Version 2.0
02/2025

CENTRE FOR CYBERSECURITY BELGIUM

Häufig gestellte Fragen (Frequently Asked Questions - FAQ) NIS2 in Belgien

Ziel dieses Dokument ist es Antworten auf häufig gestellte Fragen zum rechtlichen Rahmen von NIS2 in Belgien geben. Es ergänzt die Informationen, die bereits auf der ZCB-Website und auf Safeonweb@Work verfügbar sind.

Die Version 2.0 bringt die folgenden Änderungen mit sich (neue Nummerierung aufgrund von Einfügungen):

Hinzugefügte Fragen	Erweiterte Fragen
1.2, 1.6, 1.8, 1.13, 1.15, 1.15.1, 1.15.2, 1.15.3, 1.15.4, 1.15.5, 1.16, 1.16.1, 1.16.2, 1.16.3, 1.16.4, 1.16.5, 1.16.6, 1.16.7, 1.20, 1.21.2, 1.21.3, 1.22, 1.22.1, 1.22.2, 1.22.3, 1.22.4, 1.22.5, 1.22.6, 1.22.7, 1.22.8, 1.22.9, 1.22.10, 1.22.11, 1.22.12 2.2, 2.3, 2.6, 2.7, 2.8, 2.9 3.3.2, 3.4, 3.7, 3.8, 3.9, 3.10, 3.11, 3.13.2, 3.13.3, 3.13.4, 3.13.5, 3.13.6, 3.13.7, 3.13.8, 3.13.9, 3.13.10 4.3, 4.5, 4.7, 4.10, 4.12, 4.16 5.2, 5.3	1.3, 1.5, 1.12, 1.14, 1.17, 1.19, 1.21.1 2.4, 2.5 3.2, 3.3, 3.3.1, 3.6, 3.14 4.2.1, 4.4, 4.6, 4.9, 4.11, 4.14 5.1

Eine Entsprechungstabelle ist am Ende des Dokuments zu finden.

Inhaltsverzeichnis

Abkürzungen & Referenzen

Die folgenden Abkürzungen und Referenzen werden in diesem Dokument verwendet:

- BELAC: *Belgische Accreditatie-instelling* (Belgische Akkreditierungsstelle)
- CAB: *Conformity Assessment Body (*Konformitätsbewertungsstelle)
- CSIRT: *Computer Security Incident Response Team* (in Belgien ist das nationale CSIRT das ZCB)
- CyFun®: *Cyberfundamentals Framework*, (verfügbar auf SafeonWeb@Work)
- DORA: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (verfügbar auf Eur-Lex)
- DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (verfügbar auf Eur-Lex)
- Empfehlung (2003/361/EG): Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (verfügbar auf Eur-Lex)
- NCCN: Nationales Krisenzentrum
- NIS1-Gesetz: Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- NIS1-Richtlinie: Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (verfügbar auf Eur-Lex).
- NIS2 Königlicher Erlass: Königlicher Erlass vom 9. Juni 2024 zur Ausführung des Gesetzes vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- NIS2-Gesetz: Gesetz vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- NIS2-Richtlinie: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (verfügbar auf Eur-Lex).
- ZCB: Zentrum für Cybersicherheit Belgien (nationale Cybersicherheitsbehörde & nationales CSIRT)

1. Allgemein - Anwendungsbereich

1.1. Was sind die Ziele des NIS2-Gesetzes?

Die Richtlinie 2022/2555 (die sogenannte "NIS2-Richtlinie") und das belgische NIS2-Gesetz, das sie umsetzt, zielen darauf ab, die Cyber-Resilienz zu stärken, indem sie sich auf die folgenden Schlüsselziele konzentrieren:

1) Cybersicherheitsschutz für wesentliche Dienste, die in der Europäischen Union erbracht werden. Im Vergleich zur NIS1-Richtlinie erweitert die NIS2-Richtlinie die Zahl der wesentlichen Dienste, die in verschiedenen hochkritischen Sektoren (Beilage I) oder anderen kritischen Sektoren (Beilage II) erfasst werden. Der Anwendungsbereich wird nun hauptsächlich durch die Verwendung europäischer Definitionen (wie "Art der Einrichtung") und eines Größenkriteriums ("size cap") bestimmt;
2) Stärkung der Maßnahmen zum Management von Cybersicherheitsrisiken, die die Einrichtungen ergreifen müssen, sowie die Meldung erheblicher Sicherheitsvorfälle (mit zwei Kategorien von wesentlichen oder wichtigen Einrichtungen);
3) Förderung des Informationsaustauschs über Sicherheitsvorfälle und -risiken im Bereich der Cybersicherheit zwischen den betroffenen Einrichtungen und den nationalen CSIRTs;
4) Verstärkte Aufsicht und Sanktionen;
5) Europäische und nationale Zusammenarbeit sicherstellen.

1.2. Was hat sich zwischen dem NIS1-Gesetz und dem NIS2-Gesetz verändert?

Der Anwendungsbereich von NIS2 wurde im Vergleich zur NIS1 erheblich erweitert, wobei ein wichtiger Paradigmenwechsel stattgefunden hat. Das NIS2-Gesetz stützt sich nicht mehr auf ein formales Identifizierungsverfahren, sondern hauptsächlich auf zwei Kriterien: die von einer Einrichtung in bestimmten Sektoren oder Teilsektoren erbrachte Dienstleistung (Art der Einrichtung) und ihre Größe (entspricht einem großen oder mittleren Unternehmen). Von einigen Ausnahmen abgesehen, fallen nur Organisationen mit Sitz in Belgien unter das NIS2-Gesetz, entweder als "wesentliche" oder "wichtige" Einrichtungen. Weitere Informationen über den Anwendungsbereich von NIS2 finden Sie im Abschnitt 1.3.

Die meisten NIS1-Einrichtungen (Betreiber wesentlicher Einrichtungen oder Anbieter digitaler Dienste) unterliegen dem NIS2-Gesetz und müssen sich als NIS2-Einrichtung auf der Plattform der ZCB (https://atwork.safeonweb.be) registrieren. Einrichtungen, die sich bereits für das *Early Warning System* (EWS) des ZCB registriert haben, müssen sich ebenfalls erneut registrieren. Weitere Informationen zur Registrierung finden Sie im Abschnitt 3.13.1.

Die Maßnahmen zur Cybersicherheit, die NIS2-Einrichtungen implementieren müssen, ähneln denen von NIS1, aber das NIS2-Gesetz enthält nun eine minimale Liste spezifischer Maßnahmen. Die Anforderungen reichen vom Lieferkettenmanagement über das Schwachstellenmanagement bis hin zur Mehrfaktor-Authentifizierung (MFA) und sind expliziter und detaillierter als zuvor. Weitere Informationen über Cybersicherheitsmaßnahmen finden Sie im Abschnitt 3.2.

Das Verfahren zur Meldung von Sicherheitsvorfällen ist jetzt detaillierter und umfassender. Für wesentliche und wichtige Einrichtungen ist die Meldung eines erheblichen Sicherheitsvorfalls innerhalb bestimmter Fristen (unverzüglich und spätestens innerhalb von 24 Stunden für die Frühwarnung, 72 Stunden für die Meldung und 1 Monat für den Abschlussbericht) vorgeschrieben. Auch andere Sicherheitsvorfälle, Cyber-Bedrohungen und Beinahe-Vorfälle können freiwillig gemeldet werden. Die Plattform für die Meldung von Sicherheitsvorfällen unter NIS1 wurde durch ein neues Online-Formular ersetzt, das für jedermann zugänglich ist, ohne dass eine Anmeldung erforderlich ist (https://notif.safeonweb.be). Weitere Informationen über die Meldung von Sicherheitsvorfällen finden Sie im Abschnitt 3.3.

Für Einrichtungen, die in den Banken- und Finanzsektor der Anhänge des NIS2-Gesetzes fallen, ist die DORA-Verordnung (Digital Operational Resilience Act) eine *lex specialis*, d.h. sie ersetzt bestimmte NIS2-Verpflichtungen, z.B. in Bezug auf Cybersicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen. Weitere Informationen über DORA finden Sie im Abschnitt 1.17.

NIS2 betont die Haftung der Leitungsorgane der NIS2-Einrichtungen in Bezug auf Cybersicherheit. Weitere Informationen zu dieser Haftung finden Sie im Abschnitt 3.9.

Die Ausweitung des Anwendungsbereichs erforderte einen anderen Ansatz für die Aufsicht:

- Wesentliche Einrichtungen werden einer verpflichtenden regelmäßigen Konformitätsbewertung durch eine Konformitätsbewertungsstelle (CAB) oder alternativ einer Inspektion durch das ZCB unterzogen;
- Wichtige Einrichtungen können sich freiwillig der gleichen regelmäßigen Konformitätsbewertung unterziehen und sind in jedem Fall einer Ex-post-Kontrolle verpflichtet;

Weitere Informationen zur Aufsicht finden Sie im Kapitel 4.

Dieses neue Aufsichtskonzept enthält auch ein umfassenderes System von Verwaltungssanktionen mit verschiedenen Geldbußen und Maßnahmen, die der Aufsichtsbehörde zur Verfügung stehen. Die strafrechtlichen Sanktionen von NIS1 wurden gestrichen. Weitere Informationen über Sanktionen sind im Abschnitt 4.18 zu finden.

Was die an der Aufsicht beteiligten Behörden betrifft, so sind die sektoralen Behörden unter NIS1 alle zu sektoralen Behörden unter NIS2 geworden, auch wenn ihre Rolle angepasst wurde. Das ZCB leitet nun die Aufsicht für alle Sektoren. Weitere Informationen über die zuständigen Behörden finden Sie im Abschnitt 4.1.

1.3. Was ist der Anwendungsbereich des NIS2-Gesetzes?

Art. 3-7 NIS2-Gesetz

Das NIS2-Gesetz richtet sich an öffentliche oder private Einrichtungen, die grundsätzlich in Belgien niedergelassen sind (es gibt einige Ausnahmen zu dieser Regel) und die eine in Beilage I oder II des Gesetzes aufgeführte Dienstleistung innerhalb der Europäischen Union erbringen.

Um als dem Gesetz unterliegende Einrichtung zu gelten, genügt es, unabhängig von der Rechtsform mindestens eine der in den Beilagen I oder II des Gesetzes aufgeführten Tätigkeiten innerhalb der Europäischen Union auszuüben und zumindest die Schwellenwerte eines mittleren Unternehmen im Sinne der Empfehlung 2003/361/EG der Europäischen Kommission vom 6. Mai

2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen erfüllen (der sogenannte „Size-cap“).

Wesentliche Einrichtungen sind Organisationen, die eine in Beilage I aufgeführte Dienstleistung erbringen und die Schwellenwerte eines großen Unternehmens im Sinne der Empfehlung 2003/361/EG erfüllen.

Wichtige Einrichtungen sind Organisationen, die eine Dienstleistung erbringen:

- die entweder in Beilage I aufgeführt ist und die Schwellenwerte eines mittleren Unternehmens im Sinne der Empfehlung 2003/361/EG erfüllen; oder
- die in Beilage II aufgeführt ist und die Schwellenwerte eines mittleren oder großen Unternehmens im Sinne der Empfehlung 2003/361/EG erfüllen;

Nach Artikel 1 des Anhangs der Empfehlung 2003/361/EG gilt als "Unternehmen" jede Einrichtung, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform. Dieser Begriff kann auch die öffentliche Verwaltung oder öffentliche Einrichtungen einschließen, wenn sie (wie andere private Einrichtungen) in den Anhängen des NIS2-Gesetzes genannte kritische Dienstleistungen erbringen.

Die Größenbegrenzungsregel gilt nicht für solche Einrichtungen wie öffentliche Verwaltungen, identifizierte kritische Einrichtungen, Anbieter von Vertrauensdiensten, TLD-Namenregister und DNS-Diensteanbieter.

Es ist wichtig zu betonen, dass sich **der Anwendungsbereich des NIS2-Gesetzes auf die gesamte betroffene Einrichtung bezieht** und nicht nur auf ihre in den Beilagen des Gesetzes aufgeführten Tätigkeiten.

Sofern bei der Definition der Art der Einrichtung (Dienstleistung) im Anhang nicht die Nebentätigkeit oder der nicht wesentliche Charakter der betreffenden Tätigkeit berücksichtigt wird, fällt eine Einrichtung **auch dann** in den Anwendungsbereich des Gesetzes**, wenn die betreffende Dienstleistung, die sie erbringt, nur eine Nebentätigkeit oder ein nicht wesentlicher Teil ihrer gesamten Tätigkeit ist.**

Weitere Informationen finden Sie in den folgenden Abschnitten.

1.4. Was ist eine "Einrichtung" unter NIS2?

Art. 8, 37° NIS2-Gesetz; Art. 6 (35) NIS2-Richtlinie

Das NIS2-Gesetz gilt für Organisationen, wenn sie als "Einrichtung" im Sinne des Gesetzes qualifiziert werden können.

Eine "Einrichtung" ist im NIS2-Gesetz wie folgt definiert: "*eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann*".

Das NIS2-Gesetz gilt für alle Einrichtungen einzeln, auch wenn sie sich in einer Unternehmensgruppe befinden und/oder von derselben Holdinggesellschaft gehalten werden. Der Anwendungsbereich und die Verpflichtungen des NIS2-Gesetzes müssen daher von jeder Einrichtung individuell auf der Grundlage der von ihr erbrachten Dienstleistungen analysiert werden.

Für den Sektor der öffentlichen Verwaltung sieht die NIS2-Richtlinie einen speziellen Begriff der "Einrichtung der öffentlichen Verwaltung" vor, der es den Mitgliedstaaten ermöglicht, jede Einrichtung zu berücksichtigen, die nach ihrem nationalen öffentlichen Recht als solche anerkannt ist.

So ist es beispielsweise möglich, im Sektor der öffentlichen Verwaltung mehrere verschiedene NIS2-Einrichtungen innerhalb einer einzigen juristischen Person des öffentlichen Rechts zu unterscheiden - vorausgesetzt, dass ein rechtlich anerkannter Unterschied zwischen den verschiedenen betroffenen öffentlichen Verwaltungen gemacht werden kann.

1.5. Wie berechnet man die Größe einer Einrichtung?

Art. 3, §§ 1 und 2 NIS2-Gesetz & Empfehlung 2003/361/EG

Für die Zwecke des Anwendungsbereichs des NIS2-Gesetzes wird die Größe der Einrichtung auf Grundlage der Regeln in der Beilage der Empfehlung 2003/361/EG berechnet. Die Europäische Kommission hat dazu einen ausführlichen Leitfaden veröffentlicht und ein Berechnungstool zur Verfügung gestellt.

Eine Organisation wird als mittleres Unternehmen bezeichnet, wenn sie:

- entweder zwischen 50 und 249 Arbeiter beschäftigt (Arbeitnehmer, Zeit- oder Leiharbeitskräfte, Betriebsinhaber, Teilhaber, usw.) - Mitarbeiterzahl berechnet in Jahresarbeitseinheiten (JAE); oder
- einen Jahresumsatz von mehr als 10 Millionen Euro bis zu 50 Millionen Euro erzielt und eine Jahresbilanzsumme von mehr als 10 Millionen Euro bis zu 43 Millionen Euro aufweist.

Bei der Anwendung dieser Schwellenwerte für Finanzdaten hat die betreffende Organisation die Wahl, entweder ihren Jahresumsatz oder ihre Jahresbilanzsumme zu berücksichtigen. **Eine dieser beiden Daten kann den Schwellenwert für ein großes Unternehmen überschreiten**, ohne dass dies Auswirkungen auf die Einstufung einer Organisation als mittleres Unternehmen hat.

Eine Organisation wird als großes Unternehmen bezeichnet, wenn sie:

- entweder 250 oder mehr Arbeiter beschäftigt (Arbeitnehmer, Zeit- oder Leiharbeitskräfte, Betriebsinhaber, Teilhaber, usw.) - Mitarbeiterzahl berechnet in Jahresarbeitseinheiten (JAE); oder
- einen Jahresumsatz von mehr als 50 Millionen Euro erzielt und eine Jahresbilanzsumme von mehr als 43 Millionen Euro aufweist.

Es ist zu berücksichtigen, dass in Situationen mit "Partner"- oder "verbundenen" Unternehmen eine proportionale Konsolidierung der Daten (Mitarbeiter und Finanzen) der betroffenen Einrichtung und dieser anderen Einrichtungen durchgeführt werden muss, um die Größe zu berechnen.

Abgesehen von einigen Ausnahmen gilt ein Unternehmen als "Partner", wenn es zwischen 25% und 50% des Kapitals oder der Stimmrechte (je nachdem, welcher Anteil höher ist) in der betreffenden Einrichtung hält (oder umgekehrt). Diese Art von Beziehung beschreibt die Situation von Unternehmen, die bestimmte finanzielle Partnerschaften mit anderen Unternehmen eingehen, ohne dass das eine Unternehmen direkt oder indirekt eine tatsächliche Kontrolle über das andere ausübt.

Abgesehen von einigen Ausnahmen gilt ein Unternehmen als "verbunden", wenn es mehr als 50 % des Kapitals oder der Stimmrechte (je nachdem, welcher Anteil höher ist) in der betreffenden Einrichtung hält (oder umgekehrt).

Bei Partnerunternehmen muss das betrachtete Unternehmen zu seinen eigenen Daten einen Anteil der Mitarbeiterzahl und der Finanzdaten des anderen Unternehmens hinzufügen, um dessen Größe zu bestimmen. Dieser Anteil spiegelt den Anteil der gehaltenen Anteile oder Stimmrechte wider (je nachdem, welcher der beiden Faktoren höher ist). Im Falle von verbundenen Unternehmen muss das betreffende Unternehmen 100 % der Daten des verbundenen Unternehmens zu seinen eigenen hinzufügen.

Wenn ein Unternehmen beispielsweise zu 30 % an einem anderen Unternehmen beteiligt ist, addiert es zu seinen eigenen Zahlen 30 % der Beschäftigtenzahl, des Umsatzes und der Bilanzsumme des Partnerunternehmens. Wenn es mehrere Partnerunternehmen gibt, muss die gleiche Art von Berechnung für jedes Partnerunternehmen durchgeführt werden, das dem betreffenden Unternehmen unmittelbar vor- oder nachgelegen ist.

Im Rahmen des NIS2-Gesetzes ist jedoch ein Mechanismus vorgesehen, der es der nationalen Cybersicherheitsbehörde (ZCB) im Falle einer unverhältnismäßigen Situation ermöglicht, den Grad der Unabhängigkeit einer Einrichtung von ihren Partner- und verbundenen Unternehmen zu berücksichtigen, insbesondere in Bezug auf die Netz- und Informationssysteme, die sie zur Erbringung ihrer Dienstleistungen nutzt, und in Bezug auf die Dienstleistungen, die sie erbringt. Diese Elemente müssen dem ZCB von Fall zu Fall von der Organisation, die den Mechanismus in Anspruch nehmen möchte, nachgewiesen werden. Die Anwendung dieses Mechanismus kann dazu führen, dass eine Organisation als wichtige Einrichtung statt als wesentliche Einrichtung neu eingestuft oder ganz aus dem Geltungsbereich des Gesetzes ausgeschlossen wird.

Gemäß Artikel 4 des Anhangs der Empfehlung beziehen sich die zu berücksichtigenden Personal- und Finanzdaten auf die Daten des letzten anerkannten Rechnungslegungszeitraums, die auf Jahresbasis ab dem Datum des Rechnungsabschlusses berechnet werden, ohne Mehrwertsteuer. Um von einer Größenklasse in eine andere zu wechseln, muss das Unternehmen einen Schwellenwert in mindestens zwei aufeinanderfolgenden Jahren über- oder unterschreiten. Ein Unternehmen, das zwischen zwei Schwellenwerten schwankt, muss möglicherweise mehr als zwei Jahre zurückgehen, um seine Qualifikation zu bestimmen.

Siehe auch Abschnitt 1.21.3. und den Leitfaden zur Größenberechnung für weitere Einzelheiten.

1.6. Warum scheinen die Angaben auf der ZCB-Website und in den FAQ zum Größendeckel nicht mit den Angaben in der EU-Empfehlung 2003/361 übereinzustimmen?

Im Text der Empfehlung 2003/361 wird bei der Beschreibung der Schwellenwerte für KMU auf "und" Bezug genommen. Dies liegt daran, dass in der Empfehlung die Schwellenwerte von der größten bis zur kleinsten Unternehmensgröße beschrieben werden. Auf der Website des ZCB und für die Zwecke von NIS2 werden diese Schwellenwerte jedoch vom kleinsten bis zum größten Unternehmen beschrieben, was zu einer anderen Beschreibung führt. Wie im Folgenden erläutert, bleiben die Schwellenwerte jedoch gleich:

- "(1) Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz (JU) von **höchstens** 50 Mio. EUR erzielen oder deren Jahresbilanzsumme (JBS) sich auf **höchstens** 43 Mio. EUR beläuft."

  ➔ Im Text steht KMU = < 250 VZÄ **und** < 50 Mio. JU / < 43 Mio. JBS
  ➔ Also großes Unternehmen = > 250 VZÄ **oder** > 50 Mio. JU (und/oder) > 43 Mio. JBS

- "(2) Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR **nicht übersteigt**."

  ➔ Der Text besagt, dass kleine Unternehmen = < 50 VZÄ **und** < 10 Millionen. JU / JBS
  ➔ Also mittleres Unternehmen = > 50 VZÄ **oder** > 10 Mio. AT (und/oder) > 10 Mio. JBS, aber nicht > 250 VZÄ **oder** > 50 Mio. JU (und/oder) > 43 Mio. JBS

Dies ist eine logische Anwendung der Schwellenwerte für die Zwecke von NIS2.

Das offizielle "SME Wizard"-Tool der Europäischen Kommission, das Unternehmen dabei helfen soll zu prüfen, ob sie ein KMU sind oder nicht, bestätigt die Ergebnisse der obigen Interpretation.

Auf unserer NIS2-Seite auf Safeonweb@Work heißt es daher korrekt (im obigen Abschnitt 1.5 etwas anders formuliert):

> *"die in der Empfehlung 2003/361/EG festgelegten Schwellenwerte für die Größe eines mittleren Unternehmens **überschreiten**, d. h. eine Mitarbeiterzahl von mindestens 50 Vollzeitbeschäftigten oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Mio. Euro aufweisen;"*

Dies wird auch in unserem Scoping-Tool korrekt wiedergegeben.

Etwas weiter auf von NIS2-Seite heißt es außerdem:

> *" Anschließend muss die Mitarbeiterzahl mit den finanziellen Beträgen kombiniert werden, um die endgültige Einstufung zu erhalten: Ein Unternehmen kann sich entweder für die Einhaltung der Obergrenze für den Umsatz oder für die Bilanzsumme entscheiden. **Es kann eine der finanziellen Obergrenzen überschreiten, ohne dass dies Auswirkungen auf seinen KMU-Status hat**. Wir betrachten daher **nur den niedrigsten der beiden Beträge**."*

Dieser Text basiert auf dem offiziellen Leitfaden der Europäischen Kommission zur Anwendung der Empfehlung 2003/361/EG (S. 11).

Eine Einrichtung kann also in mehreren Situationen als mittleres Unternehmen eingestuft werden, entweder auf der Grundlage der Zahl der Vollzeitbeschäftigten oder auf der Grundlage der Finanzdaten, oder beides zusammen. Dies entspricht der Logik des Wortes "oder".

Für die Einstufung einer Einrichtung als wesentliche und wichtige Einrichtung im Sinne des NIS2-Gesetzes ist es egal, ob zuerst festgestellt wird, ob die Einrichtung eine in den Anhängen des Gesetzes aufgeführte Dienstleistung erbringt, oder ob zuerst die Größe bestimmt wird (oder die Größenbegrenzung nicht gilt). Das Endergebnis wird dasselbe sein.

1.7. Welche Sektoren und Dienstleistungen fallen unter das Gesetz?

Beilagen I und II NIS2-Gesetz, Artikel 8 NIS2-Gesetz

Die betroffene Einrichtung muss mindestens eine der in den Beilagen I oder II des Gesetzes aufgeführten Dienstleistungen erbringen (selbst wenn diese Dienstleistung nur einen untergeordneten Teil ihrer Aktivitäten ausmacht - außer wenn die Definition selbst als Kriterium den Haupt- oder Nebencharakter der erbrachten Dienstleistung verwendet), die in den folgenden Sektoren angesiedelt sind:

Sektoren mit hoher Kritikalität (Beilage I)	**Sonstige kritische Sektoren (Beilage II)**
○ Energie (Elektrizität, Fernwärme- und Fernkälte, Erdöl, Erdgas, Wasserstoff) ○ Verkehr (Luftverkehr, Schienenverkehr, Schiffsfahrt, Straßenverkehr) ○ Bankwesen ○ Finanzmarktinfrastrukturen ○ Gesundheitswesen ○ Trinkwasser ○ Abwässer ○ Digitale Infrastruktur ○ Verwaltung von IKT-Diensten ○ Öffentliche Verwaltung ○ Weltraum	○ Post- und Kurierdienste ○ Abfallbewirtschaftung ○ Produktion, Herstellung und Handel mit chemischen Stoffen ○ Produktion, Verarbeitung und Vertrieb von Lebensmitteln ○ Verarbeitendes Gewerbe/Herstellung von Waren (Medizinprodukten und In-vitro-Diagnostika; Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen; elektrischen Ausrüstungen; Maschinenbau; Kraftwagen, Kraftwagenteile; sonstiger Fahrzeugbau) ○ Anbieter digitaler Dienste ○ Forschung

Jeder Dienst, der unter das NIS2-Gesetz fällt, **ist in den Beilagen** I oder II (mit Verweis auf die Definitionen in den einschlägigen europäischen Rechtsnormen) **oder in Artikel 8 des NIS2-Gesetzes festgelegt**. Diese Definitionen müssen unbedingt konsultiert werden, um den betreffenden Dienst zu verstehen. Zu diesem Zweck sind die Beilagen auf der Website des Belgischen Staatsblatts zugänglich (unten, nach dem Gesetzestext).

Siehe auch Abschnitt 1.21.4. für weitere Informationen darüber, wie Sie feststellen können, welche Dienste Ihre Organisation in der Europäischen Union anbietet, sowie den NIS2-Anwendungsbreichtest (NIS2 scope tool).

Weitere Informationen zu den einzelnen Sektoren finden Sie im Abschnitt 1.22.

1.8. Muss die in den Anhängen genannte Dienstleistung die Haupttätigkeit der Einrichtung sein?

Art. 3 NIS2-Gesetz

In der Begründung des NIS2-Gesetzes heißt es zu Artikel 3 des Gesetzes Folgendes:

> *"Um als öffentliche oder private Einrichtung einer in Anhang I oder II des Gesetzes genannten Art zu gelten, genügt es, unabhängig von ihrer Rechtsform mindestens eine der in Anhang I oder II des Gesetzes aufgeführten Tätigkeiten auszuüben**, auch wenn diese Dienstleistung nur einen untergeordneten Teil ihrer Tätigkeit darstellt**, und die in*

Absatz 1 genannten Höchstgrenzen zu überschreiten oder eines der in den Absätzen 3 ff. genannten Kriterien zu erfüllen (siehe unten)." (Hervorhebung von uns)

Artikel 3 des NIS2-Gesetzes, der den Anwendungsbereich festlegt, bezieht sich auf öffentliche oder private Einrichtungen der in Anhang I oder II genannten Art, die ein mittleres oder großes Unternehmen im Sinne der europäischen Empfehlung 2003/361/EG darstellen.

Wie bei der Richtlinie selbst bedeutet dies in der Praxis, dass der Anwendungsbereich des NIS2-Gesetzes direkt von den Definitionen in den Anhängen I und II abhängt.

Im Allgemeinen **wird** die **Nebentätigkeit oder der nicht wesentliche Charakter der Tätigkeit für die betreffende Einrichtung in den Definitionen nicht berücksichtigt** (und hat daher keinen Einfluss auf den Anwendungsbereich des NIS2-Gesetzes). Es gibt jedoch einige wenige Ausnahmen, in denen das Kriterium der "Hauptwirtschaftstätigkeit" oder des "nicht wesentlichen Teils der allgemeinen Tätigkeit" in den Definitionen verwendet wird und tatsächlich relevant ist (z. B. in den Bereichen Abfallwirtschaft, Trinkwasser oder Abwasser).

