WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN
LOIS, DECRETS, ORDONNANCES ET REGLEMENTS

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2026/007305]

26 APRIL 2024. — Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. — Officieuze coördinatie in het Duits

De hierna volgende tekst is de officieuze coördinatie in het Duits van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (*Belgisch Staatsblad* van 17 mei 2024), zoals ze werd gewijzigd bij de wet van 19 december 2025 betreffende de weerbaarheid van kritieke entiteiten (*Belgisch Staatsblad* van 19 januari 2026).

Deze officieuze coördinatie in het Duits is opgemaakt door de Centrale dienst voor Duitse vertaling in Malmedy.

SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2026/007305]

26 AVRIL 2024. — Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. — Coordination officieuse en langue allemande

Le texte qui suit constitue la coordination officieuse en langue allemande de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (*Moniteur belge* du 17 mai 2024), telle qu'elle a été modifiée par la loi du 19 décembre 2025 relative à la résilience des entités critiques (*Moniteur belge* du 19 janvier 2026).

Cette coordination officieuse en langue allemande a été établie par le Service central de traduction allemande à Malmedy.

FÖDERALER ÖFFENTLICHER DIENST INNERES

[C − 2026/007305]

26. APRIL 2024 — Gesetz zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit. — Inoffizielle Koordinierung in deutscher Sprache

Der folgende Text ist die inoffizielle Koordinierung in deutscher Sprache des Gesetzesvom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit, so wie es abgeändert worden ist durch das Gesetz vom 19. Dezember 2025 über die Resilienz kritischer Einrichtungen.

Diese inoffizielle Koordinierung in deutscher Sprache ist von der Zentralen Dienststelle für Deutsche Übersetzungen in Malmedy erstellt worden.

FÖDERALER ÖFFENTLICHER DIENST KANZLEI DES PREMIERMINISTERS

26. APRIL 2024 — Gesetz zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit

TITEL 1 - ***Begriffsbestimmungen und allgemeine Bestimmungen***

KAPITEL 1 - *Gegenstand und Anwendungsbereich*

Abschnitt 1 - Gegenstand

Artikel 1 - Vorliegendes Gesetz regelt eine in Artikel 74 der Verfassung erwähnte Angelegenheit.

Art. 2 - Vorliegendes Gesetz dient insbesondere der Umsetzung der europäischen 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. Diese Richtlinie wird im Nachfolgenden "NIS-2-Richtlinie" genannt.

Abschnitt 2 - Anwendungsbereich

Art. 3 - § 1 - In den Grenzen von Artikel 4 und unbeschadet des Artikels 6 gilt vorliegendes Gesetz für öffentliche oder private Einrichtungen der in Anlage I oder II erwähnten Art, die:

1. nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder

2. die Schwellenwerte nach Absatz 1 desselben Artikels dieses Anhangs überschreiten.

Artikel 3 Absatz 4 des Anhangs der Empfehlung 2003/361/EG gilt nicht für die Zwecke des vorliegenden Gesetzes.

§ 2 - Bei der Anwendung von Artikel 6 Absatz 2 des Anhangs der Empfeh–lung 2003/361/EG berücksichtigt die nationale Cybersicherheitsbehörde den Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen, insbesondere in Bezug auf die Netz- und Informationssysteme, die sie bei der Erbringung ihrer Dienste nutzt, und in Bezug auf die von ihr erbrachten Dienste.

Auf der Grundlage von Absatz 1 geht die nationale Cybersicherheitsbehörde davon aus, dass eine solche Einrichtung nicht nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittleres Unternehmen gilt oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 desselben Artikels nicht überschreitet, wenn nach Berücksichtigung des Grades der Unabhängigkeit dieser Einrichtung davon ausgegangen worden wäre, dass sie nicht als mittleres Unternehmen gilt oder diese Schwellenwerte nicht überschreitet, falls nur ihre eigenen Daten berücksichtigt worden wären.

Der König kann die Kriterien festlegen, auf deren Grundlage der Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen beurteilt wird.

§ 3 - Unbeschadet des Artikels 6 gilt vorliegendes Gesetz unabhängig von der Größe der Einrichtungen auch für Einrichtungen der in Anlage I oder II erwähnten Art, wenn:

1. die Dienste erbracht werden von:

a) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten,

b) Vertrauensdiensteanbietern,

c) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern,

2. die Einrichtung gemäß Kapitel 4 des vorliegenden Titels als wesentliche oder wichtige Einrichtung eingestuft ist,

3. die Einrichtung eine Einrichtung der öffentlichen Verwaltung ist:

a) die vom Föderalstaat abhängt,

b) die von einem föderierten Teilgebiet abhängt und gemäß Artikel 11 § 2 eingestuft ist,

c) die eine Hilfeleistungszone ist im Sinne von Artikel 14 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit oder der "Service d'Incendie et d'Aide médicale urgente de la Région de Bruxelles-Capitale/Brusselse hoofdstedelijke Dienst voor Brandweer en dringende medische Hulp" (Feuerwehrdienst und Dienst für dringende medizinische Hilfe der Region Brüssel-Hauptstadt) im Sinne der Ordonnanz vom 19. Juli 1990 "portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale/houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp" (Schaffung des Feuerwehrdienstes und Dienstes für dringende medizinische Hilfe der Region Brüssel-Hauptstadt).

§ 4 - Unbeschadet des Artikels 6 gilt vorliegendes Gesetz unabhängig von der Größe der Einrichtungen auch für Einrichtungen, die als [kritische Einrichtung im Sinne des Gesetzes vom 19. Dezember 2025 über die Resilienz kritischer Einrichtungen] eingestuft sind.

§ 5 - Unabhängig von der Größe der Einrichtungen gilt vorliegendes Gesetz für Einrichtungen, die Domänennamenregistrierungsdienste erbringen.

§ 6 - Nach Konsultierung eventueller relevanter sektorspezifischer Behörden und der nationalen Cybersicherheitsbehörde kann der König durch einen im Ministerrat beratenen Erlass andere Sektoren und/oder Teilsektoren in Anlage I oder II hinzufügen oder bestehende Sektoren und/oder Teilsektoren erweitern.

[Art. 3 § 4 abgeändert durch Art. 65 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 4 - § 1 - Vorliegendes Gesetz gilt für die in Artikel 3 erwähnten Einrichtungen, die in Belgien ansässig sind und ihre Dienste in der Europäischen Union erbringen oder ihre Tätigkeiten dort ausüben.

§ 2 - In Abweichung von § 1 gilt vorliegendes Gesetz für:

1. Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, wenn sie diese Dienste in Belgien erbringen,

2. DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, wenn sie gemäß den Paragraphen 4 und 5 ihre Hauptniederlassung in Belgien haben.

§ 3 - Hat eine in § 2 Nr. 2 erwähnte Einrichtung keine Niederlassung in der Europäischen Union, bietet sie dort aber Dienste an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden.

§ 4 - Für die Zwecke der Anwendung des vorliegenden Gesetzes haben die in § 2 Nr. 2 erwähnten Einrichtungen ihre Hauptniederlassung in Belgien, wenn sie dort vorwiegend die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisiko–management treffen.

Kann der Ort, an dem diese Entscheidungen getroffen werden, nicht bestimmt werden oder liegt er nicht in der Europäischen Union, so gilt für die in § 2 Nr. 2 erwähnten Einrichtungen als Hauptniederlassung Belgien, wenn sie dort die Cybersicherheitsmaßnahmen durchführen.

Kann der Ort, an dem diese Maßnahmen durchgeführt werden, nicht bestimmt werden, so gilt für die in § 2 Nr. 2 erwähnten Einrichtungen als Hauptniederlassung Belgien, wenn sie dort die Niederlassung mit der höchsten Beschäftigtenzahl haben.

§ 5 - Für die Anwendung des vorliegenden Gesetzes wird davon ausgegangen, dass die in § 2 Nr. 2 erwähnten Einrichtungen ihre Hauptniederlassung in Belgien haben, wenn sie keine Niederlassung in der Europäischen Union haben, sie aber Dienste innerhalb der Union anbieten und ihr Vertreter in der Europäischen Union in Belgien niedergelassen ist.

§ 6 - Die Benennung eines Vertreters durch eine in § 2 Nr. 2 erwähnte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

Art. 5 - § 1 - Vorliegendes Gesetz beeinträchtigt weder die Anwendung der 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) noch der Gesetzes- und Verordnungsbestimmungen zur Ergänzung oder Verdeutlichung dieser Verordnung noch des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten.

§ 2 - Vorliegendes Gesetz beeinträchtigt nicht die Anwendung des Gesetzes vom 11. Dezember 1998 über die Einstufung, die Sicherheitsermächtigungen, Sicherheitsbescheinigungen und Sicherheitsgutachten und den öffentlichen regulierten Dienst und gilt nicht für Kommunikations- und Informationssysteme, die gemäß dem vorerwähnten Gesetz für die Verwendung von Verschlusssachen in elektronischer Form genehmigt sind.

§ 3 - Vorliegendes Gesetz beeinträchtigt nicht die Regeln, die für Nuklearunterlagen im Sinne des Gesetzes vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle gelten.

§ 4 - Vorbehaltlich der Artikel 8 und 38 und des Titels 2 gilt vorliegendes Gesetz nicht für:

1. Nachrichten- und Sicherheitsdienste wie in Artikel 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnt,

2. das Koordinierungsorgan für die Bedrohungsanalyse, eingerichtet durch Artikel 5 des Gesetzes vom 10. Juli 2006 über die Bedrohungsanalyse,

3. das Ministerium der Landesverteidigung wie in Artikel 1 des Königlichen Erlasses vom 2. Dezember 2018 zur Bestimmung der allgemeinen Struktur des Ministeriums der Landesverteidigung und zur Festlegung der Zuständigkeiten bestimmter Behörden erwähnt,

4. Polizeidienste und die Generalinspektion wie in Artikel 2 Nr. 2 und 3 des Gesetzes vom 7. Dezember 1998 zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes erwähnt,

5. Gerichtsbehörden, das heißt die Organe der rechtsprechenden Gewalt einschließlich der Staatsanwaltschaft,

6. den Föderalen Öffentlichen Dienst Justiz, errichtet durch den Königlichen Erlass vom 23. Mai 2001 zur Schaffung des Föderalen Öffentlichen Dienstes Justiz, wenn dieser Datenbanken für die in Nr. 5 erwähnten Gerichtsbehörden verwaltet,

7. Netz- und Informationssysteme der belgischen diplomatischen und konsularischen Missionen in Ländern außerhalb der Europäischen Union,

8. Einrichtungen der Klasse I im Sinne von Artikel 3.1 des Königlichen Erlasses vom 20. Juli 2001 zur Festlegung einer allgemeinen Ordnung über den Schutz der Bevölkerung, der Arbeitnehmer und der Umwelt gegen die Gefahren ionisierender Strahlungen.

In Abweichung von Absatz 1 Nr. 8 ist vorliegendes Gesetz auf die zur Übertragung von Elektrizität verwendeten Komponenten einer kerntechnischen Anlage für industrielle Stromerzeugung anwendbar.

§ 5 - Die Bestimmungen der Titel 3, 4 und 5 gelten nicht für:

1. das NCCN,

2. die in Artikel 16 erwähnte nationale Cybersicherheitsbehörde.

§ 6 - Die Paragraphen 4 und 5 finden keine Anwendung, wenn eine dieser Einrichtungen als Vertrauensdienstanbieter auftritt.

Art. 6 - § 1 - Wenn sektorspezifische Rechtsakte der Europäischen Union Einrichtungen, die in den Anwendungsbereich des vorliegenden Gesetzes fallen, vorschreiben, entweder Maßnahmen zum Cybersicherheitsrisikomanagement zu ergreifen oder erhebliche Sicherheitsvorfälle zu melden, und wenn die entsprechenden Anforderungen in ihrer Wirkung den in vorliegendem Gesetz festgelegten Verpflichtungen zumindest gleichwertig sind, finden die einschlägigen Bestimmungen des vorliegenden Gesetzes keine Anwendung auf solche Einrichtungen.

Wenn in Absatz 1 erwähnte sektorspezifische Rechtsakte der Europäischen Union nicht für alle in den Anwendungsbereich des vorliegenden Gesetzes fallenden Einrichtungen eines bestimmten Sektors gelten, kommen die einschlägigen Bestimmungen des vorliegenden Gesetzes weiterhin für Einrichtungen zur Anwendung, die nicht unter diese sektorspezifischen Rechtsakte der Europäischen Union fallen.

§ 2 - Die in § 1 Absatz 1 erwähnten Anforderungen gelten den in vorliegendem Gesetz festgelegten Verpflichtungen in ihrer Wirkung als gleichwertig, wenn:

1. die Maßnahmen zum Cybersicherheitsrisikomanagement den in Artikel 30 festgelegten Maßnahmen in ihrer Wirkung mindestens gleichwertig sind, oder

2. der sektorspezifische Rechtsakt der Europäischen Union einen unmittelbaren - gegebenenfalls automatischen und direkten - Zugang zu den Meldungen von Sicherheitsvorfällen durch das nationale CSIRT vorsieht und wenn die Anforderungen an die Meldung erheblicher Sicherheitsvorfälle in ihrer Wirkung mindestens den in den Artikeln 34 bis 37 festgelegten Anforderungen gleichwertig sind.

§ 3 - Die Bestimmungen der Titel 3 bis 5 gelten nicht für Einrichtungen aus den Sektoren Bankwesen und Finanzmarktinfrastrukturen im Sinne von Anlage I, die in den Anwendungsbereich der 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 fallen, einschließlich der Tätigkeit der Belgischen Nationalbank als Zentralverwahrer.

§ 4 - Die Bestimmungen von Titel 3 Kapitel 1, Titel 4 und Titel 5 gelten nicht für:

1. die Belgische Nationalbank, mit Ausnahme ihrer Tätigkeit als Zentralverwahrer, für die § 3 gilt,

2. Finanzinstitute, die gemäß den Artikeln 8 und 12*bis* des Gesetzes vom 22. Februar 1998 zur Festlegung des Grundlagenstatuts der Belgischen Nationalbank der Aufsicht der Belgischen Nationalbank unterliegen und nicht unter § 3 fallen.

Art. 7 - Der König kann durch einen im Ministerrat beratenen Erlass:

1. die in Artikel 6 § 1 Absatz 1 erwähnten gleichwertigen sektorspezifischen Rechtsakte genauer angeben,

2. besondere Vorschriften für die Koordination des Informationsaustauschs festlegen, einschließlich Anforderungen an die Meldung erheblicher Sicherheitsvorfälle zwischen den in Artikel 6 §§ 3 und 4 erwähnten Einrichtungen, der relevanten sektorspezifischen Behörde, der nationalen Cybersicherheitsbehörde und der für das Cyberrisikomanagement zuständigen Behörde.

KAPITEL 2 - *Begriffsbestimmungen*

Art. 8 - Für die Anwendung des vorliegenden Gesetzes bezeichnet der Ausdruck:

1. "Netz- und Informationssystem":

a) ein elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nr. 3 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation,

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, einschließlich der digitalen, elektronischen oder mechanischen Komponenten dieser Geräte, insbesondere für die Automatisierung des Betriebsablaufs, die Fernsteuerung oder die Erfassung von Echtzeit-Betriebsdaten, oder

c) digitale Daten, die von den in den Buchstaben *a)* und *b)* erwähnten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden,

2. "Sicherheit von Netz- und Informationssystemen" die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden beziehungsweise zugänglich sind, beeinträchtigen können,

3. ″Cybersicherheit″ die Cybersicherheit im Sinne von Artikel 2 Nr. 1 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), nachstehend ″Cybersicherheitsverordnung″ genannt,

4. ″nationale Cybersicherheitsstrategie″ einen kohärenten Rahmen mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance in Belgien,

5. ″Sicherheitsvorfall″ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden beziehungsweise zugänglich sind, beeinträchtigt,

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

7. ″Cybersicherheitsvorfall großen Ausmaßes″ einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit des betreffenden Mitgliedstaats der Europäischen Union übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten der Europäischen Union hat,

8. ″Bewältigung von Sicherheitsvorfällen″ alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon,

9. ″Risiko″ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird,

10. ″Cyberbedrohung″ eine Cyberbedrohung im Sinne von Artikel 2 Nr. 8 der Cybersicherheitsverordnung,

11. ″erhebliche Cyberbedrohung″ eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht,

12. ″IKT-Produkt″ ein IKT-Produkt im Sinne von Artikel 2 Nr. 12 der Cybersicherheitsverordnung,

13. ″IKT-Dienst″ einen IKT-Dienst im Sinne von Artikel 2 Nr. 13 der Cybersicherheitsverordnung,

14. ″IKT-Prozess″ einen IKT-Prozess im Sinne von Artikel 2 Nr. 14 der Cybersicherheitsverordnung,

15. ″Schwachstelle″ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann,

16. ″Norm″ eine Norm im Sinne der Begriffsbestimmung in Artikel 2 Nr. 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates, nachstehend ″Verordnung (EU) Nr. 1025/2012″ genannt,

17. ″Internet-Knoten″ eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft, noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt,

18. ″Domänennamensystem″ oder ″DNS″ ein verteiltes hierarchisches Verzeichnissystem, das die Identifizierung von Diensten und Ressourcen im Internet ermöglicht und es Endnutzergeräten erlaubt, Internet-Routing- und Konnektivitätsdienste zu nutzen, um diese Dienste und Ressourcen zu erreichen,

19. ″DNS-Diensteanbieter″ eine Einrichtung, die:

a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen anbietet oder

b) autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet,

20. ″Namenregister der Domäne oberster Stufe″ oder ″TLD-Namenregister″ eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain - TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden,

21. ″Einrichtung, die Domänennamen-Registrierungsdienste erbringt″ einen Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten,

22. ″digitaler Dienst″ einen Dienst im Sinne von Artikel 1 Absatz 1 Buchstabe b) der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft,

23. ″Vertrauensdienst″ einen Vertrauensdienst im Sinne von Artikel 3 Nr. 16 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, nachstehend ″eIDAS-Verordnung″ genannt,

24. ″Vertrauensdiensteanbieter″ einen Vertrauensdiensteanbieter im Sinne von Artikel 3 Nr. 19 der eIDAS-Verordnung,

25. ″qualifizierter Vertrauensdienst″ einen qualifizierten Vertrauensdienst im Sinne von Artikel 3 Nr. 17 der eIDAS-Verordnung,

26. ″qualifizierter Vertrauensdiensteanbieter″ einen qualifizierten Vertrauensdiensteanbieter im Sinne von Artikel 3 Nr. 20 der eIDAS-Verordnung,

27. ″Online-Marktplatz″ einen Online-Marktplatz im Sinne von Artikel I.8 Nr. 41 des Wirtschaftsgesetzbuches,

28. ″Online-Suchmaschine″ eine Online-Suchmaschine im Sinne von Artikel 2 Nr. 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten,

29. ″Cloud-Computing-Dienst″ 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,

30. ″Rechenzentrumsdienst″ 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,

