - vgl ergänzend OGH 1 Ob 716/96: „*Ein Vertragspartner ist zu einer Vertragsänderung verpflichtet, die für ihn keinerlei Nachteile, aber für die andere Partei wirtschaftliche Vorteile bringt.*“
    - bei eindeutiger Verletzung bestehender Schutzpflichten (zB Verweigerung von Verhandlungen) ist uE wiederum **ao Kündigung** des bzw **Rücktritt** vom Vertragsverhältnis(ses) argumentierbar (und eine Kündigung ggf. sogar erforderlich; aber: **Verhältnismäßigkeitsgrundsatz**!)
    - praktische Problematik: Verhandlungs- und Zustimmungspflichten des Lieferanten sind kaum nuanciert und nur sehr schwer determinierbar
      - Führung redlicher Verhandlungen hinreichend, unabhängig von deren Ergebnis? Risiko des Abbruchs von Verhandlungen liegt maßgeblich beim NIS-verpflichteten Vertragsteil

NIS 2

Sonstige Optionen zur (faktischen) Risikosteuerung

- Carve-Out kritischer Dienste / Lieferanten
  - Ausgliederung in separate, in sich abgeschlossene Netzwerke / Systemumgebungen ohne Verbindung zu kritischer IT-Infrastruktur
- Sperrung von Remote-Zugriffsmöglichkeiten und Fremdhardware
  - Zugriffssteuerung über eigene Hardware (zB Laptops) der wesentlichen / wichtigen Einrichtung
- Exit nach Aufbau einer parallelen Infrastruktur
  - zB temporär gleichzeitiger Betrieb der betroffenen Dienste über zwei Anbieter

NIS 2

Beendigung bestehender Verträge - Detailfragen

- ao Kündigung / Rücktritt aufgrund Verletzung vertraglicher (inäquivalenter) Nebenleistungspflichten nur bei besonders schwerwiegendem Vertrauensverlust denkbar (OGH 1 Ob 113/08m)
  - uE argumentierbar, sofern die Mitwirkung des Lieferanten zur Implementierung adäquater Risikomanagementmaßnahmen notwendig ist, der Lieferant diese Mitwirkung aber verweigert
  - uE **keine** automatische Pflicht zur Vertragsbeendigung, **einzelfallbezogene** Betrachtung und Abwägung
  - insbesondere **Übergangsphasen** denkbar
    - allerdings: ao Kündigung / Rücktritt muss grds unverzüglich erklärt werden, sonst konkludenter Verzicht
    - Kündigungsvorbehalt zu empfehlen → *protestatio facto contraria non valet?*
    - auch freiwillige Einräumung einer Kündigungsfrist möglich
      - praktisch aber häufig weniger zielführend → Leistungsverweigerung des Lieferanten, Bemessung der Kündigungsfrist oftmals schwierig, Risiko der Unwirksamkeit der Kündigung mangels ausreichenden, wichtigen Grundes
    - klarstellende, gesetzliche Regelung wäre wünschenswert (*de lege ferenda*)
  - vgl **DORA** (Digital Operational Resilience Act) im Finanzmarktsektor und die dort in Art 30 enthaltenen Vorgaben für Vertragsbestimmungen mit IKT-Dienstleistern
    - Pflicht zur Vereinbarung von Kündigungsrechten und Ausstiegsstrategien mit angemessenen Übergangsfristen

NIS 2

Schadenersatzpflicht des Lieferanten

- praktische Problematik: Haftungsausschlüsse und -begrenzungen
  - Durchsetzbarkeit dieser vertraglichen Haftungsbestimmungen uE allerdings *in concreto* fraglich
    - unvorhersehbare (atypische) Schäden

      (zB OGH 8 Ob 46/17y; RIS-Justiz RS0038178 [T17, T20])?
    - vorsätzliche Schadenszufügung?

NIS 2

Verletzung der NIS 2 Vorschriften - Sanktionen

- Verletzung lieferkettenbezogener Sicherungspflichten als Verwaltungsübertretung (§ 45 iVm § 32 NISG 2024)
  - wesentliche Einrichtungen: Geldstrafe in Höhe von bis zu 10 000 000 EUR oder bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist
  - wichtige Einrichtungen: Geldstrafe in Höhe von bis zu 7 000 000 EUR oder bis zu 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist
- Strafbarkeit setzt **Verschulden** zumindest im Grade der leichten Fahrlässigkeit voraus (§ 5 VStG)
  - Nichteinhaltung der objektiv gebotenen Sorgfalt trotz subjektiver Möglichkeit, diese zu erkennen und einzuhalten
  - sorgfältiges Bemühen im Rahmen des Verhältnismäßigkeitsgrundsatzes kann daher exkulpieren
  - jedoch: **sonstige Aufsichtsmaßnahmen** weiterhin möglich, da verschuldensunabhängig
    - zB behördliche Kontrollen und Sicherheitsscans, Anforderung von Informationen, Zugang zu Daten und Dokumenten

NIS 2
Handlungsempfehlungen

- Errichtung vollständiger **Lieferanten- und Assetverzeichnisse** samt Kritikalitätsbewertung und -dokumentation sowie Prozessen zur laufenden Aktualisierung
- Errichtung einer unternehmensinternen, kohärenten **Risikomanagementstrategie** samt Bezug habender **Dokumentation**
- **Evaluierung** besonders kritischer Lieferantenbeziehungen
- bei neuen Vertragsabschlüssen:
  - **Berücksichtigung** der durch die NIS 2 RL und das NISG 2024 vorgegebenen Regeln zur Lieferkettenabsicherung in den Vertragsverhandlungen
  - **Einbindung** der Lieferanten in das eigene Risikomanagementsystem durch Überbindung vorhandener Konzepte und Dokumentation auf die Vertragspartner
  - zumindest: Schaffung der **Möglichkeit zur nachträglichen Einführung** von Risikomanagementmaßnahmen mit Wirkung für die Lieferanten (Musterklausel)
- bei bestehenden Verträgen:
  - **rechtzeitige Aufnahme von Verhandlungen** mit kritischen Lieferanten zur Einbindung in das unternehmenseigene Risikomanagementsystem
  - Implementierung **risikomindernder Maßnahmen** in eigener Sphäre
  - ggf. Evaluierung eines **Umstiegs** auf neue Anbieter
  - sorgsame **Dokumentation** der Risikoeinstufung sowie getroffener Maßnahmen zur Vermeidung von Haftungen

CERHA HEMPEL

Mag. Christoph Reiter

Partner

christoph.reiter@cerhahempel.com
+43 1 514 35 531

Zugelassen als

- Rechtsanwalt, Österreich (2016)

Ausbildung

- Johannes Kepler Universität Linz (Mag. iur. 2011)

Tätigkeitsschwerpunkte

- IT/TMT
- Insolvency & Restructuring
- Corporate, M&A

Sprachen

- Deutsch
- Englisch

CERHA HEMPEL

Marcus Lusar, LL.M., BSc.

Rechtsanwaltsanwärter

marcus.lusar@cerhahempel.com
+43 1 514 35 531

Zugelassen als

- Rechtsanwaltsanwärter seit 2020

Ausbildung

- Wirtschaftsuniversität Wien (LL.M. 2019)
- Wirtschaftsuniversität Wien (BSc. 2019)

Tätigkeitsschwerpunkte

- IT/TMT
- Insolvency & Restructuring
- Corporate, M&A

Sprachen

- Deutsch
- Englisch

CERHA HEMPEL

Vielen Dank

für Ihre Aufmerksamkeit