Nur in den begrenzten Ausnahmen, die in den Definitionen der Anhänge **ausdrücklich vorgesehen sind**, **sollte der nebensächliche oder nicht wesentliche Charakter der Tätigkeit berücksichtigt werden**. Eine Einrichtung kann somit in den Anwendungsbereich des Gesetzes fallen, **auch wenn die betreffende Dienstleistung, die sie erbringt, nur ein untergeordneter oder nicht wesentlicher Teil ihrer gesamten Tätigkeit ist**, sofern in den Anhängen nichts anderes bestimmt ist**.**

Es besteht also kein Widerspruch zwischen der Begründung und den Bestimmungen des NIS2-Gesetzes (und seiner Anhänge), und die Dienstleistung muss nur dann die Haupttätigkeit einer Einrichtung sein, wenn sie in den Anhängen ausdrücklich erwähnt wird.

1.9. Ist es möglich, die vom NIS2-Gesetz erfassten Bereiche in Zukunft auszuweiten?

Der König kann den Beilagen I und II Sektoren oder Teilsektoren durch einen im Ministerrat beratenen Erlass nach Anhörung etwaiger betroffener sektoraler Behörden und der nationalen Cybersicherheitsbehörde (ZCB) hinzufügen.

Art. 3, § 6 NIS2-Gesetz

Auf diese Weise können die Anhänge erweitert werden, wenn sich in Zukunft herausstellt, dass ein bisher nicht erfasster Sektor aufgrund seiner Bedeutung für kritische gesellschaftliche und/oder wirtschaftliche Aktivitäten in den Anwendungsbereich aufgenommen werden sollte.

1.10. Ist es möglich, dass eine Einrichtung in mehrere Sektoren fällt?

Ja, es ist möglich, dass eine selbe Einrichtung in mehr als einen Sektor (abhängig von all ihren Aktivitäten) fällt. In diesem Fall sind mehrere Überlegungen zu berücksichtigen:

Art. 8, 34°; 25; 39, Abschn. 2 und 44, §1, Abs. 2 NIS2-Gesetz

- Strengere Anforderungen haben Vorrang vor weniger strengen Anforderungen. Infolgedessen und wenn das Größenkriterium erfüllt ist (großes Unternehmen), unterliegt eine Einrichtung, die Dienstleistungen erbringt, die sowohl

unter Beilage I als auch unter Beilage II fallen, insgesamt den Verpflichtungen, die für eine wesentliche Einrichtung gelten;
- Die Einrichtung kann potenziell der Aufsicht der nationalen Cybersicherheitsbehörde (ZCB) und mehrerer sektoraler Behörden unterstehen. Diese werden im Rahmen der Aufsicht zusammenarbeiten;
- Eine öffentliche Einrichtung, die hauptsächlich eine Dienstleistung ausübt, die in einem anderen Sektor der Beilagen des Gesetzes aufgeführt ist, fällt nur in diesen Sektor (und nicht gleichzeitig in diesen Sektor und in den Sektor der öffentlichen Verwaltung).

1.11. Was ist der Unterschied zwischen "wesentlichen" und "wichtigen" Einrichtungen?

Art. 39-42; 48, §§ 1 und 2; 58 und 59 NIS2-Gesetz

Wesentliche und wichtige Einrichtungen unterscheiden sich vor allem im Rahmen der Aufsicht und der Sanktionen. Wesentliche Einrichtungen werden proaktiv "*ex ante*" und reaktiv "*ex post*" beaufsichtigt. Insbesondere werden wesentliche Einrichtungen einer regelmäßigen Konformitätsbewertung unterzogen.

Wichtige Einrichtungen werden "*ex post*" beaufsichtigt, d.h. aufgrund von Beweisen, Hinweisen oder Informationen, dass eine wichtige Einrichtung gegen die gesetzlichen Verpflichtungen verstößt.

Weitere Informationen zur Aufsicht finden Sie im Abschnitt 4.4.

Ansonsten gelten für beide Arten von Einrichtungen dieselben Pflichten, z.B. in Bezug auf die Meldung von Sicherheitsvorfällen (Abschnitt 3.3.) oder das Ergreifen von Maßnahmen zum Management von Cybersicherheitsrisiken (Abschnitt 3.2.).

1.12. Wie funktioniert das zusätzliche Identifizierungsverfahren?

Art. 11 NIS2-Gesetz

Aus eigener Initiative oder auf Vorschlag der gegebenenfalls betroffenen sektoralen Behörde kann die nationale Cybersicherheitsbehörde (ZCB) eine Einrichtung unabhängig von ihrer Größe, innerhalb eines bestehenden Sektors der Anhänge des NIS2-Gesetzes, in folgenden Fällen als wesentlich oder wichtig identifizieren:

1. Die Einrichtung ist der einzige Anbieter in Belgien von mindestens einer Dienstleistung, die für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten unerlässlich ist, in einem der Sektoren oder Teilsektoren, die in den Beilagen I und II des Gesetzes aufgeführt sind;
2. Eine Störung der von der Einrichtung erbrachten Dienstleistung könnte sich wesentlich auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit auswirken;
3. Eine Störung der von der Einrichtung erbrachten Dienstleistung könnte zu einem wesentlichen Systemrisiko führen, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

4. Die Einrichtung ist aufgrund ihrer besonderen Bedeutung auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art von Dienstleistung oder für andere voneinander abhängige Sektoren in Belgien kritisch.

Ein Vorschlag für eine Identifizierungsentscheidung wird der betreffenden Einrichtung und den zuständigen sektoralen Behörden übermittelt, die innerhalb von sechzig Tagen eine Stellungnahme abgeben können.

Das ZCB bewertet die wesentlichen und wichtigen Einrichtungen mindestens alle zwei Jahre nach denselben Verfahren und aktualisiert sie gegebenenfalls.

1.13. Was geschieht, wenn eine NIS2-Einrichtung von einer anderen Organisation erworben wird?

Wenn ein Unternehmen oder eine Vereinigung eine NIS2-Einrichtung erwirbt, muss die betreffende NIS2-Einrichtung weiterhin die gesetzlichen Bestimmungen erfüllen, solange die von ihr erbrachten Dienstleistungen und die Größenkriterien bestehen bleiben. Die NIS2-Qualifikation der betreffenden Einrichtung wird nicht auf die erwerbende Organisation oder die Mutterorganisation übertragen (wenn es sich um zwei verschiedene juristische Personen handelt). Natürlich könnte auch die übernehmende Organisation selbst unter das Gesetz fallen, wenn sie einen NIS2-Dienst innerhalb der EU selbst erbringt und die Größenkriterien erfüllt.

Die Einstufung als wichtige Einrichtung unter NIS2 könnte sich nach der Übernahme ändern, da die Einrichtung bei den Berechnungen für die Größenkriterien möglicherweise größer wird. Diese können nämlich nach einem Zeitraum von zwei Jahren überprüft werden (Abschnitt 1.5). Je nach der von der NIS2-Einrichtung erbrachten Dienstleistung (Anhänge) könnte eine Vergrößerung zu einer neuen Einstufung als wesentlich anstelle von wichtig führen.

In jedem Fall muss die erwerbende Organisation möglicherweise geeignete Maßnahmen zum Management von Cybersicherheitsrisiken implementieren, da die NIS2-Einrichtung verpflichtet ist, ihre Lieferkette zu sichern, oder falls sie dieselben Netzwerke und Informationssysteme nutzen (Abschnitt 3.14).

1.14. Was bedeutet "(Haupt-)Niederlassung"? Gilt das Gesetz nur für belgische Organisationen oder auch für andere Einrichtungen?

Das belgische NIS2-Gesetz gilt grundsätzlich für Einrichtungen, die **in Belgien ansässig sind** und in der EU ihre Dienstleistungen erbringen oder ihre Geschäfte betreiben (Niederlassungsregel).

Art. 4 NIS2-Gesetz

Der Begriff "Einrichtung" wird in Artikel 8, 37° des NIS2-Gesetzes wie folgt definiert: *„eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann"*. Siehe auch Abschnitt 1.4.

Der Begriff der Niederlassung beinhaltet lediglich die tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung, unabhängig von der gewählten Rechtsform, ob es sich dabei um

den Sitz, eine einfache Zweigstelle, eine Tochtergesellschaft, eine Betriebseinheit, eine Fabrik, ein Handelsbüro, usw., handelt.

Das NIS2-Gesetz sieht drei Ausnahmen von der Niederlassungsregel in Belgien vor:

1) Wenn Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, ihre Dienste in Belgien anbieten (Dienstortregel);
2) Wenn DNS-Dienstanbieter, TLD- Namensregister, Einrichtungen, die Domänennamenregistrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste sowie Anbieter von Online-Marktplätzen, von Online-Suchmaschinen oder von Plattformen für Dienste sozialer Netzwerke, ihre Hauptniederlassung in Belgien haben (Hauptniederlassungsregel);
3) Wenn Einrichtungen der öffentlichen Verwaltung von Belgien gegründet wurden.

Um die "Hauptniederlassung" einer Einrichtung zu bestimmen, sollten die folgenden Niederlassungen in einer kaskadierenden Reihenfolge ermittelt werden (wenn das erste Kriterium nicht ermittelt werden kann oder außerhalb der EU liegt, wird das zweite oder dritte Kriterium verwendet):

1° wo die Entscheidungen über die Risikomanagementmaßnahmen im Bereich der Cybersicherheit überwiegend getroffen werden;
2° wo die Einrichtung ihre Cybersicherheitsoperationen durchführt;
3° wenn die Einrichtung die höchste Beschäftigtenzahl in der Union hat.

Wenn eine Einrichtung nicht innerhalb der EU niedergelassen ist, aber eine Dienstleistung erbringt, die der Regel der Hauptniederlassung unterliegt, muss sie einen gesetzlichen Vertreter benennen, der in einem der Mitgliedstaaten niedergelassen ist, in denen sie ihre Dienstleistungen erbringt. Wenn dieser Vertreter in Belgien ansässig ist, wird davon ausgegangen, dass die Einrichtung ihre Hauptniederlassung in Belgien hat.

Unter der Hauptniederlassungsregel, wenn eine Einrichtung mehrere Niederlassungen in verschiedenen EU-Mitgliedstaaten hat, unterliegt sie den NIS2-Verpflichtungen nur in dem Mitgliedstaat, in dem sie ihre Hauptniederlassung hat.

Für komplexere Szenarien siehe die folgenden Abschnitte.

1.15. Spezifische Fragen im Zusammenhang mit der Zuständigkeit und der Niederlassung (auf wen ist das Gesetz anwendbar?)

1.15.1. Was ist, wenn meine Organisation Dienstleistungen erbringt, die sowohl unter die Niederlassungs- als auch unter die Hauptniederlassungsregel fallen? Wie lassen sich verschiedene Zuständigkeitsregeln kombinieren?

Je nach Art der erbrachten Dienste müssen NIS2-Einrichtungen möglicherweise verschiedene Zuständigkeitsregeln kombinieren (so kann ein Telekommunikationsbetreiber öffentliche

elektronische Kommunikationsnetze anbieten, die unter die Dienstortregel fallen, Strom erzeugen, der unter die Niederlassungsregel fällt, und einen verwalteten Sicherheitsdienst anbieten, der unter die Hauptniederlassungsregel fällt) und sind möglicherweise mehreren Umsetzungsgesetzen und zuständigen Aufsichtsbehörden verpflichtet (je nach dem betroffenen Dienst und dem Standort ihrer Niederlassungen).

Die verschiedenen zuständigen nationalen Behörden werden bei Inspektionen und der Meldung von erheblichen Sicherheitsvorfällen zusammenarbeiten. Dies bedeutet jedoch, dass, in diesem Fall, die Einrichtung die Vorschriften von mindestens zwei verschiedenen Mitgliedstaaten kombinieren muss, indem sie die strengsten Vorschriften eines Mitgliedstaates auf alle ihre Dienste anwendet. Dadurch wird sichergestellt, dass die Vorschriften in mehreren Mitgliedstaaten ordnungsgemäß eingehalten werden.

1.15.2. Was ist, wenn eine Einrichtung eine Tochter-/Muttergesellschaft/Zweigstelle in einem anderen EU-Mitgliedstaat hat, die ebenfalls NIS2 einhalten muss?

Dies hängt von der Dienstleistung ab, die von der betreffenden Organisation in dem anderen Mitgliedstaat erbracht wird. Die Tochter-/Muttergesellschaft/Zweigstelle muss als "Einrichtung" im Sinne des NIS2-Gesetzes eingestuft werden (siehe Abschnitt 1.4).

Das NIS2-Gesetz **gilt für alle Organisationen einzeln**, auch wenn sie Teil einer Gruppe sind und/oder von derselben Holdinggesellschaft gehalten werden. Der Anwendungsbereich und die Verpflichtungen des NIS2-Gesetzes müssen daher von jeder Organisation individuell auf der Grundlage der von ihr erbrachten Dienstleistungen analysiert werden. Es ist also möglich, dass eine Tochtergesellschaft NIS2-konform sein muss, während eine Muttergesellschaft dies nicht muss.

In den folgenden Abschnitten werden die verschiedenen Möglichkeiten genauer analysiert.

A. Die erbrachte Dienstleistung fällt nicht unter eine der Ausnahmeregelungen der Zuständigkeit (Abschnitt 1.14)

Die Organisation in dem anderen Mitgliedstaat muss das NIS2-Gesetz des Mitgliedstaates beachten, in dem sie ansässig ist.

Beispiel: Die Muttergesellschaft hat ihren Sitz in Belgien und die Tochtergesellschaft ist in Frankreich ansässig. Beide erbringen Dienstleistungen, die in den Lebensmittelsektor fallen (Anhang II des NIS2-Gesetzes). Ihre konsolidierte Mitarbeiterzahl (Size-cap) reicht aus, um als mittlere Unternehmen eingestuft zu werden. Die Muttergesellschaft in Belgien muss NIS2 in Belgien einhalten, die Tochtergesellschaft muss NIS2 in Frankreich einhalten.

B. Die erbrachte Dienstleistung fällt unter die Dienstort-Ausnahme (elektronische Kommunikation)

Die Organisation in dem anderen Mitgliedstaat muss das NIS2-Gesetz des Mitgliedstaats/der Mitgliedstaaten beachten, in dem/denen sie ihre Dienstleistungen erbringt.

Beispiel: Die Muttergesellschaft ist in Belgien und die Tochtergesellschaft in Luxemburg ansässig. Die Tochtergesellschaft bietet öffentliche elektronische Kommunikationsdienste in Belgien, Luxemburg und Deutschland an. In Kombination mit den Daten der Muttergesellschaft

ist sie ein großes Unternehmen. Sie muss daher die NIS2-Umsetzungsgesetze von Belgien, Luxemburg und Deutschland (als wesentliche Einrichtung) einhalten. In der Praxis müssen die verschiedenen Anforderungen miteinander kombiniert und die strengsten Regeln eingehalten werden, um die Einhaltung aller drei gesetzlichen Rahmen zu gewährleisten.

C. Die erbrachte Dienstleistung fällt unter die Hauptniederlassung-Ausnahme

Die Organisation in dem anderen Mitgliedstaat muss das NIS2-Gesetz des Mitgliedstaats beachten, in dem sie ihre Hauptniederlassung hat (siehe Abschnitt 1.14).

Beispiel: Die Muttergesellschaft ist in Belgien ansässig. Sie trifft die Entscheidungen in Bezug auf Risikomanagementmaßnahmen im Bereich der Cybersicherheit überwiegend für sich selbst, aber auch für ihre Filiale in den Niederlanden. Die Muttergesellschaft erbringt keine NIS2-Dienstleistung und fällt daher selbst nicht unter NIS2. Die Filiale hat ihren Sitz in den Niederlanden, ist ein mittelgroßes Unternehmen und bietet dort verwaltete Dienste an. Da sich die Hauptniederlassung jedoch in Belgien befindet, fällt die Filiale in Belgien unter die NIS2 (und muss sich zum Beispiel nur in Belgien registrieren).

1.15.3. Was ist, wenn sich innerhalb derselben Gruppe NIS2-Einrichtungen in mehreren EU-Mitgliedstaaten befinden?

Wie im Abschnitt 1.15.2 beschrieben, kann es sein, dass die verschiedenen Organisationen je nach den von ihnen angebotenen Diensten der Zuständigkeit mehrerer Mitgliedsstaaten innerhalb der EU unterliegen.

Es ist durchaus möglich, dass ein Unternehmen einer Gruppe NIS2 in Belgien einhalten muss, während ein anderes Unternehmen NIS2 zum Beispiel in Polen einhalten muss. Wenn die Gruppe eine Holdinggesellschaft hat, muss diese auch analysieren, ob sie aufgrund einer von ihr erbrachten Dienstleistung unter NIS2 fällt (NIS2 gilt für alle Organisationen einzeln, aber die Größe wird auf Gruppenebene mit Partner- oder verbundenen Unternehmen berechnet).

1.15.4. Ein Unternehmen, das in einem NIS2-Sektoren tätig ist, muss NIS2 in Land A befolgen, seine Muttergesellschaft mit Sitz in Land B jedoch nicht. Wie funktioniert das?

Das Unternehmen Nr. 1 muss die im NIS2-Gesetz von Land A enthaltenen Verpflichtungen einhalten. Dazu gehören Registrierung, Meldung von Sicherheitsvorfällen, Cybersicherheitsmaßnahmen, usw. Die Muttergesellschaft Nr. 2 in Land B muss all diese Verpflichtungen nicht einhalten, da sie nicht unter die NIS2 fällt.

Es gibt jedoch noch andere Möglichkeiten, wie die Muttergesellschaft betroffen sein könnte:

1. Wenn die beiden Unternehmen dieselben Netzwerke und IT-Systeme teilen, erfordert die Anwendung von NIS2 auf Unternehmen Nr. 1, dass die Risikomanagementmaßnahmen im Bereich der Cybersicherheit für das gesamte System bzw. die gesamten Systeme und Netzwerke ergriffen werden, um alles zu schützen (gefahrenübergreifender Ansatz der NIS2-Risikomanagementmaßnahmen im Bereich der Cybersicherheit, siehe Abschnitt 3.2).
2. Die Verpflichtung des Unternehmens Nr. 1 im Rahmen von NIS2, die Sicherheit seiner Lieferkette zu gewährleisten, könnte es dazu veranlassen, seiner Muttergesellschaft Nr.

2 die Implementierung von Cybersicherheitsmaßnahmen aufzuerlegen (siehe Abschnitt 3.14).

Handelt es sich bei der Einrichtung in Land A nur um eine Zweigstelle (dieselbe juristische Person) des Unternehmens mit Sitz in Land B, so ist die gesamte juristische Person den NIS2-Verpflichtungen gemäß NIS2 in Land A verpflichtet (unabhängig davon, wo sich ihre Netzwerk- und Informationssysteme physisch befinden).

1.15.5. Was ist, wenn eine Organisation (Tochter-/Mutterunternehmen) außerhalb der EU ansässig ist, aber Dienstleistungen in der EU erbringt?

Grundsätzlich fallen Organisationen mit Sitz außerhalb der EU nicht unter NIS2, es sei denn, sie erbringen in der EU eine Dienstleistung, die unter eine der drei im Abschnitt 1.14 erläuterten Ausnahmeregeln der Zuständigkeit fällt.

Für die Dienstleistung, die unter die Zuständigkeitsregel für den Dienstort (elektronische Kommunikation) fällt, gilt das NIS2-Gesetz des Mitgliedstaats/der Mitgliedstaaten, in dem/denen die Organisation von außerhalb der EU ihre Dienstleistungen erbringt.

Wenn die Organisation außerhalb der EU eine Dienstleistung innerhalb der EU erbringt, die unter die Ausnahmeregel für die Hauptniederlassung fällt, muss sie einen gesetzlichen Vertreter benennen, der in einem Mitgliedstaat niedergelassen ist, in dem sie ihre Dienstleistungen erbringt. Wenn dieser Vertreter in Belgien ansässig ist, wird die Einrichtung als in Belgien ansässig betrachtet.

Das Gesetz definiert einen gesetzlichen Vertreter als: *"eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht in der Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an die Einrichtung — hinsichtlich der Pflichten dieser Einrichtung gemäß dieses Gesetzes wenden kann"*.

Um festzustellen, ob eine solche Einrichtung in der Union Dienste anbietet, sollte geprüft werden, ob sie beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website einer Einrichtung oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten sollten zur Feststellung einer solchen Absicht ebenso wenig als ausreichend betrachtet werden wie die Verwendung einer Sprache, die in dem Drittland, in dem die Einrichtung niedergelassen ist, allgemein gebräuchlich ist. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass die Einrichtung beabsichtigt, in der Union Dienste anzubieten.

Der Vertreter sollte im Auftrag der Einrichtung handeln, und es sollte für die zuständigen Behörden oder CSIRTs möglich sein, sich an ihn zu wenden. Der Vertreter sollte von der Einrichtung ausdrücklich schriftlich beauftragt werden, im Rahmen der sich aus dieser Richtlinie

ergebenden Pflichten der Einrichtung in deren Auftrag zu handeln, was auch die Meldung von Sicherheitsvorfällen einschließt.

Zur Registrierung einer Organisation mit Sitz außerhalb Belgiens siehe Abschnitt 3.13.7.

1.16. Spezifische Fragen in Bezug auf Gruppen von Organisationen oder Unternehmen

1.16.1. Wie beurteilen man den Anwendungsbereich von NIS2 in Bezug auf eine Gruppe von Organisationen oder Unternehmen?

Innerhalb einer Gruppe von Organisationen oder Unternehmen muss, wie in den vorangegangenen Abschnitten erläutert, jede juristische Person/Organisation für sich selbst und individuell analysieren, ob sie aufgrund ihrer Tätigkeiten und erbrachten Dienstleistungen in den Anwendungsbereich von NIS2 fällt. Die gemeinsame Nutzung von Daten, Netzwerken oder Informationssystemen innerhalb der Gruppe hat keinen Einfluss auf den Anwendungsbereich. Jeder Organisation wird empfohlen, die im Abschnitt 1.21 enthaltenen Erläuterungen individuell durchzugehen.

Es ist zu beachten, dass innerhalb einer Gruppe von Organisationen oder Unternehmen die Zahl der Vollzeitäquivalente und die Finanzdaten auf der Grundlage der verschiedenen Regeln der Empfehlung 2003/361/EG konsolidiert werden. For mehr Informationen, siehe Abschnitt 1.5.

1.16.2. Welche Auswirkungen hat eine NIS2-Einrichtung auf andere Organisationen oder Unternehmen innerhalb derselben Gruppe?

Siehe die Erläuterungen im Abschnitt 1.15.4.

1.16.3. Was geschieht, wenn eine andere Organisation oder ein Unternehmen derselben Gruppe dieselben IT-Netzwerke und/oder -Systeme wie eine NIS2-Einrichtung nutzt?

Wenn die beiden Organisationen dieselben Netzwerke und IT-Systeme nutzen, erfordert die Einbeziehung einer Einrichtung in den Anwendungsbereich von NIS2, dass die Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf das/die gesamte(n) gemeinsam genutzte(n) System(e) und Netzwerk(e) angewendet werden, um alles zu schützen (gemäß dem gefahrenübergreifenden Ansatz der Risikomanagementmaßnahmen im Bereich der Cybersicherheit von NIS2, siehe Abschnitt 3.2).

1.16.4. Was ist, wenn es sowohl wesentliche Einrichtungen als auch wichtige Einrichtungen innerhalb derselben Gruppe von Organisationen oder Unternehmen gibt?

Das NIS2-Gesetz gilt individuell für jede juristische Person. Einrichtungen, die nicht unter NIS2 fallen, aber Teil derselben Gruppe sind, werden von NIS2 nur in dem Maße betroffen sein, wie es

im Abschnitt 1.15.4 beschrieben ist. Ob Einrichtungen innerhalb desselben Konzerns als wesentlich oder wichtig eingestuft werden, ändert nichts an der Situation.

1.16.5. Was geschieht, wenn eine Organisation oder ein Unternehmen einen Vertrag mit einem NIS2-Dienstanbieter abschließt und zulässt, dass dieser Vertrag/Dienst von anderen Organisationen genutzt wird?

Ein Unternehmen X schließt beispielsweise einen Vertrag mit einem Anbieter digitaler Dienste - Unternehmen Y (z. B. einem Anbieter von Rechenzentren) - ab und gestattet dann die Nutzung dieses Vertrags/Dienstes durch ein Partnerunternehmen Z. In einer solchen Situation werden die NIS2-Dienste weiterhin von Unternehmen Y und nicht von Unternehmen X geliefert (solange Unternehmen X keine Rolle bei der Lieferung des NIS2-Dienstes für Unternehmen Z spielt).

1.16.6. Was ist mit Holdinggesellschaften, die (fast) kein Personal, keinen Umsatz, nur eine positive Bilanzsumme haben?

Wenn eine Holdinggesellschaft keine NIS2-Dienstleistung erbringt, fällt sie nicht unter NIS2. Ihre Mitarbeiterzahl und ihre Finanzdaten werden jedoch bei der Beurteilung der Unternehmensgröße von verbundenen Unternehmen oder Partnerunternehmen, die eine NIS2-Dienstleistung erbringen, berücksichtigt.

Abgesehen von diesen Elementen gelten auch die Erklärungen aus Abschnitt 1.15.4.

1.16.7. Was ist, wenn eine Organisation IT-Dienstleistungen für andere Organisationen innerhalb derselben Gruppe von Organisationen oder Unternehmen erbringt?

Innerhalb einer Gruppe von Organisationen oder einem Konzern muss jede einzelne Einrichtung für sich selbst und individuell analysieren, ob sie in den Anwendungsbereich von NIS2 fällt, und zwar auf der Grundlage ihrer eigenen Tätigkeiten und erbrachten Dienstleistungen (Personal- und Finanzdaten werden jedoch grundsätzlich mit verbundenen oder Partnerunternehmen konsolidiert (siehe Abschnitt 1.5).

Wenn eine Einrichtung einen NIS2-Dienst (z. B. als Anbieter verwalteter Dienste oder als Anbieter von Cloud-Computing-Diensten) für eine andere Einrichtung erbringt, kann sie (je nach Größe) unter NIS2 fallen**, auch wenn die Tätigkeit nur einer begrenzten Anzahl von Organisationen oder Unternehmen innerhalb derselben Gruppe angeboten wird**.

Anders verhält es sich jedoch, wenn zwei oder mehrere Organisationen innerhalb einer Gruppe Daten, Netzwerke oder Systeme gemeinsam nutzen (und sich die entsprechenden Kosten teilen) und nicht eine bestimmte Organisation verwaltete Dienste für die anderen bereitstellt.

Siehe auch Abschnitt 1.22.6.2 über Anbieter verwalteter Dienste.

1.17. Welche Interaktionen bestehen zwischen der DORA-Verordnung und der NIS2-Richtlinie?

Art. 6 NIS2-Gesetz
Art. 2 & 47 DORA

Die NIS2-Richtlinie und ihr Umsetzungsgesetz zielen auf bereichsübergreifende Maßnahmen zur Erhöhung der Cybersicherheit in der EU ab. Ziel ist es, die Cybersicherheit in der EU insgesamt zu verbessern und insbesondere ein hohes Maß an Cybersicherheit für bestimmte Einrichtungen zu gewährleisten, die für gesellschaftliche und wirtschaftliche Aktivitäten kritisch sind.

Die DORA-Verordnung (Digital Operational Resiliance Act) richtet sich speziell an Betreiber des Finanzsektors. Sie zielt darauf ab, die digitaler operationaler Resilienz von Informationssystemen im Finanzsektor zu verbessern und die bestehenden Vorschriften in diesem Bereich zu koordinieren.

DORA gilt für Finanzinstitute, die in Artikel 2 der Verordnung aufgelistet sind. Dabei handelt es sich um:

- Kreditinstitute,
- Zahlungsinstitute,
- Kontoinformationsdienstleister,
- E-Geld-Institute,
- Wertpapierfirmen,
- Anbieter von Krypto-Dienstleistungen,
- Zentralverwahrer,
- zentrale Gegenparteien,
- Handelsplätze,
- Transaktionsregister,
- Verwalter alternativer Investmentfonds,
- Verwaltungsgesellschaften,
- Datenbereitstellungsdienste,
- Versicherungs- und Rückversicherungsunternehmen,
- Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,
- Einrichtungen der betrieblichen Altersversorgung,
- Ratingagenturen,
- Administratoren kritischer Referenzwerte,
- Schwarmfinanzierungsdienstleister,
- Verbriefungsregister,
- IKT-Drittdienstleister.

Die Anforderungen von NIS2 und DORA überschneiden sich für Einrichtungen, die im Banken- und Finanzsektor tätig sind. Die NIS2-Richtlinie sieht daher eine *lex specialis*-Regel vor: Wenn gleichwertige sektorale Anforderungen der EU in Bezug auf Cybersicherheit und die Meldung von erheblichen Sicherheitsvorfällen bestehen, haben diese Vorrang vor den allgemeinen/sektorübergreifenden Anforderungen von NIS2.