31. ″Inhaltszustellnetz″ ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern,

32. ″Plattform für Dienste sozialer Netzwerke″ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können,

33. ″Vertreter″ eine in der Europäischen 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 beziehungsweise die nicht in der Union niedergelassen ist, zu handeln, und an die sich die nationale Cybersicherheitsbehörde - statt an die Einrichtung - hinsichtlich der Pflichten dieser Einrichtung gemäß vorliegendem Gesetz wenden kann,

34. ″Einrichtung der öffentlichen Verwaltung″ eine in Artikel 14 § 1 Absatz 1 der koordinierten Gesetze über den Staatsrat erwähnte Verwaltungsbehörde, die folgende Kriterien erfüllt:

a) Sie hat keinen gewerblichen 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 Anlagen zum Gesetz aufgeführt ist.

c) Sie ist keine juristische Person des privaten Rechts,

35. ″öffentliches elektronisches Kommunikationsnetz″ ein öffentliches elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nr. 10 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation,

36. ″elektronischer Kommunikationsdienst″ einen elektronischen Kommunikationsdienst im Sinne von Artikel 2 Nr. 5 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation,

37. ″Einrichtung″ 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,

38. ″Anbieter verwalteter Dienste″ 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 entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt,

39. ″Anbieter verwalteter Sicherheitsdienste″ einen Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt,

40. ″Forschungseinrichtung″ 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,

41. ″Empfehlung 2003/361/EG″ die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen,

42. ″Gesetz vom 13. Juni 2005″ das Gesetz vom 13. Juni 2005 über die elektronische Kommunikation,

43. [″Gesetz vom 19. Dezember 2025″ das Gesetz vom 19. Dezember 2025 über die Resilienz kritischer Einrichtungen,]

44. ″Königlicher Erlass vom 18. April 1988″ den Königlichen Erlass vom 18. April 1988 zur Schaffung des Koordinations- und Krisenzentrums der Regierung,

45. ″nationale Cybersicherheitsbehörde″ die in Artikel 16 erwähnte Behörde,

46. ″nationales CSIRT″ das nationale Computer-Notfallteam,

47. ″ENISA″ die durch den Rechtsakt zur Cybersicherheit eingerichtete Agentur der Europäischen Union für Cybersicherheit,

48. ″NCCN″ das durch den Königlichen Erlass vom 18. April 1988 eingerichtete Zentrum,

49. ″Verordnung (EU) 2016/679″ die 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),

50. ″Datenschutzbehörde″ die Aufsichtsbehörde im Sinne von Artikel 4 Nr. 21 der Verordnung (EU) 2026/679,

51. ″nationale Akkreditierungsstelle″ die Einrichtung, die in Artikel 2 Nr. 11 der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates erwähnt ist, nachstehend ″Verordnung (EG) Nr. 765/2008″ genannt,

52. ″Sicherheitspolitik für Netz- und Informationssysteme (″S.P.I.″)″ die Politik, die in der in Artikel 30 erwähnten Unterlage festgelegt ist, mit den von einer wesentlichen oder wichtigen Einrichtung zu ergreifenden Maßnahmen für die Sicherheit der Netz- und Informationssysteme,

53. ″Konformitätsbewertungsstelle″ die in Artikel 2 Nr. 13 der Verordnung (EG) Nr. 765/2008 erwähnte Einrichtung,

54. ″sektorspezifische Behörde″ die in Artikel 15 § 2 erwähnte Behörde,

55. ″CSIRTs-Netzwerk″ das gemäß Artikel 15 der NIS-2-Richtlinie eingerichtete Netzwerk der nationalen CSIRTs,

56. ″Kooperationsgruppe″ die gemäß Artikel 14 der NIS-2-Richtlinie eingerichtete Kooperationsgruppe,

57. "erheblicher Sicherheitsvorfall" einen Sicherheitsvorfall, der beträchtliche Auswirkungen auf die Erbringung einer der Dienstleistungen in den in den Anlagen I und II zum Gesetz aufgeführten Sektoren oder Teilsektoren hat und der:

1. eine schwerwiegende Betriebsstörung bei einer der Dienstleistungen, die in den in den Anlagen I und II aufgeführten Sektoren oder Teilsektoren erbracht werden, oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen könnte oder

2. andere natürliche oder juristische Personen beeinträchtigt hat oder beeinträchtigen könnte, indem er erheblichen materiellen oder immateriellen Schaden verursacht,

58. "Cyberkrise" jeglichen Cybersicherheitsvorfall, der aufgrund seiner Art oder seiner Folgen:

1. die vitalen Interessen des Landes oder die Grundbedürfnisse der Bevölkerung gefährdet,

2. dringende Entscheidungen erfordert,

3. einen koordinierten Einsatz von mehreren Diensten und Einrichtungen erfordert,

59. "Institut" das in Artikel 13 des Gesetzes vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors erwähnte Belgische Institut für Post- und Fernmeldewesen.

[Art. 8 einziger Absatz Nr. 43 ersetzt durch Art. 68 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

KAPITEL 3 - *Kategorien von Einrichtungen*

Art. 9 - Als wesentliche Einrichtungen gelten:

1. Einrichtungen der in Anlage I aufgeführten Art, die die in Artikel 2 Absatz 1 des Anhangs der Empfehlung 2003/361/EG vorgesehenen Schwellenwerte für mittlere Unternehmen überschreiten,

2. qualifizierte Vertrauensdiensteanbieter und Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter, unabhängig von ihrer Größe,

3. Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG mindestens als mittlere Unternehmen gelten,

4. Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen,

5. in Artikel 3 § 4 erwähnte Einrichtungen,

6. sonstige Einrichtungen der in Anlage I oder II aufgeführten Art, die gemäß Artikel 11 als wesentliche Einrichtungen eingestuft werden.

Art. 10 - Als wichtige Einrichtungen gelten:

1. Einrichtungen der in Anlage I oder II aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Artikel 9 gelten,

2. Einrichtungen, die gemäß Artikel 11 als wichtige Einrichtungen eingestuft wurden.

KAPITEL 4 - *Identifizierung*

Art. 11 - § 1 - Unbeschadet des Artikels 6 stuft die nationale Cybersicherheitsbehörde aus eigener Initiative oder gegebenenfalls auf Vorschlag der relevanten sektorspezifischen Behörde eine Einrichtung unabhängig von ihrer Größe in folgenden Fällen als wesentliche oder wichtige Einrichtung ein:

1. Die Einrichtung ist in Belgien der einzige Anbieter mindestens eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist, insbesondere in einem der in den Anlagen I und II zum Gesetz aufgeführten Sektoren oder Teilsektoren.

2. Eine Störung des von der Einrichtung erbrachten Dienstes könnte sich wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken.

3. Eine Störung des von der Einrichtung erbrachten Dienstes könnte zu einem wesentlichen Systemrisiko führen, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte.

4. Die Einrichtung ist aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in Belgien hat, kritisch.

§ 2 - Was Einrichtungen betrifft, die den föderierten Teilgebieten unterstehen, so identifiziert die nationale Cybersicherheitsbehörde die öffentlichen Verwaltungen, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

§ 3 - Im Rahmen der in den Paragraphen 1 und 2 erwähnten Einstufung legt die nationale Cybersicherheitsbehörde zunächst der betreffenden Einrichtung und anschließend den gegebenenfalls betroffenen föderierten Teilgebieten und relevanten sektorspezifischen Behörden einen Entscheidungsentwurf vor; diese geben innerhalb sechzig Tagen eine nicht veröffentlichte Stellungnahme ab.

Wird innerhalb der in Absatz 1 erwähnten Frist keine Stellungnahme abgegeben, kann das Fehlen einer Stellungnahme außer Acht gelassen werden.

Im Falle einer ungünstigen Stellungnahme einer sektorspezifischen Behörde und sofern die nationale Cybersicherheitsbehörde an ihrem Entscheidungsentwurf festhalten möchte, wird der Entscheidungsentwurf zusammen mit der Stellungnahme dem Strategischen Ausschuss für Nachrichten und Sicherheit vorgelegt, eingerichtet durch den Königlichen Erlass vom 22. Dezember 2020 zur Schaffung des Nationalen Sicherheitsrates, des Strategischen Ausschusses für Nachrichten und Sicherheit und des Koordinierungsausschusses für Nachrichten und Sicherheit, der eine zwingende Stellungnahme abgibt.

§ 4 - Die nationale Cybersicherheitsbehörde überprüft und aktualisiert gegebenenfalls die Liste der wesentlichen und wichtigen Einrichtungen mindestens alle zwei Jahre gemäß den in den Paragraphen 1 bis 3 erwähnten Modalitäten.

Die nationale Cybersicherheitsbehörde übermittelt die Identifizierungen und Aktualisierungen der wesentlichen Einrichtungen dem NCCN und gegebenenfalls der relevanten sektorspezifischen Behörde.

Die nationale Cybersicherheitsbehörde übermittelt die Identifizierungen und Aktualisierungen der wichtigen Einrichtungen gegebenenfalls der relevanten sektorspezifischen Behörde.

§ 5 - In den in § 1 erwähnten Fällen kann der König durch einen im Ministerrat beratenen Erlass eine Einrichtung, die nicht zu den in der Anlage erwähnten Sektoren gehört, als wesentliche oder wichtige Einrichtung einstufen.

Art. 12 - Im Rahmen der in Artikel 11 erwähnten Einstufung übermittelt die betreffende Einrichtung auf Ersuchen der nationalen Cybersicherheitsbehörde oder der sektorspezifischen Behörde alle Informationen, die für ihre mögliche Einstufung nützlich sind.

KAPITEL 5 - *Registrierung der Einrichtungen*

Art. 13 - § 1 - Innerhalb fünf Monaten nach Inkrafttreten des Gesetzes oder nach der in Artikel 11 erwähnten Einstufung lassen sich wesentliche Einrichtungen, wichtige Einrichtungen und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, bei der nationalen Cybersicherheitsbehörde gemäß den von dieser Behörde festgelegten praktischen Modalitäten registrieren und übermitteln sie ihr folgende Informationen:

1. ihren Namen und ihre Registrierungsnummer bei der Zentralen Datenbank der Unternehmen (ZDU) oder eine gleichwertige Registrierung in der Europäischen Union,

2. ihre Anschrift und aktuellen Kontaktdaten, einschließlich der E-Mail-Adressen, IP-Adressbereiche und Telefonnummern,

3. gegebenenfalls den relevanten Sektor und Teilsektor gemäß Anlage I oder II und

4. gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie Dienste erbringen, die in den Anwendungsbereich des vorliegenden Gesetzes fallen.

Der König kann diese Liste von Informationen ergänzen.

§ 2 - Wenn die in § 1 Absatz 1 erwähnte Einrichtung aufgrund einer gesetzlichen Verpflichtung bestimmte der in § 1 erwähnten Informationen der relevanten sektorspezifischen Behörde bereits übermittelt, ergänzt diese Einrichtung in Abweichung von § 1 Absatz 1 diese Informationen bei dieser sektorspezifischen Behörde.

Die in § 1 Absatz 1 erwähnte Einrichtung übermittelt die Informationen innerhalb fünf Monaten nach Inkrafttreten des Gesetzes gemäß den von der vorerwähnten Behörde festgelegten praktischen Modalitäten.

§ 3 - Die in § 1 Absatz 1 erwähnten Einrichtungen teilen alle Änderungen der gemäß § 1 Absatz 1 und § 2 Absatz 1 übermittelten Angaben unverzüglich mit, in jedem Fall jedoch innerhalb zweier Wochen ab dem Zeitpunkt der Änderung.

§ 4 - Die relevante sektorspezifische Behörde übermittelt die gemäß den Paragraphen 2 und 3 erhobenen Informationen an die nationale Cybersicherheitsbehörde.

Die nationale Cybersicherheitsbehörde trifft die erforderlichen Maßnahmen, damit die sektorspezifischen Behörden die übermittelten Daten in Bezug auf die sie betreffenden Sektoren einsehen können.

Art. 14 - § 1 - Innerhalb zweier Monate nach Inkrafttreten des Gesetzes übermitteln DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke der nationalen Cybersicherheitsbehörde gemäß den in Artikel 13 § 1 Absatz 1 erwähnten Modalitäten zumindest folgende Informationen:

1. ihren Namen,

2. gegebenenfalls den relevanten Sektor und Teilsektor und die Art der betreffenden Einrichtung gemäß Anlage I oder II,

3. Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen sind, Anschrift ihres gemäß Artikel 4 § 3 benannten Vertreters,

4. ihre aktuellen Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern, und gegebenenfalls ihres gemäß Artikel 4 § 3 benannten Vertreters,

5. die Mitgliedstaaten, in denen die Einrichtungen Dienste erbringen, die in den Anwendungsbereich des vorliegenden Gesetzes fallen, und

6. ihre IP-Adressbereiche.

§ 2 - Die in § 1 erwähnten Einrichtungen teilen der nationalen Cybersicherheitsbehörde alle Änderungen der gemäß § 1 übermittelten Angaben unverzüglich mit, in jedem Fall jedoch innerhalb dreier Monate ab dem Zeitpunkt der Änderung.

§ 3 - In Abweichung von § 1 werden die in diesem Paragraphen erwähnten Angaben über qualifizierte Vertrauensdiensteanbieter in Belgien, die der in Artikel 17 der eIDAS-Verordnung erwähnten Aufsichtsstelle bereits übermittelt wurden, von dieser Stelle gemäß den vom König festgelegten Modalitäten der nationalen Cybersicherheitsbehörde übermittelt.

TITEL 2 - *Zuständige Behörden und Zusammenarbeit auf nationaler Ebene*

KAPITEL 1 - *Zuständige Behörden*

Abschnitt 1 - Benennung der zuständigen Behörden

Art. 15 - § 1 - Der König benennt die nationale Cybersicherheitsbehörde.

§ 2 - Nach Stellungnahme der nationalen Cybersicherheitsbehörde kann der König durch einen im Ministerrat beratenen Erlass eine sektorspezifische Behörde und gegebenenfalls einen sektorspezifischen Inspektionsdienst benennen, die für einen bestimmten Sektor oder Teilsektor mit der Überwachung der Umsetzung der in Artikel 33 erwähnten zusätzlichen sektor- oder teilsektorspezifischen Risikomanagementmaßnahmen im Bereich der Cybersicherheit beauftragt sind.

Im Rahmen der in Absatz 1 erwähnten Benennung berücksichtigt der König die Identität der im Rahmen des [Gesetzes vom 19. Dezember 2025] benannten sektorspezifischen Behörden und sektorspezifischen Inspektionsdienste.

Der König kann durch einen im Ministerrat beratenen Erlass sektorspezifische Behörden einrichten, die sich aus Vertretern des Föderalstaats, der Gemeinschaften und der Regionen zusammensetzen, gemäß den Modalitäten von Artikel 92*ter* des Sondergesetzes vom 8. August 1980 zur Reform der Institutionen.

In Abweichung von Absatz 1 werden die durch Gesetz eingerichteten und geregelten sektorspezifischen Behörden und sektorspezifischen Inspektionsdienste im vorliegenden Gesetz selbst benannt.

[Art. 15 § 2 Abs. 2 abgeändert durch Art. 69 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Abschnitt 2 - Nationale Cybersicherheitsbehörde

Art. 16 - Die nationale Cybersicherheitsbehörde ist zuständig für die Überwachung und Koordination der Umsetzung des vorliegenden Gesetzes, für die Aufsicht über die Umsetzung des vorliegenden Gesetzes durch wesentliche und wichtige Einrichtungen und für das Management von Cyberkrisen und Cybersicherheitsvorfällen gemäß Artikel 18.

Zu diesem Zweck nimmt die nationale Cybersicherheitsbehörde die Aufgaben wahr der zuständigen Behörde für wesentliche und wichtige Einrichtungen, des nationalen CSIRT, der zentralen nationalen Anlaufstelle für die Ausführung des vorliegenden Gesetzes und der Vertretung Belgiens in der Kooperationsgruppe, im CSIRTs-Netzwerk und in dem in Artikel 26 der NIS-2-Richtlinie erwähnten Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe).

Unterabschnitt 1 - Aufgaben in der Rolle als zuständige Behörde für Cybersicherheit

Art. 17 - Die nationale Cybersicherheitsbehörde ist mit folgenden Aufgaben beauftragt:

1. Gewährleistung der Koordination zwischen den zuständigen Behörden im Rahmen der Anwendung des vorliegenden Gesetzes und zwischen den verschiedenen Dienststellen und Behörden, die in Belgien für die Cybersicherheit zuständig sind,

2. Beobachtung, Koordination und Beaufsichtigung der Ausführung der in Artikel 28 erwähnten nationalen Cybersicherheitsstrategie,

3. Identifizierung der wesentlichen und wichtigen Einrichtungen gemäß Artikel 11,

4. Überwachung der Umsetzung des Gesetzes durch die wesentlichen und wichtigen Einrichtungen gemäß Titel 4,

5. Gewährleistung der Koordination zwischen den öffentlichen Behörden und dem privaten oder wissenschaftlichen Sektor,

6. Formulierung von Vorschlägen zur Anpassung des gesetzlichen und verordnungsrechtlichen Rahmens im Bereich der Cybersicherheit,

7. Aufsetzen, Verbreiten und Beaufsichtigung der Ausführung von Standards, Richtlinien und Normen im Bereich der Cybersicherheit für die verschiedenen Informationssysteme,

8. Koordination der belgischen Vertretung in internationalen Foren zur Cybersicherheit, der Erfüllung internationaler Verpflichtungen und der Vorschläge hinsichtlich des nationalen Standpunktes in diesem Bereich,

9. Fungieren als zentrale Anlaufstelle, die im Rahmen der Anwendung des vorliegenden Gesetzes die grenzüberschreitende Zusammenarbeit der belgischen Behörden mit den zuständigen Behörden der anderen Mitgliedstaaten der Europäischen Union und gegebenenfalls mit der Europäischen Kommission und der ENISA gewährleistet und die sektorübergreifende Zusammenarbeit mit anderen zuständigen belgischen Behörden gewährleistet,

10. Koordination der Beurteilung und Zertifizierung der Sicherheit von Informations- und Kommunikationssystemen,

11. Informierung und Sensibilisierung von Nutzern von Informations- und Kommunikationssystemen,

12. Gewährung im Rahmen ihrer Haushaltsmittel und gemäß den vom König festgelegten Bedingungen von Zuschüssen für Projekte und Aktivitäten im Bereich der Cybersicherheit,

13. Erleichterung und Förderung der Organisation von Schulungen zum Thema Cybersicherheit für Personalmitglieder von wesentlichen oder wichtigen Einrichtungen,

14. Erstellung einer Liste der wesentlichen und wichtigen Einrichtungen und der Einrichtungen, die Domänennamen-Registrierungsdienste erbringen; anschließend regelmäßige, mindestens alle zwei Jahre erfolgende Überprüfung dieser Liste und gegebenenfalls Aktualisierung dieser Liste.