IKT-Drittanbieter, die unter DORA fallen, sind jedoch nicht von der *lex specialis*-Regel betroffen und können den Verpflichtungen von DORA und NIS2 unterliegen.

Es ist wichtig zu beachten, dass NIS2-Einrichtungen im Banken- und Finanzsektor mit Sitz in Belgien sich weiterhin wie die anderen NIS2-Einrichtungen registrieren müssen. Erhebliche Sicherheitsvorfälle, die von DORA-Einrichtungen über ihren eigenen Meldemechanismus gemeldet werden, werden von den zuständigen Behörden (Nationalbank von Belgien und FSMA) an die ZCB weitergeleitet.

1.18. Fallen kritische Infrastrukturen (oder kritische Einrichtungen, die im Rahmen der CER-Richtlinie identifiziert wurden) in den Anwendungsbereich des NIS2-Gesetzes?

Art. 9, 5° und 25, §2 NIS2-Gesetz

Ja, der Betreiber einer oder mehrerer kritischer Infrastrukturen, die im Rahmen des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (oder als kritische Einrichtungen im Sinne der Richtlinie 2022/2557 - CER-Richtlinie) identifiziert wurden, gilt als wesentliche Einrichtung im Sinne des NIS2-Gesetzes.

Die NIS2-Behörden und die nach dem Gesetz vom 1. Juli 2011 (und dem zukünftigen CER-Gesetz welches die CER-Richtlinie umsetzen wird) zuständigen Behörden arbeiten bei der Aufsicht über diese Einrichtungen zusammen.

Weitere Informationen zu kritischen Infrastrukturen finden Sie auf der Website des Nationalen Krisenzentrums.

1.19. Können NACE-Codes verwendet werden, um festzustellen, ob eine Einrichtung unter das NIS2-Gesetz fällt?

Beilagen I und II NIS2-Gesetz

Einige der in den Beilagen I und II aufgeführten Dienstleistungen beziehen sich tatsächlich auf NACE-Codes. Einrichtungen mit Sitz in Belgien, die unter diese NACE-Codes fallende Dienstleistungen erbringen, sollten daher sorgfältig prüfen, ob das NIS2-Gesetz auf sie anwendbar ist.

Für alle Einrichtungen, die nicht unter die oben genannten Möglichkeiten aus den Anhängen des NIS2-Gesetzes fallen, stellen die NACE-Codes **keine ausreichende Grundlage** dar um festzustellen ob eine Einrichtung unter das NIS2-Gesetze fällt. Einige NACE-Codes können von Einrichtungen zwar vorläufig verwendet werden, doch ist eine genauere Überprüfung ihrer genauen erbrachten Dienstleistungen erforderlich, um festzustellen, ob sie unter den oftmals restriktiveren Anwendungsbereich des NIS2-Gesetzes fallen oder nicht. Die Angabe eines bestimmten NACE-Codes in der Zentralen Datenbank der Unternehmen (ZDU) hat keine Auswirkungen auf den Anwendungsbereich für diese Arten von Einrichtungen.

1.20. Fallen Konformitätsbewertungsstellen in den Anwendungsbereich des Gesetzes?

Die Dienstleistungen, die normalerweise von Konformitätsbewertungsstellen (KBS/CABs) erbracht werden, sind als solche nicht in der Liste der Einrichtungen der Anhänge I und II des NIS2-Gesetzes enthalten. Dies hat zur Folge, dass CABs, die ihre Tätigkeit auf die

Konformitätsbewertung beschränken, nicht in den Anwendungsbereich des NIS2-Gesetzes fallen.

CABs, die zusätzlich Dienstleistungen erbringen, die in Anhang I oder II des NIS2-Gesetzes beschrieben sind, können jedoch in den Anwendungsbereich des Gesetzes fallen, wenn sie auch das Größenkriterium erfüllen, selbst wenn diese Dienstleistungen nur eine Nebenleistung zu ihrer Haupttätigkeit darstellen.

1.21. Mit welcher Methode kann man feststellen ob eine Organisation in den Anwendungsbereich des NIS2-Gesetzes fällt?

Die unten beschriebene Methode stellt die einzelnen Schritte der Überlegung im Zusammenhang mit dem Anwendungsbereich des NIS2-Gesetzes dar. Diese Methode erhebt jedoch keinen Anspruch auf Vollständigkeit oder als einzig anwendbare Methode.

Dieser Abschnitt behandelt die folgenden Punkte:

1. Vor des Prüfung des NIS2-Gesetzes:
    a. Betreibt meine Organisation eine kritische Infrastruktur im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (oder des künftigen CER-Gesetzes)?
    b. Fällt meine Organisation unter DORA?
2. Wie groß ist meine Organisation?
3. Welche Dienstleistung(en) erbringt meine Organisation in der Europäischen Union?
4. Wo in Europa ist meine Organisation ansässig?
5. Könnte meine Organisation später identifiziert werden oder befindet sie sich in der Lieferkette einer NIS2-Einrichtung?

Siehe hierzu auch unseren NIS2-Anwendungsbreichtest (NIS2 scope tool).

1.21.1. Vor der Prüfung des NIS2-Gesetzes

Bevor wir mit der eigentlichen Analyse beginnen, müssen wir uns zunächst mit zwei Möglichkeiten beschäftigen, die einen großen Einfluss darauf haben, wie der Anwendungsbereich des NIS2-Gesetzes für die betroffenen Organisationen funktioniert.

A. Betreibt meine Organisation eine kritische Infrastruktur im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (oder des künftigen CER-Gesetzes)?

Artikel 3, §4 des NIS2-Gesetzes besagt, dass das Gesetz automatisch für Einrichtungen gilt, die, unabhängig von ihrer Größe, im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (und in Zukunft für kritische Einrichtungen im Sinne der CER-Richtlinie) als Betreiber einer kritischen Infrastruktur identifiziert wurden.

Die Betreiber einer kritischen Infrastruktur müssen daher nicht analysieren, ob ihre Organisation in den Anwendungsbereich der NIS2-Richtlinie fällt oder nicht: Sie fallen unter das NIS2-Gesetz und werden automatisch als wesentliche Einrichtungen qualifiziert.

B. Fällt meine Organisation unter DORA?

Einrichtungen mit Sitz in Belgien, die unter die DORA-Verordnung fallen, sind von den wesentlichen Anforderungen des NIS2-Gesetzes ausgenommen.

Siehe Abschnitt 1.17.

1.21.2. Ist meine Organisation eine "Einrichtung" (Unternehmensgruppe)?

Damit das Gesetz anwendbar ist, muss eine Organisation als "Einrichtung" gemäß Artikel 8, 37° des NIS2-Gesetzes qualifiziert sein: "*eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann*".

Dieses Element ist besonders wichtig für größere Organisationen oder Unternehmensgruppen, bei denen Niederlassungen in anderen Mitgliedstaaten, wie z. B. Zweigniederlassungen, möglicherweise nicht in der Lage sind, unter eigenem Namen zu handeln oder Rechte auszuüben und Verpflichtungen einzugehen. In einem solchen Fall würde das NIS2-Gesetz für das Unternehmen gelten, das die Rechtspersönlichkeit der Zweigniederlassung besitzt.

1.21.3. Wie groß ist meine Organisation?

Um in den Anwendungsbereich des NIS2-Gesetzes zu fallen, muss eine Einrichtung eine bestimmte Größe haben. Um diese Größe zu berechnen, bezieht sich das NIS2-Gesetz auf die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Diese Empfehlung legt die Schwellenwerte fest, ab denen ein Unternehmen (jede Einrichtung, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform) als kleines, mittleres oder großes Unternehmen eingestuft werden kann. Außer in Ausnahmefällen fallen nur mittlere und große Unternehmen in den Anwendungsbereich des NIS2-Gesetzes.

Zur Feststellung der Größe sind zwei Bedingungen zu prüfen: die Mitarbeiterzahl (gemessen in Jahresarbeitseinheiten (JAE)[1]) und die finanziellen Beträge (Jahresumsatz und/oder Jahresbilanzsumme).

Die Mitarbeiterzahl muss mit den finanziellen Beträgen kombiniert werden, um die Unternehmensgröße zu ermitteln: Ein Unternehmen kann sich dafür entscheiden, entweder die Umsatzobergrenze oder die Bilanzsummengrenze einzuhalten. Es **kann eine der finanziellen Obergrenzen überschreiten, ohne dass dies Auswirkungen auf seinen Status als KMU hat**. Grundsätzlich **berücksichtigen wir daher nur den niedrigeren der beiden** Beträge.

Beispiel 1: Ein Unternehmen mit 35 JAE (klein) hat einen Jahresumsatz von 1.000.000 € (klein) und eine Jahresbilanzsumme von 50.000.000 € (groß). Bei den finanziellen Beträgen entscheidet sie

[1] Die Jahresarbeitseinheiten (JAE) entsprechen der Anzahl der Personen, die in dem betreffenden Unternehmen oder für dieses Unternehmen während des gesamten Jahres vollzeitlich gearbeitet haben. Die Arbeit von Personen, die nicht das ganze Jahr über gearbeitet haben, oder die Teilzeitarbeit, unabhängig von der Dauer der Teilzeitarbeit, oder Saisonarbeit wird als Bruchteil einer JAE gezählt.

sich dafür, nur den niedrigsten zu berücksichtigen: ihren Umsatz. Es handelt sich also um ein Klein- oder Kleinstunternehmen.

Beispiel 2: Ein Unternehmen mit 80 JAE (mittelgroß) hat einen Jahresumsatz von 1.000.000 € (klein) und eine Jahresbilanzsumme von 70.000.000 € (groß). Bei den finanziellen Beträgen entscheidet sie sich dafür, nur den kleinsten zu berücksichtigen: ihren Umsatz. Da der Umsatz klein, die Mitarbeiterzahl aber mittelgroß ist, handelt es sich um ein mittelgroßes Unternehmen.

Eine visuelle Zusammenfassung der möglichen Unternehmensgrößen finden Sie auf unserer Website.

Wenn wir die verschiedenen möglichen Größen mit dem Dienstleistungskriterium kombinieren, ergibt sich folgender Anwendungsbereich:

- Ein mittleres Unternehmen beschäftigt zwischen 50 und 249 JAE oder hat einen Jahresumsatz/eine Jahresbilanzsumme von mehr als 10 Millionen EUR:
  - ➔ Fällt als "wichtige Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage II des Gesetzes aufgeführte Dienstleistung erbringt.
  - ➔ Fällt **grundsätzlich** als "wichtige Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage I des Gesetzes aufgeführte Dienstleistung erbring.
- Ein großes Unternehmen beschäftigt mindestens 250 JAE oder hat einen Jahresumsatz von mehr als 50 Mio. EUR und eine Jahresbilanzsumme von mehr als 43 Mio. EUR:
  - ➔ Fällt als "wesentliche Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage II des Gesetzes aufgeführte Dienstleistung erbring.
  - ➔ Fällt **grundsätzlich** als "wesentliche Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage I des Gesetzes aufgeführte Dienstleistung erbring.

Die Empfehlung sieht insbesondere vor, dass bei Einrichtungen, die als "verbundene Unternehmen" oder "Partnerunternehmen" gruppiert sind, je nach den festgelegten Kriterien die Daten (Mitarbeiterzahl & Finanzbeträge) der anderen Einrichtungen, die Teil der Gruppe von Einrichtungen sind, bei der Berechnung der Größe berücksichtigt werden (siehe auch Abschnitt 1.5.).

Für weitere Informationen zur Anwendung der Empfehlung empfehlen wir dringend, den Benutzerleitfaden für die Definition von KMU der Kommission zu konsultieren. Er enthält alle Kriterien und visuelle Beispiele, die Ihnen bei der Anwendung der Empfehlung helfen sollen. Die Kommission hat außerdem ein Tool entwickelt, mit dem Sie die Größe Ihrer Organisation testen können.

Es gibt jedoch einige **Ausnahmen**. Die folgenden Arten der Einrichtungen fallen unabhängig von ihrer Größe in den Anwendungsbereich des NIS2-Gesetzes:

- Qualifizierte Vertrauensdiensteanbieter (wichtig);
- Nicht qualifizierte Vertrauensdiensteanbieter (wichtig, wenn es sich um ein Kleinst-, kleines oder mittlere Unternehmen handelt, und wesentlich, wenn es sich um ein großes Unternehmen handelt);
- DNS-Dienstanbieter (wesentlich);
- TLD-Namensregistrierung (wesentlich);
- Einrichtungen, die Domänennamenregistrierungsdienste erbringen (nur für die Registrierungspflicht);
- Anbieter öffentlicher elektronischer Kommunikationsnetze (wesentlich);

- Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten (wesentlich);
- Einrichtungen, die als Betreiber kritischer Infrastrukturen gemäß dem Gesetz vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (wesentlich) identifiziert wurden;
- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen (wesentlich);

Im folgenden Abschnitt wird erläutert, wie man die Definitionen der von diesen Arten von Einrichtungen erbrachten Dienstleistungen finden kann.

1.21.4. Welche Dienstleistung(en) erbringt meine Organisation in der Europäischen Union?

Sobald die Größe einer Einrichtung bekannt ist, muss als nächstes eine detaillierte Analyse aller Dienstleistungen, die die Einrichtung für Dritte erbringt, nach Sektoren oder Teilsektoren durchgeführt werden. Es ist wichtig, eine Topographie jeder Dienstleistung zu erstellen, selbst wenn diese nur eine Nebentätigkeit der Einrichtung darstellt (es sei denn, die Definition der Dienstleistung berücksichtigt ob die betreffende Dienstleistung eine Haupt- oder Nebentätigkeit ist).

In den Beilagen I und II (oder den Definitionen) des NIS2-Gesetzes werden die betreffenden Dienste ("Art der Einrichtung") im Einzelnen aufgeführt, häufig mit einem Verweis auf die entsprechenden europäischen Rechtsvorschriften oder die in Artikel 8 des Gesetzes vorgesehenen Definitionen.

Die verschiedenen Sektoren und Teilsektoren sind wie folgt:

Sektoren mit hoher Kritikalität (Beilage I)	Sonstige kritische Sektoren (Beilage II)
1. Energie a. Elektrizität b. Fernwärme und Fernkälte c. Erdöl d. Erdgas e. Wasserstoff 2. Verkehr a. Luftverkehr b. Schienenverkehr c. Schiffsfahrt d. Straßenverkehr 3. Bankwesen 4. Finanzmarktinfrastrukturen 5. Gesundheitswesen 6. Trinkwasser 7. Abwasser 8. Digitale Infrastruktur 9. Verwaltung von IKT-Diensten (B2B) 10. Öffentliche Verwaltung 11. Weltraum	1. Post- und Kurierdienste 2. Abfallbewirtschaftung 3. Produktion, Herstellung und Handel mit chemischen Stoffen 4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln 5. Verarbeitendes Gewerbe/Herstellung von Waren a. Herstellung von Medizinprodukten und In-vitro-Diagnostika b. Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen c. Herstellung von elektrischen Ausrüstungen d. Maschinenbau e. Herstellung von Kraftwagen und Kraftwagenteilen f. Sonstiger Fahrzeugbau 6. Anbieter Digitaler Dienste 7. Forschung

Es geht also darum, die von der Organisation erbrachten Dienstleistungen mit den oben genannten Definitionen aus den Beilagen in Verbindung zu bringen. Die Bedingung der erbrachten Dienstleistung ist dann erfüllt, wenn die beiden übereinstimmen. Es ist durchaus möglich, dass eine Organisation mehrere Dienstleistungen erbringt, die in verschiedenen Sektoren aufgelistet sind (siehe hierzu Abschnitt 1.10.).

Zusammenfassend sind die "wichtigen" und "wesentlichen" Einrichtungen die folgenden (mit Ausnahme der am Ende des Abschnitts 1.21.3. aufgelisteten Arten von Einrichtungen):

	Mittleres Unternehmen	**Großes Unternehmen**
Dienstleistungen in Beilage I	Wichtig	Wesentlich
Dienstleistungen in Beilage II	Wichtig	Wichtig

1.21.5. Die Niederlassung

Grundsätzlich gilt das belgische NIS2-Gesetz für Einrichtungen, die **in Belgien niedergelassen sind und in der EU ihre Dienstleistungen erbringen oder ihre Geschäfte betreiben**.

Der Begriff der Niederlassung setzt lediglich die tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus, unabhängig davon, welche Rechtsform gewählt wird.

Je nach Art der Einrichtung gibt es jedoch einige Ausnahmen von der Regel, dass Einrichtungen in Belgien ansässig sein müssen. Die Regeln für den territorialen Anwendungsbereich/die Zuständigkeit des belgischen NIS2-Gesetzes werden in Abschnitt 1.14 erläutert.

1.21.6. Zusätzliche Identifizierung und Lieferkette

Ungeachtet der oben genannten Regeln hat das ZCB die Möglichkeit, bei Bedarf bestimmte Einrichtungen, die in Belgien ansässig und in den in den Beilagen zum NIS2-Gesetz aufgeführten Sektoren tätig sind, zu identifizieren. Diese zusätzliche Identifizierung erfolgt in Absprache mit der betroffenen Organisation - siehe Abschnitt 1.12 "Identifizierung".

Unabhängig vom Anwendungsbereich des NIS2-Gesetzes ist zu berücksichtigen, dass eine große Anzahl von Organisationen indirekt von den neuen gesetzlichen Anforderungen betroffen sein wird, wenn sie sich in der Lieferkette einer oder mehrerer NIS2-Einrichtungen befinden. Letztere sind verpflichtet, die Sicherheit ihrer eigenen Lieferkette zu gewährleisten, und können daher ihren unmittelbaren Anbietern oder Dienstanbietern vertraglich Verpflichtungen auferlegen. Weitere Erläuterungen dazu finden Sie in Abschnitt 3.14.

1.22. Spezifische Fragen in Bezug auf bestimmte Arten von Einrichtungen und Sektoren

1.22.1. Anhang I - 1. Energie - (a) Elektrizität

1.22.1.1. Fallen Organisationen, die Strom hauptsächlich für den Eigenverbrauch erzeugen (einschließlich PV-Anlagen usw.), in den Anwendungsbereich des Gesetzes?

Anhang I NIS2-Gesetz & Richtlinie (EU) 2019/944

Gemäß Artikel 3 in Verbindung mit Anhang I, Punkt (1)(a) Bindestrich 4 des NIS2-Gesetzes fallen "Erzeuger im Sinne von Artikel 2, Punkt (38), der Richtlinie (EU) 2019/944" in den Anwendungsbereich, wenn sie als mittlere Unternehmen gemäß Artikel 2 des Anhangs der Empfehlung 2003/361/EG gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten.

In Artikel 2 Nummer 38 der Richtlinie (EU) 2019/944 wird der Begriff **"Erzeuger"** definiert als "eine natürliche oder juristische Person, die Strom erzeugt", während der Begriff **"Erzeugung"** gemäß Artikel 2 Nummer 37 der Richtlinie (EU) 2019/944 als "die Erzeugung von Strom" definiert wird.

Nach diesen Definitionen gelten Einrichtungen, die an das Stromnetz angeschlossene PV- oder Windkraftanlagen betreiben, auch wenn sie den selbst erzeugten Strom überwiegend selbst verbrauchen, als Erzeuger im Sinne von Artikel 2 Nummer 38 der Richtlinie (EU) 2019/944 und fallen somit in den Anwendungsbereich von NIS2, wenn sie mindestens ein mittlergroßes Unternehmen sind.

Auf EU-Ebene hat man sich jedoch darauf geeinigt, dass es sich bei diesen "Erzeugern" nicht um die hochkritischen Einrichtungen handelt, auf die die NIS2-Richtlinie für den Teilsektor Elektrizität abzielt. Daher kann auf sie eine weniger strenge Aufsicht angewandt werden.

In Belgien behalten Einrichtungen, die unter die Definition einer Dienstleistung im Teilsektor Elektrizität fallen, **nur** weil sie hauptsächlich Strom für den **Eigenverbrauch** erzeugen, ihre NIS2-Qualifikation (wesentlich oder wichtig), sind aber einer weniger strengen Aufsicht verpflichtet. In der Praxis müssen sie sich nach wie vor registrieren, erhebliche Sicherheitsvorfälle melden und Cybersicherheitsmaßnahmen ergreifen, aber die Verwendung einer **niedrigeren Sicherheitsstufe des CyberFundamentals (CyFun®) Framework** (z. B. Basic) zur Erfüllung ihrer Pflichten wird als verhältnismäßig angesehen. Diese Lösung berücksichtigt die eher begrenzten gesellschaftlichen und wirtschaftlichen Auswirkungen ihrer Stromerzeugung.

1.22.1.2. Was fällt unter "Betreiber von Ladepunkten"?

In Anhang I, Teilsektor Elektrizität des NIS2-Gesetzes ist die Rede von "Betreiber[n] von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters". Da keine weiteren Definitionen vorliegen, sind die Wörter in ihrer üblichen Bedeutung zu verstehen.

Die Definition beinhaltet die folgenden Bedingungen:

1) Ein Betreiber eines Ladepunkts
2) Zuständig für die Verwaltung und den Betrieb des genannten Ladepunkts

3) Die Aufladung erfolgt für Endnutzer (auch im Namen und Auftrag eines Mobilitätsdienstleisters)

Wenn beispielsweise ein Supermarkt auf seinem Parkplatz Ladepunkte aufstellt, kann er unter NIS2 fallen, wenn er für die Verwaltung und den Betrieb der Ladestation zuständig ist. Diese Verwaltung und der Betrieb werden häufig vertraglich an eine dritte Organisation delegiert, auch wenn die Ladestationen mit dem Namen des Supermarktes gelabelt sind. Eine Organisation muss also konkret prüfen, ob sie eine Ladestation selbst verwaltet und betreibt oder ob diese Dienstleistung einer dritten Organisation überlassen wird.

1.22.2. Anhang I - 1. Energie - (c) Erdöl

1.22.2.1. Was fällt unter den Begriff "Betreiber von Erdöl-Fernleitungen"?

Das NIS2-Gesetz und sein Anhang enthalten keine Definition des Begriffs "Betreiber von Erdöl-Fernleitungen". Der Begriff ist daher in seiner üblichen Bedeutung zu verstehen.

1.22.3. Anhang I - 2. Verkehr

Der Sektor Verkehr umfasst mehrere Teilsektoren und Arten von Einrichtungen:

a) Luft:
    a. Luftfahrtunternehmen
    b. Flughafenleitungsorgane
    c. Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
b) Schienenverkehr:
    a. Infrastrukturbetreiber
    b. Eisenbahnunternehmen
c) Schifffahrt:
    a. Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt
    b. Leitungsorgane von Häfen
    c. Betreiber von Schiffsverkehrsdiensten
d) Straßenverkehr:
    a. Straßenverkehrsbehörden
    b. Betreiber intelligenter Verkehrssysteme

1.22.4. Anhang I - 5. Gesundheitswesen

Der Sektor Gesundheitswesen umfasst mehrere Arten von Einrichtungen:

- Gesundheitsdienstleister
- EU-Referenzlaboratorien
- Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben
- Einrichtungen, die pharmazeutische Erzeugnisse herstellen
- Einrichtungen, die Medizinprodukte herstellen, die im Falle einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden

1.22.4.1. Welche Organisationen fallen unter die Definition eines Gesundheitsdienstleisters (Krankenhäuser, Altenheime, häusliche Pflege, usw.)?

Gesundheitsdienstleister in Anhang I, 5. Gesundheitswesen, beziehen sich auf Gesundheitsdienstleister gemäß der Definition in Artikel 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates und sind definiert als: "jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt."

Um festzustellen, ob eine Organisation unter die Definition des Gesundheitsdienstleisters fällt, sollte geprüft werden, ob diese Einrichtungen "Gesundheitsversorgung" erbringen:

1) Gesundheitsversorgung wird in dieser Richtlinie definiert als "Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten". Dies könnte zum Beispiel die Verwendung von Spritzen, Injektionen usw. sein
2) Die Richtlinie definiert "Angehörige der Gesundheitsberufe" als "einen Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, einen Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt".

Jede betroffene Einrichtung sollte sich daher selbst vergewissern, ob es sich bei den von der Einrichtung durchgeführten Tätigkeiten um Gesundheitsdienstleistungen/Gesundheitsversorgung durch Angehörige der Gesundheitsberufe handelt oder ob diese Einrichtungen lediglich Pflegeleistungen erbringen.

Unter Gesundheitsdienstleistungen fallen zum Beispiel: Altenpflege, psychiatrische Pflege, Krankenhäuser, Rehabilitationszentren, Altenheime, stationäre Pflege, häusliche Krankenpflege, Zentren für ambulante Rehabilitation, Ärzte, Krankenschwestern, ... Einrichtungen, die Menschen mit Behinderungen betreuen, und gewöhnliche/spezialisierte Bildungseinrichtungen können ebenfalls darunter fallen, wenn in diesen Einrichtungen auch Tätigkeiten im Zusammenhang mit der Gesundheitsversorgung angeboten werden.

Einrichtungen, die in der Regel keine Gesundheitsdienstleistungen erbringen, sind z. B.: häusliche Pflege (nur Hausarbeit wird geleistet), Kinderbetreuung, ...

Es ist wichtig, dass jede Organisation ihre eigenen Aktivitäten in der Praxis analysiert, um zu überprüfen, ob sie Gesundheitsdienstleistungen erbringt. Wie bereits erwähnt, müssen alle Tätigkeiten einer Einrichtung berücksichtigt werden, um festzustellen, ob eine Einrichtung eine NIS2-Einrichtung ist. Auch Nebentätigkeiten können dazu führen, dass eine Einrichtung unter NIS2 fällt, nicht nur ihre Haupttätigkeit. Wichtig ist auch, dass eine Einrichtung, die eine NIS2-Tätigkeit ausübt und das Größenkriterium erfüllt, dem NIS2-Gesetz als Ganzes (für alle ihre Netzwerke und Informationssysteme) verpflichtet ist.

1.22.4.2. Was ist der Unterschied zwischen "Pflege" und "Gesundheitsversorgung"?

Gesundheitsversorgung bedeutet Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten.

Der Begriff "Pflege" ist breiter gefasst und kann z. B. auch Kinderbetreuung, häusliche Pflegeaktivitäten, usw. umfassen.

1.22.4.3. Müssen Altenheime denselben Verpflichtungen nachkommen wie andere Gesundheitsdienstleister?

Altenheime fallen unter die Definition eines Gesundheitsdienstleisters (siehe Abschnitt 1.22.4.1). Sie sind daher, wenn sie die Größenkriterien erfüllen und in Belgien ansässig sind, entweder eine wesentliche Einrichtung oder eine wichtige Einrichtung im Sinne des NIS2-Gesetzes.

Auf EU-Ebene hat man sich jedoch darauf geeinigt, dass diese "Gesundheitsdienstleister" nicht zu den hochkritischen Einrichtungen gehören, auf die die NIS2-Richtlinie im Gesundheitssektor abzielt. Daher kann auf sie eine weniger strenge Aufsicht angewandt werden.

In Belgien behalten Einrichtungen, die unter die Definition eines Gesundheitsdienstleisters fallen, **nur** weil sie ein **Altersheim** haben, ihre NIS2-Qualifikation (wesentlich oder wichtig), sind aber einer weniger strengen Aufsicht verpflichtet. In der Praxis müssen sie sich nach wie vor registrieren, erhebliche Sicherheitsvorfälle melden und Cybersicherheitsmaßnahmen ergreifen, aber die Verwendung einer **niedrigeren Sicherheitsstufe des CyberFundamentals (CyFun®) Framework** (z. B. Basic) zur Erfüllung ihrer Pflichten wird als verhältnismäßig angesehen. Diese Lösung berücksichtigt die eher begrenzten gesellschaftlichen und wirtschaftlichen Auswirkungen ihrer Gesundheitsdienste.

1.22.4.4. Was ist, wenn meine Organisation keine eigenen medizinischen Fachkräfte beschäftigt?

Im Rahmen von NIS2 muss eine Organisation einen NIS2-Dienst selbst erbringen, um in den Anwendungsbereich zu fallen. Dies bedeutet, dass Organisationen, die kein eigenes medizinisches Fachpersonal beschäftigen, sondern Dritte mit der Erbringung der Gesundheitsdienstleistung beauftragen, nicht als Gesundheitsdienstleister in den Anwendungsbereich fallen würden.

1.22.4.5. Fallen Einrichtungen, die Medizinprodukte herstellen, unter das NIS2-Gesetz?

Einrichtungen, die Medizinprodukte herstellen, die bei einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden (Liste der kritischen Produkte für Notlagen im Bereich der öffentlichen Gesundheit), fallen im Sinne von Artikel 22 der Verordnung (EU) 2022/123 unter Anhang I, Sektor 5. Gesundheit des NIS2-Gesetzes.

Diese Verordnung bezieht sich auf eine Liste, die von der Exekutiv-Lenkungsgruppe für Arzneimittelknappheit und Arzneimittelsicherheit in Notfällen zu erstellen ist. Sie bezieht sich auf Kategorien von Medizinprodukten, die im Zusammenhang mit einer Notlage im Bereich der

öffentlichen Gesundheit als kritisch angesehen werden. Derzeit ist noch keine solche Liste verfügbar.

Einrichtungen, die Medizinprodukte herstellen, können auch unter Anhang II, Sektor 5, Teilsektor a) Herstellung von Medizinprodukten und In-vitro-Diagnostika fallen. Weitere Informationen zu diesem Teilsektor finden Sie im Abschnitt 1.22.11).

Darüber hinaus werden die meisten Einrichtungen, die Medizinprodukte herstellen, in die Lieferkette von NIS2-Einrichtungen fallen (z. B. Gesundheitsdienstleister aus Anhang I, Sektor 5). Einrichtungen, die unter das NIS2-Gesetz fallen, müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um ihre Netzwerk- und Informationssysteme zu sichern. Eine dieser Maßnahmen ist die Sicherheit der Lieferkette, einschließlich sicherheitsrelevanter Aspekte in den Beziehungen zwischen jeder Einrichtung und ihren direkten Lieferanten oder Dienstleistern. Weitere Informationen zu den Verpflichtungen in der Lieferkette finden Sie im Abschnitt 3.14.

1.22.4.6. Fallen Apotheken unter NIS2?

Apotheken können potenziell in mehrere Sektoren fallen, vor allem im Gesundheitssektor.

Betrachtet man erstens die Definition eines Gesundheitsdienstleisters, wie im Abschnitt 1.22.4.1 erläutert, können Apotheker in Belgien in bestimmten Situationen Injektionen und Impfstoffe verabreichen. Diese Handlungen können als Gesundheitsdienstleistungen betrachtet werden, wodurch die betreffenden Apotheken in den Anwendungsbereich von NIS2 fallen. Hier hängt also alles davon ab, ob der Apotheker Gesundheitsdienstleistungen erbringt oder nicht.

Zweitens könnten Apotheken theoretisch "Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben" sein, wenn sie ihre eigenen pharmazeutischen Produkte erforschen und entwickeln (siehe Abschnitt 1.22.4.7, Punkt A.). Diese FuE/R&D-Tätigkeiten sind jedoch zumeist Unternehmen vorbehalten, die sich auf die pharmazeutische Forschung spezialisiert haben.

Drittens könnten Apotheken auch "Einrichtungen zur Herstellung von pharmazeutischen Grundstoffen und pharmazeutischen Zubereitungen im Sinne von Abschnitt C, Abteilung 21 der NACE Rev. 2" sein (siehe Abschnitt 1.22.4.7, Punkt B.), wenn sie den erforderlichen NACE-Code haben.

Viertens könnten Apotheken durch die Herstellung von Erzeugnissen oder den Vertrieb von Stoffen oder Gemischen in Anhang II, Sektor 3., Produktion, Herstellung und Handel mit chemischen Stoffen fallen. Für weitere Informationen siehe Abschnitt 1.22.9.

Schließlich könnten Apotheken theoretisch unter Anhang II, Sektor 5. Verarbeitendes Gewerbe fallen, wenn sie medizinische Geräte herstellen. Für weitere Informationen siehe Abschnitt 1.22.11.1.

Als Apotheke müssen diese fünf verschiedenen Möglichkeiten analysiert werden, um festzustellen, ob sie unter NIS2 fallen oder nicht. Beachten Sie, dass eine Apotheke für diese fünf Möglichkeiten mindestens ein mittleres Unternehmen sein muss (siehe Abschnitt 1.5).

1.22.4.7. Fallen auch andere gesundheitsbezogene Unternehmen oder Unternehmen der pharmazeutischen Lieferkette unter NIS2?

A. Einrichtungen, die Forschungs- und Entwicklungstätigkeiten für Arzneimittel durchführen

Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne von Artikel 1 Nummer 2 der Richtlinie 2001/83/EG ausüben, fallen unter Anhang I, Sektor Gesundheitswesen. Dies sind Einrichtungen, die Forschungs- und Entwicklungstätigkeiten durchführen von:

> *"a) Alle Stoffe oder Stoffzusammensetzungen, die als Mittel mit Eigenschaften zur Heilung oder zur Verhütung menschlicher Krankheiten bestimmt sind, oder;*
>
> *b) alle Stoffe oder Stoffzusammensetzungen, die im oder am menschlichen Körper verwendet oder einem Menschen verabreicht werden können, um entweder die menschlichen physiologischen Funktionen durch eine pharmakologische, immunologische oder metabolische Wirkung wiederherzustellen, zu korrigieren oder zu beeinflussen oder eine medizinische Diagnose zu erstellen".*

Es ist wichtig zu beachten, dass Forschungseinrichtungen auch unter Anhang II, Sektor 7. Forschung fallen können. Für weitere Informationen siehe Abschnitt 1.22.12.

B. Einrichtungen, die pharmazeutische Erzeugnisse herstellen

Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen, fallen unter Anhang I, Sektor Gesundheitswesen. Diese Einrichtungen haben folgende NACE-Codes:

- 21.10 Herstellung von pharmazeutischen Grundstoffen
- 21.20 Herstellung von pharmazeutischen Erzeugnissen

Der NACE-Code einer belgischen Organisation kann zum Beispiel auf der Website der Zentralen Datenbank der Unternehmen überprüft werden.

C. Einrichtungen, die chemische Stoffe produzieren, herstellen und handeln

Diese Einrichtungen fallen unter den Chemiesektor von Anhang II. Weitere Informationen finden Sie im Abschnitt 1.22.9.

D. Pharmazeutische Großhändler (Verkauf von pharmazeutischen Produkten)

Der Verkauf von pharmazeutischen Produkten an Verbraucher oder Unternehmen ist in den Anhängen des NIS2-Gesetzes nicht ausdrücklich vorgesehen. Sie könnten jedoch unter den Vertrieb von Chemikalien fallen, wenn die Kriterien und Definitionen erfüllt sind, wie im Abschnitt 1.22.9.2 erläutert.

E. Kurierdienste für Arzneimittel

Kurierdienste für Arzneimittel fallen nicht unter Anhang I, Sektor 5. Gesundheitswesen. In bestimmten Fällen können sie jedoch unter den Sektor 1. Post- und Kurierdienste in Anhang II fallen.

Weitere Informationen finden Sie im Abschnitt 1.22.8.

F. Sozialversicherungskassen

Sozialversicherungskassen sind in den Anhängen des NIS2-Gesetzes nicht ausdrücklich genannt. Wenn es sich um private Einrichtungen handelt, die ausschließlich diese Dienstleistung erbringen, fallen sie nicht in den Anwendungsbereich von NIS2.

Öffentliche Sozialversicherungskassen könnten jedoch in den Sektor Öffentliche Verwaltung von Anhang I fallen, wenn die unterschiedlichen Kriterien erfüllt werden. Für weitere Informationen siehe Abschnitt 2.1.

G. Anbieter von gesundheitsbezogener Software

Wie bei den Anbietern anderer Software müssen die Definitionen von Anbietern von Cloud-Computing-Diensten und verwalteter Dienste analysiert werden. Weitere Informationen finden Sie in den Abschnitten 1.22.6.1 bzw. 1.22.7. Darüber hinaus können auch Anbieter gesundheitsbezogener Software unter die Lieferkettenverpflichtungen fallen (weitere Informationen in Abschnitt 3.14).

H. Netzwerke für Gesundheitsdaten (eHealth)

Anbieter von Netzwerken für Gesundheitsdaten (wie CoZo, Réseau de Santé Wallon oder Réseau de Santé Bruxellois) fallen nicht unter die Definitionen des Gesundheitssektors in Anhang I.

Diese Arten von Einrichtungen könnten jedoch unter die Definitionen in den Bereichen der digitalen Infrastruktur fallen, beispielsweise als Anbieter von Rechenzentrumsdiensten, Anbieter von Cloud-Computing-Diensten oder Anbieter von verwalteten Diensten. Dazu müssen sie mindestens ein mittleres Unternehmen sein. Diese Arten von Einrichtungen müssen daher prüfen, ob ihre Tätigkeiten den Definitionen aus diesem Sektor entsprechen. Für weitere Informationen siehe die Abschnitte 1.22.6 und 1.22.7 unten.

Ob sie auch in den Bereich der öffentlichen Verwaltung fallen können, hängt von ihrer Rechtsform ab. Am wichtigsten ist, dass es sich um öffentlich-rechtliche Einrichtungen handeln muss. Weitere Informationen finden Sie im Abschnitt 2.1.

1.22.5. Anhang I - 6. Trinkwasser

1.22.5.1. Welche Organisationen gelten als "Lieferanten von und Unternehmen der Versorgung mit Wasser für den menschlichen Gebrauch"?

Der Begriff "Wasser für den menschlichen Gebrauch" ist in Artikel 2, (1) der Richtlinie (EU) 2020/2184 definiert. Es umfasst:

"a) alles Wasser, sei es im ursprünglichen Zustand oder nach Aufbereitung, das sowohl in öffentlichen als auch in privaten Örtlichkeiten zum Trinken, zum Kochen, zur Zubereitung von Speisen oder zu anderen häuslichen Zwecken bestimmt ist, und zwar ungeachtet seiner Herkunft und ungeachtet dessen, ob es aus einem Verteilungsnetz oder in Tankfahrzeugen bereitgestellt oder in Flaschen oder andere Behältnisse abgefüllt wird, einschließlich Quellwasser;
(b) alles Wasser, das in einem Lebensmittelunternehmen für die Herstellung, Behandlung, Konservierung oder zum Inverkehrbringen von für den menschlichen Gebrauch bestimmten Erzeugnissen oder Substanzen verwendet wird;".

Der Anhang des NIS2-Gesetzes fügt hinzu, dass Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung

anderer Rohstoffe und Güter ist, ausgeschlossen sind. Das Wort "wesentlich" könnte wie folgt interpretiert werden: Die Verteilung von Wasser wäre "wesentlich", wenn der Lieferant seine Tätigkeit ohne die Lieferung von Wasser für den menschlichen Gebrauch nicht effektiv fortsetzen könnte.

Beispiele für Organisationen, die unter diese Definition fallen, sind Unternehmen, die (in Flaschen abgefülltes) Wasser verkaufen, und die nicht in der Lage wären, ihre operationellen Tätigkeiten fortzusetzen, wenn der Verkauf dieses Wassers eingestellt würde. Siehe auch Abschnitt 1.22.10 über die Herstellung und den Vertrieb von Lebensmitteln.

1.22.6. Anhang I - 8. Digitale Infrastruktur

1.22.6.1. Was genau ist ein Anbieter von Cloud-Computing-Diensten?

Art. 8 NIS2-Gesetz; Erwägungsgrund 33 NIS2-Richtlinie; NIS2-Folgenabschätzung

Artikel 8, 29° des NIS2-Gesetzes definiert einen Anbieter von Cloud Computing-Diensten als "einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind."

Erwägungsgrund 33 von NIS2-Richtlinie verdeutlicht dies weiter: *" Cloud-Computing-Dienste sollten digitale Dienste umfassen, die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind. Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste.*

- *Der Begriff „umfassender Fernzugang“ wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern.*
- *Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können.*
- *Der Begriff „elastischer Pool“ wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann.*
- *Der Begriff „gemeinsam nutzbar“ wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird.*
- *Der Begriff „verteilt“ wird verwendet, um Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.*

Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die

gemeinschaftliche, die öffentliche und die hybride Cloud umfassen. Die Cloud-Computing-Dienst- und Bereitstellungsmodelle haben dieselbe Bedeutung wie die in der Norm ISO/IEC 17788:2014 definierten Dienst- und Bereitstellungsmodelle. Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden."

In der Folgenabschätzung der NIS2-Richtlinie von 2020[2] nennt die Europäische Kommission Beispiele für Unternehmen, die als Anbieter von Cloud Computing-Diensten in Frage kommen. Anbieter von SaaS, IaaS und PaaS wurden ausdrücklich genannt:

- *SaaS: instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting*
- *IaaS: cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)*
- *PaaS: cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.*

Die Elemente der obigen Liste sind Beispiele und daher nicht erschöpfend.

Anbieter von Cloud-Computing-Diensten werden daher in einem weiten Sinne definiert und umfassen Anbieter von SaaS, IaaS und PaaS.

1.22.6.2. Was genau ist ein Anbieter von Rechenzentrumsdiensten?

Ein Anbieter von Rechenzentrumsdiensten wird in Artikel 8, 30° des NIS2-Gesetzes definiert als ein Anbieter von "einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden".

In Erwägungsgrund 35 von NIS2-Richtlinie heißt es dazu: *"Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die Sicherheit von Netz- und Informationssystemen zu begegnen, sollte die vorliegende Richtlinie daher für Anbieter von Rechenzentrumsdiensten gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. [...]*

[2] Arbeitsdokument der Kommissionsdienststellen. Folgenabschätzungsbericht zum Dokument "Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148", SWD (2020) 345 final, 16. Dezember 2020, Teil 2/3, online unter https://ec.europa.eu/newsroom/dae/redirection/document/72178, Seite 45.

Der Begriff „Rechenzentrumsdienst“ sollte nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden".

Die am Ende des Erwägungsgrunds genannte Ausnahme gilt nicht, wenn innerhalb einer Unternehmensgruppe eines der Unternehmen dieser Gruppe Rechenzentrumsdienste für ein anderes Unternehmen erbringt.

1.22.7. Anhang I - 9. Verwaltung von IKT-Diensten (B2B): Was genau ist ein Anbieter verwalteter Dienste (Helpdesk, B2B, etc.)?

Artikel 8, 38° des NIS2-Gesetzes definiert einen Anbieter verwalteter Dienste (Managed service provider - MSP) als: "eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt".

Es ist zu beachten, dass zwei Begriffe dieser Definition auch im NIS2-Gesetz oder anderen Rechtsinstrumenten definiert sind:

- "IKT-Produkt" ist ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems (Verordnung (EU) 2019/881, Artikel 2, (12));
- "Netzwerk- und Informationssysteme" bedeutet:
    a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1972;
    b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
    c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.

Die Definition des Begriffs "Anbieter verwalteter Dienste" ist relativ weit gefasst und umfasst drei verschiedene Bedingungen:

1) Entweder Installation, Verwaltung, Betrieb oder Wartung;
2) Entweder von IKT-Produkten, Netzen, Infrastrukturen, Anwendungen oder anderen Netz- und Informationssystemen;
3) Durch Unterstützung oder aktive Verwaltung (vor Ort oder aus der Ferne).

Diese 3 Bedingungen müssen alle kumulativ erfüllt sein, um unter die Definition zu fallen. Die in der Definition aufgeführten Tätigkeiten/Aufgaben schließen sich nicht gegenseitig aus. Mehrere von ihnen können von ein und derselben Einrichtung ausgeführt werden. Es gibt keine weiteren Bedingungen, die bei der Prüfung, ob eine Organisation ein Anbieter verwalteter Dienste ist, berücksichtigt werden müssen. Zum Beispiel muss die Bezeichnung "Anbieter verwalteter Dienste" nicht ausdrücklich in einem Vertrag verwendet werden.

Beispiele für einen Anbieter verwalteter Dienste sind:

- ein Helpdesk, das den Benutzern eines Netzwerks oder einer Anwendung operationelle Unterstützung per Fernwartung bietet;
- ein Softwareentwickler, der Fernunterstützung bei der Installation und/oder Wartung seiner Anwendungen anbietet;
- einen Wartungsdienst für die Netzwerke des Kunden und andere Tätigkeiten, die in den Räumlichkeiten des Kunden durchgeführt werden.

Neben der Definition ist der Begriff "Business-to-Business" in Anhang I des NIS2-Gesetzes so zu verstehen, dass er sich auf alle Beziehungen zwischen Dienstleistungserbringern und anderen Organisationen/Berufsgruppen (Unternehmen, Behörden, Handwerker, freie Berufe, Verbände, Einrichtungen in derselben Gruppe, usw.) bezieht, im Gegensatz zu Dienstleistungen, die für die Allgemeinheit/Privatpersonen erbracht werden ("Business-to-Customers"). Die Tatsache, dass eine Einrichtung keinen Gewinn erzielt oder keinen kommerziellen Nutzen hat, scheint kein Kriterium für den Ausschluss einer Einrichtung aus diesem Sektor zu sein.

Die Auslegung der Begriffe "Unterstützung" und "aktive Verwaltung" sind ebenfalls wichtig für die Definition eines Anbieters verwalteter Dienste. Wie bei der juristischen Interpretierung europäischer Texte üblich, müssen die Begriffe in ihrer üblichen Bedeutung verstanden werden, wenn es in dem betreffenden Rechtsinstrument keine Definition gibt.

Die Interpretation dieser beiden Begriffe könnte also wie folgt lauten:

- Der Begriff "Unterstützung" könnte sich auf die Bereitstellung von Hilfe beziehen. Im Zusammenhang mit einem MSP könnte dies bedeuten, dass man Kunden hilft, wenn sie Probleme haben oder Anleitung brauchen. Der Begriff wäre also eher reaktiv. Er könnte auch die Fehlersuche, bewährte Verfahren, Hilfe bei der Einrichtung und Konfiguration usw. umfassen.

- Bei der "aktiven Verwaltung" scheint das Konzept eher proaktiv zu sein. Im Zusammenhang mit einem MSP scheint die "Verwaltung" insbesondere die Verwaltung und Überwachung der Systeme, Anwendungen, Netzwerke usw. eines Kunden zu umfassen. Sie könnte auch die Systemüberwachung, die regelmäßige Wartung und Aktualisierung sowie allgemein die Gewährleistung des ordnungsgemäßen Betriebs der betreffenden Netz- und Informationssysteme umfassen, ohne dass der Kunde dies ausdrücklich fragt.

"Aus der Ferne" bedeutet einfach, dass die Tätigkeit nicht in den Räumlichkeiten des Kunden durchgeführt wird (sie könnte also in den Büros einer Organisation stattfinden).

1.22.8. Anhang II - 1. Post- und Kurierdienste: Fallen Kurierdienste und/oder die Verteilung von Medikamenten in diesen Bereich?

Dieser Sektor umfasst die Anbieter von Postdiensten gemäß der Definition in Artikel 2, Punkt (1a) der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten. Diese Richtlinie enthält mehrere Definitionen:

- Postdiensteanbieter: "Unternehmen, die einen oder mehrere Postdienste erbringen".
- Postdienste: "Dienste im Zusammenhang mit der Abholung, dem Sortieren, dem Transport und der Zustellung von Postsendungen"

Um herauszufinden, ob dies auch für Kurierdienste gilt, müssen wir uns auch das Gesetz vom 26. Januar 2018 über Postdienstleistungen (Postgesetz) ansehen. Dieses Gesetz enthält die folgenden Definitionen:

- Postsendung "eine Sendung, die in der endgültigen Form adressiert ist, an die sie vom Postdienstleister versandt werden soll, mit einem Gewicht von bis zu 31,5 kg".
- Postpaket oder Päckchen: "eine Postsendung, die Waren mit oder ohne Handelswert enthält, ausgenommen Briefsendungen, mit einem Gewicht von bis zu 31,5 kg;"

Die Zustellung eines Arzneimittels durch einen Kurier fällt in den Anwendungsbereich des Postgesetzes (und damit auch von NIS2), wenn es die gesetzlichen Kriterien erfüllt, was bei den Kriterien, die den Begriff des Postpakets definieren, häufig der Fall ist: Gewicht weniger als 31.5 kg, ein Produkt, das nicht durch Artikel 24, § 1, 6° des Königlichen Erlasses vom 14. März 2022 über Postdienste von den Postdiensten ausgeschlossen ist (es handelt sich nicht um ein Betäubungsmittel oder ein psychotropes Medikament wie Flunitrazepam, es ist kein gefälschtes Produkt, usw.), das Medikament muss verpackt sein, und die Verpackung muss die Adresse des Empfängers (oder einen Code zur Identifizierung des Ortes der Verteilung) tragen.

Die Zustellung von losen, nicht individualisierten Waren fällt nicht unter die Definition eines Postpakets, und diejenigen, die solche Zustellungen vornehmen, sind daher keine Postdiensteanbieter, die in diesen Bereich des NIS2-Gesetzes fallen.

1.22.9. Produktion, Herstellung und Handel mit chemischen Stoffen

Dieser Sektor umfasst "Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates, die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren".

1.22.9.1. Was ist mit "Stoffen" und "Gemischen" gemeint?

Art. 3, Punkte (1) & (2) REACH-Verordnung

Ein **Stoff** ist definiert als "*chemisches Element und seine Verbindungen in natürlicher Form oder gewonnen durch ein Herstellungsverfahren, einschließlich der zur Wahrung seiner Stabilität notwendigen Zusatzstoffe und der durch das angewandte Verfahren bedingten Verunreinigungen, aber mit Ausnahme von Lösungsmitteln, die von dem Stoff ohne Beeinträchtigung seiner Stabilität und ohne Änderung seiner Zusammensetzung abgetrennt werden können* ".

Ein **Gemisch** ist definiert als "*Gemenge, Gemische oder Lösungen, die aus zwei oder mehr Stoffen bestehen*".

Indem das NIS2-Gesetz auf Unternehmen Bezug nimmt, die im Sektor "Produktion, Herstellung und Handel mit chemischen Stoffen" **Stoffe** herstellen und mit **Stoffen** oder **Gemischen** handeln, scheint es sich auf alle chemischen Stoffe zu beziehen, unabhängig davon, ob es sich um potenziell gefährliche Industriechemikalien handelt oder ob sie in Produkten des täglichen Lebens verwendet werden.

1.22.9.2. Welche Arten von Einrichtungen fallen in den Anwendungsbereich von NIS2 als Unternehmen, die Stoffe herstellen und mit Stoffen oder Gemischen handeln?

Ein Hersteller im Sinne von REACH ist eine "*natürliche oder juristische Person mit Sitz in der Gemeinschaft, die in der Gemeinschaft einen Stoff herstellt*". Stoffe und Gemische sind so zu verstehen, wie im Abschnitt 1.22.9.1 erläutert.

Der Folgenabschätzungsbericht der NIS2-Richtlinie enthält qualitative Aspekte, die die Einbeziehung in den Anwendungsbereich des NIS-Rahmenwerks untermauern, und bezieht sich dabei auf gefährliche Chemikalien. Obwohl der Verweis auf gefährliche Chemikalien im Folgenabschätzungsbericht nicht im Rechtstext enthalten ist, scheint er darauf hinzuweisen, dass der Gesetzgeber nicht beabsichtigte, Unternehmen einzubeziehen, die irgendeine Art von chemischen Elementen herstellen oder vertreiben.

Es ist auch notwendig, die in der REACH-Verordnung festgelegte Registrierungspflicht zu berücksichtigen, da die Registrierungspflicht ein wichtiges Instrument zur Gewährleistung des Zwecks der REACH-Verordnung ist. Wie in den Erwägungsgründen (17)-(19) der REACH-Verordnung ausgeführt, sollten alle verfügbaren und relevanten Informationen über Stoffe als solche, in Zubereitungen und in Erzeugnissen gesammelt werden, um die Ermittlung gefährlicher Eigenschaften zu unterstützen, und Empfehlungen zu Risikomanagementmaßnahmen sollten systematisch über die Lieferketten weitergeleitet werden, soweit dies vernünftigerweise erforderlich ist, um schädliche Auswirkungen auf die menschliche Gesundheit und die Umwelt zu verhindern. Die Verantwortung für das Risikomanagement von Stoffen sollte bei den natürlichen oder juristischen Personen liegen, die diese Stoffe herstellen, einführen, in Verkehr bringen oder verwenden. Daher sollten die Registrierungsvorschriften die Hersteller und Importeure verpflichten, Daten über die von ihnen hergestellten oder eingeführten Stoffe zu generieren, diese Daten zur Bewertung der mit diesen Stoffen verbundenen Risiken zu verwenden und geeignete Maßnahmen für das Risikomanagement zu entwickeln und zu empfehlen. Um sicherzustellen, dass sie diesen Verpflichtungen tatsächlich nachkommen, sowie aus Gründen der Transparenz sollten sie bei der Registrierung verpflichtet werden, der Europäischen Chemikalienagentur ein Dossier mit all diesen Informationen vorzulegen. Registrierte Stoffe sollten auf dem Binnenmarkt in Verkehr gebracht werden dürfen.

Der Anwendungsbereich dieser Definition betrifft also in erster Linie Einrichtungen, die der Registrierungspflicht gemäß der REACH-Verordnung unterliegen.

Zwar könnten auch andere Organisationen, die nicht der Registrierungspflicht unterliegen, als Unternehmen eingestuft werden, die **Stoffe herstellen** und **mit Stoffen oder Gemischen** im Sinne von Artikel 3 Nummern 9 und 14 der REACH-Verordnung **handeln**, doch hat man sich auf EU-Ebene darauf geeinigt, dass diese Unternehmen nicht zu den kritischen Einrichtungen gehören, auf die die NIS2-Richtlinie im chemischen Sektor abzielt. Daher kann auf sie eine weniger strenge Aufsicht angewandt werden.

In Belgien bleiben Einrichtungen, die unter die Definition eines Herstellers fallen, sich aber nicht gemäß der REACH-Verordnung registriert müssen, NIS2-Einrichtungen (wesentliche oder wichtige Einrichtungen), unterliegen aber einer weniger strengen Aufsicht. In der Praxis müssen sie sich nach wie vor registrieren, erhebliche Sicherheitsvorfälle melden und Cybersicherheitsmaßnahmen anwenden, doch wird die Anwendung einer **niedrigeren Sicherheitsstufe des CyberFundamentals (CyFun®) Framework** (z. B. Basic) zur Erfüllung ihrer

Pflichten als verhältnismäßig angesehen. Diese Lösung berücksichtigt die eher begrenzten gesellschaftlichen und wirtschaftlichen Auswirkungen ihrer Dienstleistung.

1.22.9.3. Fällt ein Einzelhändler unter den Vertrieb von Stoffen oder Gemischen?

Gemäß Anhang II, Punkt (3) des NIS2-Gesetzes bezieht sich die Definition für den Begriff "Handel von Chemikalien" auf Artikel 3, Punkt (14) der Verordnung (EG) 1907/2006 (REACH-Verordnung).

Gemäß dieser Verordnung ist ein Händler eine „*natürliche oder juristische Person mit Sitz in der Gemeinschaft, die einen Stoff als solchen oder in einem Gemisch lediglich lagert und an Dritte in Verkehr bringt; darunter fallen auch Einzelhändler*". In Artikel 3 (12) der REACH-Verordnung wird der Begriff "Inverkehrbringen" definiert als "*entgeltliche oder unentgeltliche Abgabe an Dritte oder Bereitstellung für Dritte. Die Einfuhr gilt als Inverkehrbringen*", und es wird präzisiert, dass die Einfuhr als Inverkehrbringen gilt. Die Definition umfasst die Bereitstellung eines Produkts, unabhängig davon, ob das Produkt zum ersten Mal auf den Markt gebracht wird oder nicht.

Daher fällt ein Einzelhändler von chemischen Stoffen oder Gemischen unter diese Definition des Händlers (vorausgesetzt, dass die übrigen Elemente der Anwendbarkeit erfüllt sind).

1.22.9.4. Welche Arten von Einrichtungen fallen in den Anwendungsbereich von NIS2 als Unternehmen, die Erzeugnisse aus Stoffen oder Gemischen herstellen?

Unternehmen, die Erzeugnisse aus Stoffen oder Gemischen im Sinne von Artikel 3, Punkt (3) der Verordnung (EG) Nr. 1907/2006 (REACH-Verordnung) herstellen, fallen in den Anwendungsbereich des NIS2-Gesetzes, wenn sie als mittlere Unternehmen eingestuft sind oder die Schwellenwerte für mittlere Unternehmen überschreiten.

In Artikel 3, Punkt (4) der REACH-Verordnung wird der Begriff **"Produzent eines Erzeugnisses"** definiert als "*eine natürliche oder juristische Person, die ein Erzeugnis in der Gemeinschaft produziert oder zusammensetzt*". Eine Einrichtung ist also Produzent eines Erzeugnisses, wenn sie in der EU Erzeugnisse herstellt, unabhängig davon, wie das Erzeugnis produziert wird und ob es in Verkehr gebracht wird.