Unterabschnitt 2 - Aufgaben in der Rolle in Bezug auf das Cyberkrisenmanagement

Art. 18 - Unbeschadet der Artikel 8 und 9 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit und seiner Ausführungserlasse und unbeschadet der Zuständigkeiten des NCCN hat die nationale Cybersicherheitsbehörde im Rahmen ihrer Rolle in Bezug auf das Cyberkrisenmanagement folgende Aufgaben:

1. Erfassung - in Zusammenarbeit mit dem NCCN - der Kapazitäten, Ressourcen und Verfahren, die im Falle einer Cyberkrise eingesetzt werden können,

2. Überwachung - in Zusammenarbeit mit dem NCCN - der Ausarbeitung, Aktualisierung und Umsetzung des in Artikel 29 erwähnten nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle und Cyberkrisen,

3. Gewährleistung der Rolle des Koordinators bei der Bewältigung von Cyberkrisen und Cybersicherheitsvorfällen, gegebenenfalls gemäß dem in Nr. 2 erwähnten Plan.

Unterabschnitt 3 - Aufgaben und Pflichten im Zusammenhang mit der Rolle als nationales CSIRT

Art. 19 - § 1 - Das nationale CSIRT hat folgende Aufgaben:

1. Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene und auf Anfrage Bereitstellung von Unterstützung für betreffende wesentliche und wichtige Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit,

2. Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie an die zuständigen Behörden und andere einschlägige Interessenträger, möglichst echtzeitnah,

3. Reaktion auf Sicherheitsvorfälle und gegebenenfalls Unterstützung der betreffenden wesentlichen und wichtigen Einrichtungen,

4. Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit,

5. auf Ersuchen einer wesentlichen oder wichtigen Einrichtung proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen (Schwachstellenscan),

6. Beteiligung am CSIRTs-Netzwerk, wirksame, effiziente und sichere Zusammenarbeit in diesem Netzwerk und - im Rahmen seiner Kapazitäten und Kompetenzen - auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks auf deren Ersuchen,

7. gegebenenfalls Wahrnehmung der Aufgabe eines Koordinators für die Zwecke einer koordinierten Offenlegung von Schwachstellen nach Artikel 22,

8. Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch,

9. Durchführung einer proaktiven nicht intrusiven Überprüfung öffentlich zugänglicher Netz- und Informationssysteme, um anfällige oder unsicher konfigurierte Netz- und Informationssysteme zu ermitteln und die betreffenden Einrichtungen zu unterrichten; eine solche Überprüfung darf keine nachteilige Auswirkung auf das Funktionieren der Dienste der Einrichtung haben,

10. Erkennung, Beobachtung und Analyse von IT-Sicherheitsproblemen,

11. Aufbau von Kooperationsbeziehungen mit einschlägigen Interessenträgern des Privatsektors, um die Ziele des vorliegenden Gesetzes erreichen zu können,

12. Erleichterung der Zusammenarbeit nach Nr. 11 durch Förderung der Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien in folgenden Bereichen:

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) Krisenmanagement und

c) koordinierte Offenlegung von Schwachstellen nach Artikel 22,

13. Kooperation und gegebenenfalls Austausch von einschlägigen Informationen gemäß Artikel 27 mit den in diesem Artikel erwähnten Gemeinschaften,

14. Teilnahme an den gemäß Artikel 19 der NIS-2-Richtlinie durchgeführten Peer-Reviews.

Nach Stellungnahme des nationalen CSIRT kann der König diesem CSIRT durch einen im Ministerrat beratenen Erlass zusätzliche Aufgaben anvertrauen.

§ 2 - Bei der Durchführung der in § 1 erwähnten Aufgaben kann das nationale CSIRT auf der Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.

Art. 20 - Die Anforderungen an das nationale CSIRT umfassen Folgendes:

1. Verfügbarkeit einer geeigneten, sicheren und widerstandsfähigen Kommunikations- und Informationsinfrastruktur, die es ihm ermöglicht, Informationen mit wesentlichen und wichtigen Einrichtungen und anderen Beteiligten auszutauschen,

2. Gewährleistung eines hohen Grads der Verfügbarkeit seiner Kommunikationskanäle, indem es punktuellen Ausfällen vorbeugt und mehrere Kanäle bereitstellt, damit es jederzeit erreichbar bleibt und selbst mit anderen Kontakt aufnehmen kann; deutliche Festlegung von Kommunikationskanälen und deren Bekanntmachung an CSIRT-Nutzer und Kooperationspartner,

3. Verfügbarkeit von Räumlichkeiten und Informationssystemen an sicheren Standorten,

4. Verfügbarkeit eines geeigneten Systems zur Verwaltung und Weiterleitung von Anfragen, insbesondere um wirksame und effiziente Übergaben zu erleichtern,

5. Sicherstellung der Vertraulichkeit und Vertrauenswürdigkeit seiner Tätigkeiten,

6. Personalausstattung, durch die eine ständige Bereitschaft seiner Dienste gewährleistet werden kann, und Sicherstellung einer entsprechenden Schulung seines Personals,

7. Verfügbarkeit von Redundanzsystemen und Ausweicharbeitsräumen, um die Kontinuität seiner Dienste sicherzustellen.

Art. 21 - § 1 - Im Rahmen der Ausübung seiner Befugnisse ergreift das nationale CSIRT alle geeigneten Maßnahmen, um die in den Artikeln 19 und 20 bestimmten Ziele umzusetzen. Diese Maßnahmen müssen in einem angemessenen Verhältnis zu den Zielen stehen und die Grundsätze der Objektivität, Transparenz und Nichtdiskriminierung beachten.

§ 2 - Wenn es für die Erfüllung der in Artikel 19 § 1 Nr. 1 bis 5 aufgeführten Aufgaben des nationalen CSIRT absolut notwendig ist, kann das nationale CSIRT die in Artikel 2 Absatz 1 Nr. 5 des Gesetzes vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors erwähnten Identifizierungsdaten oder die Metadaten der elektronischen Kommunikation im Sinne von Artikel 2 Nr. 93 des Gesetzes vom 13. Juni 2005 von einem in Artikel 2 Nr. 11 des vorerwähnten Gesetzes vom 13. Juni 2005 erwähnten Betreiber erhalten, der diese Daten aufbewahrt.

Unbeschadet der Zuständigkeiten von Personen, die gerichtspolizeiliche Aufträge erfüllen, und der Gerichtsbehörden und ohne in diese einzugreifen, werden mit den vorerwähnten Aufgaben folgende Zwecke verfolgt:

1. ohne strafrechtliche Zwecke, Vorbeugung, Ermittlung und Erkennung von Straftaten, die online oder über ein elektronisches Kommunikationsnetz beziehungsweise über einen elektronischen Kommunikationsdienst begangen werden, einschließlich der Taten, die unter schwere Kriminalität fallen.

2. Vorbeugung von ernsthaften Bedrohungen für die öffentliche Sicherheit,

3. Prüfung von Sicherheitsmängeln in elektronischen Kommunikationsnetzen oder diensten oder Informationssystemen.

Das nationale CSIRT kann je nach Dringlichkeit eines Antrags festlegen, innerhalb welcher Frist der Betreiber darauf antworten muss.

§ 3 - Wenn das nationale CSIRT einen Antrag auf Identifizierungsdaten im Sinne von Artikel 2 Absatz 1 Nr. 5 des Gesetzes vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors an einen Betreiber richtet, wird dieser Antrag von dem hierarchischen Vorgesetzten genehmigt.

§ 4 - Wenn das nationale CSIRT einen Antrag auf Metadaten der elektronischen Kommunikation im Sinne von Artikel 2 Nr. 93 des Gesetzes vom 13. Juni 2005, die nicht in § 3 erwähnte Daten sind, an einen Betreiber richtet, unterliegt dieser Antrag einer vorherigen Kontrolle durch die Datenschutzbehörde.

In dringenden und ordnungsgemäß begründeten Fällen kann das nationale CSIRT die in Absatz 1 erwähnte vorherige Kontrolle übergehen und die Daten direkt beantragen. Dieser Antrag wird unverzüglich an die in Absatz 1 erwähnte Behörde geschickt, um eine spätere Kontrolle zu ermöglichen.

Wenn sich die Datenschutzbehörde nach Abschluss der in Absatz 2 erwähnten Kontrolle weigert, die Gültigkeit des in Absatz 1 erwähnten Antrags auf Metadaten der elektronischen Kommunikation zu bestätigen, bringt das nationale CSIRT dies unverzüglich dem betreffenden Betreiber zur Kenntnis und löscht die erhaltenen Metadaten.

§ 5 - Der Generaldirektor des nationalen CSIRT bestimmt ausdrücklich die Personen, die zur Verarbeitung der in vorliegendem Artikel erwähnten elektronischen Kommunikationsdaten befugt sind.

§ 6 - Das nationale CSIRT unterrichtet die betroffenen natürlichen Personen soweit möglich über den Zugang zu ihren elektronischen Kommunikationsdaten, wenn dies die Erfüllung seiner Aufgaben oder eine laufende Untersuchung nicht mehr gefährden kann und wenn diese Personen identifiziert werden können.

§ 7 - Unbeschadet der Artikel 28*quinquies* § 1 und 57 § 1 des Strafprozessgesetzbuches darf das nationale CSIRT zur Erreichung dieser Ziele alle verfügbaren Informationen in seinem Besitz haben, anderen Personen preisgeben oder unter andere Personen verbreiten oder von ihnen Gebrauch machen, selbst wenn diese Daten aus dem unbefugten Zugriff Dritter auf ein Datenverarbeitungssystem stammen.

§ 8 - Das nationale CSIRT führt seine Aufträge mit der gebotenen Vorsicht aus, die von einer öffentlichen Behörde erwartet werden darf; dabei muss stets vorrangig dafür gesorgt werden, dass der Betrieb des Datenverarbeitungssystems nicht beeinträchtigt wird, und alle angemessenen Vorkehrungen getroffen werden, damit dem Datenverarbeitungssystem keine materiellen Schäden zugefügt werden.

Der Generaldirektor des nationalen CSIRT gewährleistet die Einhaltung der in vorliegendem Artikel erwähnten Bedingungen. Dazu werden interne Verfahren ausgearbeitet.

Art. 22 - § 1 - Als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen fungiert das nationale CSIRT als vertrauenswürdiger Vermittler und erleichtert es auf Ersuchen einer der beiden Seiten erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder IKT-Dienste.

Zu den Aufgaben des nationalen CSIRT gehört in diesem Rahmen insbesondere:

1. betreffende Einrichtungen zu ermitteln und zu kontaktieren,

2. natürliche oder juristische Personen, die eine Schwachstelle melden, zu unterstützen und

3. Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen, die mehrere Einrichtungen betreffen, zu koordinieren.

§ 2 - Natürliche oder juristische Personen können dem nationalen CSIRT eine potenzielle Schwachstelle, auf Wunsch anonym, melden.

Die Meldung erfolgt schriftlich gemäß dem auf der Website des nationalen CSIRT beschriebenen Verfahren.

Diese Meldung beeinträchtigt nicht die Anwendung des Gesetzes vom 28. November 2022 zum Schutz von Personen, die Verstöße innerhalb einer juristischen Person des privaten Sektors gegen das Unionsrecht oder das nationale Recht melden, oder der Gesetzesbestimmungen über den Schutz von Personen, die Verstöße innerhalb einer juristischen Person des öffentlichen Sektors gegen das Unionsrecht oder das nationale Recht melden.

§ 3 - Das nationale CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden, und sorgt für die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person, sofern diese Person dies beantragt und die in Artikel 23 erwähnten Bedingungen erfüllt.

Das nationale CSIRT gewährleistet die Vollständigkeit, Integrität, dauerhafte Speicherung und Vertraulichkeit der im Zuge der Meldung übermittelten Informationen.

Der Zugriff auf diese Informationen ist auf die vom Generaldirektor des nationalen CSIRT ermächtigten Personen beschränkt, es sei denn, die Weitergabe dieser Informationen ist für die Erfüllung der in vorliegendem Artikel aufgeführten Aufgaben erforderlich.

§ 4 - Unter Einhaltung der in Artikel 21 §§ 1 und 4 aufgeführten Bedingungen kann das nationale CSIRT die Sicherheit eines Netz- und Informationssystems beobachten, untersuchen und testen, um zu bestimmen, ob eine potenzielle Schwachstelle vorliegt, oder um die vom Hinweisgeber verwendeten Methoden zu überprüfen.

§ 5 - Wenn die gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten haben könnte, arbeitet das nationale CSIRT gegebenenfalls mit den anderen als Koordinatoren benannten CSIRTs innerhalb des CSIRTs-Netzwerks zusammen.

§ 6 - Der Generaldirektor des nationalen CSIRT gewährleistet die Einhaltung der in vorliegendem Artikel erwähnten Bedingungen. Dazu werden interne Verfahren ausgearbeitet.

Art. 23 - § 1 - Im Rahmen des in Artikel 22 erwähnten Verfahrens begehen Hinweisgeber keinen Verstoß gegen die Artikel 314*bis*, 458, 550*bis*, 550*ter* des Strafgesetzbuches und gegen Artikel 145 des Gesetzes vom 13. Juni 2005, vorausgesetzt:

1. sie haben ohne betrügerische Absicht oder Schädigungsabsicht gehandelt,

2. sie haben der für das System verantwortlichen Organisation und dem nationalen CSIRT so schnell wie möglich und spätestens vierundzwanzig Stunden nach Entdeckung einer potenziellen Schwachstelle eine vereinfachte Meldung übermittelt, die die Identifizierung des betroffenen Systems und eine kurze Beschreibung der potenziellen Schwachstelle enthält,

3. sie haben der für das System verantwortlichen Organisation, gegebenenfalls unter Einhaltung der von dieser Organisation festgelegten Meldevorschriften, und dem nationalen CSIRT gemäß dem in Artikel 22 § 2 erwähnten Verfahren unverzüglich und spätestens zweiundsiebzig Stunden nach Entdeckung einer potenziellen Schwachstelle eine vollständige Meldung übermittelt,

4. sie sind nicht über das hinaus gegangen, was notwendig und verhältnismäßig war, um dem Vorhandensein einer Schwachstelle nachzugehen und sie zu melden,

5. sie haben die Informationen in Bezug auf die entdeckte Schwachstelle und die anfälligen Systeme nicht ohne die Zustimmung des nationalen CSIRT offengelegt,

6. sie haben in Bezug auf Netzwerke und Systeme der in Artikel 5 §§ 4 und 5 erwähnten Organisationen und der Gerichtsorgane und in Bezug auf die von diesen Stellen oder in ihrem Auftrag verarbeiteten Informationen vor Begehung dieser Taten eine schriftliche Vereinbarung mit dem zuständigen Dienst über die Modalitäten und die Methodik getroffen, die im Rahmen der Suche nach potenziellen Schwachstellen anzuwenden sind.

§ 2 - Bei Personen, die Informationen über eine potenzielle Schwachstelle melden, die sie in ihrem beruflichen Kontext erlangt haben, wird nicht davon ausgegangen, dass sie die Wahrung des Berufsgeheimnisses verletzt haben, und sie können in keiner Weise für die Übermittlung von Informationen, die zur Meldung einer potenziellen Schwachstelle an das nationale CSIRT erforderlich sind, haftbar gemacht werden.

§ 3 - Eine weitere mögliche Haftung von Hinweisgebern aufgrund von Handlungen oder Unterlassungen, die für die Durchführung des in Artikel 22 erwähnten Verfahrens nicht erforderlich sind und den Bedingungen von § 1 nicht entsprechen, unterliegt weiterhin dem geltenden Recht.

Abschnitt 3 - Eventuelle sektorspezifische Behörden

Art. 24 - Unbeschadet der übrigen Bestimmungen kann eine sektorspezifische Behörde:

1. sektorspezifische Übungen organisieren, koordinieren oder daran teilnehmen, was die in den Artikeln 30 und 33 erwähnten Maßnahmen betrifft,

2. die Auswirkungen eines Sicherheitsvorfalls auf den Sektor analysieren und bewältigen,

3. sich an den Arbeiten der Kooperationsgruppe zu Themen beteiligen, die in ihren Zuständigkeitsbereich fallen,

4. die Einrichtungen ihres Sektors sensibilisieren.

KAPITEL 2 - *Zusammenarbeit auf nationaler Ebene*

Art. 25 - § 1 - Die in Kapitel 1 des vorliegenden Titels erwähnten Behörden arbeiten zusammen, um den in vorliegendem Gesetz aufgeführten Verpflichtungen nachzukommen.

§ 2 - Wie für die Ausführung des vorliegenden Gesetzes erforderlich arbeiten die in § 1 erwähnten Behörden auf nationaler Ebene ebenfalls mit dem NCCN, den Verwaltungsdiensten des Staates, den Verwaltungsbehörden, einschließlich der nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 und Nr. 2018/1139, den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, der Belgischen Nationalbank, der Autorität Finanzielle Dienste und Märkte, dem Institut, den gemäß dem [Gesetz vom 19. Dezember 2025] zuständigen Behörden, den Gerichtsbehörden, den im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Nachrichten- und Sicherheitsdiensten, den im Gesetz vom 7. Dezember 1998 zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes erwähnten Polizeidiensten und den Datenschutzbehörden zusammen.

§ 3 - Wesentliche und wichtige Einrichtungen und in Kapitel 1 des vorliegenden Titels erwähnte Behörden arbeiten ständig durch einen adäquaten Informationsaustausch im Bereich Sicherheit von Netz- und Informationssystemen zusammen.

§ 4 - In Kapitel 1 des vorliegenden Titels erwähnte Behörden und im Rahmen des [Gesetzes vom 19. Dezember 2025] zuständige Behörden arbeiten zusammen und tauschen regelmäßig Informationen aus hinsichtlich der Identifizierung kritischer Einrichtungen, zu Risiken, Cyberbedrohungen und Sicherheitsvorfällen und zu nicht cyberbezogenen Risiken, Bedrohungen und Sicherheitsvorfällen, die [kritische Einrichtungen im Sinne des Gesetzes vom 19. Dezember 2025] betreffen, und zu den als Reaktion auf diese Risiken, Bedrohungen und Sicherheitsvorfälle ergriffenen Maßnahmen.

§ 5 - In Kapitel 1 des vorliegenden Titels erwähnte Behörden und zuständige Behörden gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, der 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 und dem Gesetz vom 13. Juni 2005 tauschen regelmäßig einschlägige Informationen aus, auch in Bezug auf einschlägige Sicherheitsvorfälle und Cyberbedrohung.

§ 6 - Die nationale Cybersicherheitsbehörde richtet eine Koordinierungs- und Bewertungsplattform ein, damit die in Artikel 15 erwähnten Behörden und das NCCN im Rahmen der Ausführung des vorliegenden Gesetzes Informationen austauschen und sich abstimmen können.

[Art. 25 § 2 abgeändert durch Art. 70 Nr. 1 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026); § 4 abgeändert durch Art. 70 Nr. 2 und 3 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

KAPITEL 3 - *Vertraulichkeit und Informationsaustausch*

Art. 26 - § 1 - Vorliegender Artikel beeinträchtigt nicht die Anwendung des Gesetzes vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle, des Gesetzes vom 11. April 1994 über die Öffentlichkeit der Verwaltung oder anderer Gesetzesbestimmungen, die die Vertraulichkeit von Informationen in Bezug auf die wesentlichen Interessen der nationalen öffentlichen Sicherheit gewährleisten.

§ 2 - Personen, die bei der Konformitätsbewertung oder der Aufsicht berufsbedingt ihre Mitwirkung gewähren müssen, unterliegen der Geheimhaltungspflicht. Wer diese Geheimhaltungspflicht verletzt, wird mit den in Artikel 458 des Strafgesetzbuches vorgesehenen Strafen bestraft.

Personen, die aufgrund ihres Standes oder Berufes Kenntnis haben von ihnen anvertrauten Geheimnissen, ist es erlaubt, diese für die Ausführung des vorliegenden Gesetzes preiszugeben.

Diese Personen holen die Zustimmung der in Artikel 5 § 4 erwähnten Behörden ein, sofern diese von einem Geheimnis betroffen sind.

§ 3 - In Kapitel 1 des vorliegenden Titels erwähnte Behörden, wesentliche oder wichtige Einrichtungen beziehungsweise ihre Subunternehmer beschränken den Zugriff auf Informationen in Bezug auf die Ausführung des vorliegenden Gesetzes auf Personen, die für die Ausübung ihres Amtes oder die Ausführung ihres Auftrags in Verbindung mit der Ausführung des vorliegenden Gesetzes Kenntnis von diesen Informationen und Zugriff auf sie haben müssen.

§ 4 - Informationen, die den in Kapitel 1 des vorliegenden Titels erwähnten Behörden von wesentlichen oder wichtigen Einrichtungen bereitgestellt werden, dürfen mit den Behörden der Europäischen Union und mit belgischen oder ausländischen Behörden ausgetauscht werden, wenn dieser Austausch für die Anwendung von Gesetzesbestimmungen erforderlich ist.

Auszutauschende Informationen werden auf das beschränkt, was für das verfolgte Ziel relevant und angemessen ist, insbesondere für die Einhaltung der Verordnung (EU) 2016/679. Bei diesem Informationsaustausch werden die Vertraulichkeit der betreffenden Informationen gewahrt und die Sicherheit und die geschäftlichen Interessen der wesentlichen oder wichtigen Einrichtungen geschützt.

Art. 27 - § 1 - In den Anwendungsbereich des vorliegenden Gesetzes fallende Einrichtungen und gegebenenfalls andere betroffene Einrichtungen, die nicht in den Anwendungsbereich des vorliegenden Gesetzes fallen, können auf freiwilliger Basis untereinander im Rahmen von Gemeinschaften relevante Cybersicherheitsinformationen austauschen, einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen, sofern:

1. dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen,

2. durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen sich zu verbreiten eingedämmt beziehungsweise verhindert wird, eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von

Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden oder indem die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird.

§ 2 - Der in § 1 erwähnte Informationsaustausch erfolgt im Wege von Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen.

§ 3 - Die nationale Cybersicherheitsbehörde erleichtert die Festlegung der in § 2 erwähnten Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit. In solchen Vereinbarungen können operative Elemente, einschließlich der Nutzung spezieller IKT-Plattformen und Automatisierungsinstrumente, Inhalt und Bedingungen der Vereinbarungen über den Informationsaustausch bestimmt werden. Die nationale Cybersicherheitsbehörde und eventuelle sektorspezifische Behörden können Bedingungen für die Nutzung der Informationen festlegen, die sie den in § 1 erwähnten Gemeinschaften zur Verfügung stellen.

§ 4 - Wesentliche und wichtige Einrichtungen unterrichten die nationale Cybersicherheitsbehörde beim Abschluss der in § 2 erwähnten Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit über ihre Beteiligung an solchen Vereinbarungen oder gegebenenfalls über ihren Rücktritt von solchen Vereinbarungen, sobald dieser wirksam wird.

KAPITEL 4 - *Nationale Cybersicherheitsstrategie*

Art. 28 - § 1 - Nach Stellungnahme des Nationalen Sicherheitsrates, der in Artikel 15 erwähnten Behörden, des NCCN und gegebenenfalls der Datenschutzbehörden erlassen die im Rat versammelten Minister die nationale Cybersicherheitsstrategie und aktualisieren sie mindestens alle fünf Jahre auf der Grundlage von Leistungsindikatoren.

Diese Strategie enthält die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus.

§ 2 - Die nationale Cybersicherheitsstrategie umfasst unter anderem Folgendes:

1. Ziele und Prioritäten der nationalen Cybersicherheitsstrategie, die insbesondere die in den Anlagen I und II aufgeführten Sektoren abdecken,

2. einen Steuerungsrahmen zur Verwirklichung der in Nr. 1 erwähnten Ziele und Prioritäten, der die Aufgaben und Zuständigkeiten der öffentlichen Behörden und anderer betroffener Interessenträger und die in § 3 erwähnten Konzepte umfasst,

3. einen Steuerungsrahmen, in dem die Aufgaben und Zuständigkeiten der jeweiligen Interessenträger in Belgien klargestellt und die Zusammenarbeit und Koordinierung in Belgien zwischen den in Kapitel 1 des vorliegenden Titels erwähnten Behörden und die Koordinierung und Zusammenarbeit zwischen diesen Behörden und den nach sektorspezifischen Rechtsakten der Europäischen Union zuständigen Behörden untermauert werden,

4. einen Mechanismus zur Ermittlung von relevanten Anlagen und eine Bewertung der Cybersicherheitsrisiken in Belgien,

5. die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor,

6. eine Liste der verschiedenen Behörden und Interessenträger, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind,

7. einen politischen Rahmen für eine verstärkte Koordinierung zwischen den in Kapitel 1 des vorliegenden Titels erwähnten Behörden und den nach [dem Gesetz vom 19. Dezember 2025] zuständigen Behörden zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle im Bereich der Cybersicherheit und über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle und für die Wahrnehmung von Aufsichtsaufgaben, soweit zutreffend,

8. einen Plan, einschließlich erforderlicher Maßnahmen, zur Steigerung des allgemeinen Grads der Sensibilisierung der Bürger für Cybersicherheit,

9. eine Aufstellung der Ausbildungs-, Sensibilisierungs- und Schulungsprogramme im Zusammenhang mit der nationalen Cybersicherheitsstrategie,

10. eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Cybersicherheitsstrategie.

§ 3 - Im Rahmen der nationalen Cybersicherheitsstrategie werden Konzepte angenommen:

1. für die Cybersicherheit in der Lieferkette für IKT-Produkte und IKT-Dienste, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden,

2. für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und IKT-Dienste bei der Vergabe öffentlicher Aufträge, einschließlich hinsichtlich der Zertifizierung der Cybersicherheit, der Verschlüsselung und der Nutzung quelloffener Cybersicherheitsprodukte,

3. für das Vorgehen bei Schwachstellen, das die Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen nach Artikel 22 umfasst,

4. im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets, erforderlichenfalls einschließlich der Cybersicherheit von Unterseekommunikationskabeln,

5. zur Förderung der Entwicklung und Integration einschlägiger fortgeschrittener Technologien, damit Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf dem neuesten Stand zur Anwendung gelangen,

6. zur Förderung und Entwicklung der allgemeinen und beruflichen Bildung im Bereich der Cybersicherheit, von Kompetenzen, Sensibilisierungsmaßnahmen und Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit sowie der Anleitung zu guten Vorgehensweisen und Kontrollen im Bereich der Cyberhygiene für Bürger, Interessenträger und Einrichtungen,

7. zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung, der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur,

8. mit einschlägigen Verfahren und geeigneten Instrumenten für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheitsinformationen zwischen Einrichtungen zu unterstützen,

9. zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Betriebe, insbesondere vom Anwendungsbereich des vorliegenden Gesetzes ausgenommener KMB, durch Bereitstellung leicht zugänglicher Orientierungshilfen und Unterstützung für ihre spezifischen Bedürfnisse,

10. zur Förderung eines aktiven Cyberschutzes.

[Art. 28 § 2 einziger Absatz Nr. 7 abgeändert durch Art. 71 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

KAPITEL 5 - *Nationaler Plan für die Reaktion auf Cybersicherheitsvorfälle und Cyberkrisen*

Art. 29 - § 1 - Der König legt durch einen im Ministerrat beratenen Erlass einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle und Cyberkrisen fest. Dieser Plan ist eine nationaler Plan im Sinne von Artikel 9 § 2 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit.

§ 2 - Unbeschadet der Bestandteile, die in den nationalen Plänen enthalten sein müssen, wird im nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle und Cyberkrisen insbesondere Folgendes festgelegt:

1. Ziele der nationalen Vorsorgemaßnahmen und -tätigkeiten,

2. Aufgaben und Zuständigkeiten der Behörden für das Cyberkrisenmanagement,

3. Verfahren für das Cyberkrisenmanagement, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und Kanäle für den Informationsaustausch,

4. nationale Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen,

5. einschlägige öffentliche und private Interessenträger und betroffene Infrastruktur,

6. zwischen den zuständigen nationalen Behörden und Stellen vereinbarte nationale Verfahren und Regelungen, die gewährleisten sollen, dass Belgien sich wirksam am koordinierten Management von Cybersicherheitsvorfällen und Cyberkrisen auf Ebene der Europäischen Union beteiligt und dieses Management unterstützt.

TITEL 3 - *Risikomanagementmaßnahmen im Bereich der Cybersicherheit und Berichtspflichten*

KAPITEL 1 - *Risikomanagementmaßnahmen im Bereich der Cybersicherheit*

Art. 30 - § 1 - Wesentliche und wichtige Einrichtungen ergreifen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

§ 2 - Die in § 1 erwähnten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

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

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 und gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,

11. Konzepte zur koordinierten Offenlegung von Schwachstellen.

§ 4 - Wesentliche und wichtige Einrichtungen berücksichtigen bei der Erwägung geeigneter Maßnahmen nach § 3 Nr. 4 die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse.

Diese Maßnahmen müssen im Einklang mit den Ergebnissen der auf Ebene der Europäischen Union koordinierten Bewertungen der Sicherheitsrisiken für kritische Lieferketten stehen.

§ 5 - Wesentliche und wichtige Einrichtungen führen auf der Grundlage eines gefahrenübergreifenden Ansatzes eine Risikoanalyse durch, die darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und erstellen auf der Grundlage dieser Analyse eine S.P.I., die mindestens die in § 3 erwähnten Aspekte umfasst.

§ 6 - Stellt eine wesentliche oder wichtige Einrichtung fest, dass sie den in § 3 erwähnten Maßnahmen nicht nachkommt, ergreift sie unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen.

Art. 31 - § 1 - Die Leitungsorgane wesentlicher und wichtiger Einrichtungen billigen die von diesen Einrichtungen zur Einhaltung von Artikel 30 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit, überwachen ihre Umsetzung und sind für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich.

Dieser Artikel lässt die für öffentliche Einrichtungen geltenden Haftungsregelungen und die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

§ 2 - Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen nehmen an Schulungen teil, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Art. 32 - Wesentliche oder wichtige Einrichtungen sind für die durchgeführte Risikoanalyse und für Auswahl und Umsetzung der in Artikel 30 § 1 erwähnten Maßnahmen verantwortlich.

Art. 33 - Nach Konsultierung der nationalen Cybersicherheitsbehörde, gegebenenfalls der relevanten sektorspezifischen Behörde und der betroffenen föderierten Teilgebiete kann der König durch einen im Ministerrat beratenen Erlass angemessene und verhältnismäßige zusätzliche Risikomanagementmaßnahmen im Bereich der Cybersicherheit anordnen.

KAPITEL 2 - *Meldung von Sicherheitsvorfällen*

Abschnitt 1 - Meldepflicht

Art. 34 - § 1 - Wesentliche und wichtige Einrichtungen unterrichten unverzüglich das nationale CSIRT über jeden erheblichen Sicherheitsvorfall gemäß Modalitäten, die in einem zwischen dem nationalen CSIRT und dem NCCN geschlossenen Protokoll festgelegt sind. Diese Einrichtungen übermitteln unter anderem alle Informationen, die es dem nationalen CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

Gegebenenfalls unterrichten die betreffenden Einrichtungen die Empfänger ihrer Dienste unverzüglich über erhebliche Sicherheitsvorfälle, die die Erbringung von Diensten in den in den Anlagen I und II aufgeführten Sektoren oder Teilsektoren beeinträchtigen könnten.

Das nationale CSIRT übermittelt die in Absatz 1 erwähnten Meldungen unverzüglich den gegebenenfalls zuständigen sektorspezifischen Behörden. Meldungen der wesentlichen Einrichtungen werden ebenfalls dem NCCN übermittelt.

§ 2 - Gegebenenfalls teilen die betreffenden Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst.

§ 3 - Nach Konsultierung der nationalen Cybersicherheitsbehörde, der sektorspezifischen Behörden, des NCCN und der föderierten Teilgebiete kann der König durch einen im Ministerrat beratenen Erlass genaue Meldeschwellen festlegen, die sich nach dem Ausmaß der Auswirkungen oder der Dringlichkeit eines Sicherheitsvorfalls richten.

§ 4 - Mit der bloßen Meldung eines Sicherheitsvorfalls wird keine höhere Haftung der meldenden Einrichtung begründet.

Art. 35 - § 1 - Für die Zwecke der in Artikel 34 § 1 Absatz 1 erwähnten Meldung übermitteln die betreffenden Einrichtungen dem nationalen CSIRT Folgendes:

1. unverzüglich, in jedem Fall aber innerhalb vierundzwanzig Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,

2. unverzüglich, in jedem Fall aber innerhalb zweiundsiebzig Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die in Nr. 1 erwähnten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden,

3. auf Ersuchen des nationalen CSIRT oder gegebenenfalls der relevanten sektorspezifischen Behörde einen Zwischenbericht über relevante Statusaktualisierungen,

4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nr. 2 einen Abschlussbericht, der Folgendes enthält:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen,

b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat,

c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen,

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls,

5. im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des in Nr. 4 erwähnten Abschlussberichts, einen Fortschrittsbericht zu diesem Zeitpunkt und einen Abschlussbericht innerhalb eines Monats nach endgültiger Abhandlung des Sicherheitsvorfalls.

§ 2 - In Abweichung von § 1 Nr. 2 unterrichtet ein Vertrauensdiensteanbieter das nationale CSIRT in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb vierundzwanzig Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls.

§ 3 - Das nationale CSIRT übermittelt die in den Paragraphen 1 und 2 erwähnten Meldungen unverzüglich den gegebenenfalls zuständigen sektorspezifischen Behörden. Meldungen der wesentlichen Einrichtungen werden ebenfalls dem NCCN übermittelt.

Art. 36 - § 1 - Das nationale CSIRT übermittelt der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb vierundzwanzig Stunden nach Eingang der Frühwarnung gemäß Artikel 35 § 1 Nr. 1 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen.

§ 2 - Das nationale CSIRT leistet auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das nationale CSIRT ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

Art. 37 - § 1 - Gegebenenfalls und insbesondere, wenn der erhebliche Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet das nationale CSIRT unverzüglich die anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Sicherheitsvorfall. Diese Informationen umfassen die Art der gemäß Artikel 35 erhaltenen Informationen. Dabei wahrt das nationale CSIRT im Einklang mit dem Recht der Europäischen Union oder dem nationalen Recht die Sicherheit und das wirtschaftliche Interesse der Einrichtung und die Vertraulichkeit der bereitgestellten Informationen.

§ 2 - Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, kann das nationale CSIRT nach Konsultation der betreffenden Einrichtung, des NCCN, gegebenenfalls der relevanten sektorspezifischen Behörde und des betreffenden Ministers die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

§ 3 - Auf Ersuchen der relevanten sektorspezifischen Behörde leitet die nationale Cybersicherheitsbehörde die nach Artikel 34 § 1 Absatz 1 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

§ 4 - Die nationale Cybersicherheitsbehörde legt der ENISA alle drei Monate einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, Sicherheitsvorfällen, Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß Artikel 34 § 1 Absatz 1 und Artikel 38 § 1 gemeldet wurden.

§ 5 - Das nationale CSIRT stellt den gemäß dem [Gesetz vom 19. Dezember 2025] zuständigen Behörden Informationen über erhebliche Sicherheitsvorfälle, Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung, die gemäß Artikel 34 § 1 Absatz 1 und Artikel 38 § 1 von den [kritischen Einrichtungen im Sinne des Gesetzes vom 19. Dezember 2025] gemeldet wurden.

[Art. 37 § 5 abgeändert durch Art. 72 Nr. 1 und 2 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Abschnitt 2 - Freiwillige Meldung

Art. 38 - § 1 - Zusätzlich zu der Berichtspflicht nach Artikel 34 können dem nationalen CSIRT auf freiwilliger Basis Meldungen übermittelt werden von:

1. wesentlichen und wichtigen Einrichtungen in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle,

2. anderen als den in Nr. 1 erwähnten Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich des vorliegenden Gesetzes fallen, in Bezug auf erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle.

§ 2 - Die in § 1 erwähnten freiwilligen Meldungen werden so behandelt wie die in Abschnitt 1 des vorliegenden Kapitels erwähnten Pflichtmeldungen.

Pflichtmeldungen können jedoch vorrangig vor freiwilligen Meldungen bearbeitet werden.

Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten führen freiwillige Meldungen nicht dazu, dass eine in Artikel 44 erwähnte Kontrolle eingeleitet wird oder dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

TITEL 4 - *Aufsicht und Sanktionen*

KAPITEL 1 - *Aufsicht*

Abschnitt 1 - Regelmäßige Konformitätsbewertung

Art. 39 - Wesentliche Einrichtungen unterziehen sich einer regelmäßigen Bewertung der Konformität der Umsetzung der in Artikel 30 erwähnten Maßnahmen zum Cybersicherheitsrisikomanagement auf der Grundlage der vom König festgelegten Modalitäten und Referenzrahmen:

1. entweder indem sie sich für eine in Artikel 40 erwähnte regelmäßige Konformitätsbewertung auf der Grundlage eines der vom König festgelegten Referenzrahmen entscheiden

2. oder indem sie sich der Kontrolle durch die nationale Cybersicherheitsbehörde auf der Grundlage der vom König festgelegten Modalitäten unterziehen.

In Abweichung von Absatz 1 und auf Antrag der relevanten sektorspezifischen Behörde werden die in Absatz 1 Nr. 2 erwähnten Kontrollen gemeinsam unter der Leitung der nationalen Cybersicherheitsbehörde durchgeführt oder gegebenenfalls mit Zustimmung der nationalen Cybersicherheitsbehörde dem zuständigen Inspektionsdienst übertragen.

Legt der König mehrere Referenzrahmen fest, wählen die wesentlichen Einrichtungen den Referenzrahmen, dem sie sich unterwerfen.