Für die Definition von Erzeugnissen verweist das NIS2-Gesetz auf Artikel 3, Punkt (3), der REACH-Verordnung. Gemäß Artikel 3, Punkt (3) der REACH-Verordnung ist ein **Erzeugnis** ein "*Gegenstand, der bei der Herstellung eine spezifische Form, Oberfläche oder Gestalt erhält, die in größerem Maße als die chemische Zusammensetzung seine Funktion bestimmt*". Beispiele für Erzeugnisse sind Kleidung, Bodenbeläge, Möbel, Schmuck, Zeitungen und Kunststoffverpackungen.

Bei der Auslegung der Frage, inwieweit **Produzent eines Erzeugnisses** in den Anwendungsbereich des NIS2-Gesetzes fallen, ist jedoch zu berücksichtigen, dass die erste Spalte von Anhang II Punkt (3) des NIS2-Gesetzes den Sektor als "Produktion, Herstellung und Handel mit chemischen Stoffen" definiert und damit den Anwendungsbereich der dritten Spalte von Anhang II Punkt (3) insofern einschränkt, als Chemikalien Gegenstand der Herstellungs-, Produktions- und Handelstätigkeit der in der dritten Spalte von Anhang II Punkt (3) genannten Einrichtungen sein sollten.

Darüber hinaus definiert das NIS2-Gesetz in Anhang II, Punkt (5) einen separaten Sektor für das verarbeitende Gewerbe, in dem es den Anwendungsbereich auf die Herstellung von Medizinprodukten, In-vitro-Diagnostika, Datenverarbeitungsgeräten, elektronischen Erzeugnissen, optischen Erzeugnissen, elektrischen Ausrüstungen, Maschinenbau, Kraftwagen, Kraftwagenteilen, und sonstigem Fahrzeugbau beschränkt. Da die Definition von Erzeugnissen im Rahmen der REACH-Verordnung sehr weit gefasst ist, würde die Spezifizierung des Anwendungsbereichs des Sektors "Verarbeitendes Gewerbe" gemäß Anhang II Nummer 5 ins Leere laufen, wenn jedes Unternehmen, das Erzeugnisse im Sinne von Artikel 3 Nummer 3 der REACH-Verordnung herstellt, als in den Anwendungsbereich von Anhang II Nummer 3 des NIS2-Gesetzes fallend betrachtet würde.

Daher sollten die in der dritten Spalte von Anhang II Nummer 3 genannten Arten von Einrichtungen, die in diesem Sektor als Unternehmen tätig sind, die Erzeugnisse im Sinne von Artikel 3 Nummer 3 der REACH-Verordnung aus Stoffen oder Gemischen herstellen, nicht Einrichtungen umfassen, die gemäß Anhang II Nummer 5 auch in den Anwendungsbereich des Sektors "Verarbeitendes Gewerbe" fallen.

Der Anwendungsbereich dieser Definition betrifft somit in erster Linie Einrichtungen, die gemäß der REACH-Verordnung der Pflicht zur Registrierung und Anmeldung von Stoffen in Erzeugnissen unterliegen.

In Bezug auf andere Einrichtungen, die nicht der Pflicht zur Registrierung und Anmeldung von Stoffen in Erzeugnissen unterliegen, die aber auch als Unternehmen eingestuft werden könnten, die Erzeugnisse aus Stoffen oder Gemischen herstellen, wurde auf EU-Ebene vereinbart, dass diese Unternehmen nicht zu den kritischen Einrichtungen gehören, auf die die NIS2-Richtlinie im chemischen Sektor abzielt. Daher kann auf sie eine weniger strenge Aufsicht angewandt werden.

In Belgien bleiben Einrichtungen, die unter die Definition eines Unternehmens fallen, das Erzeugnisse aus Stoffen oder Gemischen herstellt, aber nicht gemäß der REACH-Verordnung registriert werden müssen, NIS2-Einrichtungen (wesentliche oder wichtige Einrichtungen), unterliegen aber einer weniger strengen Aufsicht. In der Praxis müssen sie sich nach wie vor registrieren lassen, erhebliche Sicherheitsvorfälle melden und Cybersicherheitsmaßnahmen anwenden, aber die Verwendung einer **niedrigeren Sicherheitsstufe des CyberFundamentals (CyFun®) Framework** (z. B. Basic) zur Erfüllung ihrer Pflichten wird als verhältnismäßig angesehen. Diese Lösung trägt den eher begrenzten gesellschaftlichen und wirtschaftlichen Auswirkungen ihrer Dienste Rechnung.

1.22.10. Anhang II - 4. Herstellung, Verarbeitung und Vertrieb von Lebensmitteln

Dieser Sektor umfasst Lebensmittelunternehmen gemäß der Definition in Artikel 3 Absatz 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates, die im Großhandel und in der industriellen Produktion und Verarbeitung tätig sind. Ein Lebensmittelunternehmen ist definiert als "*alle Unternehmen, gleichgültig, ob sie auf Gewinnerzielung ausgerichtet sind oder nicht und ob sie öffentlich oder privat sind, die eine mit der Produktion, der Verarbeitung und dem Vertrieb von Lebensmitteln zusammenhängende Tätigkeit ausführen*".

Anhang II des NIS2-Gesetzes fügt hinzu, dass es nur für Lebensmittelunternehmen gilt, die "im Großhandel und in der industriellen Produktion und Verarbeitung tätig sind". Der Schwerpunkt liegt hier auf dem Großhandel, was einen B2B-Faktor impliziert (im Gegensatz zu B2C). Mit dieser

Betonung soll der Einzelhandel aus dem Anwendungsbereich herausgehalten werden. In ähnlicher Weise soll die "industrielle Produktion und Verarbeitung" die Produktion und Verarbeitung auf die groß angelegte Lebensmittelproduktion und -verarbeitung beschränken.

Es genügt, dass das Lebensmittelunternehmen eine der folgenden Tätigkeiten ausübt, um unter diesen Sektor zu fallen: Großhandel, industrielle Produktion oder industrielle Verarbeitung von Lebensmitteln. Diese Elemente sind nicht kumulativ, sondern alternative Bedingungen.

Wie im Abschnitt 1.8 erläutert, reicht es aus, wenn eine der drei Tätigkeiten lediglich eine Nebentätigkeit einer Organisation ist.

1.22.10.1. Fallen Supermärkte unter den Sektor Lebensmittel in Anhang II, Sektor 4 von NIS2?

Wie im Abschnitt 1.22.10 erwähnt, konzentriert sich der Sektor Produktion, Verarbeitung und Vertrieb von Lebensmitteln auf den Großhandel, die industrielle Produktion oder die industrielle Verarbeitung von Lebensmitteln. Supermärkte sind Einzelhändler. Im Allgemeinen fallen sie nicht unter Anhang II, Sektor 4.

Wenn jedoch eine Supermarktkette bestimmte Lebensmittel in großem Umfang herstellt (z. B. unter ihrem eigenen Label), fällt die Einrichtung, die diese Waren herstellt, unter die industrielle Produktion und damit unter diesen Sektor. Die Tatsache, dass die Einrichtung diese Lebensmittel ausschließlich für die Belieferung ihrer eigenen Supermärkte herstellt, spielt für die Einstufung in diesen Sektor keine Rolle. Die anderen Einrichtungen innerhalb der Restaurantgruppe werden in die Lieferkette dieser Einrichtung fallen. Weitere Informationen zur Lieferkette finden Sie im Abschnitt 3.14.

1.22.10.2. Fallen Restaurants unter Anhang II, Sektor 4 von NIS2?

Wie im Abschnitt 1.22.10 erwähnt, konzentriert sich der Sektor Produktion, Verarbeitung und Vertrieb von Lebensmitteln auf den Großhandel, die industrielle Produktion oder die industrielle Verarbeitung von Lebensmitteln. Restaurants fallen im Prinzip nicht unter diese drei Möglichkeiten und somit nicht unter Anhang II, Sektor 4 des NIS2-Gesetzes.

Wenn jedoch eine Restaurantkette bestimmte Lebensmittelprodukte in großem Umfang herstellt (z. B. unter ihrem eigenen Label), fällt die Einrichtung, die diese Waren herstellt, unter die industrielle Produktion und damit unter diesen Sektor. Die Tatsache, dass die Einrichtung diese Lebensmittel ausschließlich für die Belieferung ihrer eigenen Restaurants herstellt, spielt für die Einstufung in diesen Sektor keine Rolle. Die anderen Einrichtungen innerhalb der Restaurantkette fallen unter die Lieferkette dieser Einrichtung. Weitere Informationen zur Lieferkette finden Sie im Abschnitt 3.14.

1.22.11. Anhang II - 5. Verarbeitendes Gewerbe/Herstellung von Waren

1.22.11.1. Was bedeutet die "Herstellung von Medizinprodukten und In-vitro-Diagnostika"?

Einrichtungen, die Medizinprodukte im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 herstellen, mit Ausnahme der in Anhang I Nummer 5 fünfter

Gedankenstrich des NIS2-Gesetzes genannten Einrichtungen, die pharmazeutische Erzeugnisse herstellen, fallen unter diesen Teilsektor von Anhang II 5. Verarbeitendes Gewerbe.

Ein Medizinprodukt ist definiert als: *" ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:*

- *Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,*
- *Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,*
- *Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,*
- *Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben.*
- *und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann*

Die folgenden Produkte gelten ebenfalls als Medizinprodukte:

- *Produkte zur Empfängnisverhütung oder -förderung,*
- *Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.“*

Ein *In-vitro*-Diagnostikum ist definiert als: „*ein Medizinprodukt, das als Reagenz, Reagenzprodukt, Kalibrator, Kontrollmaterial, Kit, Instrument, Apparat, Gerät, Software oder System — einzeln oder in Verbindung miteinander — vom Hersteller zur In-vitro-Untersuchung von aus dem menschlichen Körper stammenden Proben, einschließlich Blut- und Gewebespenden, bestimmt ist und ausschließlich oder hauptsächlich dazu dient, Informationen zu einem oder mehreren der folgenden Punkte zu liefern:*

a) über physiologische oder pathologische Prozesse oder Zustände,
b) über kongenitale körperliche oder geistige Beeinträchtigungen,
c) über die Prädisposition für einen bestimmten gesundheitlichen Zustand oder eine bestimmte Krankheit,
d) zur Feststellung der Unbedenklichkeit und Verträglichkeit bei den potenziellen Empfängern,
e) über die voraussichtliche Wirkung einer Behandlung oder die voraussichtlichen Reaktionen darauf oder
f) zur Festlegung oder Überwachung therapeutischer Maßnahmen.

Probenbehältnisse gelten als auch In-vitro-Diagnostika;".

Darüber hinaus können Einrichtungen, die Medizinprodukte herstellen, die bei einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden, auch unter Anhang I, 5. Gesundheit fallen. Weitere Informationen finden Sie im Abschnitt 1.22.4.5.

Zusätzlich zu der oben beschriebenen Situation werden die meisten Einrichtungen, die Medizinprodukte herstellen, in die Lieferkette von NIS2-Einrichtungen fallen (z. B. Gesundheitsdienstleister aus Anhang I, Sektor 5). Einrichtungen, die unter das NIS2-Gesetz fallen, müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um ihr Netzwerk- und Informationssystem zu sichern. Eine dieser Maßnahmen ist die Sicherheit der Lieferkette, einschließlich sicherheitsrelevanter Aspekte in Bezug auf die Beziehungen zwischen jeder Einrichtung und ihren direkten Lieferanten oder Dienstleistern. Weitere Informationen zu den Verpflichtungen in der Lieferkette finden Sie im Abschnitt 3.14.

1.22.12. Anhang II - 7. Forschung

Forschungseinrichtungen fallen unter Anhang II, 7. Forschung und werden definiert als "eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt".

1.22.12.1. Decken Forschungseinrichtungen auch Sponsoren ab?

Forschungseinrichtungen fallen unter Anhang II, 7. Forschung und sind wie oben definiert.

Die NIS2-Richtlinie liefert in ihrem Erwägungsgrund 36 einige Hintergrundinformationen zu dieser Definition:

> *Forschungstätigkeiten spielen eine Schlüsselrolle bei der Entwicklung neuer Produkte und Prozesse. Viele dieser Tätigkeiten werden von Einrichtungen durchgeführt, die ihre Forschungsergebnisse zu kommerziellen Zwecken teilen, verbreiten oder nutzen. Diese Einrichtungen können daher wichtige Akteure in Wertschöpfungsketten sein, was die Sicherheit ihrer Netz- und Informationssysteme zu einem integralen Bestandteil der allgemeinen Cybersicherheit des Binnenmarkts macht. Unter Forschungseinrichtungen sind unter anderem Einrichtungen zu verstehen, die sich im Wesentlichen auf die Durchführung von angewandter Forschung oder experimenteller Entwicklung im Sinne des Frascati-Handbuchs der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung von 2015 (Leitlinien zur Erfassung von Daten zu Forschung und experimenteller Entwicklung sowie zur entsprechenden Berichterstattung) konzentrieren, um ihre Ergebnisse für kommerzielle Zwecke wie die Herstellung oder Entwicklung eines Produkts oder eines Verfahrens, die Erbringung eines Dienstes, oder dessen Vermarktung zu nutzen.*

Gemäß dem Frascati-Handbuch (2015) ist angewandte Forschung eine originäre Untersuchung, die unternommen wird, um neues Wissen zu erlangen. Experimentelle Entwicklung ist systematische Arbeit, die auf Erkenntnissen aus Forschung und praktischer Erfahrung basiert und zusätzliches Wissen erzeugt, das darauf abzielt, neue Produkte oder Verfahren zu entwickeln oder bestehende Produkte oder Verfahren zu verbessern.

Der kommerzielle Zweck ist weit gefasst und umfasst die *Herstellung oder Entwicklung eines Produkts oder eines Verfahrens, die Erbringung eines Dienstes, oder dessen Vermarktung*. Wenn das Ziel der Forschungstätigkeiten die Herstellung eines neuen Produkts ist, liegt ein kommerzieller Zweck der Forschung vor.

Die von Sponsoren erbrachten Dienstleistungen umfassen keine angewandte Forschung oder experimentelle Entwicklung, sondern lediglich die Finanzierung von Forschungsaktivitäten durch

eine andere Organisation. Daher fallen diese Organisationen, die nicht die eigentliche NIS2-Dienstleistung erbringen, nicht in den Anwendungsbereich des NIS2-Gesetzes.

1.22.12.2. Sind Bildungseinrichtungen "Forschungseinrichtungen"?

Wie in der im Abschnitt 1.22.12 genannten Definition angegeben, sind Bildungseinrichtungen ausdrücklich ausgeschlossen. Letztere könnten jedoch dennoch unter die NIS2 fallen, wenn sie Teil des öffentlichen Sektors sind. Weitere Informationen sind im Abschnitt 2.7 zu finden.

2. Öffentlicher Sektor

2.1. Welchen Anwendungsbereich hat das Gesetz für den öffentlichen Sektor?

Art. 8, 34° und Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Art. 8, 34° des Gesetzes definiert eine "Einrichtung der öffentlichen Verwaltung" als eine Verwaltungsbehörde im Sinne von Art. 14, § 1, Abs. 1 der koordinierten Gesetze über den Staatsrat, die folgende Kriterien erfüllt:

a) sie hat keinen industriellen oder kommerziellen Charakter;
b) sie übt nicht hauptberuflich eine Tätigkeit aus, die in der Spalte Art der Einrichtung eines anderen Sektors oder Teilsektors in einer der Beilagen des Gesetzes aufgeführt ist;
c) sie ist keine juristische Person des Privatrechts.

Für die Definition einer Einrichtung der öffentlichen Verwaltung legt Artikel 6, 35) der Richtlinie fest, dass der Begriff gemäß dem nationalen Recht als solcher anerkannt werden muss, mit Ausnahme der Justiz, der Parlamente und der Zentralbanken. Daher wurde beschlossen, auf bestehende Begriffe im belgischen Recht zu verweisen, die die betreffenden Einrichtungen abdecken, um die Anwendung unterschiedlicher Begriffe nicht zu vervielfachen.

Im vorliegenden Fall übernimmt die Definition den Begriff der Verwaltungsbehörde gemäß Artikel 14, §1 , Absatz 1 der koordinierten Gesetze vom 12. Januar 1973 über den Staatsrat (siehe Abschnitt 2.2), der die Kriterien hinzugefügt werden, dass sie keinen industriellen oder kommerziellen Charakter hat, nicht hauptberuflich eine Tätigkeit ausübt, die unter einen der anderen Sektoren oder Teilsektoren fällt, die in den Anlagen des Gesetzes aufgeführt sind, und keine juristische Person des Privatrechts ist.

Diese Definition muss mit den Arten von Einrichtungen in Beilage I, Sektor 10 (Öffentliche Verwaltung) kombiniert werden:

- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen;
- Einrichtungen der öffentlichen Verwaltung, die von den föderierten Teilstaaten abhängen, identifiziert gemäß Artikel 11, § 2 des Gesetzes;
- Die Hilfeleistungszonen im Sinne von Artikel 14 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit oder der Dienst für Brandschutz und medizinische Nothilfe der Region Brüssel-Hauptstadt, der durch die Verordnung vom 19. Juli 1990 über die Schaffung eines Dienstes für Brandschutz und medizinische Nothilfe der Region Brüssel-Hauptstadt geschaffen wurde.

Der Begriff der Abhängigkeit (die von X „abhängen“) wurde von Artikel 5 des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten inspiriert. Er ermöglicht es, insbesondere Einrichtungen zu erfassen, die Teil einer Verwaltungsebene sind, weil sie von diesen Behörden gegründet wurden, ihre Tätigkeit mehrheitlich von diesen Behörden finanziert wird, die Verwaltung der Kontrolle dieser Behörden unterliegt, oder weil bei denen mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans von diesen Behörden ernannt werden.

Siehe auch die folgenden Abschnitte dieses Kapitels für weitere Einzelheiten.

2.2. Was ist eine "Verwaltungsbehörde"?

Nach der Rechtsprechung des Staatsrats gilt eine Einrichtung des öffentlichen Rechts automatisch als Verwaltungsbehörde im Sinne von Artikel 14, § 1 der koordinierten Gesetze vom 12. Januar 1973 über den Staatsrat, wenn sie Befugnisse der Exekutive ausübt.

Um zu prüfen, ob eine juristische Person des Privatrechts als Verwaltungsbehörde eingestuft werden kann, werden die folgenden Kriterien angewandt:

1) von den Behörden des Föderalstaats, der Teilgebiete, der Provinzen oder der Gemeinden geschaffen oder anerkannt;
2) mit einer öffentlichen Aufgabe betraut;
3) nicht Teil der Judikative oder der Legislative;
4) Betrieb von den Behörden bestimmt und kontrolliert;
5) kann Entscheidungen treffen, die für Dritte verbindlich sind.

Diese fünf Kriterien müssen kumulativ erfüllt sein, damit eine privatrechtliche Einrichtung als Verwaltungsbehörde eingestuft werden kann.

2.3. Was ist mit Organisationen des öffentlichen Sektors, die in einem anderen NIS2-Sektor tätig sind (z. B. ein öffentliches Krankenhaus, eine interkommunale Organisation oder ein öffentliches Altenheim)?

Wie die Definition in Art. 8, 34° (siehe Abschnitt 2.1), ist eine öffentliche Einrichtung, die hauptsächlich eine Dienstleistung erbringt, die in einem anderen Sektor oder Teilsektor eines der Anhänge des Gesetzes aufgeführt ist**, den Vorschriften dieses Sektors und nicht dem Sektor der öffentlichen Verwaltung verpflichtet.**

Dazu gehören zum Beispiel:

- eine Interkommunale, die Gas und/oder Strom liefert;
- eine Interkommunale für die Trinkwasserversorgung;
- eine Interkommunale für Abfallentsorgung;
- ein öffentliches Krankenhaus;
- ein öffentliches Altersheim;
- eine öffentliche IKT-Dienstleistungsorganisation;
- einen öffentlichen Postdienst;
- einen öffentlichen Flughafen;
- usw.

Gehören diese Beispiele zu einer lokalen öffentlichen Verwaltung (dieselbe juristische Person), so fällt die gesamte Organisation nur in den (die) betroffenen Sektor(en) in den Geltungsbereich des Gesetzes. Lokale öffentliche Verwaltungen fallen in der Tat nicht in den Sektor der öffentlichen Verwaltung in Anhang I des NIS2-Gesetzes. Weitere Informationen über lokale öffentliche Verwaltungen finden Sie im Abschnitt 2.4.

Wenn eine öffentliche Verwaltung, die vom Föderalstaat oder den Teilgebieten abhängt, auch eine Dienstleistung erbringt (nicht als ihre Haupttätigkeit), die unter einen anderen NIS2-Sektor

fällt (dieselbe juristische Person), fällt sie in beide Sektoren und muss die strengsten Verpflichtungen aus beiden anwenden (und sich somit auch in beiden registrieren). Wenn öffentliche Verwaltungen, die von den Teilgebieten abhängen, in mehrere Sektoren fallen, müssen sie nicht warten, bis sie identifiziert sind, um die sich aus dem NIS2-Gesetz ergebenden Verpflichtungen anzuwenden und sich zu registrieren.

2.4. Fallen lokale öffentliche Einrichtungen in den Anwendungsbereich des Gesetzes?

Art. 8, 34° Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Lokale öffentliche Einrichtungen (Gemeinden, Provinzen, Interkommunale, ÖSHZ, Regiebetriebe, usw.) **unterliegen nicht automatisch den Anforderungen des NIS2-Gesetzes**. Sie sind in der Tat nicht ausdrücklich in den Anhängen des NIS2-Gesetzes im öffentlichen Sektor aufgeführt.

Auch wenn lokale öffentliche Verwaltungen, wie die oben genannten, der Definition in Artikel 8, 34° entsprechen (siehe Abschnitt 2.1), sind sie weder vom Föderalstaat noch von Teilgebieten abhängig.

Gemäß dem in Artikel 162 der Verfassung verankerten Grundsatz der lokalen Selbstverwaltung, werden die lokalen Einrichtungen trotz der Ausübung einer Aufsichts- oder Finanzierungskontrolle nicht als Einrichtung der öffentlichen Verwaltung betrachtet, die im Sinne der Beilage I des NIS2-Gesetzes von den föderierten Teilgebieten oder dem Föderalstaat abhängen.

Diese lokalen Einrichtungen fallen **jedoch** in den Anwendungsbereich des NIS2-Gesetzes, wenn sie eine in Anhang I oder II des Gesetzes aufgeführte Dienstleistung erbringen und mindestens als mittleres Unternehmen einzustufen sind. Ihre Einstufung als wesentliche oder wichtige Einrichtung im Sinne des Gesetzes hängt dann von der erbrachten Dienstleistung und ihrer Größe ab (siehe auch Abschnitt 1.5).

Lokale öffentliche Einrichtungen können auch über Artikel 11 § 1 (Identifizierung durch die nationale Cybersicherheitsbehörde - ZCB) identifiziert werden, sofern das in Artikel 11 § 3 vorgesehenen Konzertierungsverfahren eingehalten wird. Die Initiative für eine solche Identifizierung könnte auf Antrag der nationalen Cybersicherheitsbehörde, der betroffenen Einrichtung oder auch einer Region erfolgen.

2.5. Unterliegen regionale oder gemeinschaftliche öffentliche Einrichtungen den Verpflichtungen des Gesetzes?

Art. 11, §2-3 und Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Regionale und gemeinschaftliche öffentliche Verwaltungen sind Teil des Sektors der öffentlichen Verwaltung im Anhang I des NIS2-Gesetz und ausdrücklich als "Einrichtungen der öffentlichen Verwaltung, die von den Teilgebieten abhängen" bezeichnet. Dazu gehören insbesondere die föderierte öffentlichen Verwaltungen, aber auch verschiedene öffentliche Einrichtungen, die von der den Teilgebieten geschaffen, finanziert oder anderweitig verwaltet werden, unter der Voraussetzung, dass sie der Definition von Artikel 8, 34° des NIS2-Gesetzes entsprechen (siehe Abschnitt 2.1).

Dennoch muss zuvor ein formelles Identifizierungsverfahren von der nationalen Cybersicherheitsbehörde (ZCB) durchgeführt werden. Dabei werden auf Grundlage einer Risikoanalyse Einrichtungen bewertet, die Dienstleistungen erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Aktivitäten haben könnte.

Gemäß Artikel 11, § 2 und 3 des NIS2-Gesetzes erfolgt diese Identifizierung in Absprache mit den betroffenen öffentlichen Einrichtungen und den Regierungen der föderierten Einheiten. Nach Abschluss dieses Verfahrens kann die regionale oder gemeinschaftliche öffentliche Einrichtung als wesentliche Einrichtung oder wichtige Einrichtung bezeichnet werden.

Wenn eine Einrichtung der öffentlichen Verwaltung, die von einem Teilgebiet abhängt, auch in einem anderen Bereich des NIS2-Gesetzes tätig ist, ist der oben beschriebene Identifizierungsprozess nicht erforderlich, damit das NIS2-Gesetz Anwendung findet (siehe auch Abschnitt 2.3).

Informationen zur Registrierung finden Sie im Abschnitt 2.8.

2.6. Welches Personal muss bei der Berechnung der Größe meiner (lokalen) Einrichtung der öffentlichen Verwaltung berücksichtigt werden?

Solange sie nicht formell als NIS2-Einrichtung identifiziert ist und je nach den erbrachten Diensten, muss eine föderierte öffentliche Verwaltung oder eine lokale öffentliche Verwaltung möglicherweise ihre Größe berechnen.

Öffentliche Einrichtungen müssen das gesamte Personal berücksichtigen, das **innerhalb der juristischen Person** dieser öffentlichen Einrichtung arbeitet. Gemäß dem Benutzerleitfaden zur KMU-Definition der Europäischen Kommission *" umfasst Vollzeit-, Teilzeit- und Zeitarbeitskräfte sowie Saisonpersonal und schließt folgende Gruppen ein:*

- *Lohn- und Gehaltsempfänger;*
- *für das Unternehmen tätige Personen, die zu ihm entsandt wurden und nach nationalem Recht als Arbeitnehmer gelten (kann auch Zeit- oder sogenannte Leiharbeitskräfte einschließen);*
- *mitarbeitende Eigentümer;*
- *Teilhaber, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen".*

Dies gilt nicht für:

- *"Auszubildende oder in der beruflichen Ausbildung stehende Personen mit Lehr- oder Berufsausbildungsvertrag;*
- *Mitarbeiter im Mutterschafts- oder Elternurlaub".*

Die für die Berechnung des Size-cap erforderliche Mitarbeiteranzahl (siehe Abschnitt 1.5) wird in JAE (Jahresarbeitseinheiten) ausgedrückt. Personen, die in dem betroffenen Unternehmen oder auf Rechnung dieses Unternehmens während des gesamten Berichtsjahres einer Vollzeitbeschäftigung nachgegangen sind. Für die Arbeit von Personen, die nicht das ganze Jahr gearbeitet haben oder die im Rahmen einer Teilzeitregelung oder für Saisonarbeit tätig waren, wird der jeweilige Bruchteil an JAE gezählt.

In diesem Zusammenhang sollte eine Person, die nur einen Teil des Jahres mit einem befristeten Vertrag oder im Rahmen einer Entsendung gearbeitet hat, als Bruchteil einer Einheit auf der Grundlage der Anzahl der im Vorjahr geleisteten Arbeitstage (geteilt durch die Arbeitstage des Jahres) gezählt werden.

Personal, das von einem öffentlichen Sozialhilfezentrum (ÖSHZ) zur Verfügung gestellt wird, um in einer Organisation gemäß Artikel 60, §7 des Organgesetzes vom 8. Juli 1976 über öffentliche Sozialhilfezentren zu arbeiten, wird bei der Berechnung des Personalbestands als Leiharbeiter berücksichtigt.

Es ist wichtig zu beachten, dass die Bestimmungen zur Konsolidierung der Daten von Partnerunternehmen und verbundenen Unternehmen aus der Empfehlung 2003/361/EG nicht für öffentliche Verwaltungen gelten. Dies bedeutet, dass nur die Daten der Verwaltung selbst berücksichtigt werden müssen. Wenn beispielsweise eine Gemeinde, die Trinkwasserdienstleistungen erbringt, auch eine Schule betreibt, muss sie die Daten der Schule nur dann berücksichtigen, wenn diese Schule zur gleichen rechtlichen Person gehört wie die Gemeinde.