Art. 40 - § 1 - Die in Artikel 39 Absatz 1 Nr. 1 erwähnte regelmäßige Konformitätsbewertung wird von einer gemäß den vom König festgelegten Bedingungen von der nationalen Cybersicherheitsbehörde zugelassenen Konformitätsbewertungsstelle durchgeführt.

Für die Kontrolle von Einrichtungen, die als [kritische Einrichtungen im Sinne des Gesetzes vom 19. Dezember 2025] eingestuft sind, und von Einrichtungen der öffentlichen Verwaltung verfügen die Konformitätsbewertungsstelle und natürliche Personen, die die Konformität bewerten, über eine Sicherheitsermächtigung.

§ 2 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde kann jederzeit gemäß den Bestimmungen des vorliegenden Kapitels überprüfen, ob Konformitätsbewertungsstellen die in § 1 erwähnten Zulassungsbedingungen einhalten.

[Art. 40 § 1 Abs. 2 abgeändert durch Art. 73 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 41 - Wichtige Einrichtungen können sich freiwillig einer in Artikel 39 Absatz 1 Nr. 1 erwähnten regelmäßigen Bewertung der Konformität der Umsetzung der in Artikel 30 § 3 erwähnten Maßnahmen zum Cybersicherheitsrisikomanagement auf der Grundlage der vom König festgelegten Modalitäten und Referenzrahmen unterziehen.

Art. 42 - Bei wesentlichen und wichtigen Einrichtungen, die sich einer regelmäßigen Konformitätsbewertung gemäß Artikel 39 Absatz 1 Nr. 1 beziehungsweise den Artikeln 39 und 41 unterziehen, wird bis zum Gegenbeweis davon ausgegangen, dass sie die in Artikel 30 erwähnten Verpflichtungen erfüllen.

Art. 43 - Eine Liste der von der nationalen Cybersicherheitsbehörde gemäß Artikel 40 zugelassenen Konformitätsbewertungsstellen ist bei der nationalen Cybersicherheitsbehörde erhältlich, die diese Liste auf dem neuesten Stand hält.

Abschnitt 2 - Allgemeine Bestimmungen über den Inspektionsdienst

Art. 44 - § 1 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde überprüft, ob wesentliche und wichtige Einrichtungen die Maßnahmen zum Cybersicherheitsrisikomanagement und die Regeln zur Meldung von Sicherheitsvorfällen einhalten.

In Abweichung von Absatz 1 und auf Antrag der relevanten sektorspezifischen Behörde werden die Kontrollen gemeinsam unter der Leitung der nationalen Cybersicherheitsbehörde durchgeführt oder mit Zustimmung der nationalen Cybersicherheitsbehörde gegebenenfalls dem zuständigen Inspektionsdienst übertragen.

Die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst oder, falls kein sektorspezifischer Inspektionsdienst durch Gesetz oder vom König benannt wurde, der Inspektionsdienst der nationalen Cybersicherheitsbehörde kann überprüfen, ob wichtige oder wesentliche Einrichtungen die in Artikel 33 erwähnten zusätzlichen Maßnahmen zum Cybersicherheitsrisikomanagement in einem bestimmten Sektor oder Teilsektor einhalten.

§ 2 - Bei der Anforderung von Informationen oder Beweismitteln geben der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst den Zweck der Anforderung, die konkret angeforderten Informationen oder Beweismittel und die Frist an, innerhalb deren diese vorzulegen sind.

Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst können Sachverständige hinzuziehen.

§ 3 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst können die in vorliegendem Titel erwähnten Aufsichtsaufgaben auf der Grundlage eines risikobasierten Ansatzes priorisieren.

§ 4 - Unbeschadet der Zuständigkeiten und Aufgaben der Datenschutzbehörden arbeiten der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nr. 12 der Verordnung (EU) 2016/679 führen, eng mit den Datenschutzbehörden zusammen.

Art. 45 - § 1 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst unterrichten bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse - mit denen sichergestellt werden soll, dass [kritische Einrichtungen im Sinne des Gesetzes vom 19. Dezember 2025] vorliegendes Gesetz erfüllen - die gemäß dem [Gesetz vom 19. Dezember 2025] zuständigen Behörden. Gegebenenfalls können die gemäß dem [Gesetz vom 19. Dezember 2025] zuständigen Behörden den Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder den zuständigen sektorspezifischen Inspektionsdienst ersuchen, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf [eine kritische Einrichtung im Sinne des Gesetzes vom 19. Dezember 2025] auszuüben.

§ 2 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst arbeiten mit den gemäß der 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 jeweils zuständigen Behörden zusammen. Insbesondere unterrichten der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse - mit denen sichergestellt werden soll, dass wesentliche oder wichtige Einrichtungen, die als kritische IKT-Drittanbieter gemäß Artikel 31 dieser Verordnung benannt wurden, vorliegendes Gesetz erfüllen - das gemäß Artikel 32 Absatz 1 dieser Verordnung eingerichtete Überwachungsforum.

[Art. 45 § 1 abgeändert durch Art. 74 Nr. 1 bis 3 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 46 - § 1 - Befinden sich die Netz- und Informationssysteme einer Einrichtung außerhalb des belgischen Staatsgebiets, können der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst in Absprache mit der nationalen Cybersicherheitsbehörde die zuständigen Aufsichtsbehörden anderer Mitgliedstaaten um Zusammenarbeit und Unterstützung ersuchen.

Im Rahmen der in Absatz 1 erwähnten Ersuchen:

1. können der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst zuständige Aufsichtsbehörden anderer Mitgliedstaaten ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen,

2. können der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst unter Angabe von Gründen zuständige Aufsichtsbehörden anderer Mitgliedstaaten um Amtshilfe ersuchen, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können.

Die in Absatz 2 Nr. 2 erwähnte Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen.

§ 2 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst arbeiten - in einem ihren zur Verfügung stehenden Ressourcen angemessenen Umfang und sofern sie zuständig sind - mit den zuständigen Aufsichtsbehörden für Cybersicherheit anderer Mitgliedstaaten auf deren Ersuchen hin zusammen und leisten ihnen Amtshilfe, wenn sich die Netz- und Informationssysteme der betreffenden Einrichtung auf belgischem Staatsgebiet befinden.

In Bezug auf das in Absatz 1 erwähnte Ersuchen gilt Folgendes:

1. Die nationale Cybersicherheitsbehörde zentralisiert die Informationen und Ersuchen zu den von ihr selbst und gegebenenfalls von der relevanten sektorspezifischen Behörde oder dem zuständigen sektorspezifischen Inspektionsdienst getroffenen Aufsichts- und Durchsetzungsmaßnahmen und übermittelt sie den für Cybersicherheit zuständigen Aufsichtsbehörden anderer Mitgliedstaaten.

2. Das betreffende Ersuchen kann Aufsichts- und Durchsetzungsmaßnahmen betreffen.

3. Das betreffende Ersuchen kann unter Angabe von Gründen Amtshilfe betreffen, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können.

Die in Absatz 2 Nr. 3 erwähnte Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen.

Die ersuchte Behörde darf ein Amtshilfeersuchen nur ablehnen, wenn festgestellt wird, dass sie für die erbetene Amtshilfe nicht zuständig ist, dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde steht oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung beziehungsweise Ausführung den wesentlichen Interessen im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung Belgiens zuwiderlaufen würde. Bevor diese Behörde ein solches Ersuchen ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden und - auf Ersuchen eines der betreffenden Mitgliedstaaten - die Europäische Kommission und die ENISA.

§ 3 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde oder der zuständige sektorspezifische Inspektionsdienst können im gegenseitigen Einvernehmen unter sich und/oder mit zuständigen Aufsichtsbehörden anderer Mitgliedstaaten gemeinsame Aufsichtsmaßnahmen durchführen.

§ 4 - Vorliegender Artikel ist nicht auf diplomatische und konsularische Missionen anwendbar.

Art. 47 - § 1 - Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes erhalten eine Legitimationskarte, deren Muster vom König festgelegt wird.

§ 2 - Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes und Sachverständige, die für Inspektionen hinzugezogen werden, dürfen in Unternehmen oder Einrichtungen, mit deren Kontrolle sie beauftragt sind, keinerlei direkte oder indirekte Interessen haben, die ihre Objektivität beeinträchtigen können. Sie leisten den Eid vor dem leitenden Beamten ihres Dienstes.

In Artikel 44 § 1 erwähnte Behörden ergreifen erforderliche Maßnahmen zur Gewährleistung der Unabhängigkeit ihrer Personalmitglieder und zur Vorbeugung, Ermittlung und Beilegung von Interessenkonflikten bei der Wahrnehmung ihrer Aufgaben.

Der Begriff des Interessenkonflikts bezieht sich zumindest auf Situationen, in denen ein Mitglied des Personals der in Artikel 44 § 1 erwähnten Behörden direkt oder indirekt ein finanzielles, wirtschaftliches oder sonstiges persönliches Interesse hat, das im Rahmen seines Auftrags oder seiner Aufgaben als Beeinträchtigung seiner Unparteilichkeit und Unabhängigkeit wahrgenommen werden könnte.

§ 3 - Die Mitglieder des Personals der in Artikel 44 § 1 erwähnten Behörden erhalten von Drittpersonen im Rahmen ihrer Zuständigkeiten keine direkten oder indirekten Weisungen und holen solche Weisungen auch nicht ein.

Es ist ihnen untersagt, bei Beratungen oder Beschlüssen über Akten anwesend zu sein, an denen sie selbst oder ihre Verwandten oder Verschwägerten bis zum dritten Grad ein persönliches oder direktes Interesse haben.

Der König kann ebenfalls andere Situationen als Interessenkonflikte bestimmen.

Abschnitt 3 - Beaufsichtigung der Einrichtungen durch den Inspektionsdienst

Art. 48 - § 1 - Unbeschadet der in Artikel 8 des Strafprozessgesetzbuches vorgesehenen Zuständigkeiten der Gerichtspolizeioffiziere verfügen die vereidigten Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes bei der Ausführung ihres Aufsichtsauftrags sowohl im Rahmen von Verwaltungshandlungen als auch im Rahmen der Feststellung von Verstößen gegen vorliegendes Gesetz über folgende Kontrollbefugnisse:

1. Zugang zu Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind, anfordern und Kopien davon erhalten, insbesondere zu Nachweisen für die Umsetzung der Cybersicherheitskonzepte, zum Beispiel zu den Ergebnissen von Konformitätsbewertungen oder Sicherheitsaudits und den entsprechenden zugrunde liegenden Nachweisen,

2. vor Ort oder extern Untersuchungen, Kontrollen und Vernehmungen durchführen, einschließlich von geschulten Fachleuten durchgeführter Stichprobenkontrollen,

3. wesentliche Einrichtungen regelmäßigen und gezielten Sicherheitsprüfungen, die von einer unabhängigen Stelle durchgeführt werden, unterziehen auf der Grundlage von Risikobewertungen des zuständigen Inspektionsdienstes oder der kontrollierten Einrichtung oder anderer verfügbarer risikobezogener Informationen,

4. Informationen anfordern, die sie für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit, insbesondere dokumentierte Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die nationale Cybersicherheitsbehörde oder gegebenenfalls an die sektorspezifische Behörde gemäß Titel 1 und der Umsetzung des vorliegenden Gesetzes für erforderlich halten,

5. Ad-hoc-Prüfungen durchführen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder eines Verstoßes gegen vorliegendes Gesetzes gerechtfertigt sind,

6. Sicherheitsscans durchführen auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung,

7. die Personalien der Personen aufnehmen, die sich an Orten, die die Einrichtung nutzt, befinden und deren Vernehmung sie für die Ausführung ihres Auftrags für notwendig erachten. Zu diesem Zweck können sie von diesen Personen die Vorlage offizieller Identifizierungsdokumente fordern,

8. gegebenenfalls im Rahmen der Anwendung von Gewalt die Unterstützung der Dienste der föderalen oder lokalen Polizei anfordern,

9. zur Ausführung der Bestimmungen des vorliegenden Gesetzes bei den in Artikel 9 des Gesetzes vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle erwähnten Personalmitgliedern Informationen anfordern,

10. ohne vorherige Ankündigung auf Vorlage ihrer Legitimationskarte alle Orte betreten, die die Einrichtung nutzt; zu bewohnten Räumlichkeiten haben sie nur mit vorheriger Ermächtigung des Untersuchungsrichters Zugang.

§ 2 - Im Rahmen der Beaufsichtigung wichtiger Einrichtungen werden die in § 1 erwähnten Kontrollbefugnisse nachträglich ausgeübt auf der Grundlage von Nachweisen, Hinweisen oder Informationen, wonach eine wichtige Einrichtung vorliegendes Gesetz nicht einhält.

§ 3 - Um eine Ermächtigung zum Betreten bewohnter Räumlichkeiten zu erhalten, richten die Personalmitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes einen mit Gründen versehenen Antrag an den Untersuchungsrichter. Dieser Antrag enthält mindestens:

1. die Identifizierung der bewohnten Räumlichkeiten, zu denen sie Zugang haben möchten,

2. die eventuellen Verstöße, die Gegenstand der Kontrolle sind,

3. alle Unterlagen und Auskünfte, aus denen hervorgeht, dass der Rückgriff auf dieses Mittel notwendig ist.

Der Untersuchungsrichter entscheidet binnen einer Frist von höchstens achtundvierzig Stunden nach Erhalt des Antrags. Die Entscheidung des Untersuchungsrichters ist mit Gründen versehen. Falls binnen der vorgeschriebenen Frist keine Entscheidung getroffen worden ist, wird davon ausgegangen, dass das Betreten der Räumlichkeiten verweigert wird. Der Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls die relevante

sektorspezifische Behörde beziehungsweise der zuständige sektorspezifische Inspektionsdienst kann gegen die Verweigerungsentscheidung oder das Ausbleiben einer Entscheidung innerhalb fünfzehn Tag nach Notifizierung der Entscheidung beziehungsweise Ablauf der Frist bei der Anklagekammer Beschwerde einlegen.

Besuche in bewohnten Räumlichkeiten ohne Erlaubnis des Bewohners werden zwischen fünf und einundzwanzig Uhr und von mindestens zwei Mitgliedern des Inspektionsdienstes gemeinsam vorgenommen.

§ 4 - Zu Beginn jeder Vernehmung wird der befragten Person mitgeteilt:

1. dass ihre Erklärungen als Beweismittel in Gerichtsverfahren verwendet werden können,

2. dass sie beantragen kann, dass alle ihr gestellten Fragen und von ihr gegebenen Antworten wortgetreu festgehalten werden,

3. dass sie das Recht hat zu schweigen und sich nicht selber zu belasten.

Befragte Personen dürfen Unterlagen in ihrem Besitz verwenden, ohne dass dies zum Aufschub der Vernehmung führen kann. Sie können während der Vernehmung oder danach verlangen, dass diese Unterlagen dem Vernehmungsprotokoll beigefügt werden.

Im Vernehmungsprotokoll wird der Zeitpunkt, zu dem die Vernehmung beginnt, eventuell unterbrochen und wieder aufgenommen wird und endet, genau angegeben. Darin wird die Identität der Personen, die bei der Vernehmung beziehungsweise bei einem Teil der Vernehmung mitgewirkt haben, genau angegeben.

Am Ende der Vernehmung hat die befragte Person das Recht, das Vernehmungsprotokoll zu lesen oder um Vorlesung zu bitten. Sie darf ihre Erklärungen korrigieren oder ergänzen lassen.

Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes, die eine Person befragen, informieren sie darüber, dass sie eine Kopie des Textes ihrer Vernehmung beantragen darf. Diese Kopie wird ihr kostenlos ausgehändigt.

§ 5 - Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes dürfen Einsicht in alle Datenträger und darin enthaltene Daten nehmen. Sie dürfen sich vor Ort das Datenverarbeitungssystem und die darin enthaltenen Daten, die sie für ihre Untersuchungen und Feststellungen benötigen, vorzeigen lassen und kostenlos Auszüge, Duplikate oder Kopien daraus beziehungsweise davon in einer von ihnen gewählten lesbaren und verständlichen Form anfertigen oder beantragen.

Wenn es nicht möglich ist, Kopien vor Ort anzufertigen, dürfen Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes das Datenverarbeitungssystem und die darin enthaltenen Daten gegen Empfangsbestätigung mit Beschlagnahmeverzeichnis beschlagnahmen.

§ 6 - Um die auf der Grundlage von § 5 begonnene Suche in einem Datenverarbeitungssystem oder einem Teil davon auf ein Datenverarbeitungssystem oder einen Teil davon auszuweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet, kann der Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde beziehungsweise der zuständige sektorspezifische Inspektionsdienst einen Untersuchungsrichter darum ersuchen einzugreifen.

§ 7 - Stellt der Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde beziehungsweise der zuständige sektorspezifische Inspektionsdienst im Zuge der Beaufsichtigung oder Durchsetzung fest, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 30 und 34 bis 37 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nr. 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichten sie unverzüglich die Datenschutzbehörden.

Ist die zuständige Datenschutzbehörde in einem anderen Mitgliedstaat als Belgien angesiedelt, setzt der Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde beziehungsweise der zuständige sektorspezifische Inspektionsdienst die in Belgien angesiedelte Datenschutzbehörde über die mögliche Verletzung des Schutzes personenbezogener Daten nach Absatz 1 in Kenntnis.

§ 8 - Bei der Ausübung ihrer in vorliegendem Artikel erwähnten Kontrollbefugnisse sorgen vereidigte Mitglieder der in Artikel 44 § 1 erwähnten Behörden dafür, dass die von ihnen angewandten Mittel für die Kontrolle geeignet und erforderlich sind.

Art. 49 - § 1 - Nach jeder Inspektion erstellen Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes einen Bericht und übermitteln der inspizierten Einrichtung eine Kopie davon.

§ 2 - Die nationale Cybersicherheitsbehörde und die etwaige sektorspezifische Behörde übermitteln sich gegenseitig ihre Inspektionsberichte.

Art. 50 - § 1 - Die beaufsichtigte Einrichtung gewährt den Mitgliedern des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes bei der Ausübung ihrer Aufgaben ihre volle Mitwirkung, insbesondere um sie bestmöglich über alle bestehenden Sicherheitsmaßnahmen zu informieren.

Falls erforderlich stellt die Einrichtung den Mitgliedern des Inspektionsdienstes der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde oder des zuständigen sektorspezifischen Inspektionsdienstes das erforderliche Sicherheitsmaterial zur Verfügung, damit sie die Sicherheitsvorschriften bei den Inspektionen einhalten können.

§ 2 - Die Kosten der Inspektionen gehen nicht zu Lasten der Einrichtungen.

In Abweichung von vorhergehendem Absatz kann der König für jeden Sektor oder Teilsektor durch einen im Ministerrat beratenen Erlass und nach Stellungnahme der nationalen Cybersicherheitsbehörde und gegebenenfalls der relevanten sektorspezifischen Behörde Gebühren für Inspektionsleistungen bestimmen. Der König legt die Berechnungs- und Zahlungsmodalitäten fest.

§ 3 - Die Tatsache, dass jemand die Ausführung einer Kontrolle durch Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde oder gegebenenfalls der relevanten sektorspezifischen Behörde beziehungsweise des zuständigen sektorspezifischen Inspektionsdienstes vorsätzlich verhindert oder behindert, sich weigert, die anlässlich dieser Kontrolle von ihm verlangten Informationen zu übermitteln, oder wissentlich falsche oder unvollständige Angaben macht, wird von den vereidigten Mitgliedern des Inspektionsdienstes der nationalen Cybersicherheitsbehörde oder gegebenenfalls der relevanten sektorspezifischen Behörde beziehungsweise des zuständigen sektorspezifischen Inspektionsdienstes in einem Protokoll festgehalten.

KAPITEL 2 - *Administrative Maßnahmen und Geldbußen*

Abschnitt 1 - Verfahren

Art. 51 - § 1 - Werden ein oder mehrere Verstöße gegen Anforderungen, die durch vorliegendes Gesetz, seine Ausführungserlasse oder individuelle diesbezügliche Verwaltungsbeschlüsse auferlegt werden, festgestellt, können vereidigte Mitglieder des Inspektionsdienstes der nationalen Cybersicherheitsbehörde oder gegebenenfalls der relevanten sektorspezifischen Behörde beziehungsweise des zuständigen sektorspezifischen Inspektionsdienstes dies gemäß Artikel 44 § 1 in einem Protokoll festhalten.

Mit Einverständnis der nationalen Cybersicherheitsbehörde kann die sektorspezifische Behörde einer Einrichtung die in Abschnitt 2 erwähnten administrativen Maßnahmen und Geldbußen auferlegen.

Die nationale Cybersicherheitsbehörde unterrichtet die relevante sektorspezifische Behörde, wenn sie beabsichtigt, einer Einrichtung in den Artikeln 58 und 59 erwähnte administrative Maßnahmen und Geldbußen aufzuerlegen.

Erhalten die in den Absätzen 1 und 2 erwähnten Behörden im Zuge der Beaufsichtigung Kenntnis davon, dass ein in Absatz 1 oder 2 erwähnter Verstoß einer wesentlichen oder wichtigen Einrichtung eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nr. 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichten sie unverzüglich die zuständigen Datenschutzbehörden.

§ 2 - Auf der Grundlage des in § 1 erwähnten Protokolls und gegebenenfalls der in Artikel 49 § 1 erwähnten einschlägigen Berichte kann die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde einen Entscheidungsentwurf erstellen, der mindestens die Referenzangaben des Protokolls, durch das der Verstoß festgestellt wird und in dem die Taten aufgeführt werden, die der Einleitung des Verfahrens zugrunde liegen, eine oder mehrere der in Artikel 58 und/oder 59 erwähnten administrativen Maßnahmen oder Geldbußen, die in Betracht gezogen werden, und die Frist, innerhalb deren die betreffende Einrichtung die administrativen Maßnahmen umsetzen müsste, enthält.

Die in Absatz 1 erwähnte Frist wird unter Berücksichtigung der Betriebsbedingungen der Einrichtung und der zu ergreifenden Maßnahmen bestimmt.

§ 3 - Die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde übermittelt der betreffenden Einrichtung den in § 2 erwähnten Entscheidungsentwurf und legt dabei ausführlich die Gründe für die geplanten administrativen Maßnahmen und/oder Geldbußen dar und weist sie auf ihr Recht hin, innerhalb dreißig Tagen ab Erhalt dieser Information schriftlich ihre Verteidigungsmittel einzureichen oder um Anhörung zu ersuchen. Es wird davon ausgegangen, dass der Zuwiderhandelnde die Information am sechsten Tag nach Versendung des vorerwähnten Entscheidungsentwurfs erhalten hat.

In Abweichung von Absatz 1 wird der Entscheidungsentwurf der betreffenden Einrichtung in begründeten Ausnahmefällen nicht vorab übermittelt, wenn dies ein sofortiges Eingreifen zur Verhinderung oder Bewältigung eines Vorfalls behindern würde.

§ 4 - Nachdem die betreffende Einrichtung ihre Verteidigungsmittel geltend machen konnte, nach Ablauf der in § 3 Absatz 1 erwähnten Frist oder in dem in § 3 Absatz 2 erwähnten Fall behält die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde den in § 2 Absatz 1 erwähnten Entscheidungsentwurf bei, ändert ihn oder verzichtet darauf, wobei sie der Einrichtungskategorie, zu der die betreffende Einrichtung gehört, deren Verteidigungsmitteln und den in Artikel 54 erwähnten Elementen Rechnung trägt.

Art. 52 - § 1 - Erweisen sich die gemäß Artikel 58 Nr. 1 bis 4 und 6 ergriffenen Durchsetzungsmaßnahmen als unwirksam, kann die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde eine Frist festsetzen, innerhalb deren die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder ihre Anforderungen zu erfüllen.

§ 2 - Kommt eine wesentliche Einrichtung den in der Entscheidung nach Artikel 51 § 4 enthaltenen Maßnahmen nicht nach, hält die Behörde, die diese Entscheidung getroffen hat, den Sachverhalt in einem Protokoll fest.

§ 3 - Auf der Grundlage des in § 2 erwähnten Protokolls erstellt die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde einen Entscheidungsentwurf, der mindestens eine oder mehrere der in den Artikeln 59 und/oder 60 erwähnten administrativen Maßnahmen oder Geldbußen enthält, die in Betracht gezogen werden.

§ 4 - Die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde übermittelt der betreffenden Einrichtung den in § 3 erwähnten Entscheidungsentwurf und legt dabei ausführlich die Gründe für die geplanten administrativen Maßnahmen und/oder Geldbußen dar und weist sie auf ihr Recht hin, innerhalb dreißig Tagen ab Erhalt dieser Information schriftlich ihre Verteidigungsmittel einzureichen oder um Anhörung zu ersuchen. Es wird davon ausgegangen, dass der Zuwiderhandelnde die Information am sechsten Tag nach Versendung des vorerwähnten Entscheidungsentwurfs erhalten hat.

In Abweichung von Absatz 1 wird der Entscheidungsentwurf der betreffenden Einrichtung in begründeten Ausnahmefällen nicht vorab übermittelt, wenn dies ein sofortiges Eingreifen zur Verhinderung oder Bewältigung eines Vorfalls behindern würde.

§ 5 - Nachdem die betreffende Einrichtung ihre Verteidigungsmittel geltend machen konnte, nach Ablauf der in § 4 Absatz 1 erwähnten Frist oder in dem in § 4 Absatz 2 erwähnten Fall behält die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde den in § 3 erwähnten Entscheidungsentwurf bei, ändert ihn oder verzichtet darauf, wobei sie den Verteidigungsmitteln der betreffenden Einrichtung und den in Artikel 54 erwähnten Elementen Rechnung trägt.

Art. 53 - Die von den vereidigten Mitgliedern des Inspektionsdienstes erstellten Protokolle haben Beweiskraft bis zum Gegenbeweis.

Art. 54 - § 1 - Bei der Ergreifung von Durchsetzungsmaßnahmen im Rahmen der in den Artikeln 51 und 52 erwähnten Verfahren hält die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde die Verteidigungsrechte ein und trägt den Umständen des Einzelfalls Rechnung und berücksichtigt dabei zumindest Folgendes:

1. in den Artikeln 9 und 10 erwähnte Kategorie, zu der die betreffende Einrichtung gehört,

2. Schwere des Verstoßes und Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, wobei unter anderem Folgendes immer als schwerer Verstoß anzusehen ist:

a) wiederholte Verstöße,

b) unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen,

c) Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden,

d) Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes vom Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls von der relevanten sektorspezifischen Behörde beziehungsweise dem zuständigen sektorspezifischen Inspektionsdienst angeordnet wurden,

e) Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementmaßnahmen im Bereich der Cybersicherheit oder Berichtspflichten gemäß Titel 3,

3. Dauer des Verstoßes,

4. einschlägige frühere Verstöße der betreffenden Einrichtung,

5. verursachter materieller oder immaterieller Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und Zahl der betroffenen Nutzer,

6. etwaiger Vorsatz oder etwaige Fahrlässigkeit des Urhebers des Verstoßes,

7. von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens,

8. Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren,

9. Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit dem Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls mit der relevanten sektorspezifischen Behörde beziehungsweise dem zuständigen sektorspezifischen Inspektionsdienst.

§ 2 - Verhängen Datenschutzbehörden gemäß Artikel 58 Absatz 2 Buchstabe i) der Verordnung (EU) 2016/679 eine administrative Geldbuße, verhängt die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde für einen Verstoß, der sich aus demselben Verhalten ergibt wie der Verstoß, der Gegenstand der administrativen Geldbuße nach Artikel 58 Absatz 2 Buchstabe i) der erwähnten Verordnung war, keine administrative Geldbuße.

Art. 55 - § 1 - In den Artikeln 51 und 52 erwähnte Entscheidungen werden den Zuwiderhandelnden per Einschreibesendung notifiziert.

§ 2 - Durch eine Entscheidung gemäß Artikel 51 oder 52 auferlegte administrative Geldbußen sind innerhalb sechzig Tagen nach Erhalt der in § 1 erwähnten Einschreibesendung zu entrichten.

Diese Frist kann je nach Höhe der administrativen Geldbuße verlängert werden.

Die in Absatz 1 erwähnte Frist beginnt spätestens sechs Tage nach Versand der in § 1 erwähnten Einschreibesendung.

§ 3 - Wird in einer Entscheidung gemäß Artikel 51 oder 52 eine andere administrative Maßnahme als eine administrative Geldbuße vorgesehen, wird in dieser Entscheidung die Frist angegeben, innerhalb deren die Maßnahme durchzuführen ist.

§ 4 - Die nationale Cybersicherheitsbehörde und gegebenenfalls die relevante sektorspezifische Behörde teilen sich ihre in Artikel 51 oder 52 erwähnten Entscheidungen gegenseitig mit.

Art. 56 - § 1 - Versäumt es die betreffende Einrichtung, die administrative Geldbuße innerhalb der vorgegebenen Frist zu bezahlen, ist die Entscheidung zur Auferlegung einer administrativen Geldbuße vollstreckbar und kann die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde einen Zwangsbefehl erlassen.

Zwangsbefehle werden von einem gesetzlichen Vertreter der nationalen Cybersicherheitsbehörde oder gegebenenfalls der relevanten sektorspezifischen Behörde oder einem zu diesem Zweck ermächtigten Personalmitglied erlassen.

§ 2 - Die Zustellung des Zwangsbefehls an den Zuwiderhandelnden erfolgt per Gerichtsvollzieherurkunde. Die Zustellung beinhaltet einen Zahlungsbefehl, in dem unter Androhung der Vollstreckung durch Pfändung dazu aufgefordert wird, binnen achtundvierzig Stunden zu zahlen, und eine buchhalterische Rechtfertigung für die eingeforderten Beträge und eine Kopie der Vollstreckbarerklärung.

§ 3 - Der Zuwiderhandelnde kann vor dem Pfändungsrichter gegen den Zwangsbefehl Einspruch erheben.

Der Einspruch muss zur Vermeidung der Nichtigkeit mit Gründen versehen sein. Er wird binnen fünfzehn Tagen nach Zustellung des Zwangsbefehls durch eine Ladung an die nationale Cybersicherheitsbehörde oder gegebenenfalls an die relevante sektorspezifische Behörde per Gerichtsvollzieherurkunde erhoben.

Die Bestimmungen von Teil I Kapitel VIII des Gerichtsgesetzbuches einschließlich der in Artikel 50 Absatz 2 und Artikel 55 dieses Gesetzbuches vorgesehenen Verlängerungen finden Anwendung auf diese Frist.

Die Einlegung des Einspruchs gegen den Zwangsbefehl setzt die Vollstreckung des Zwangsbefehls und die Verjährung der im Zwangsbefehl enthaltenen Forderung aus, bis über die Begründetheit des Einspruchs befunden worden ist. Zu einem früheren Zeitpunkt bereits durchgeführten Pfändungen behalten ihre sichernde Wirkung.

§ 4 - Die nationale Cybersicherheitsbehörde oder gegebenenfalls die relevante sektorspezifische Behörde darf unter Anwendung der in Teil V des Gerichtsgesetzbuches vorgesehenen Vollstreckungsmittel eine Sicherungspfändung vornehmen lassen und den Zwangsbefehl vollstrecken.

Teilzahlungen infolge der Zustellung eines Zwangsbefehls verhindern nicht die Fortsetzung von Verfolgungen.

§ 5 - Kosten für die Zustellung des Zwangsbefehls und Kosten für die Vollstreckung oder die Sicherungsmaßnahmen gehen zu Lasten des Zuwiderhandelnden.

Sie werden nach den Regeln festgelegt, die für Handlungen der Gerichtsvollzieher in Zivil- und Handelssachen gelten.

Art. 57 - Taten verjähren in drei Jahren ab ihrer Begehung. Die Verjährung wird nur durch Untersuchungs- oder Verfolgungshandlungen eines Inspektionsdienstes unterbrochen. Mit diesen Handlungen beginnt eine neue Frist gleicher Dauer, auch gegenüber Personen, die nicht davon betroffen sind.

Administrative Maßnahmen oder Geldbußen verjähren in fünf Jahren ab dem Datum, an dem sie vollstreckt werden müssen. Die Verjährungsfrist wird im Falle einer Beschwerde gegen die administrative Entscheidung ausgesetzt.

Abschnitt 2 - Administrative Maßnahmen und Geldbußen

Art. 58 - Auf der Grundlage von Artikel 51 können gegen Einrichtungen folgende administrative Maßnahmen verhängt werden:

1. Warnungen über Verstöße gegen vorliegendes Gesetz durch die betreffenden Einrichtungen herausgeben,

2. verbindliche Anweisungen oder Anordnungen erlassen, um die betreffenden Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen vorliegendes Gesetz zu beheben,

3. die betreffenden Einrichtungen anweisen, das gegen vorliegendes Gesetz verstoßende Verhalten einzustellen und von Wiederholungen abzusehen,

4. die betreffenden Einrichtungen anweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Titel 3 im Einklang stehen, beziehungsweise die im selben Titel festgelegten Berichtspflichten zu erfüllen,

5. die betreffenden Einrichtungen anweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können,

6. die betreffenden Einrichtungen anweisen, im Rahmen einer Sicherheitsprüfung formulierte Empfehlungen innerhalb einer angemessenen Frist umzusetzen,

7. die betreffenden Einrichtungen anweisen, Aspekte der Verstöße gegen vorliegendes Gesetz entsprechend bestimmten Vorgaben öffentlich bekannt zu machen,

8. wenn die betreffende Einrichtung eine wesentliche Einrichtung ist, für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten benennen, der die Einhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und der Berichtspflichten wie in Titel 3 erwähnt durch die betreffenden Einrichtungen überwacht.

Wenn die betreffende Einrichtung eine wesentliche Einrichtung ist, betreffen die in Absatz 1 Nr. 2 erwähnten verbindlichen Anweisungen auch Maßnahmen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind, und Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung.

Art. 59 - Auf der Grundlage von Artikel 51 oder 52 können gegen Einrichtungen folgende administrative Geldbußen verhängt werden:

1. Mit einer Geldbuße von 500 bis zu 125.000 EUR wird belegt, wer den in Artikel 12 erwähnten Berichtspflichten nicht nachkommt.

2. Mit einer Geldbuße von 500 bis zu 200.000 EUR wird eine Einrichtung belegt, die einer für Rechnung der Einrichtung handelnden Person nachteilige Folgen verursacht, weil diese Person in gutem Glauben und im Rahmen ihrer Aufgaben die sich aus vorliegendem Gesetz ergebenden Verpflichtungen erfüllt.

3. Unbeschadet des Artikels 48 § 4 Absatz 1 Nr. 3 wird mit einer Geldbuße von 500 bis zu 200.000 EUR belegt, wer den in vorliegendem Titel erwähnten Kontrollpflichten nicht nachkommt.

4. Mit einer Geldbuße von 500 bis 7.000.000 EUR oder 1,4 Prozent des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr des Unternehmens, dem die wichtige Einrichtung angehört, wobei der höhere Betrag maßgeblich ist, wird eine wichtige Einrichtung belegt, die den in Titel 3 erwähnten Verpflichtungen hinsichtlich der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und/oder den Berichtspflichten nicht nachkommt.

5. Mit einer Geldbuße von 500 bis 10.000.000 EUR oder 2 Prozent des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr des Unternehmens, dem die wesentliche Einheit angehört, wobei der höhere Betrag maßgeblich ist, wird eine wesentliche Einrichtung belegt, die den in Titel 3 erwähnten Verpflichtungen hinsichtlich der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und/oder den Berichtspflichten nicht nachkommt.

Bei Rückfälligkeit aufgrund der gleichen Verstöße binnen einer Frist von drei Jahren wird die administrative Geldbuße verdoppelt.

Das Zusammentreffen mehrerer Verstöße kann zu einer einzigen administrativen Geldbuße führen, die im Verhältnis zur Schwere der Gesamtheit der Taten steht.

Art. 60 - Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, können gegen wesentliche Einrichtungen auf der Grundlage von Artikel 52 folgende administrative Maßnahmen verhängt werden:

1. die nationale Cybersicherheitsbehörde auffordern, die Zertifizierung oder Genehmigung für einen Teil oder alle von der wesentlichen Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen,

2. natürlichen Personen, die auf Geschäftsführungs- beziehungsweise Vorstandsebene oder Ebene des gesetzlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind, vorübergehend untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen.

Die in Absatz 1 erwähnten vorübergehenden Aussetzungen oder Verbote werden nur so lange angewandt, bis die betreffende Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Durchsetzungsmaßnahmen verhängt wurden, zu erfüllen.

Art. 61 - Natürliche Personen, die für eine wesentliche oder wichtige Einrichtung verantwortlich sind oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als gesetzliche Vertreter der wesentlichen oder wichtigen Einrichtung handeln, sind befugt zu gewährleisten, dass die Einrichtung vorliegendes Gesetz erfüllt. Diese Personen haften für Verstöße gegen ihre Pflicht, die Einhaltung des vorliegenden Gesetzes zu gewährleisten.

Vorliegender Artikel lässt die für öffentliche Einrichtungen geltenden Haftungsregelungen und die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

TITEL 5 - *Besondere Bestimmungen für den Bereich der öffentlichen Verwaltung*

Art. 62 - Die in den Artikeln 59 und 60 erwähnten administrativen Maßnahmen und Geldbußen gelten nicht für Einrichtungen, die dem Bereich der öffentlichen Verwaltung angehören.

Art. 63 - § 1 - Der König ist ermächtigt, eine Behörde als Konformitätsbewertungsstelle aller oder eines Teils der Einrichtungen der öffentlichen Verwaltung zu benennen.

§ 2 - Die in § 1 erwähnte Behörde wird gemäß den vom König festgelegten Modalitäten von der nationalen Cybersicherheitsbehörde zugelassen, um die in Artikel 39 Absatz 1 Nr. 1 erwähnte regelmäßige Konformitätsbewertung durchzuführen.

Die in Absatz 1 erwähnte Zulassung bezieht sich auf einen oder mehrere der in Artikel 39 erwähnten Referenzrahmen.