2.7. Fallen Bildungseinrichtungen in den Geltungsbereich des Gesetzes?

Beilagen I und II & Art. 8, 34° NIS2-Gesetz

Zum einen ist der Bildungssektor in den Anhängen I und II des NIS2-Gesetzes nicht ausdrücklich aufgeführt. Private Bildungseinrichtungen fallen somit nicht in den Anwendungsbereich des NIS2-Gesetzes.

Andererseits **könnten öffentliche** Bildungseinrichtungen, wie öffentliche Universitäten oder öffentliche Schulen, in die Definition einer "Einrichtung der öffentlichen Verwaltung" einbezogen werden. Um dies zu tun, müssen sie:

- Die Größenkriterien (Size-cap) erfüllen (siehe Abschnitt 1.3.);
- in Belgien niedergelassen sein (siehe Abschnitt 1.14.);
- der Definition einer Einrichtung der öffentlichen Verwaltung in Artikel 8, 34° NIS2-Gesetz entsprechen (siehe Abschnitte 2.1 und 2.2);
- vom Föderalstaat oder den föderierten Teilgebieten abhängen (siehe Abschnitt 2.1);
- wenn sie von den föderierten Teilgebieten abhängen: gemäß Art. 11, § 2 identifiziert werden (siehe Abschnitt 2.5).

Darüber hinaus könnte eine Bildungseinrichtung auch als "Gesundheitsdienstleister" (siehe Abschnitt 1.22.4.1) im Sinne von Anhang I des NIS2-Gesetzes gelten, wenn sie z. B. ein Universitätskrankenhaus betreibt, das Teil derselben rechtlichen Person ist (ist dies nicht der Fall, fällt nur das Krankenhaus in den Anwendungsbereich, wenn der Size-cap erreicht wird).

2.8. Wann und wie sollten sich Einrichtungen des öffentlichen Sektors registrieren?

Je nachdem, welche Einrichtungen des öffentlichen Sektors betroffen sind, gelten unterschiedliche Regelungen:

- Für öffentliche Einrichtungen, die vom Föderalstaat abhängen, gilt seit Inkrafttreten des Gesetzes die normale Registrierungsfrist (bis zum 18. März 2025).
- Für öffentliche Einrichtungen, die von den föderierten Teilgebieten abhängen, beträgt die Registrierungsfrist 5 Monate nach der förmlichen Identifizierung der betreffenden Einrichtung durch das ZCB (Benachrichtigungsschreiben).
- Für Hilfeleistungszonen gilt seit Inkrafttreten des Gesetzes die normale Anmeldefrist (bis zum 18. März 2025).

Es ist wichtig zu beachten, dass diese Fristen nur gelten, wenn die betreffende Organisation ausschließlich dem Sektor der öffentlichen Verwaltung angehört. Fällt sie auch in einen anderen Sektor, können strengere Fristen gelten.

Die Anmeldung erfolgt über unsere Plattform Safeonweb@Work (siehe Abschnitt 3.13.1).

2.9. Gelten die Sanktionen auch für Einrichtungen der öffentlichen Verwaltung? Was ist, wenn die Organisation auch zu einem anderen Sektor gehört?

Gemäß Artikel 62 des NIS2-Gesetzes können alle im Abschnitt 4.18.1 genannten Verwaltungsmaßnahmen als Reaktion auf einen Verstoß gegen das Gesetz durch Einrichtungen der öffentlichen Verwaltung ergriffen werden. Diese Einrichtungen können jedoch nicht zu den im Abschnitt 4.17 genannten Geldbußen und einigen spezifischen Verwaltungsmaßnahmen verpflichtet werden.

Diese Aussagen gelten auch, wenn eine Einrichtung der öffentlichen Verwaltung gleichzeitig dem Sektor der öffentlichen Verwaltung und einem anderen NIS2-Sektor angehört (die vorteilhaftere Regelung hat Vorrang vor der anderen).

Eine öffentliche Einrichtung, die hauptsächlich eine in der Spalte "Art der Einrichtung" eines anderen Sektors oder Teilsektors aufgeführte Tätigkeit ausübt, kann jedoch mit Geldbußen und spezifischen administrativen Maßnahmen belegt werden (da sie nicht unter die Definition einer Einrichtung der öffentlichen Verwaltung fällt).

3. Verpflichtungen

3.1. Welche rechtlichen Verpflichtungen bestehen für die betroffenen Einrichtungen?

Aus dem NIS2-Gesetz ergeben sich mehrere Pflichten für wesentliche und wichtige Einrichtungen:

- das Ergreifen angemessener Cybersicherheitsmaßnahmen;
- die rechtzeitige Meldung erheblicher Sicherheitsvorfälle;
- die Registrierung bei den zuständigen Behörden (Plattform des ZCB für die meisten Einrichtungen);
- die Ausbildung für Mitglieder der Leitungsorgane (Abschnitt 3.9.);
- die Durchführung regelmäßiger Konformitätsbewertungen (obligatorisch für wesentliche Einrichtungen und freiwillig für wichtige Einrichtungen);
- den Austausch von Informationen und die Zusammenarbeit mit den zuständigen Behörden.

Diese verschiedenen Pflichten werden in den folgenden Abschnitten erläutert.

3.2. Welche Verpflichtungen bestehen hinsichtlich der Cybersicherheitsmaßnahmen?

Art. 30, 31 und 42 NIS2-Gesetz

Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige (technische, operative und organisatorische) Maßnahmen ergreifen, um Risiken zu bewältigen, die die Sicherheit der Netz- und Informationssysteme bedrohen, die diese Einrichtungen im Rahmen ihrer Geschäftstätigkeit oder bei der Erbringung ihrer Dienste nutzen, und um die Folgen von Sicherheitsvorfällen für die Empfänger ihrer Dienste und für andere Dienste zu beseitigen oder zu verringern.

Es ist wichtig zu betonen, dass sich **der Anwendungsbereich des NIS2-Gesetzes im Gegensatz zum NIS1-Gesetz auf die gesamte betroffene Einrichtung bezieht** und nicht nur auf ihre in den Beilagen des Gesetzes aufgeführten Tätigkeiten.

Um die praktische Umsetzung dieser Cybersicherheitsmaßnahmen zu erleichtern, hat das ZCB bereits einen Referenzkader entwickelt und den betroffenen Einrichtungen kostenlos zur Verfügung gestellt: das "Cyberfundamentals Framework" (CyFun®) mit verschiedenen Stufen und einem Analysetool, das es ermöglicht, die am besten geeignete Stufe für eine Einrichtung zu bestimmen. Das Gesetz und sein Königlicher Erlass werden wesentlichen und wichtigen Einrichtungen, die sich für die Verwendung des CyFun®-Frameworks oder der internationalen Norm ISO/IEC 27001 (mit dem NIS2-konformen Anwendungsbereich - d.h. alle Netz- und Informationssysteme) entscheiden, eine **Konformitätsvermutung** in Bezug auf die Sicherheitsmaßnahmen bieten.

Die im Gesetz enthaltenen Mindestmaßnahmen basieren auf einem gefahrenübergreifenden Ansatz, der darauf abzielt, Netz- und Informationssysteme sowie deren physische Umgebung vor Sicherheitsvorfällen zu schützen, und zumindest folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
2. Bewältigung von Sicherheitsvorfällen;
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung;
11. Eine Politik für die koordinierten Offenlegung von Schwachstellen.

Die von wesentlichen und wichtigen Einrichtungen zu treffenden Maßnahmen müssen **geeignet und verhältnismäßig** sein. In diesem Zusammenhang ist es wichtig, klarzustellen, dass die Maßnahmen zum Management von Cybersicherheitsrisiken in einem **angemessenen Verhältnis zu den Risiken stehen sollten,** denen das betreffende Netz- und Informationssystem ausgesetzt ist, um zu verhindern, dass die finanzielle und administrative Belastung der wesentlichen und wichtigen Einrichtungen unverhältnismäßig hoch ist. In diesem Zusammenhang berücksichtigen die Einrichtungen insbesondere **den Stand der Technik** dieser Maßnahmen sowie gegebenenfalls einschlägige europäische oder internationale **Normen** und die **Kosten für die Umsetzung** dieser Maßnahmen.

Es sei darauf hingewiesen, dass einige NIS2-Einrichtungen die Durchführungsverordnung 2024/2690 der Kommission vom 17. Oktober 2024 befolgen müssen, in der die technischen und methodischen Anforderungen an Risikomanagementmaßnahmen im Bereich der Cybersicherheit festgelegt sind (siehe Abschnitt 5.1).

3.3. Welche Verpflichtungen bestehen hinsichtlich der Meldung von Sicherheitsvorfällen?

Weitere Informationen zur Meldung von Sicherheitsvorfällen finden Sie auf unserer Website und in unserem Leitfaden zur Meldung von Sicherheitsvorfällen.

3.3.1. Allgemeine Regeln

Art. 8, 5° und 57°; 34 und 35 NIS2-Gesetz

Ein Sicherheitsvorfall ist gesetzlich definiert als *"ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt"*.

Im Falle eines erheblichen Sicherheitsvorfalls muss die Einrichtung diesen dem nationalen CSIRT (ZCB) und in einigen Fällen auch den Empfängern ihrer Dienstleistungen melden.

In unserem Leitfaden zur Meldung von Sicherheitsvorfällen finden Sie weitere Informationen zu erheblichen Sicherheitsvorfällen.

Die Meldung erfolgt in mehreren Schritten (siehe Abschnitt 3.3.3): zunächst eine Frühwarnung innerhalb von 24 Stunden nach Entdeckung des Sicherheitsvorfalls (*Early warning)*, dann eine ordnungsgemäße Meldung des Sicherheitsvorfalls innerhalb von 72 Stunden nach Entdeckung des Vorfalls (*Initial assessment of the incident)* und schließlich ein Abschlussbericht spätestens einen Monat nach der Meldung des Sicherheitsvorfalls (*Final report*). In der Zwischenzeit kann der nationale CSIRT Zwischenberichte anfordern.

Das ZCB hat einen umfassenden Leitfaden dazu entwickelt, wann und wie ein Sicherheitsvorfall gemeldet werden sollte. Die aktuellste Version des Leitfadens finden Sie auf unserer Website oder über diesen direkten Link: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20DE.pdf.

NIS2-Sicherheitsvorfälle können dem ZCB über seine Plattform http://notif.safeonweb.be/ gemeldet werden.

Weitere Informationen finden Sie auch hier: https://ccb.belgium.be/de/cert/einen-vorfall-melden.

3.3.2. Wann ist ein Sicherheitsvorfall "erheblich"?

Das NIS2-Gesetz verpflichtet alle Einrichtungen in seinem Anwendungsbereich, der ZCB jeden Sicherheitsvorfall zu melden, der als "erheblicher" Sicherheitsvorfall betrachtet werden kann. Ein solcher Sicherheitsvorfall wird im Gesetz wie folgt definiert:

"Jeder Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung einer der in den Anhängen I und II des Gesetzes aufgeführten Dienstleistungen hat und der:

1° *schwerwiegende Betriebsstörungen eines der in den in Anhang I und II aufgeführten Sektoren oder Teilsektoren erbrachten Dienstes oder einen finanziellen Verlust für die betreffende Einrichtung verursacht hat oder verursachen kann, oder*
2° *andere natürliche oder juristische Personen durch erhebliche materielle, körperliche oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann*".

Erstens muss der Sicherheitsvorfall sich auf die Erbringung einer der Dienste auswirken, die in den in Beilage I und II des Gesetzes aufgeführten Sektoren oder Teilsektoren erbracht werden, d.h. er **muss sich auf die Netz- und Informationssysteme auswirken, die die Erbringung einer oder mehrerer dieser Dienste unterstützen** (z.B. Stromverteilung).

Die Meldepflicht bezieht sich daher nur auf Netz- und Informationssysteme, auf die die betroffene Einrichtung angewiesen ist, um die in den Beilagen des Gesetzes aufgeführten Dienste zu erbringen. Ein Sicherheitsvorfall, der ein isoliertes Informationssystem betrifft, das nicht mit der Bereitstellung der genannten Dienste in Verbindung steht, muss daher nicht gemeldet werden.

Zweitens muss die Auswirkung erheblich sein, d.h. sie muss mindestens eine der folgenden drei Situationen verursachen oder verursachen können:

- eine **schwerwiegende Betriebsstörung** bei einer der erbrachten Dienstleistungen (in den Sektoren oder Teilsektoren, die in Beilage I und II des NIS2-Gesetzes aufgeführt sind);
- **finanzielle Verluste für die betroffene Einrichtung**;
- **erhebliche materielle, körperliche oder moralische Schäden für andere natürliche oder juristische Personen**.

Weitere Informationen zur Meldung von Sicherheitsvorfällen finden Sie in unserem **NIS2-Leitfaden zur Meldung von Sicherheitsvorfällen.**[3]

NIS2-Sicherheitsvorfälle können über unser Webformular für die Meldung von Sicherheitsvorfällen gemeldet werden: **https://notif.safeonweb.be**.

3.3.3. Empfänger einer obligatorischen Meldung eines erheblichen Sicherheitsvorfalls

Grundsätzlich muss jede NIS2-Einrichtung einen Sicherheitsvorfall nur dem ZCB melden. Das ZCB leitet die Meldungen an etwaige sektorale Behörden sowie an das Krisenzentrum (für wesentliche Einrichtungen) weiter.

Art. 34, §1 NIS2-Gesetz

Diese Regel gilt jedoch nicht für Einrichtungen, die unter die DORA-Verordnung im Banken- und Finanzsektor fallen. Die Einrichtungen in diesen beiden Sektoren melden ihren Sicherheitsvorfall je nach Fall der Belgischen Nationalbank (BNB) oder der Finanzdienstleistungs- und Marktaufsichtsbehörde (FSMA), die die Meldung des Vorfalls automatisch an das ZCB weiterleiten.

Gegebenenfalls teilt die Einrichtung den Empfängern ihres Dienstes erhebliche Sicherheitsvorfälle mit, die die von der Einrichtung erbrachten Dienste beeinträchtigen könnten. Sie meldet den Empfängern, die potenziell von einer erheblichen Cyberbedrohung betroffen sind, auch alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können, und informiert sie über alle Korrekturen und Maßnahmen, die sie als Reaktion anwenden können. Soweit angemessen, unterrichten die Einrichtungen diese Empfänger auch über die erhebliche Cyberbedrohung selbst.

Art. 34, §2 NIS2-Gesetz

3.3.4. Verfahren zur Meldung eines Sicherheitsvorfalls

Die Meldung von erheblichen Sicherheitsvorfällen erfolgt in mehreren Schritten:

Art. 35 NIS2-Gesetz

[3] https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20DE.pdf
Siehe auch den Durchführungsrechtsakt der Kommission (Abschnitt 5.1).

1. unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, übermittelt die Einrichtung eine Frühwarnung;
2. unverzüglich, in jedem Fall aber innerhalb von 72 Stunden (24h für Vertrauensdienstanbieter) nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, übermittelt die Einrichtung eine Meldung über den Sicherheitsvorfall;
3. auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde übermittelt die Einrichtung einen Zwischenbericht über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Punkt 2, übermittelt die Einrichtung einen Abschlussbericht;
5. im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts, übermittelt die betroffene Einrichtung einen Fortschrittsbericht und dann, innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls, einen Abschlussbericht.

In der Praxis kann eine Meldung von Sicherheitsvorfällen über unsere Plattform erfolgen: http://notif.safeonweb.be/.

3.3.5. Informationen, die bei der Meldung eines Sicherheitsvorfalls übermittelt werden müssen

Die verschiedenen Schritte der Meldung beinhalten unterschiedliche Informationen, die übermittelt werden müssen:

Art. 35 NIS2-Gesetz

- Die Frühwarnung gibt an, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall durch rechtswidrige oder böswillige Handlungen verursacht worden sein könnte, und ob er grenzüberschreitende Auswirkungen haben könnte. Diese Frühwarnung umfasst nur die Informationen, die erforderlich sind, um den Sicherheitsvorfall dem CSIRT zur Kenntnis zu bringen, und ermöglicht es der betroffenen Einrichtung gegebenenfalls Unterstützung anzufordern.
  Diese Warnung darf die Ressourcen der meldenden Einrichtung nicht von den Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen abziehen. Diese sollten Vorrang haben, um zu verhindern, dass die Meldepflichten für Sicherheitsvorfälle die Ressourcen von der Bewältigung wichtiger Sicherheitsvorfälle abziehen oder die diesbezüglichen Bemühungen der Einrichtung auf andere Weise gefährden.
- Die Meldung eines Sicherheitsvorfalls innerhalb von 72 Stunden dient dazu, die im Rahmen der Frühwarnung mitgeteilten Informationen zu aktualisieren. Sie liefert außerdem eine erste Bewertung des Sicherheitsvorfalls, einschließlich des Schweregrads und der Auswirkungen, sowie Kompromittierungsindikatoren, sofern diese verfügbar sind.
  Wie bei der Frühwarnung dürfen auch bei der Meldung von Vorfällen keine Ressourcen der Einrichtung abgezogen werden, um zu vermeiden, dass die Meldepflichten für Vorfälle Ressourcen von der Bewältigung erheblicher Sicherheitsvorfälle abziehen oder die diesbezüglichen Bemühungen der Einrichtung auf andere Weise beeinträchtigen.
- Der Zwischenbericht enthält relevante Aktualisierungen der Situation.
- Der Abschlussbericht sollte eine detaillierte Beschreibung des Sicherheitsvorfalls enthalten, einschließlich der Schwere und der Auswirkungen, der Art der Bedrohung oder der tieferen Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat, der

angewandten und laufenden Maßnahmen zur Schadensbegrenzung und gegebenenfalls der grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

- Der Fortschrittsbericht enthält so weit wie möglich die Informationen, die im Abschlussbericht enthalten sein sollten und die sich zum Zeitpunkt der Übermittlung des Fortschrittsberichts im Besitz der Einrichtung befanden.

3.3.6. Vertraulichkeitsregeln, die für die bei einem Sicherheitsvorfall übermittelten Informationen gelten

Art. 26, §3-4 NIS2-Gesetz

Die NIS2-Einrichtung und ihre Auftragsverarbeiter beschränken den Zugang zu Informationen über Sicherheitsvorfälle im Sinne des NIS2-Gesetzes auf diejenigen Personen, die zur Wahrnehmung ihrer Aufgaben oder Pflichten im Zusammenhang mit diesem Gesetz davon Kenntnis haben müssen und Zugang dazu benötigen.

Dies gilt auch für das ZCB (nationaler CSIRT), dem NCCN und der sektoralen Behörde.

Die dem ZCB, dem NCCN und der sektoralen Behörde von einer NIS2-Einrichtung zur Verfügung gestellten Informationen können mit Behörden anderer EU-Mitgliedstaaten und mit anderen belgischen Behörden ausgetauscht werden, wenn dieser Austausch für die Anwendung gesetzlicher Bestimmungen erforderlich ist.

Diese Informationsweitergabe beschränkt sich jedoch auf das, was für den Zweck dieses Austauschs relevant und verhältnismäßig ist, wobei die EU-Verordnung 2016/679 (DSGVO), die Vertraulichkeit der betroffenen Informationen, die Sicherheit und die Geschäftsinteressen der NIS2-Einrichtungen beachtet werden müssen.

3.4. Wo kann ich einen NIS2-Sicherheitsvorfall melden?

Alle NIS2-Sicherheitsvorfälle können über unser Online-Meldeformular gemeldet werden: http://notif.safeonweb.be/.

Weitere Informationen über die Meldung von Sicherheitsvorfällen finden Sie auf unserer Website.

Siehe auch unseren Leitfaden zur Meldung von Sicherheitsvorfällen für weitere Informationen über erhebliche Sicherheitsvorfälle.

3.5. Was passiert, wenn es zu einem Sicherheitsvorfall kommt, bei dem auch personenbezogene Daten betroffen sind?

Wie bereits jetzt werden die Sicherheitsvorfallmeldungen im Rahmen des Gesetzes nicht die möglichen Meldungen im Falle einer Verletzung personenbezogener Daten, z. B. an die belgische Datenschutzbehörde (DSB), ersetzen. Es werden weiterhin zwei getrennte Meldungen erforderlich sein.

Das Gesetz sieht jedoch eine verstärkte Zusammenarbeit zwischen der nationalen Behörde für Cybersicherheit und den Datenschutzbehörden vor. Diese Zusammenarbeit könnte zur Entwicklung gemeinsamer Instrumente führen.

Die zuständige Datenschutzbehörde kann auf deren Website benachrichtigt werden.

3.6. Ist es möglich, Sicherheitsvorfälle oder Cyberbedrohungen freiwillig zu melden?

Art. 38 NIS2-Gesetz

Ja. Das nationale CSIRT (ZCB) kann auch auf freiwilliger Basis, von NIS oder nicht-NIS2 Einrichtungen, Meldungen über Sicherheitsvorfälle, Cyberbedrohungen oder auch Beinahe-Vorfällen erhalten.

Eine Cyberbedrohung bezeichnet "einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte".

Ein Beinahe-Vorfall ist „ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist".

Diese freiwilligen Meldungen werden auf die gleiche Weise bearbeitet wie verpflichtende Benachrichtigungen, aber verpflichtende Meldungen können dennoch vorrangig behandelt werden.

Eine freiwillige Meldung führt nicht unmittelbar zu einer Inspektion der Einrichtung, die die Meldung vorgenommen hat, oder erlegt ihr zusätzliche Verpflichtungen auf, denen sie nicht unterworfen gewesen wäre, wenn sie die Meldung nicht vorgenommen hätte.

Siehe dazu das in Abschnitt 3.3. erläuterte Verfahren.

3.7. Was passiert, wenn bei meinem Lieferanten oder einem Unternehmen meiner Gruppe ein Sicherheitsvorfall auftritt? Wer muss Meldung erstatten? Was ist, wenn der Vorfall in mehreren Mitgliedstaaten auftritt?

Jede unter NIS2 fallende Organisation, die von einem erheblichen Sicherheitsvorfall betroffen ist, muss diesen den zuständigen NIS2-Behörden in der EU einzeln melden. Alle anderen Organisationen können ihre Sicherheitsvorfälle auch freiwillig über die im Abschnitt 3.3.1 genannte Plattform an das ZCB melden.

Wird der Sicherheitsvorfall, der den Lieferanten oder ein anderes Unternehmen der Gruppe betrifft, auch zu einem erheblichen Sicherheitsvorfall für die betreffende NIS2-Einrichtung, so muss diese ihn melden. NIS2-Einrichtungen und ihre Zulieferer oder Partnerunternehmen sollten miteinander kommunizieren und sich gegenseitig über Sicherheitsvorfälle informieren, die die Erbringung ihrer Dienstleistungen betreffen.

Betrifft der erhebliche Sicherheitsvorfall mehrere Unternehmen (oder ein Unternehmen), die (das) in verschiedenen Mitgliedstaaten niedergelassen sind (ist), so muss der Vorfall gemäß den Regeln über die Zuständigkeit gemeldet werden, wie im Abschnitt 1.14 erläutert. In bestimmten Ausnahmefällen ist es möglich, dass der Sicherheitsvorfall in mehreren Mitgliedstaaten gemeldet

werden muss (z. B. ein Unternehmen mit einer juristischen Person, das in mehreren Mitgliedstaaten niedergelassen ist und nicht nur unter die Ausnahmeregel der Hauptniederlassung fällt). In der Praxis betrifft ein Sicherheitsvorfall häufig nur einen Mitgliedstaat, so dass die Einrichtung ihn nur in einem Mitgliedstaat melden muss.

3.8. Was fällt unter die beiden Haftungsregelungen des Gesetzes (Art. 31 und 61)?

Siehe auch die Abschnitte 3.9 und 3.10 unten.

Artikel 31, § 1 des NIS2-Gesetzes sieht vor, dass Leitungsorgane für Verstöße ihrer Einrichtungen gegen Artikel 30 (Cybersicherheitsmaßnahmen) haften. Nach der Organtheorie wird die Haftung der juristischen Person grundsätzlich durch das Handeln ihrer Organe ausgelöst, wie in Artikel 2:49 des Gesetzbuches der Gesellschaften und Vereinigungen vorgesehen.

Die Theorie der kumulativen Haftung ist jedoch auf die zivilrechtliche Haftung anwendbar, insbesondere unter den Bedingungen und in den Grenzen, die in den Artikeln 2:56 bis 2:58 des Gesetzbuches der Gesellschaften und Vereinigungen festgelegt sind, so dass die zivilrechtliche Haftung der Mitglieder der Leitungsorgane (zumindest der Mitglieder der Verwaltungsorgane) unter der doppelten Bedingung eintreten kann, dass das Verschulden außervertraglicher Natur ist und offensichtlich den Rahmen überschreitet, in dem sich normalerweise umsichtige und sorgfältige Geschäftsführer unter den gleichen Umständen bewegen würden.

Darüber hinaus begründet Artikel 61, Absatz 1 des NIS2-Gesetzes eine besondere Haftung für jede natürliche Person, die für eine wesentliche oder wichtige Einrichtung verantwortlich ist oder als gesetzlicher Vertreter einer wesentlichen oder wichtigen Einrichtung aufgrund der Befugnis handelt, diese zu vertreten, in ihrem Namen Entscheidungen zu treffen oder ihre Kontrolle auszuüben, dies durch ihrer Befugnis, dafür zu sorgen, dass die Einrichtung das NIS2-Gesetz einhält. Diese Personen haften für Verstöße gegen ihre Pflicht, für die Einhaltung des NIS2-Gesetzes zu sorgen.

Vom Standpunkt der Verwaltungsmaßnahmen erlaubt das NIS2-Gesetz bei wiederholten Verstößen das vorübergehende Verbot für jede natürliche Person, die Führungsaufgaben auf der Ebene des Geschäftsführers oder des gesetzlichen Vertreters in der betreffenden wesentlichen Einrichtung wahrnimmt, diese Führungsaufgaben in dieser Einrichtung auszuüben, bis die betreffende wesentliche Einrichtung die erforderlichen Maßnahmen zur Behebung der Mängel oder zur Erfüllung der Anforderungen der zuständigen Behörde (Artikel 60, Absatz 1, 2° und Absatz 2, NIS2-Gesetz; siehe auch Abschnitt 4.18.2).

Schließlich ist festzustellen, dass das NIS2-Gesetz die Anwendung der strafrechtlichen Verantwortlichkeit nicht ausschließt. Die strafrechtliche Verantwortlichkeit juristischer Personen schließt die Verantwortlichkeit natürlicher Personen, die dieselben Handlungen begangen oder sich an ihnen beteiligt haben, nicht aus.

Mit Ausnahme der Bestimmung über Verwaltungsmaßnahmen, die nur für wesentliche Einrichtungen gilt, sind die oben genannten Elemente sowohl für wesentliche als auch für wichtige Einrichtungen anwendbar.

3.9. Welche Pflichten und Verantwortlichkeiten hat das Management?

Art. 31 & 61 NIS2-Gesetz

Die Leitungsorgane der NIS2-Einrichtungen müssen die Maßnahmen zum Management von Cybersicherheitsrisiken genehmigen und deren Umsetzung überwachen. Verstößt die Einrichtung gegen ihre Verpflichtung zur Durchführung von Risikomanagementmaßnahmen, ist das Leitungsorgan dafür verantwortlich.

Die Mitglieder des Leitungsorgans müssen eine Schulung absolvieren, um sicherzustellen, dass sie über ausreichende Kenntnisse und Fähigkeiten verfügen, um Risiken zu ermitteln und das Management von Cybersicherheitsrisiken und deren Auswirkungen auf die von der Einrichtung erbrachten Dienstleistungen zu bewerten.

Die Verantwortlichen und/oder gesetzlichen Vertreter einer NIS2-Einrichtung müssen befugt sein, die Einhaltung des NIS2-Gesetzes durch die Einrichtung zu gewährleisten. Sie haften für die Nichterfüllung dieser Pflicht.

Das Ziel dieser Verantwortlichkeit ist es, die Cybersicherheit zu einem Thema zu machen, das für die betroffenen Einrichtungen wirklich wichtig ist.

Diese Haftungsvorschriften berühren nicht die für öffentliche Einrichtungen geltenden Haftungsvorschriften sowie die Haftung von Beamten und gewählten oder ernannten Amtsträgern.

Es ist zu beachten, dass natürliche Personen, die in einer NIS2-Einrichtung Führungsaufgaben auf der Ebene des Geschäftsführers oder des gesetzlichen Vertreters wahrnehmen, bei Verstößen gegen die Anforderungen des NIS2-Gesetzes vorübergehend von der Ausübung von Führungsaufgaben in dieser Einrichtung ausgeschlossen werden können.