Art. 64 - Der Inspektionsdienst der nationalen Cybersicherheitsbehörde oder gegebenenfalls der vom König für den Bereich der öffentlichen Verwaltung benannte sektorspezifische Inspektionsdienst übt seine Aufsichtsaufgaben in operativer Unabhängigkeit gegenüber den beaufsichtigten Einrichtungen der öffentlichen Verwaltung aus.

Art. 65 - Artikel 47 ist auf den in Artikel 64 erwähnten Inspektionsdienst anwendbar.

TITEL 6 - ***Verarbeitung personenbezogener Daten***

KAPITEL 1 - *Grundsätze der Datenverarbeitung*

Art. 66 - Für vorliegenden Titel gelten die Begriffsbestimmungen der Verordnung (EU) 2016/679.

Art. 67 - Die Verarbeitung personenbezogener Daten erfolgt zu folgenden Zwecken:

1. Verbesserung der Cybersicherheit durch Anstreben eines höheren Schutzniveaus für Netz- und Informationssysteme, Stärkung von Präventions- und Sicherheitsmaßnahmen, Verhinderung von Sicherheitsvorfällen und Abwehr von Cyberbedrohungen,

2. Wahrnehmung der Aufgaben der nationalen Cybersicherheitsbehörde, insbesondere Identifizierung von Einrichtungen, Information und Sensibilisierung der Nutzer von Informations- und Kommunikationssystemen, Gewährung von Zuschüssen und internationale Zusammenarbeit zwischen der nationalen Cybersicherheitsbehörde, den zuständigen Behörden der anderen Mitgliedstaaten, den internationalen Foren für Cybersicherheit, der ENISA und der Europäischen Kommission,

3. Bewältigung von Cyberkrisen und Cybersicherheitsvorfällen,

4. Erfüllung der Aufgaben des nationalen CSIRT gemäß folgenden Artikeln:

a) 19 § 1,

b) 21 § 2 Absatz 2 Nr. 1 bis 3,

c) 22 §§ 2 bis 6,

d) 37 §§ 1 bis 3 und § 5,

5. Zusammenarbeit, insbesondere Informationsaustausch zwischen der nationalen Cybersicherheitsbehörde, gegebenenfalls den sektorspezifischen Behörden, dem NCCN, den im Rahmen des [Gesetzes vom 19. Dezember 2025] zuständigen Behörden und den in Artikel 25 § 2 erwähnten Behörden im Rahmen der Ausführung des vorliegenden Gesetzes und des [Gesetzes vom 19. Dezember 2025],

6. Zusammenarbeit zwischen den wesentlichen und wichtigen Einrichtungen und den in Titel 2 Kapitel 1 erwähnten Behörden,

7. Informationsaustausch zwischen den in Artikel 25 § 5 erwähnten Behörden,

8. Kontinuität der von wichtigen oder wesentlichen Einrichtungen erbrachten Dienstleistungen,

9. Meldung von Sicherheitsvorfällen und Beinahe-Vorfällen,

10. Kontrolle und Beaufsichtigung der wesentlichen und wichtigen Einrichtungen und Vorbereitung, Organisation, Durchführung und Nachverfolgung von administrativen Maßnahmen und Geldbußen.

[Art. 67 einziger Absatz Nr. 5 abgeändert durch Art. 75 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 68 - Folgende Kategorien von personenbezogenen Daten werden von den für die Verarbeitung Verantwortlichen verarbeitet:

1. für den in Artikel 67 Nr. 1 erwähnten Zweck: Identifizierungs-, Verbindungs-, Standort- und elektronische Kommunikationsdaten - im Sinne von Artikel 2 Nr. 91 des Gesetzes vom 13. Juni 2005 - der Personen, die von den in Artikel 67 Nr. 1 erwähnten Aufgaben der Verbesserung der Cybersicherheit, der Stärkung von Präventions- und Sicherheitsmaßnahmen, der Verhinderung von Sicherheitsvorfällen und der Abwehr von Cyberbedrohungen betroffen sind,

2. für den in Artikel 67 Nr. 2 erwähnten Zweck: Identifizierungs-, Verbindungs-, Standort- und elektronische Kommunikationsdaten - im Sinne von Artikel 2 Nr. 91 des Gesetzes vom 13. Juni 2005 - der Personen, die von der Wahrnehmung der Aufgaben der nationalen Cybersicherheitsbehörde betroffen sind,

3. für den in Artikel 67 Nr. 3 erwähnten Zweck: Identifizierungs-, Verbindungs-, Standort- und elektronische Kommunikationsdaten - im Sinne von Artikel 2 Nr. 91 des Gesetzes vom 13. Juni 2005 - der Personen, die von Cyberkrisen und Cybersicherheitsvorfällen betroffen sind,

4. für den in Artikel 67 Nr. 4 erwähnten Zweck: Identifizierungs-, Verbindungs-, Standort- und elektronische Kommunikationsdaten - im Sinne von Artikel 2 Nr. 91 des Gesetzes vom 13. Juni 2005 - und Metadaten der elektronischen Kommunikation - im Sinne von Artikel 2 Nr. 93 des vorerwähnten Gesetzes vom 13. Juni 2025 - der Personen, die von der Erfüllung der Aufgaben des nationalen CSIRT betroffen sind,

5. für den in Artikel 67 Nr. 5 erwähnten Zweck: Identifizierungsdaten der Personen, die von der Zusammenarbeit im Rahmen des [Gesetzes vom 19. Dezember 2025] betroffen sind,

6. für den in Artikel 67 Nr. 6 erwähnten Zweck: Identifizierungsdaten der Personen, die von der Zusammenarbeit betroffen sind,

7. für den in Artikel 67 Nr. 7 erwähnten Zweck: Identifizierungsdaten der Personen, die vom Informationsaustausch betroffen sind,

8. für den in Artikel 67 Nr. 8 erwähnten Zweck: Identifizierungsdaten der Personen, die von der Gewährleistung der Kontinuität der Dienstleistungen betroffen sind,

9. für den in Artikel 67 Nr. 9 erwähnten Zweck: Identifizierungs-, Verbindungs-, Standort- und elektronische Kommunikationsdaten - im Sinne von Artikel 2 Nr. 91 des Gesetzes vom 13. Juni 2005 - der Personen, die von dem Meldungsvorgang betroffen sind,

10. für den in Artikel 67 Nr. 10 erwähnten Zweck: personenbezogene Daten der von diesen Kontrollen, dieser Beaufsichtigung oder diesen Sanktionen betroffenen Personen, die für die Ausübung der Kontroll-, Aufsichts- und Sanktionsaufgaben erforderlich und relevant sind.

[Art. 68 einziger Absatz Nr. 5 abgeändert durch Art. 76 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 69 - Personenbezogene Daten folgender Kategorien von Personen können verarbeitet werden:

1. Personen, die unmittelbar an den Aufgaben beteiligt sind, die der nationalen Cybersicherheitsbehörde gemäß Titel 2 übertragen worden sind,

2. Personen, die den Verpflichtungen unterliegen, die den wesentlichen und wichtigen Einrichtungen gemäß Titel 3 obliegen,

3. Personen, die an einem Sicherheitsvorfall beteiligt sind,

4. Personen, die unmittelbar an den in Titel 4 erwähnten Aufsichts-, Kontroll- und Sanktionsmaßnahmen beteiligt sind.

Art. 70 - Folgende Einrichtungen sind für die von ihnen zur Erreichung der in Artikel 67 erwähnten Zwecke durchgeführten Verarbeitungen verantwortlich:

1. die nationale Cybersicherheitsbehörde,

2. das NCCN,

3. gegebenenfalls die relevante sektorspezifische Behörde,

4. gegebenenfalls der sektorspezifische Inspektionsdienst,

5. wesentliche und wichtige Einrichtungen,

6. Einrichtungen, die Domänennamen-Registrierungsdienste erbringen,

7. in Artikel 23 § 1 Nr. 6 erwähnte Behörden.

KAPITEL 2 - *Speicherfrist*

Art. 71 - Personenbezogene Daten, die im Rahmen der in vorliegendem Gesetz erwähnten Verarbeitungen zur Erfüllung der in Artikel 67 vorgesehenen Zwecke verarbeitet werden, werden unbeschadet etwaiger Rechtsbehelfe von dem für die Verarbeitung Verantwortlichen während fünf Jahren nach Abschluss der letzten Verarbeitung und höchstens während zehn Jahren nach der ersten Verarbeitung aufbewahrt.

KAPITEL 3 - *Beschränkung der Rechte der betroffenen Personen*

Art. 72 - § 1 - In Anwendung von Artikel 23 Absatz 1 Buchstabe a) bis e) und h) der Verordnung (EU) 2016/679 werden bestimmte in dieser Verordnung vorgesehene Pflichten und Rechte gemäß den Bestimmungen des vorliegenden Kapitels beschränkt oder ausgeschlossen. Diese Beschränkungen beziehungsweise Ausschlüsse dürfen den Wesensgehalt der Grundrechte und -freiheiten nicht beeinträchtigen und müssen in dem für den verfolgten Zweck unbedingt erforderlichen Umfang angewandt werden.

§ 2 - Für den in Artikel 67 Nr. 10 erwähnten Zweck finden die Artikel 12 bis 16, 18 und 19 der erwähnten Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten durch eine in Artikel 15 erwähnte Behörde, sofern die Ausübung der in diesen Artikeln verankerten Rechte die Erfordernisse der Kontrolle, der Beaufsichtigung oder der Verrichtungen zu deren Vorbereitung beeinträchtigen würde.

§ 3 - Die Befreiung gilt für die in Artikel 68 Nr. 10 erwähnten Kategorien personenbezogener Daten. Diese Befreiung gilt ebenfalls für vorbereitende Verrichtungen oder Verfahren im Hinblick auf die eventuelle Anwendung einer Verwaltungsstrafe.

§ 4 - Die Befreiung gilt nur während des Zeitraums, in dem die betreffende Person kontrolliert oder beaufsichtigt wird oder ihr gegenüber Verrichtungen zur Vorbereitung der Kontrolle oder Beaufsichtigung vorgenommen werden, soweit die Ausübung der Rechte, die Gegenstand der in vorliegendem Artikel erwähnten Befreiung sind, die Erfordernisse der Kontrolle, der Beaufsichtigung oder der Verrichtungen zu deren Vorbereitung beeinträchtigen würde, und gilt in jedem Fall nur bis zu einem Jahr nach Beginn einer Kontrolle, einer Beaufsichtigung oder der Verrichtungen zu deren Vorbereitung.

Die Dauer der in Absatz 1 erwähnten vorbereitenden Verrichtungen, während deren die in § 2 erwähnten Artikel keine Anwendung finden, darf ein Jahr ab Eingang eines Antrags in Bezug auf die Anwendung eines in diesen Artikeln verankerten Rechts nicht überschreiten.

§ 5 - Für die Verarbeitung Verantwortliche, die nicht alle Bestimmungen des vorliegenden Titels und insbesondere von Artikel 73 einhalten, können die Befreiung nicht in Anspruch nehmen.

Art. 73 - § 1 - Der betreffende für die Verarbeitung Verantwortliche gewährt der betroffenen Person in begrenztem Umfang Zugang zu Informationen über die Verarbeitung ihrer personenbezogenen Daten, sofern diese Mitteilung die Umsetzung der Ziele des vorliegenden Gesetzes nicht gefährdet. Dabei wird sichergestellt, dass die betroffene Person nicht weiß, ob gegen sie ermittelt wird oder nicht, und sie kann in keinem Fall personenbezogene Daten berichtigen, löschen, einschränken, mitteilen, an einen Dritten übertragen oder jede Form der Verarbeitung dieser Daten, die im oben bestimmten Rahmen erforderlich ist, einstellen.

§ 2 - Die Verweigerung oder Einschränkung der Rechte, die durch die in Artikel 72 § 2 erwähnten Artikel vorgesehen sind, muss aufgehoben werden:

1. für Maßnahmen, die durch die Pflichten in Bezug auf die Meldung von Sicherheitsvorfällen gerechtfertigt sind, wenn die Bearbeitung eines Sicherheitsvorfalls durch die in den Artikeln 34 und 38 erwähnten Behörden beendet ist,

2. für Maßnahmen, die durch die Pflichten aufgrund von Titel 4 gerechtfertigt sind, wenn die Kontrolle, die Beaufsichtigung oder die Verrichtungen zu deren Vorbereitung durch den Inspektionsdienst beendet sind, und während des Zeitraums, in dem gegebenenfalls die sektorspezifische Behörde Dokumente des Inspektionsdienstes im Hinblick auf eine Verfolgung bearbeitet,

3. spätestens ein Jahr nach Eingang des Antrags in Anwendung der in Artikel 72 § 2 erwähnten Artikel, es sei denn, eine Kontrolle beziehungsweise Beaufsichtigung läuft gerade.

§ 3 - Der betreffende für die Verarbeitung Verantwortliche hebt die Verweigerung oder Einschränkung der Rechte, die durch die in Artikel 72 § 2 erwähnten Artikel vorgesehen sind, ebenfalls auf, sobald eine solche Maßnahme für einen der in Artikel 67 erwähnten Zwecke nicht mehr erforderlich ist.

§ 4 - In allen Fällen, in denen die Paragraphen 2 und 3 Anwendung finden, unterrichtet der Datenschutzbeauftragte die betroffene(n) Person(en) schriftlich über die Aufhebung der Verweigerung beziehungsweise Einschränkung.

KAPITEL 4 - *Einschränkungen der Pflichten in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten*

Art. 74 - Der betreffende für die Verarbeitung Verantwortliche ist vorbehaltlich der Erlaubnis der nationalen Cybersicherheitsbehörde davon befreit, eine oder mehrere bestimmte betroffene Personen im Sinne von Artikel 34 der Verordnung (EU) 2016/679 über eine Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, sofern und soweit eine solche individuelle Benachrichtigung die Erfüllung der in Artikel 72 § 2 erwähnten Zwecke zu gefährden droht.

TITEL 7 - *Schlussbestimmungen*

KAPITEL 1 - *Übergangsbestimmung*

[*Abschnitt 1* - Übergangsbestimmung]

[Unterteilung Abschnitt 1 eingefügt durch Art. 66 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 75 - Der König legt die Fristen fest, innerhalb deren die wesentlichen Einrichtungen ihre ersten regelmäßigen Konformitätsbewertungen gemäß Artikel 39 durchführen.

[*Abschnitt 2* - Auslegungsbestimmung zu den Artikeln 8 und 38 und zu den Bestimmungen des Titels 2

[Abschnitt 2 mit Art. 75/1 eingefügt durch Art. 67 des G. vom 19. Dezember 2025 (B.S. vom 19. Januar 2026)]

Art. 75/1 - Die Artikel 8 und 38 und die Bestimmungen des Titels 2 sind so auszulegen, dass sie für natürliche oder juristische Personen gelten, die in Belgien anwesend oder ansässig sind.]

KAPITEL 2 - *Abänderungsbestimmungen*

Abschnitt 1 - Abänderungen des Gesetzes vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle

Art. 76 - In Artikel 1 des Gesetzes vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle, zuletzt abgeändert durch das Gesetz vom 7. Februar 2024, werden die Wörter ″- Gesetz vom 7. April 2019: Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit,″ durch die Wörter ″- NIS-2-Gesetz: Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit,″ ersetzt.

Art. 77 - In Kapitel III Abschnitt 1 desselben Gesetzes wird Artikel 15*ter*, eingefügt durch das Gesetz vom 7. April 2019, wie folgt ersetzt:

″Art. 15*ter* - Die Agentur wird als sektorspezifischer Inspektionsdienst im Sinne des NIS-2-Gesetzes für den Energiesektor benannt in Bezug auf zusätzliche Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die auf die zur Übertragung von Elektrizität verwendeten Komponenten einer kerntechnischen Anlage für industrielle Stromerzeugung anwendbar sind.

Nach Stellungnahme der Agentur legt der König die praktischen Modalitäten der Inspektionen fest.″

Abschnitt 2 - Abänderungen des Gesetzes vom 22. Februar 1998 zur Festlegung des Grundlagenstatuts der Belgischen Nationalbank

Art. 78 - 80 - *[Abänderungen des Gesetzes vom 22. Februar 1998 zur Festlegung des Grundlagenstatuts der Belgischen Nationalbank]*

Abschnitt 3 - Abänderung des Gesetzes vom 2. August 2002 über die Aufsicht über den Finanzsektor und die Finanzdienstleistungen

Art. 81 - In Artikel 75 § 1 Nr. 15 des Gesetzes vom 2. August 2002 über die Aufsicht über den Finanzsektor und die Finanzdienstleistungen, zuletzt abgeändert durch das Gesetz vom 20. Juli 2020, werden die Wörter ″Artikel 7 des Gesetzes vom 7. April 02019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit″ durch die Wörter ″Artikel 15 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit″ ersetzt.

Abschnitt 4 - Abänderungen des Gesetzes vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors

Art. 82 - 83 - *[Abänderungen des Gesetzes vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors]*

Abschnitt 5 - Abänderungen des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation

Art. 84 - Artikel 1 Absatz 2 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, zuletzt abgeändert durch das Gesetz vom 21. Dezember 2021, wird durch eine Nr. 7 mit folgendem Wortlaut ergänzt:

″7. 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.″

Art. 85 - Artikel 2 desselben Gesetzes, zuletzt abgeändert durch das Gesetz vom 20. Juli 2022, wird wie folgt abgeändert:

1. Nummer 48/1 wird wie folgt ersetzt:

″48/1. ″Namenregister der Domäne oberster Stufe″ oder ″TLD-Namenregister″: eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain - TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden,″.

2. Eine Nr. 48/3 mit folgendem Wortlaut wird eingefügt:

″48/3. ″Einrichtung, die Domänennamen-Registrierungsdienste erbringt″: einen Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa einen Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten,″.

3. Die Nummern 62/2 und 62/3 werden wie folgt ersetzt:

″62/2. ″Netz- und Informationssystem″:

a) ein elektronisches Kommunikationsnetz im Sinne von Nr. 3,

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, einschließlich der digitalen, elektronischen oder mechanischen Komponenten dieser Geräte, insbesondere für die Automatisierung des Betriebsablaufs, die Fernsteuerung oder die Erfassung von Echtzeit-Betriebsdaten, oder

c) digitale Daten, die von den in den Buchstaben *a)* und *b)* erwähnten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden,

62/3. ″Sicherheit von Netz- und Informationssystemen″: die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden beziehungsweise zugänglich sind, beeinträchtigen können,″.

4. Nummern 62/4 bis 62/8 mit folgendem Wortlaut werden eingefügt:

"62/4. "Sicherheitsvorfall": ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden beziehungsweise zugänglich sind, beeinträchtigt,

62/5. "Cybersicherheit": die Cybersicherheit im Sinne von Artikel 2 Nr. 1 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit),

62/6. "Bewältigung von Sicherheitsvorfällen": alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon,

62/7. "Cyberbedrohung": eine Cyberbedrohung im Sinne von Artikel 2 Nr. 8 der Verordnung (EU) 2019/881,

62/8. "erheblicher Cyberbedrohung": eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht,".