3.10. Was ist ein "Leitungsorgan"?

Der Begriff "Leitungsorgan" wird in der Richtlinie nicht definiert.

In der Begründung zum NIS2-Gesetz wird "Mitglied eines Leitungsorgans" wie folgt definiert:

Jede natürliche oder juristische Person, die:

(i) eine Funktion bei oder in Verbindung mit einer Einrichtung ausübt, die sie dazu berechtigt, (a) die betreffende Einrichtung zu verwalten und zu vertreten oder (b) im Namen und für Rechnung der Einrichtung Entscheidungen zu treffen, die für diese rechtlich bindend sind, oder in einem Organ der Einrichtung an solchen Entscheidungen mitzuwirken, oder

(ii) die Kontrolle über die Einrichtung ausübt, d.h. die rechtliche oder tatsächliche Befugnis, einen entscheidenden Einfluss auf die Bestellung der Mehrheit der Verwaltungsratsmitglieder oder Geschäftsführer der Einrichtung oder auf die Ausrichtung ihrer Geschäftsführung auszuüben.

Wenn es sich bei der Einrichtung um eine Gesellschaft nach belgischem Recht handelt, wird eine solche Kontrolle gemäß den Artikeln 1:14 bis 1:18 des Gesetzbuches der Gesellschaften und Vereinigungen bestimmt.

Wenn die Person, deren Rolle untersucht wird, eine juristische Person ist, wird der Begriff "Mitglied eines Leitungsorgans" rekursiv untersucht und umfasst sowohl die betreffende juristische Person als auch jedes Mitglied eines Leitungsorgans der genannten juristischen Person.

3.11. Welchen Inhalt sollte die Schulung für das Management haben?

Die Schulung der Mitglieder des Leitungsorgans soll sie in die Lage versetzen, die ihnen gesetzlich zugewiesenen Aufgaben ordnungsgemäß zu erfüllen, d. h. Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu genehmigen und die Implementierung dieser Maßnahmen zu überwachen. Es gibt keine Angaben zu den genauen Ausbildungsanforderungen. Inhalt und Dauer der Schulung sind daher den Einrichtungen überlassen.

Unser CyberFundamentals Framework enthält Informationen über den Schulungsprozess, insbesondere in Bezug auf Inhalt und Zielgruppen. In der Sicherheitsstufe Important findet sich zum Beispiel ab Seite 28 (CyFun® 2023) der Abschnitt über Schulungen.

Als Aufsichtsbehörde kann das ZCB weder Schulungen für NIS2 Einrichtungen anbieten, noch können wir spezifische Schulungsprogramme empfehlen.

3.12. Welche rechtlichen Bedingungen gelten für die Nutzung des Schutzrahmens bei der Suche und Meldung von Schwachstellen (ethisches Hacking)?

Das NIS2-Gesetz übernimmt die Bestimmungen des NIS1-Gesetzes, das einen Schutzrahmen (*safe harbour*) für "ethische Hacker" oder "digitale Whistleblower" vorsieht.

Art. 22 und 23 NIS2-Gesetz

Um von dem Schutzrahmen zu profitieren, muss eine Person:

- Ohne betrügerische oder schädliche Absicht handeln;
- Innerhalb von 24 Stunden nach der Entdeckung der Schwachstelle eine vereinfachte Meldung sowohl an das nationale CSIRT als auch an die verantwortliche Organisation senden;
- Innerhalb von 72 Stunden nach der Entdeckung eine vollständige Benachrichtigung an dieselben Adressaten senden;
- Nur innerhalb der Grenzen des Notwendigen und der Verhältnismäßigkeit handeln, um die Existenz einer Schwachstelle zu überprüfen und zu berichten;
- Es unterlassen eine Schwachstelle ohne Zustimmung des nationalen CSIRT öffentlich zu machen.

Außerdem müssen ethische Hacker, um die Netz- und Informationssysteme bestimmter Behörden wie Nachrichtendienste, dem Verteidigungsministerium, Justizbehörden, usw. nach

Schwachstellen durchsuchen zu können, zunächst eine Vereinbarung mit diesen Einrichtungen treffen.

Das ZCB bietet auf ihrer Website allgemeine Informationen über ethisches Hacking an, einschließlich einer Seite, die dem Meldeverfahren gewidmet ist.

3.13. Was sind die Verpflichtungen in Punkto Registrierung?

3.13.1. Wie registrieren sich NIS2-Einrichtungen?

Wesentliche und wichtige Einrichtungen müssen sich auf dem ZCB-Portal Safeonweb@Work registrieren.

Art. 13 NIS2-Gesetz

Die Frist für die Registrierung hängt von der Art der Einrichtung ab. Grundsätzlich haben wesentliche und wichtige Einrichtungen sowie Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, **fünf Monate** nach Inkrafttreten des Gesetzes, d.h. bis zum **18. März 2025**, Zeit, sich zu registrieren. Bei der Registrierung müssen sie die folgenden Informationen bereitstellen:

1) Ihr Name und die Registrierungsnummer der Zentralen Datenbank der Unternehmen (ZDU) oder eine gleichwertige Registrierung in der Europäischen Union;
2) Ihre aktuelle Adresse und Kontaktangaben, einschließlich E-Mail-Adresse, IP-Adresse und Telefonnummer;
3) Gegebenenfalls der betreffende Sektor und Teilsektor gemäß Anhang I oder II des Gesetzes;
4) Gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie Dienstleistungen erbringen, die in den Geltungsbereich des Gesetzes fallen.

Eine Ausnahme besteht für Einrichtungen, die diese Informationen bereits aufgrund einer gesetzlichen Verpflichtung einer sektoralen NIS2-Behörde mitgeteilt haben. In diesem Fall müssen die Informationen bei dieser Behörde lediglich vervollständigt werden. Wenn sich die Informationen ändern, müssen sie innerhalb von zwei Wochen nachgereicht werden.

Für die folgenden Arten von Einrichtungen aus den digitalen Sektoren gibt es eine leicht angepasste Regelung:

Art. 14 NIS2-Gesetz

- DNS-Dienstanbieter;
- TLD- Namensregister;
- Einrichtungen, die Domänennamen-Registrierungsdienste erbringen;
- Anbieter von Cloud-Computing-Diensten;
- Anbieter von Rechenzentrumsdienstleistungen;
- Anbieter von Inhaltszustellnetzen;
- Anbieter verwalteter Dienste;
- Anbieter verwalteter Sicherheitsdienste;
- Anbieter von Online-Marktplätzen;
- Anbieter von Online-Suchmaschinen; und
- Anbieter von Plattformen für Dienste sozialer Netzwerke.

Sie müssen sich innerhalb von **zwei Monaten** nach Inkrafttreten des Gesetzes, d.h. bis zum **18. Dezember 2024**, registrieren und die folgenden Informationen mitteilen:

1) Ihr Name;
2) Ihr Sektor, Teilsektor und die Art der Einrichtung, wie in Anhang I bzw. II aufgeführt;
3) Die Anschrift ihres Hauptgeschäftssitzes und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen sind, die Anschrift ihres Vertreters;
4) Ihre aktuellen Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern, sowie ggf. die ihres Vertreters;
5) Die Mitgliedstaaten, in denen sie ihre Dienstleistungen erbringen, die in den Geltungsbereich des Gesetzes fallen;
6) Ihre IP-Adressbereiche.

Auch hier ist jede Einrichtung verpflichtet, das ZCB unverzüglich über jede Änderung ihrer Angaben zu informieren.

In der Praxis werden einige dieser Informationen direkt von der Zentralen Datenbank der Unternehmen (ZDU) während des Registrierungsprozesses eingeholt.

3.13.2. Wie kann ich meine Organisation registrieren?

Alle praktischen Einzelheiten zum Registrierungsverfahren werden in unserem NIS2-Registrierungsleitfaden, der online verfügbar ist, erläutert.

Kurz gesagt: Die gesetzlichen Vertreter einer Organisation, die in der Zentralen Datenbank der Unternehmen (ZDU) aufgeführt ist (suchen Sie hier nach Ihrer Organisation), können sich mit der Plattform My eGov Role Management verbinden, um jedem geeigneten belgischen Bürger die erforderlichen Genehmigungen zu erteilen, um eine Organisation auf unserer Safeonweb@Work-Plattform zu registrieren. Alle Informationen finden Sie in diesem Leitfaden.

3.13.3. Wie kann ich feststellen, ob meine Organisation bereits registriert ist?

Die im Abschnitt 3.13.2 angegebene Person muss sich mit der Plattform verbinden, um dies zu überprüfen.

3.13.4. Welche Einrichtungen müssen sich in einer Unternehmensgruppe registrieren? Kann sich nur das Holdingunternehmen registrieren?

Innerhalb einer Unternehmensgruppe **müssen sich alle** Organisationen/getrennte juristische Entitäten (je nach Art der erbrachten Dienstleistungen auch das Holdingsunternehmen), die unter NIS2 fallen**, einzeln registrieren**. das Holdingsunternehmen kann sich nicht anstelle der Unternehmen seiner Gruppe registrieren.

3.13.5. Was ist, wenn meine Organisation Abteilungen oder Untereinheiten hat, die verschiedene Arten von Einrichtungen sind?

Gehören diese Abteilungen oder Untereinheiten alle zu ein und derselben Einrichtung, muss diese Einrichtung sich als alle diese verschiedenen Arten von Einrichtungen registrieren.

Handelt es sich bei den verschiedenen Untereinheiten um getrennte juristische Personen, die alle als "Einrichtung" im Sinne von NIS2 gelten (siehe Abschnitt 1.4), müssen sie sich alle getrennt registriert.

3.13.6. Müssen sich Organisationen in der Lieferkette von NIS2-Einrichtungen sich registrieren?

Nur Organisationen, die in den Anwendungsbereich von NIS2 fallen, müssen sich registrieren. Es ist möglich, dass Organisationen in der Lieferkette von NIS2-Einrichtungen selbst keine NIS2-Einrichtungen sind und sich daher nicht registrieren müssen.

Weitere Informationen zur Lieferkette finden Sie im Abschnitt 3.14.

3.13.7. Wie kann sich eine Organisation mit Sitz außerhalb Belgiens registrieren? Wie kann ein gesetzlicher Vertreter eine Organisation registrieren?

Es gibt zwei Ausnahmesituationen, in denen sich Organisationen außerhalb Belgiens registrieren lassen müssen:

1) Sie bieten elektronische Kommunikationsdienste oder -netzwerke in Belgien an (siehe Abschnitt 1.14);
2) Sie fallen unter die Hauptniederlassungsregelung (siehe Abschnitt 1.14), sind außerhalb der EU niedergelassen, erbringen Dienstleistungen in Belgien, haben Belgien als ihren Sitz in der EU gewählt und benennen dort einen gesetzlichen Vertreter.

Wenn sich Organisationen in diesen beiden Fällen nicht über die Safeonweb@Work-Website anmelden können, sollten sie das ZCB über info@ccb.belgium.be kontaktieren.

3.13.8. Muss ich mich erneut registrieren, wenn meine Organisation bereits unter NIS1 fällt?

Ja, die Organisation muss sich erneut registrieren.

3.13.9. Wie kann ich nachweisen, dass meine Organisation registriert ist?

NIS2-Organisationen können das ZCB über info@ccb.belgium.be bitten, ihnen ein Dokument als Nachweis für ihre Registrierung zur Verfügung zu stellen.

Dieses manuelle Verfahren wird bald durch ein Dokument ersetzt, das auf der Plattform heruntergeladen werden kann.

3.13.10. Was wird das ZCB mit Organisationen tun, die sich nicht registrieren lassen?

Das ZCB wird auf der Grundlage der Informationen, die ihm als föderale Behörde zur Verfügung stehen, proaktiv versuchen, Einrichtungen zu suchen und zu erreichen, die sich nicht registriert

haben. Es ist wichtig zu beachten, dass Einrichtungen, die sich nicht registriert haben, vorgeworfen werden kann, gegen das NIS2-Gesetz verstoßen zu haben und sich möglicherweise proportionalen Maßnahmen und Geldbußen aussetzen können.

3.14. Lieferkette/Supply chain: Wie kann eine Einrichtung die Beziehungen zu ihren Lieferanten und direkten Dienstleistern verwalten?

Art. 30, §3, 4° NIS2-Gesetz

Als Teil der Mindestliste von Risikomanagementmaßnahmen im Bereich der Cybersicherheit müssen Einrichtungen, die unter das NIS2-Gesetz fallen, geeignete und verhältnismäßige Maßnahmen ergreifen, um ihr Netzwerk- und Informationssystem zu sichern.

Eine dieser Maßnahmen ist die Sicherheit der Lieferkette der Einrichtung. Dazu gehören die Sicherheitsaspekte der Beziehungen zwischen jeder Einrichtung und ihren **direkten Lieferanten oder Dienstleistern**.

Diese Verpflichtung wirkt in zwei Richtungen: Einerseits müssen NIS2-Einrichtungen von den Organisationen in ihrer Lieferkette (wie direkte Anbieter oder Diensteanbieter) entsprechende Risikomanagementmaßnahmen im Bereich der Cybersicherheit verlangen und diese überwachen, andererseits müssen nicht von NIS2 betroffene Einrichtungen derlei Maßnahmen in zweckmäßigem und angemessenem Umfang ergreifen.

Dabei legt das NIS2-Gesetz nicht fest, wie dieser Verpflichtung durch die NIS2-Einrichtungen nachzukommen ist. So liegt insbesondere die Überprüfung der pflichtgemäßen Umsetzung der genannten Maßnahmen entlang der direkten Lieferkette bei den Einrichtungen selbst. Um den Nachweis der Pflichterfüllung entlang der zu vereinfachen, empfiehlt das ZCB allen NIS2-Einrichtungen, von den Organisationen in der Lieferkette vertraglich ein Label oder Zertifikat zum Beispiel gemäß dem CyberFundamentals (CyFun®) Framework zu verlangen.

Bei laufenden Verträgen mit Lieferanten und Dienstleistern obliegt es der Einrichtung, die derzeit geltenden Bestimmungen zu prüfen und sicherzustellen, dass sie den Verpflichtungen entsprechen. Bestehende Verträge müssen gegebenenfalls überarbeitet werden. Die NIS2-Einrichtung sollte ausreichende vertragliche Schutzvorkehrungen für den Fall treffen, dass die Organisation in ihrer Lieferkette ihren Verpflichtungen nicht nachkommt. Wann die Verträge angepasst werden sollten, ist dem Zeitplan im Abschnitt 4.14 zu entnehmen.

Um die richtige CyFun®-Stufe zu wählen, die den Lieferanten und Dienstleistern auferlegt werden soll, muss die NIS2 eine Risikobewertung vornehmen und auf der Grundlage des Ergebnisses die am besten geeignete Stufe auferlegen. Zu diesem Zweck könnte das CyFun® Risk Assessment Tool verwendet werden.

Das ZCB empfiehlt ebenfalls allen nicht dem NIS2-Gesetz unterliegenden Einrichtungen die Einführung entsprechender zweckmäßiger und angemessener Risikomanagementmaßnahmen für den Fall, dass sie in die Lieferkette einer NIS2-Einrichtung geraten. Hier hilft wiederum das CyFun® Framework bei der Ermittlung und Umsetzung konkreter Maßnahmen, wie sie gegebenenfalls verlangt werden können.

Weder eine bestimmte Beteiligung von NIS2-Einrichtung an einer Organisation in ihrer Lieferkette noch deren Größe haben Auswirkungen auf den Anwendungsbereich dieser Verpflichtung. Sie können sich lediglich auf die Risikobewertung von NIS2-Einrichtungen in der Lieferkette auswirken.

Zur Bewältigung von Sicherheitsvorfällen bei Zulieferern siehe Abschnitt 3.7. Siehe auch Abschnitt 3.9 über die Verantwortung der Leitungsorgane für Risikomanagementmaßnahmen im Bereich der Cybersicherheit.

3.15. Welche Vertraulichkeitsverpflichtungen müssen beachtet werden?

Art. 26 NIS2-Gesetz

Die zuständigen Behörden, wesentliche oder wichtige Einrichtungen und ihre Auftragsverarbeiter beschränken den Zugang zu Informationen im Rahmen des NIS2-Gesetzes auf Personen, die zur Wahrnehmung ihrer Aufgaben oder Pflichten im Zusammenhang mit der Durchführung des Gesetzes Kenntnis von den Informationen haben und/oder Zugang zu ihnen haben müssen.

Informationen, die den zuständigen Behörden von wesentlichen oder wichtigen Einrichtungen zur Verfügung gestellt werden, können jedoch mit Behörden in der Europäischen Union, mit belgischen Behörden oder mit ausländischen Behörden ausgetauscht werden, wenn ein solcher Austausch für die Anwendung von Rechtsvorschriften erforderlich ist.

Die ausgetauschten Informationen beschränken sich auf das, was relevant ist, und stehen in einem angemessenen Verhältnis zum Zweck des Informationsaustauschs, insbesondere im Einklang mit der Verordnung (EU) 2016/679 (DSGVO). Dieser Informationsaustausch wahrt die Vertraulichkeit der relevanten Informationen und schützt die Sicherheit und die Geschäftsinteressen wesentlicher oder wichtiger Einrichtungen.

Art. 27 NIS2-Gesetz

Das Gesetz sieht jedoch die Möglichkeit vor, freiwillig Informationen auszutauschen, die für die Cybersicherheit relevant sind, darunter insbesondere Informationen über Cyberbedrohungen, verhinderte Sicherheitsvorfälle, Schwachstellen, etc. Dieser Austausch findet unter bestimmten Bedingungen im Rahmen von Informationsaustauschgemeinschaften statt, die durch Vereinbarungen über die gemeinsame Nutzung von Informationen umgesetzt werden.

4. Kontrolle / Aufsicht

4.1. Wer sind die zuständigen Behörden?

Art. 15, 16 ff. NIS2-Gesetz und Art. 3 NIS2 Königlicher Erlass

4.1.1. Das Zentrum für Cybersicherheit Belgien (ZCB)

Die nationale Cybersicherheitsbehörde (ZCB) ist für die Koordinierung und Überwachung des Gesetzes zuständig. Zu diesem Zweck kombiniert das Gesetz die bestehenden Aufgaben der ZCB mit den in der NIS2-Richtlinie vorgesehenen Ergänzungen, insbesondere in Bezug auf die Aufsicht über Einrichtungen. Der ZCB ist für die Aufsicht über wesentliche und wichtige Einrichtungen zuständig (mit Unterstützung der sektoralen Behörden) und ist die zentrale Kontaktstelle für die Umsetzung von NIS2.

Das nationale Computersicherheits-Ereignis- und Reaktionsteam (*National Computer Security Incident Response Team*, CSIRT) ist ebenfalls Teil der nationalen Cybersicherheitsbehörde. Die NIS2-Einrichtungen sind verpflichtet, diesem CSIRT erhebliche Sicherheitsvorfälle zu melden.

4.1.2. Sektorspezifische Behörden

Die folgenden sektoralen Behörden wurden benannt:

1. **für den Energiesektor**: der für Energie zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
2. **für den Verkehrssektor:**
    a. In Bezug auf den Transportsektor, mit Ausnahme des Wassertransports: der für den Transport zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
    b. In Bezug auf den Wassertransport: der für die maritime Mobilität zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
3. **für den Gesundheitswesen-Sektor:**
    a. In Bezug auf Einrichtungen, die Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben; Einrichtungen, die pharmazeutische Erzeugnisse herstellen; und Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden: die Föderale Agentur für Arzneimittel und Gesundheitsprodukte (AFMPS/FAGG);
    b. Der für Volksgesundheit zuständige Föderalminister, oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung;
4. **für den Bereich digitale Infrastruktur: das** Belgische Institut für Postdienste und Telekommunikation (BIPT);

5. **in Bezug auf Vertrauensdienstanbieter**: der für Wirtschaft zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
6. **für den Bereich der digitalen Anbieter**: der für Wirtschaft zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
7. **für die Bereiche Raumfahrt und Forschung**: der für Wissenschaftspolitik zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
8. **für Trinkwasser**: das Nationale Sicherheitskomitee für die Bereitstellung und Verteilung von Trinkwasser;
9. **für den Bankensektor**: die Belgische Nationalbank (BNB);
10. **für den Bereich der Finanzmarktinfrastruktur**: die Finanzdienstleistungs- und Marktaufsichtsbehörde (FSMA).

Die sektoralen Behörden haben eine Reihe von Kompetenzen. Weitere Informationen finden Sie in Abschnitt 4.8.

Einrichtungen, die unter eine sektorale Behörde fallen, können sich an diese wenden, um Informationen und Unterstützung zu erhalten, usw.

4.1.3. Das Nationale Krisenzentrum (NCCN)

Das Nationale Krisenzentrum ist auch an der Umsetzung des NIS2-Gesetzes beteiligt, insbesondere in Bezug auf die Meldung von Sicherheitsvorfällen, das Cyber-Krisenmanagement und die von den Betreibern kritischer Infrastrukturen und kritischen Einrichtungen (die der CER-Richtlinie unterliegen) umgesetzten Maßnahmen zur Gewährleistung der physischen Sicherheit.

4.2. Welche Rahmenwerke können von NIS2-Einrichtungen zum Nachweis ihrer Konformität verwendet werden?

Art. 5, §1 NIS2 Königlicher Erlass

Wesentliche Einrichtungen, die einer Pflicht zur regelmäßigen Konformitätsbewertung unterliegen, können sich für die Verwendung eines der beiden im Königlichen Erlass von NIS2 genannten Rahmenwerk entscheiden.

Die Verwendung dieser Rahmen zur Kontrolle wird im nächsten Abschnitt erläutert (4.4.).

4.2.1. Das CyberFundamentals (CyFun®) Framework

Das CyberFundamentals (CyFun®) Framework[4] ist ein Rahmenwerk mit konkreten Maßnahmen um:

- Daten zu schützen;
- das Risiko der häufigsten Cyberangriffe erheblich zu reduzieren;
- die Cyber-Resilienz einer Organisation zu erhöhen.

Um der Schwere der Bedrohung, der eine Organisation ausgesetzt ist, gerecht zu werden, gibt es neben der Ausgangsstufe Small drei weitere Sicherheitsstufen: Basic, Important und Essential.

[4] https://cyfun.be

Das Rahmenwerk wurde mit Hilfe von Angriffsprofilen des CERT (aus erfolgreichen Angriffen gewonnen) validiert. Die Schlussfolgerung lautet:

- Maßnahmen der Sicherheitsstufe „Basic" können 82 % der Angriffe abdecken;
- Maßnahmen der Sicherheitsstufe „Important" können 94 % der Angriffe abdecken;
- Maßnahmen der Sicherheitsstufe „Essential" können 100 % der Angriffe abdecken.

Darüber hinaus ist das CyFun® Framework:

- **Auf anerkannten Normen basiert**: CyFun® wählt relevante Kontrollen auf der Grundlage gemeinsamer Standards wie NIST CSF, ISO/IEC 27001, CIS-Controls und IEC 62443 aus;
- **entspricht den Maßnahmen, die notwendig sind**, um die wichtigsten vom ZCB identifizierten Angriffe zu verhindern;
- **Von jedem selbst verwendbar**: Zu jeder Kontrolle gibt es eine Anleitung, die bei der Implementierung hilft. Das Selbstbewertungstool von CyFun hilft den Überblick über eine Implementierung zu behalten;
- **Zur Validierung einer Implementierung**: Man kann seine Implementierung validieren, indem man eine Bewertung durch eine zugelassene Konformitätsbewertungsstelle anfordert. Diese Bescheinigung dient als Nachweis für die Implementierung gegenüber Kunden und Behörden (z. B. zur Einhaltung von NIS2).

Das CyFun® Framework ist bezüglich NIS2 für die regelmäßige Konformitätsbewertung wesentlicher Einrichtungen, aber auch für wichtige Einrichtungen besonders nützlich. Es ist kostenlos verfügbar und bietet unkomplizierte Lösungen für Risikobewertung, Selbstbewertung und die konkrete Umsetzung der vom NIS2-Gesetz geforderten Mindestmaßnahmen für das Risikomanagement im Bereich der Cybersicherheit. Darüber hinaus wird bei einer validierten oder zertifizierten Implementierung des CyFun®-Frameworks davon ausgegangen, dass die betreffenden Einrichtungen im Rahmen der Aufsicht gemäß NIS2 konform sind.

Das ZCB empfiehlt allen NIS2-Einrichtungen nachdrücklich, das CyFun®-Framework zu verwenden, welches auf unserer Safeonweb@Work Website öffentlich und kostenlos verfügbar ist.

4.2.2. ISO/IEC 27001

Die europäische Norm ISO/IEC 27001 ist eine international anerkannte technische Norm, die den allgemeinen und strukturierten Ansatz für ein Sicherheitsmanagement für jedes Informationssystem festlegt. Es handelt sich also um eine Grundnorm, die die allgemeinen Grundsätze für die Umsetzung aller Sicherheitsmaßnahmen eines Informationssystems festlegt und in allen Sektoren anwendbar ist.

Die letzte Fassung stammt aus dem Jahr 2022, wurde aber ohne Angabe eines Datums in den Königlichen Erlass übernommen, damit immer die neueste Fassung angewendet werden kann.

Weitere Informationen sind auf der offiziellen Website zu finden.

4.3. Wo kann ich weitere Informationen über CyFun® finden?

Alle Informationen, Dokumente, Anleitungen usw. sind auf **Fehler! Linkreferenz ungültig.**zentralisiert.

CyFun® hat auch eine eigene FAQ unter: https://atwork.safeonweb.be/cyberfundamentals-frequently-asked-questions-faq.

4.4. Wie werden betroffenen Einrichtungen kontrolliert? Kann das ZCB CyFun Zertifizierungen vergeben?

Art. 39 ff. NIS2-Gesetz
Art. 6-13 NIS2 Königlicher Erlass

Wenn man im Zusammenhang mit dem Gesetz von Kontrolle/Aufsicht spricht, muss man zwischen zwei Kategorien von Einrichtungen unterscheiden: wesentliche Einrichtungen und wichtige Einrichtungen.

Wesentliche Einrichtungen müssen sich einer regelmäßigen Konformitätsbewertung unterziehen. Diese Bewertung wird auf der Grundlage der von der Einrichtung getroffenen Wahl zwischen drei Optionen durchgeführt:

- entweder eine CyberFundamentals (CyFun®)-Zertifizierung, die von einer vom ZCB zugelassenen Konformitätsbewertungsstelle (KBS/CAB) vergeben wird (nach Akkreditierung durch BELAC);
- oder eine ISO/IEC 27001-Zertifizierung, die von einem CAB ausgestellt wurde, das von einer Akkreditierungsstelle akkreditiert wurde, die das Abkommen über die gegenseitige Anerkennung (MLA), unter das die ISO/IEC 27001-Norm fällt, im Rahmen der Europäischen Kooperation für Akkreditierung (EA) oder des Internationalen Akkreditierungsforums (IAF) unterzeichnet hat, und vom ZCB zugelassen wurde;
- oder eine Inspektion durch den Inspektionsdienst das ZCB (oder durch einen sektoralen Inspektionsdienst).

Der Inspektionsdienst kann auch jederzeit wesentliche Einrichtungen kontrollieren (wenn kein Sicherheitsvorfall vorliegt - *ex ante* - und nach einem Vorfall oder wenn genügend Beweise für die Nichteinhaltung des Gesetzes vorliegen - *ex post*).

Bei wichtigen Einrichtungen erfolgt die Aufsicht nur "*ex post*" durch den Inspektionsdienst, d.h. nach einem Sicherheitsvorfall oder aufgrund von Beweisen, Hinweisen oder Informationen, dass eine wichtige Einrichtung ihren Verpflichtungen nicht nachkommt (Art. 48, §2 NIS2-Gesetz). Daher unterliegen sie grundsätzlich keiner regelmäßigen Konformitätsbewertung. Diese Einrichtungen können sich jedoch freiwillig denselben Regelungen unterziehen wie wesentliche Einrichtungen.

Für die Modalitäten der vom Inspektionsdienst durchgeführten Inspektion siehe Abschnitt 4.15.

Das ZCB führt keine regelmäßigen Konformitätsbewertungen von NIS2-Einrichtungen durch, die zu einer Konformitätsvermutung führen könnten, und vergibt daher auch keine CyFun®-Zertifizierungen. Dies dürfen nur CABs.

4.5. Muss eine Organisation eine CyFun®-Zertifizierung oder -Verifizierung erhalten, wenn sie ISO/IEC 27001 anwenden will?

Nein, eine CyFun®-Zertifizierung oder -Verifizierung ist kein notwendiger Zwischenschritt, um eine ISO/IEC 27001-Zertifizierung zu erhalten.

Es ist jedoch möglich, ein CyFun Label zu erhalten, indem man eine bestehende ISO/IEC 27001 Zertifizierung mit dem richtigen Anwendungsbereich und *Statement of Applicability* verwendet. Dazu müssen die erforderlichen Dokumente über die Registerkarte "Labels" auf dem Dashboard Ihrer registrierten Organisation auf Safeonweb@Work hochgeladen werden.

4.6. Was ist eine Konformitätsbewertungsstelle (KBS/CAB)?

Eine Konformitätsbewertungsstelle (*Conformity Assessment Body* - "CAB") ist eine Stelle, die die Einhaltung der Anforderungen des CyFun®-Rahmenwerks oder der ISO/IEC 27001 Norm (die im Rahmen des NIS2-Gesetzes angewendet wird) durch NIS2-Einrichtungen, die der regelmäßigen Konformitätsbewertung unterliegen (obligatorisch für wesentliche, freiwillig für wichtige Einrichtungen), überwacht und zertifiziert.

Im Rahmen von CyFun® ist ein CAB von der belgischen Akkreditierungsbehörde (BELAC) akkreditiert und von der ZCB zugelassen. Im Rahmen von ISO/IEC 27001 ist es von einer Akkreditierungsstelle akkreditiert, die das Abkommen über gegenseitige Anerkennung (MLA), unter das die Norm ISO/IEC 27001 fällt, im Rahmen der Europäischen Kooperation für Akkreditierung (EA) oder des Internationalen Akkreditierungsforums (IAF) unterzeichnet hat, und vom ZCB zugelassen. Weitere Informationen finden Sie in den Zulassungsbedingungen von CABs auf unserer Website.

4.7. Wo kann ich weitere Informationen über CABs finden?

Alle Informationen über die Akkreditierung in Belgien finden Sie auf der offiziellen Website von BELAC: https://economie.fgov.be/en/themes/quality-and-safety/accreditation.

Weitere Informationen zu CABs im Rahmen von CyFun® finden Sie hier auf unserer Website: https://atwork.safeonweb.be/de/konformitaetsbewertungsstelle-cab.

4.8. Was sind die Aufgaben der sektoralen Behörden?

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 und 52 NIS2-Gesetz

Die sektoralen Behörden spielen im Rahmen des NIS2-Gesetzes ebenfalls eine Rolle, da sie über besonderes Wissen und Fachkenntnisse in den jeweiligen Sektoren verfügen. Sie können ggf. bei den folgenden Aufgaben tätig werden:

- Zusätzliche Identifikation;
- Registrierung von Einrichtungen;
- Organisation von sektoralen Übungen;
- Analyse und Bewältigung der Folgen eines Sicherheitsvorfalls für einen Sektor;
- Teilnahme an einigen Arbeiten der NIS-Kooperationsgruppe;
- Sensibilisierung der Einrichtungen in ihren Sektoren;
- Zusammenarbeit auf nationaler Ebene;
- Zusätzliche Maßnahmen zum Management von Cybersicherheitsrisiken;
- Benachrichtigung über Sicherheitsvorfälle;
- Aufsicht und Inspektion (gemeinsam oder delegiert);
- Administrative Bußgelder.

4.9. Wie kann eine Einrichtung nachweisen, dass sie ihre Pflichten erfüllt? Was ist eine Konformitätsvermutung?

Art. 42 NIS2-Gesetz
Art. 5, §1 NIS2 Königlicher Erlass

Im Rahmen der regelmäßigen Konformitätsbewertung - die für wesentliche Einrichtungen obligatorisch ist - wird es für die Einrichtung möglich sein, eine Zertifizierung oder ein Siegel zu erhalten, bei dem bis zum Beweis des Gegenteils davon ausgegangen werden kann, dass die Einrichtung ihre Verpflichtungen in Bezug auf die Cybersicherheit erfüllt.

Diese Zertifizierung wird auf den beiden im Königlichen Erlass genannten Rahmenwerken basieren: den CyberFundamentals oder der internationalen Norm ISO/IEC 27001 (mit dem richtigen Anwendungsbereich und *Statement of Applicability*). Siehe in diesem Zusammenhang auch Abschnitt 4.2.

Es ist wichtig zu beachten, dass der **Anwendungsbereich einer Zertifizierung mit dem Anwendungsbereich des NIS2-Gesetzes übereinstimmen** muss, d.h. sie muss alle Netzwerke und Informationssysteme einer Organisation als Ganzes umfassen, andernfalls kann die Organisation aufgrund der Zertifizierung nicht von der Konformitätsvermutung profitieren.

Selbstverständlich kann eine Einrichtung auch einen anderes Rahmenwerk oder technischen Standard verwenden, um ihre rechtlichen Anforderungen an die Cybersicherheit umzusetzen. In diesem Fall gibt es jedoch keine Konformitätsvermutung, und dem Inspektionsdienst muss anhand einer Mapping-Tabelle mit einem der beiden genannten Standards nachgewiesen werden, dass alle erforderlichen Maßnahmen umsetzt wurden.

4.10. Kann der Anwendungsbereich einer Zertifizierung oder Verifizierung auf die NIS2-bezogenen Dienste und Tätigkeiten beschränkt werden?

Wie im Abschnitt 4.9 erwähnt, darf der Anwendungsbereich einer Zertifizierung oder Verifizierung nicht kleiner sein als der Anwendungsbereich des NIS2-Gesetzes, der die gesamte Organisation umfasst.

4.11. Kann eine Einrichtung eine niedrigere CyFun® Sicherheitsstufe als die ihrer Kategorie entsprechende verwenden? Ändert sich dadurch ihre NIS2-Qualifikation?

Art. 7 NIS2 Königlicher Erlass

Der Königliche Erlass lässt einer Einrichtung die Möglichkeit, eine niedrigere CyFun®-Stufe zu verwenden (z.B. die Verwendung der Sicherheitsstufe Important für eine wesentliche Einrichtung), sofern sie dies auf Grundlage ihrer Risikoanalyse objektiv rechtfertigen kann. Diese Entscheidung liegt in der alleinigen Verantwortung der betreffenden Einrichtung und hat **keinen Einfluss auf ihre rechtliche Einstufung als wesentliche oder wichtige Einrichtung**. Es ist zu betonen, dass diese Wahl jederzeit vom Inspektionsdienst im Rahmen seiner Kontrollaufgaben in Frage gestellt werden kann.

Die ZCB bietet ein auf Safeonweb@Work verfügbares Risikobewertungstool an, damit eine Einrichtung eine fundierte Auswahl der für sie geeigneten CyFun®-Sicherheitsstufe treffen kann.

4.12. Benötigen Organisationen die Zustimmung des ZCB, um eine niedrigere Stufe von CyFun® zu verwenden?

Nein, die NIS2-Einrichtungen müssen das ZCB nicht um eine Bestätigung ihrer Analyse bitten, um eine niedrigere Sicherheitsstufe von CyFun® zu verwenden. Wie im Abschnitt 4.11 angegeben, ist jede NIS2-Einrichtung selbst für diese Entscheidung verantwortlich. Die Begründung für diese Wahl muss nur intern dokumentiert werden.

Bei einer Inspektion kann der betreffende Inspektionsdienst die von der Einrichtung getroffene Wahl kontrollieren.

4.13. Kann eine Einrichtung, die unter NIS1 ein Betreiber wesentlicher Dienste (BWD) war, ihre ISO27001-Zertifizierung behalten?

Art. 8, 12 und 14-15 NIS2 Königlicher Erlass

Wenn eine Einrichtung, die unter NIS1 Betreiber eines wesentlichen Dienstes (BWD) war, über eine ISO/IEC 27001 Zertifizierung verfügt, kann sie ihre Zertifizierung im Rahmen der von NIS2 ausgelegten regelmäßigen Konformitätsbewertung vorlegen. Bei Bedarf muss der Geltungsbereich der Zertifizierung erweitert werden, um sicherzustellen, dass sie alle Netz- und Informationssysteme der betreffenden Einrichtung abdeckt.

Die Zertifizierung muss von einer Konformitätsbewertungsstelle durchgeführt werden, die von BELAC in Belgien (oder von einer anderen akkreditierten europäischen nationalen Stelle, wenn die Zertifizierung aus einem anderen Mitgliedstaat stammt) akkreditiert und vom ZCB zugelassen ist.

4.14. [Zeitleiste] Ab wann müssen die betroffenen Einrichtungen die Verpflichtungen aus dem Gesetz umsetzen?

Art. 13 & 75 NIS2-Gesetz

Art. 22-23 NIS2 Königlicher Erlass

Die meisten im NIS2-Gesetzeskader festgelegten Verpflichtungen gelten ab dem 18. Oktober 2024. Das Gesetz bzw. der königliche Erlass räumt den Einrichtungen bei einigen Verpflichtungen jedoch längere Fristen für die Umsetzung ein.

Ab dem 18. Oktober 2024 gelten insbesondere die folgenden Verpflichtungen:

- Implementierung von Mindestrisikomanagementmaßnahmen im Bereich der Cybersicherheit;
- Meldung aller erheblichen Sicherheitsvorfälle;
- Wahrnehmen der Aufsichtsplichten und Zusammenarbeit mit den zuständigen Behörden;

- Für Leitungsorgane: Genehmigung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Überwachung der Umsetzung entsprechender Maßnahmen, Haftung für Rechtsverletzungen durch die Einrichtung und Teilnahme an Cybersicherheitsschulungen.

Zur Registrierung der Einrichtungen beim ZCB über Safeonweb@Work legt das Gesetz folgende Fristen fest:

- Gehören die Dienstleistungen einer Einrichtung gemäß dem jeweiligen Anhang zu den digitalen Sektoren (siehe Liste in Art. 14, §1 des Gesetzes), hat die Einrichtung ab dem 18. Oktober 2024 2 Monate Zeit für die Registrierung (**spätestens bis zum 18. Dezember 2024**).
- Alle übrigen Einrichtungen haben 5 Monate nach dem 18. Oktober 2024, um sich zu registrieren (**spätestens bis zum 18. März 2024**).

Auch bei der Aufsicht/regelmäßigen Konformitätsbewertung wesentlicher Einrichtungen wird unterschieden:

- Bei Nutzung des CyberFundamentals (CyFun®) Frameworks:
  - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie die **Sicherheitsstufe Basic** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie eine Verifizierung durch eine akkreditierte und autorisierte Konformitätsbewertungsstelle (hiernach ein „CAB“) durchführen lassen müssen;
  - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie **Sicherheitsstufe Important** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie entweder eine Basic- oder eine Important-Verifizierung durch eine akkreditierte und autorisierte CAB erhalten müssen.
    Falls erforderlich, können sie eine erste Verifizierung auf Stufe Basic und eine Verifizierung auf Stufe Important nach einer zusätzlichen Frist von 12 Monaten durchführen (**spätestens bis zum 18. April 2027**);
  - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie **Sicherheitsstufe Essential** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie entweder eine Basic- oder eine Important-Verifizierung durch ein akkreditiertes und autorisiertes CAB erhalten müssen.
    Sie haben eine zusätzliche Frist von 12 Monaten (**spätestens bis zum 18. April 2027**), innerhalb derer sie eine Sicherheitsstufe Essential-Zertifizierung durch ein akkreditiertes und autorisiertes CAB erhalten müssen.
- Entscheidet sich eine Einrichtung für ein Zertifikat gemäß ISO/IEC 27001, muss sie ihren Anwendungsbereich und ihr *Statement of Applicability* bis zum 18. April 2026 an das ZCB übermitteln und bis zum 18. April 2027 eine Zertifizierung durch eine CAB erhalten.
- Entscheidet sich eine Einrichtung für die direkte Überprüfung durch das ZCB:
  - **Bis spätestens dem 18. April 2026**: Entweder Einreichung der Selbstbewertung von CyFun® Sicherheitsstufe Basic oder Important, oder der ISO/IEC 27001-Informationssicherheitsrichtlinie, den Anwendungsbereich und das *Statement of Applicability* an das ZCB übermitteln;
  - **Bis spätestens dem 18. April 2027**: Bericht über den Konformitätsfortschritt.

Wichtige Einrichtungen sind nicht Gegenstand einer regelmäßigen obligatorischen Konformitätsbewertung (Ex-post-Aufsicht). Unter Beachtung der Angemessenheit und Verhältnismäßigkeit der Cybersicherheitsmaßnahmen wird der Inspektionsdienst wichtige Einrichtungen beaufsichtigen, wobei ein ähnlicher Zeitraum von 18 Monaten nach Inkrafttreten des Gesetzes eingehalten werden muss (damit sie das erforderliche Niveau vollständig erreichen können).

Wenn sich beispielsweise Anfang 2025 ein bedeutender Cybervorfall ereignet, muss die betreffende Einrichtung die erforderlichen Maßnahmen zur Bewältigung dieses Vorfalls ergreifen und ihn dem ZCB melden, möglicherweise unter der Aufsicht der zuständigen Inspektionsdienste. Aus diesem Grund fordern wir alle NIS2-Einrichtungen auf, mit der Umsetzung der erforderlichen Maßnahmen nicht bis zum Ablauf der Registrierungsfrist und ihrer ersten Konformitätsbewertungen zu warten.

4.15. Wie wird die Inspektion durchgeführt?

Art. 44 ff. NIS2-Gesetz

Der Inspektionsdienst der nationalen Cybersicherheitsbehörde ist zuständig für das Durchführen von Inspektionen zur Überprüfung, ob wesentliche und wichtige Einrichtungen die Maßnahmen zum Management von Cybersicherheitsrisiken und die Vorschriften für die Meldung von Sicherheitsvorfällen einhalten.

Inspektionen wesentlicher Einrichtungen können sowohl *ex ante* (proaktiv) als auch *ex post* (reaktiv) durchgeführt werden. Sie werden vom Inspektionsdienst das ZCB oder vom benannten sektorielle Inspektionsdienst (spezifische/ergänzende sektorielle Maßnahmen) durchgeführt. Diese Inspektionen können auf Antrag der sektoriellen Behörde gemeinsam von den oben genannten Behörden durchgeführt werden.

Wesentliche Einrichtungen sind darüber hinaus verpflichtet, sich regelmäßigen Konformitätsbewertungen zu unterziehen. Wichtige Einrichtungen können sich auch freiwillig einer Konformitätsbewertung auf der Grundlage von ISO/IEC 27001 oder den CyberFundamentals unterziehen (siehe Abschnitt 4.4.).

Ex-post-Inspektionen wichtiger Einrichtungen werden auf der Grundlage von Indikatoren durchgeführt, wie z.B. dem Auftreten eines Sicherheitsvorfalls oder objektiven Beweisen für mögliche Mängel. Auch hier kann die Inspektion vom Inspektionsdienst des ZCB, dem benannten sektorielle Inspektionsdienst oder von beiden durchgeführt werden. Das Ziel der gemeinsamen Kontrollen oder der an den sektorielle Inspektionsdienst delegierten Kontrollen ist es zu vereinfachen und die staatlichen Ressourcen zu rationalisieren.

Die Inspektoren können sich vor Ort begeben, Feststellungen durch Protokolle treffen und Berichte verfassen. Auf der Grundlage dieser Feststellungen kann ein Verfahren eingeleitet werden, in dem die Einrichtung aufgefordert wird, einen Verstoß abzustellen und gegebenenfalls geeignete Verwaltungsmaßnahmen zu ergreifen, die von einer Verwarnung bis hin zu einem Bußgeld reichen können.

4.16. Was passiert, wenn meine Organisation nach 18 Monaten nicht nachweisen kann, dass sie die Vorschriften einhält?

Bei ihren Kontrollen wird der Inspektionsdienst großen Wert darauf legen, wie sich eine Organisation im Laufe der Zeit auf ihr Ziel hin entwickelt hat. Es ist daher von großer Bedeutung, dass praktische Fortschritte bei der Einhaltung der Vorschriften nachgewiesen werden können.

Das Hauptziel des ZCB ist es, in enger Zusammenarbeit mit allen betroffenen Einrichtungen ein hohes Cybersicherheitsniveau im ganzen Land zu erreichen. Dennoch gibt es Situationen, in denen Sanktionen erforderlich sein können. Zu diesem Zweck sieht das Gesetz (Titel 4, Kapitel 2) ein spezielles Verfahren vor, das die Interaktion zwischen dem ZCB und der betroffenen Einrichtung regelt. Dieses Verfahren beinhaltet insbesondere die Verpflichtung des ZCB (oder einer sektoralen Behörde), die Einrichtung über seine Absicht zu informieren, eine Sanktion zu verhängen. Es versteht sich von selbst, dass dieser Entwurf einer Sanktionsentscheidung mit einer ausreichenden Begründung versehen sein muss. Die Einrichtung hat dann die Möglichkeit, sich zu verteidigen.

Sollte eine Sanktion dennoch für notwendig erachtet werden, muss das ZCB eine bestimmte Mindestanzahl von Elementen berücksichtigen, um eine angemessene und verhältnismäßige Sanktion zu bestimmen; zum Beispiel die Kategorie der Einrichtung, frühere Verstöße, die Schwere des Verstoßes, seine Dauer, Schäden, Fahrlässigkeit usw.

In jedem Fall kann die zuständige Inspektion bei Nichteinhaltung der Vorschriften geeignete Maßnahmen ergreifen und/oder Bußgelder verhängen, um sicherzustellen, dass die Organisation die gesetzlichen Vorschriften einhält. Je nachdem, wie sich diese Maßnahmen und/oder Geldbußen auf das Verhalten der Organisation auswirken, können weitere Maßnahmen und/oder Geldbußen verhängt werden, bis die Einhaltung der Vorschriften erreicht ist.

Weitere Informationen über Maßnahmen und Bußgelder finden Sie in den Abschnitten 4.17 und 4.18.

4.17. Sind Verwaltungsmaßnahmen und Geldstrafen verhältnismäßig? Wie hoch sind die Bußgelder?

Art. 59 NIS2-Gesetz

Das Ziel von Verwaltungsmaßnahmen und Geldstrafen ist es, die Cybersicherheit wesentlicher und wichtiger Einrichtungen zu erhöhen. Unter Einhaltung der gesetzlich vorgeschriebenen Verfahren (einschließlich der Anhörung der betroffenen Einrichtung, siehe Art. 51-57) können verhältnismäßige Verwaltungsmaßnahmen oder Geldbußen verhängt werden, wobei die Schwere der Verstöße, das Verhalten der Einrichtung und mögliche Wiederholungsfälle berücksichtigt werden.

Die folgenden Verwaltungsmaßnahmen können verhängt werden:

1. 500 bis 125.000 Euro für jeden, der den Informationspflichten nach Artikel 12 nicht nachkommt;
2. 500 bis 200.000 Euro für die Einrichtung, die eine für sie handelnden Person negative Konsequenzen erleiden lässt, weil diese in gutem Glauben und im Rahmen ihrer Aufgaben ihren Verpflichtungen aus diesem Gesetz nachkommt;
3. 500 bis 200.000 Euro für jene, die ihren Kontrollpflichten nicht nachkommen;

4. 500 bis 7.000.000 Euro oder 1,4% des gesamten weltweit im vorangegangenen Geschäftsjahr erzielten Jahresumsatzes des Unternehmens, zu dem die wichtige Einrichtung gehört (je nachdem, welcher Betrag höher ist): für die wichtige Einrichtung, die ihren Verpflichtungen in Bezug auf Maßnahmen zum Management von Cybersicherheitsrisiken und/oder zur Meldung von Sicherheitsvorfällen nicht nachkommt;
5. 500 bis 10.000.000 Euro oder 2% des gesamten weltweit im vorangegangenen Geschäftsjahr erzielten Jahresumsatzes des Unternehmens, dem die wesentliche Einrichtung angehört (je nachdem, welcher Betrag höher ist): für die wesentliche Einrichtung, die ihren Verpflichtungen in Bezug auf Maßnahmen zum Management von Cybersicherheitsrisiken und/oder zur Meldung von Sicherheitsvorfällen nicht nachkommt.

Die Verwaltungsstrafe wird verdoppelt, wenn innerhalb von drei Jahren ein Rückfall für denselben Sachverhalt vorliegt.

Das Zusammentreffen mehrerer Verstöße kann zu einer einzigen Verwaltungsstrafe kommen, die der Schwere der gesamten Tat angemessen ist.

4.18. Welche anderen Verwaltungsmaßnahmen können ergriffen werden?

4.18.1. Grundlegende Maßnahmen

Gegen wesentliche und wichtige Einrichtungen können folgende Verwaltungsmaßnahmen verhängt werden:

Art. 58 NIS2-Gesetz

1. Warnungen wegen Gesetzesverstößen der betreffenden Einrichtungen aussprechen;
2. verbindliche Anweisungen oder eine Anordnung erlassen, in denen die betroffenen Einrichtungen aufgefordert werden, die festgestellten Mängel oder Rechtsverstöße zu beheben;
3. die betroffenen Einrichtungen anweisen, ein Verhalten, das gegen das Gesetz verstößt, zu beenden und es nicht zu wiederholen;
4. die betroffenen Einrichtungen anweisen, die Einhaltung ihrer Maßnahmen zum Management von Cybersicherheitsrisiken zu gewährleisten oder die festgelegten Verpflichtungen zur Meldung von Sicherheitsvorfällen konkret und innerhalb einer bestimmten Frist zu erfüllen;
5. die betroffenen Einrichtungen anweisen, die natürlichen oder juristischen Personen, für die sie Dienstleistungen erbringen oder Tätigkeiten ausüben und die von einer erheblichen Cyberbedrohung betroffen sein könnten, über die Art der Bedrohung sowie über alle Präventiv- oder Abhilfemaßnahmen zu informieren, die diese natürlichen oder juristischen Personen als Reaktion auf die Bedrohung ergreifen könnten;
6. die betroffenen Einrichtungen anweisen, die nach einem Sicherheitsaudit ausgesprochenen Empfehlungen innerhalb einer angemessenen Frist umzusetzen;
7. die betroffenen Einrichtungen anweisen, die Aspekte von Gesetzesverstößen in besonderer Weise zu veröffentlichen;

Wenn es sich bei der betroffenen Einrichtung um eine wesentliche Einrichtung handelt:

- Das ZCB kann für einen bestimmten Zeitraum einen Kontrollbeauftragten mit genau festgelegten Aufgaben ernennen, der die Aufsicht darüber führt, dass die betreffenden Einrichtungen die Maßnahmen zum Management von Cybersicherheitsrisiken und zur Meldung von Sicherheitsvorfällen einhalten;
- Die verbindlichen Anweisungen nach Nummer 2 beziehen sich auch auf die Maßnahmen zur Vermeidung oder Behebung eines Sicherheitsvorfalls, sowie auf die Fristen für die Durchführung dieser Maßnahmen und die Berichterstattung über die Durchführung.

4.18.2. Zusätzliche Maßnahmen

Werden die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen, können den wesentlichen Einrichtungen die folgenden Verwaltungsmaßnahmen auferlegt werden:

Art. 60 NIS2-Gesetz

2. das vorrübergehende Aussetzen eine Zertifizierung oder Genehmigung in Bezug auf alle oder einen Teil der von der betreffenden Einrichtung erbrachten einschlägigen Dienstleistungen oder durchgeführten Tätigkeiten;
3. das vorrübergehende Aussetzen der Führungsaufgaben einer natürlichen Person, die in der betreffenden Einrichtung auf der Ebene des Geschäftsführers oder des gesetzlichen Vertreters Führungsaufgaben wahrnimmt.

Die in Nummer 1 genannten vorübergehenden Aussetzungen oder Verbote werden nur so lange angewandt, bis die betreffende Einrichtung die erforderlichen Maßnahmen ergriffen hat, um die Mängel zu beheben oder den Anforderungen der zuständigen Behörde nachzukommen, die die Anwendung dieser Maßnahmen veranlasst hat.

5. Andere

5.1. Muss die Europäische Kommission noch Durchführungsrechtsakte erlassen?

Eine Durchführungsverordnung wurde von der Europäischen Kommission angenommen. Sie trägt die Bezeichnung Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt.

Diese Durchführungsverordnung ist auf Eur-Lex verfügbar.

Die NIS2-Richtlinie gibt der Europäischen Kommission die Befugnis, in bestimmten Fällen eine Durchführungsverordnung zu erlassen.

Artikel 21, § 5, Abschn. 1 der Richtlinie betrifft die technischen und methodischen Anforderungen im Zusammenhang mit Risikomanagementmaßnahmen für DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter.

Artikel 23, § 11 der Richtlinie befasst sich mit dem Begriff des erheblichen Sicherheitsvorfalls für DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke.

Die NIS2-Richtlinie sieht auch die (fakultative) Möglichkeit weiterer Durchführungsverordnungen vor:

- eine Durchführungsverordnung mit technischen und methodischen Anforderungen und sektorspezifischen Anforderungen für andere Arten von wesentlichen und wichtigen Einrichtungen (Art. 21, § 5, Abs. 2);
- eine Durchführungsverordnung, in der die Art der Informationen, das Format und das Verfahren für Meldungen und Mitteilungen von Sicherheitsvorfällen genauer festgelegt werden (Art. 23, § 11, Abs. 1);
- eine Durchführungsverordnung, die den Begriff des erheblichen Sicherheitsvorfalls für andere Arten von wesentlichen und wichtigen Einrichtungen präzisiert (Art. 23, § 11, Abs. 2, in fine);

Derzeit gibt es jedoch keine Projekte für diese Durchführungsverordnungen.

5.2. Gibt es innerhalb einer Organisation eine bestimmte Person, die für die Implementierung der Cybersicherheitsmaßnahmen zuständig ist?

Das NIS2-Gesetz schreibt nicht vor, dass eine bestimmte Person (wie ein DSB im Rahmen der DSGVO) innerhalb der Organisation mit der Implementierung von NIS2-Anforderungen betraut werden muss.

5.3. Gibt es eine öffentliche Liste aller wichtigen und wesentlichen Einrichtungen?

Die NIS2-Richtlinie verpflichtet die Mitgliedstaaten, eine Liste aller wesentlichen und wichtigen Einrichtungen zu erstellen und der NIS-Kooperationsgruppe und der Europäischen Kommission statistische Informationen über diese Liste (Anzahl der Einrichtungen nach Sektoren oder Teilsektoren) zu übermitteln.

Art. 3, § 3 - 6 NIS2-Richtlinie

Diese Liste ist jedoch nicht öffentlich zugänglich.

6. Entsprechungstabelle

FAQ Version 1.0	FAQ Version 2.0
1.1	1.1
	1.2
1.2	1.3
	1.4
1.3	1.5
	1.6
1.4	1.7
	1.8
1.5	1.9
1.6	1.10
1.7	1.11
1.8	1.12
	1.13
1.9	1.14
	1.15
	1.15.1
	1.15.2
	1.15.3
	1.15.4
	1.15.5
	1.16
	1.16.1
	1.16.2
	1.16.3
	1.16.4
	1.16.5
	1.16.6
	1.16.7
1.10	1.17
1.11	1.18
1.12	2.7
1.13	1.19
	1.20
1.14	1.21
1.14.1	1.21.1
	1.21.2
1.14.2	1.21.3
1.14.3	1.21.4
1.14.4	1.21.5
1.14.5	1.21.6
	1.22

	1.22.1
	1.22.2
	1.22.3
	1.22.4
	1.22.5
	1.22.6
	1.22.7
	1.22.8
	1.22.9
	1.22.10
	1.22.11
	1.22.12
2.1	2.1
	2.2
	2.2
2.2	2.4
2.3	2.5
	2.6
	2.7
	2.8
	2.9
3.1	3.1
3.2	3.2
3.3	3.3
3.3.1	3.3.1
	3.3.2
3.3.2	3.3.3
3.3.3	3.3.4
3.3.4	3.3.5
3.3.5	3.3.6
	3.4
3.4	3.5
3.5	3.6
	3.7
	3.8
	3.11
3.6	3.12
3.7	3.13
	3.13.1
	3.13.2
	3.13.3
	3.13.4
	3.13.5
	3.13.6
	3.13.7

	3.13.8
	3.13.9
	3.13.10
3.8	3.14
3.9	3.15
4.1	4.1
4.1.1	4.1.1
4.1.2	4.1.2
4.1.3	4.1.3
4.2	4.2
4.2.1	4.2.1
4.2.2	4.2.2
	4.3
4.3	4.4
	4.5
4.4	4.6
	4.7
4.5	4.8
4.6	4.9
	4.10
4.7	4.11
	4.12
4.8	4.13
4.9	4.14
4.10	4.15
	4.16
4.11	4.17
4.12	4.18
4.12.1	4.18.1
4.12.2	4.18.2
4.13	3.9
4.14	3.10
5.1	5.1
	5.2
	5.3