5. Der Artikel wird durch eine Nr. 94 mit folgendem Wortlaut ergänzt:

"94. "Anbieter digitaler Infrastruktur": eine Einrichtung aus dem Sektor der digitalen Infrastruktur mit Ausnahme von Vertrauensdiensteanbietern im Sinne von Artikel 8 Nr. 24 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit."

Art. 86 - In Artikel 6 Nr. 4 desselben Gesetzes, ersetzt durch das Gesetz vom 21. Dezember 2021, werden die Wörter "Netze und Dienste" durch die Wörter "Netz- und Informationssysteme" ersetzt.

Art. 87 - In Artikel 105 § 1 Nr. 2 desselben Gesetzes, ersetzt durch das Gesetz vom 17. Februar 2022, werden die Wörter "oder als Betreiber wesentlicher Dienste im Sinne des Gesetzes vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit" aufgehoben.

Art. 88 - Artikel 107/2 desselben Gesetzes, eingefügt durch das Gesetz vom 21. Dezember 2021, wird wie folgt ersetzt:

"Art. 107/2 - § 1 - Unbeschadet der Bestimmungen des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit analysieren Anbieter digitaler Infrastruktur die Risiken in Bezug auf die Sicherheit ihrer Netz- und Informationssysteme. Das Institut kann die Modalitäten dieser Risikoanalyse festlegen.

§ 2 - Unbeschadet der 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, nachstehend "DSGVO" genannt, und des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten, nachstehend "Gesetz vom 30. Juli 2018" genannt, sorgen Betreiber zumindest dafür, dass:

1. sichergestellt ist, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten, die sie verarbeiten,

2. gespeicherte oder übermittelte personenbezogene Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe geschützt sind und

3. die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten sichergestellt ist.

Das Institut ist ermächtigt, die von diesen Betreibern getroffenen Maßnahmen zu prüfen und Empfehlungen zu bewährten Verfahren im Zusammenhang mit dem mit Hilfe dieser Maßnahmen zu erreichenden Sicherheitsniveau abzugeben.

§ 3 - Betreiber treffen alle notwendigen Maßnahmen, Vorbeugungsmaßnahmen einbegriffen, um die möglichst vollständige Verfügbarkeit von Sprachkommunikationsdiensten und Internetzugangsdiensten bei außerordentlichen Netzausfällen oder in Fällen höherer Gewalt sicherzustellen.

Der König kann auf Vorschlag des Instituts oder aus eigener Initiative nach Stellungnahme des Instituts diese Maßnahmen näher bestimmen.

§ 4 - Betreiber bieten ihren Teilnehmern unter Berücksichtigung der technischen Möglichkeiten kostenlos angemessene sichere Dienste an, die Endnutzern erlauben, den Empfang unerbetener elektronischer Nachrichten aller Art zu vermeiden."

Art. 89 - Artikel 107/3 desselben Gesetzes, eingefügt durch das Gesetz vom 21. Dezember 2021, wird wie folgt ersetzt:

"Art. 107/3 - § 1 - Im Falle einer erheblichen Cyberbedrohung informieren Anbieter digitaler Infrastruktur das Institut über die Cyberbedrohung, über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können, und über die Maßnahmen, die sie ergriffen haben oder zu ergreifen erwägen.

Das Institut kann die Fälle, in denen eine Information mitgeteilt werden muss, und die Modalitäten dieser Mitteilung näher bestimmen.

§ 2 - Im Fall einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Betreiber von elektronischen Kommunikationsdiensten unverzüglich die Datenschutzbehörde, die ihrerseits unverzüglich das Institut davon benachrichtigt.

Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten die personenbezogenen Daten oder Teilnehmer oder Personen in ihrer Privatsphäre beeinträchtigt werden, so benachrichtigt der Betreiber von elektronischen Kommunikationsdiensten auch den Teilnehmer beziehungsweise die Person unverzüglich von der Verletzung.

Die Datenschutzbehörde prüft, ob der Betreiber diese Verpflichtung einhält; wenn sie der Ansicht ist, dass dies nicht der Fall ist, setzt sie das Institut davon in Kenntnis.

Der Betreiber von elektronischen Kommunikationsdiensten braucht die betroffenen Teilnehmer oder Personen nicht von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn er zur Zufriedenheit des Instituts nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Diese technischen Schutzmaßnahmen verschlüsseln die Daten für alle Personen, die nicht befugt sind, Zugang zu den Daten zu haben.

Unbeschadet der Pflicht des Betreibers von elektronischen Kommunikationsdiensten, die betroffenen Teilnehmer und Personen zu benachrichtigen, kann das Institut, wenn dieser Betreiber die Teilnehmer beziehungsweise Personen noch nicht über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, diesen Betreiber auf Ersuchen der Datenschutzbehörde nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung zur Benachrichtigung auffordern.

In der an die Teilnehmer beziehungsweise Personen gerichteten Benachrichtigung werden mindestens die Art der Verletzung des Schutzes personenbezogener Daten und die Kontaktstellen, bei denen weitere Informationen erhältlich sind, genannt und Maßnahmen zur Begrenzung der möglichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten empfohlen.

In der an die Datenschutzbehörde gerichteten Benachrichtigung werden zusätzlich die Folgen der Verletzung des Schutzes personenbezogener Daten und die Maßnahmen, die vom Betreiber von elektronischen Kommunikationsdiensten nach der Verletzung vorgeschlagen oder ergriffen wurden, dargelegt.

§ 3 - Vorbehaltlich eventueller technischer Durchführungsmaßnahmen, die nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG von der Europäischen Kommission ausgehen, und nach Stellungnahme der Datenschutzbehörde kann das Institut Leitlinien annehmen und gegebenenfalls Anweisungen erteilen in Bezug auf die Umstände, unter denen die Benachrichtigung seitens der Betreiber von elektronischen Kommunikationsdiensten über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

Vorbehaltlich eventueller technischer Durchführungsmaßnahmen, die nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG von der Europäischen Kommission ausgehen, und nach Stellungnahme des Instituts kann die Datenschutzbehörde Leitlinien annehmen und gegebenenfalls Anweisungen in Bezug auf das Format und die Verfahrensweise für die Benachrichtigung erteilen.

Betreiber von elektronischen Kommunikationsdiensten führen ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten, das Angaben zu den Umständen der Verletzungen, zu deren Auswirkungen und zu den ergriffenen Abhilfemaßnahmen enthält, wobei diese Angaben der Datenschutzbehörde und dem Institut die Prüfung der Einhaltung der Bestimmungen von § 2 ermöglichen müssen. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen."

Art. 90 - Artikel 107/4 desselben Gesetzes, eingefügt durch das Gesetz vom 21. Dezember 2021, wird wie folgt ersetzt:

"Art. 107/4 - § 1 - Vorliegender Artikel gilt unbeschadet der Bestimmungen des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit, insbesondere hinsichtlich der Aufsichtsbefugnisse der sektorspezifischen Behörde oder des sektorspezifischen Inspektionsdienstes.

§ 2 - Das Institut kann im Rahmen der Artikel 107/2 und 107/3 und der Artikel 30 und 33 des vorerwähnten Gesetzes vom 26. April 2024 Anbietern digitaler Infrastruktur verbindliche Anweisungen erteilen, auch zu den Maßnahmen, die erforderlich sind, um einen Sicherheitsvorfall zu beheben oder, wenn eine erhebliche Cyberbedrohung festgestellt wurde, zu verhindern, und zu den Fristen für die Umsetzung dieser Anweisungen.

§ 3 - Im Rahmen der Aufsicht gemäß den Artikeln 107/2 und 107/3 und der Artikel 30 und 33 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit kann das Institut Anbieter digitaler Infrastruktur folgenden Maßnahmen unterwerfen:

a) Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführter Stichprobenkontrollen,

b) regelmäßigen und gezielten Sicherheitsprüfungen, die von einer unabhängigen Stelle oder vom Institut durchgeführt werden,

c) Ad-hoc-Prüfungen,

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit dem Anbieter digitaler Infrastruktur,

e) Anforderung von Informationen, die für die Bewertung der vom betreffenden Anbieter digitaler Infrastruktur ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind,

f) Ersuchen um Zugang zu Daten, Dokumenten und sonstigen Informationen, die das Institut für die Erfüllung seiner Aufsichtsaufgaben für erforderlich hält,

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, zum Beispiel der Ergebnisse von Sicherheitsaudits, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

Die in Absatz 1 Buchstabe *b)* erwähnten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die vom Institut oder von der geprüften Einrichtung durchgeführt wurden, oder auf andere verfügbare Informationen zu den Risiken.

Wird die in Absatz 1 Buchstabe *b)* erwähnte Sicherheitsprüfung von einer unabhängigen Stelle durchgeführt, schlägt der betreffende Anbieter digitaler Infrastruktur dem Institut eine oder mehrere Stellen zur Billigung vor. Das Institut erteilt seine Billigung, wenn die unabhängige Stelle für die Durchführung der Prüfung qualifiziert ist und unabhängig vom Anbieter digitaler Infrastruktur ist. Billigt das Institut innerhalb der von ihm bei seinem Ersuchen festgelegten Frist keine Stelle, so bestimmt es selbst die unabhängige Stelle. Diese Stelle übermittelt dem Institut den vollständigen Bericht und die Ergebnisse in Bezug auf diese Prüfung. Die Prüfungskosten trägt der Anbieter digitaler Infrastruktur, es sei denn, das Institut beschließt in ordnungsgemäß begründeten Fällen etwas anderes.

Bei der Ausübung seiner Befugnisse gemäß Absatz 1 Buchstabe *e)*, *f)* oder *g)* gibt das Institut den Zweck der Anforderung beziehungsweise des Ersuchens und der angeforderten Informationen an.

Das Institut kann die Modalitäten für die Bereitstellung der Informationen zur Risikoanalyse durch Anbieter digitaler Infrastruktur festlegen.

Auf Verlangen des Instituts nimmt ein Anbieter digitaler Infrastruktur an einer Übung im Zusammenhang mit der Sicherheit von Netz- oder Informationssystemen teil oder organisiert eine solche Übung.

Auf Verlangen des Instituts und im Rahmen der Bewältigung von Sicherheitsvorfällen teilt ein Anbieter digitaler Infrastruktur dem Institut eine ständig verfügbare Kontaktstelle mit.

§ 4 - Auf Ersuchen des Instituts und zur Untersuchung eines Falls der Nichteinhaltung der Artikel 30 und 33 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit oder einer Durchsetzungsmaßnahme sowie seiner Auswirkungen auf die Sicherheit der Netz- und Informationssysteme gewähren Anbieter digitaler Infrastruktur dem Institut Zugang zu allen Teilen ihres Netzes.

§ 5 - Unbeschadet der Befugnisse der nationalen Cybersicherheitsbehörde koordiniert das Institut die Initiativen in Bezug auf die Sicherheit öffentlicher elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste.

Es überwacht Erkennung, Beobachtung und Analyse von Sicherheitsproblemen und kann Nutzer diesbezüglich auf dem Laufenden halten.

§ 6 - Bei Nichteinhaltung des vorliegenden Artikels oder einer auf der Grundlage des vorliegenden Artikels getroffenen Entscheidung des Instituts durch einen Anbieter digitaler Infrastruktur können die in Titel 4 Kapitel 2 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit erwähnten administrativen Maßnahmen oder Geldbußen auferlegt werden."

Art. 91 - In Artikel 126/3 § 3 Buchstabe *l)* desselben Gesetzes, eingefügt durch das Gesetz vom 20. Juli 2022, werden die Wörter "wesentlicher Dienste von Betreibern wesentlicher Dienste unterstützen, die auf der Grundlage des Gesetzes vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit bestimmt worden sind" durch die Wörter "von Diensten wesentlicher Einrichtungen im Sinne des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit unterstützen" ersetzt.

Art. 92 - Artikel 164/1 desselben Gesetzes, eingefügt durch das Gesetz vom 10. Juli 2012, wird wie folgt abgeändert:

1. Die Wörter "Internetdomainnamen-Registrierungsstelle für die Top-Level-Domain" werden durch die Wörter "TLD-Namenregister für die Top-Level-Domain" ersetzt.

2. In Nr. 4 werden die Wörter "einer neuen Internetdomainnamen-Registrierungsstelle" durch die Wörter "eines neuen TLD-Namenregisters" ersetzt.

3. In Nr. 4 werden die Wörter "der Internetdomainnamen-Registrierungsstelle" durch die Wörter "des TLD-Namenregisters" ersetzt.

4. *[Abänderung des niederländischen Textes von Nr. 5]*

Art. 93 - Artikel 164/2 desselben Gesetzes wird wie folgt abgeändert:

1. Der Begriff "Internetdomainnamen-Registrierungsstelle" wird jeweils durch den Begriff "TLD-Namenregister" ersetzt.

2. *[Abänderung des niederländischen Textes]*

Art. 94 - In Titel VI Kapitel 3 desselben Gesetzes wird ein Artikel 164/3 mit folgendem Wortlaut eingefügt:

"Art. 164/3 - § 1 - TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sammeln und pflegen mit der gebotenen Sorgfalt in einer eigenen Datenbank genaue und vollständige Domänennamen-Registrierungsdaten im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten.

§ 2 - Die in § 1 erwähnten Domänennamen-Registrierungsdaten enthalten die erforderlichen Angaben, anhand deren die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.

Diese Informationen enthalten mindestens Folgendes:

1. Domänennamen,

2. Datum der Registrierung,

3. Namen des Domäneninhabers, seine E-Mail-Adresse und Telefonnummer,

4. Kontakt-E-Mail-Adresse und Telefonnummer der Anlaufstelle, die den Domänennamen verwaltet, falls diese sich von denen des Domäneninhabers unterscheiden.

Nach Stellungnahme des Instituts kann der König anordnen, dass Anbieter und Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten die Domänennamen-Registrierungsdaten an Registrare weitergeben, und hierfür die Modalitäten festlegen.

Die Einhaltung der in vorliegendem Artikel erwähnten Verpflichtungen darf nicht zu einer doppelten Erhebung von Domänennamen-Registrierungsdaten bei der betreffenden Person führen. Zu diesem Zweck arbeiten TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, miteinander zusammen.

Nach Stellungnahme des Instituts kann der König die Modalitäten dieser Zusammenarbeit näher bestimmen.

§ 2 - TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, verfügen über Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, mit denen sichergestellt wird, dass die in § 1 Absatz 1 erwähnten Datenbanken genaue und vollständige Angaben enthalten. Diese Vorgaben und Verfahren werden öffentlich zugänglich gemacht.

Sind die in § 1 Absatz 2 aufgeführten Domänennamen-Registrierungsdaten fehlerhaft, ungenau oder unvollständig, sperren TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich den Betrieb dieses Domänennamens, bis der Inhaber des Domänennamens die Registrierungsdaten korrigiert, sodass sie korrekt, genau und vollständig werden.

Tut der Inhaber des Domänennamens dies nicht innerhalb der Frist, die vom TLD-Namenregister oder von der Einrichtung, die Domänennamen-Registrierungsdienste erbringt, festgelegt wird, wird der Domänenname gelöscht.

Die Übertragung eines gesperrten Domänennamens an eine Einrichtung, die Domänennamen-Registrierungsdienste erbringt, ist untersagt.

§ 3 - TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, machen unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich.

§ 4 - TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, stellen die in § 1 Absatz 2 erwähnten Daten berechtigten Zugangsnachfragern unverzüglich und in jedem Fall innerhalb zweiundsiebzig Stunden oder im Dringlichkeitsfall innerhalb vierundzwanzig Stunden nach Eingang eines Antrags auf Zugang kostenlos bereit.

Unter berechtigten Zugangsnachfragern sind natürliche oder juristische Personen zu verstehen, die einen Antrag auf Prüfung, Feststellung, Durchsetzung oder Verteidigung gemäß strafrechtlichen, zivilrechtlichen oder sonstigen Bestimmungen des Unionsrechts oder des belgischen Rechts stellen.

Als berechtigte Zugangsnachfrager gelten:

1. jegliche Personen im Zusammenhang mit Verstößen gegen geistige Eigentumsrechte und verwandte Schutzrechte,

2. das Institut,

3. das ZCB,

4. das nationale CSIRT,

5. die Polizeidienste,

6. die Gerichtsbehörden,

7. die Nachrichten- und Sicherheitsdienste,

8. der FÖD Wirtschaft,

9. der FÖD Finanzen.

Nach Stellungnahme des Instituts kann der König weitere berechtigte Zugangsnachfrager in diese Liste aufnehmen.

TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, bieten Zugangsnachfragern die Möglichkeit, ihren Antrag auf einfache Weise einzureichen.

Von Dringlichkeit ist die Rede, wenn die Nutzung eines Domänennamens zu lebensbedrohlichen Situationen und/oder zu irreparablen Schäden führen kann.

Bei Ablehnung eines ordnungsgemäß begründeten Antrags werden die Gründe angegeben.

Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten werden öffentlich zugänglich gemacht.

TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, dürfen den Inhaber eines Domänennamens nicht davon in Kenntnis setzen, dass ein in Absatz 1 erwähnter Antrag gestellt worden ist.

§ 5 - Das Institut kann einem TLD-Namenregister oder einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, verbindliche Anweisungen erteilen, um die Einhaltung des vorliegenden Artikels sicherzustellen.

§ 6 - Verstößt ein TLD-Namenregister oder eine Einrichtung, die Domänennamen-Registrierungsdienste erbringt, gegen vorliegenden Artikel, gegen einen Königlichen Erlass zur Ausführung des vorliegenden Artikels oder gegen eine vom Institut erlassene verbindliche Anweisung, kann das Institut die in Kapitel 2 des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit erwähnten administrativen Maßnahmen oder Geldbußen auferlegen."

Abschnitt 6 - Abänderungen des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU

Art. 95 - 96 - *[Abänderungen des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU]*

KAPITEL 3 - *Aufhebungsbestimmung*

Art. 97 - Das Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit wird aufgehoben.

KAPITEL 4 - *Inkrafttreten*

Art. 98 - Vorliegendes Gesetz tritt am 18. Oktober 2024 in Kraft.

Anlage I zum Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	- Elektrizitätsunternehmen im Sinne des Artikels 2 Nr. 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU, die die Funktion "Versorgung" im Sinne des Artikels 2 Nr. 12 dieser Richtlinie wahrnehmen
		- Verteilernetzbetreiber im Sinne des Artikels 2 Nr. 29 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
		- Übertragungsnetzbetreiber im Sinne des Artikels 2 Nr. 35 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU
		- Erzeuger im Sinne des Artikels 2 Nr. 38 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU
		- Nominierte Strommarktbetreiber im Sinne des Artikels 2 Nr. 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt
		- Marktteilnehmer im Sinne des Artikels 2 Nr. 25 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nr. 18, 20 und 59 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU anbieten
		- Betreiber 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
	b) Fernwärme und -kälte	- Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nr. 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen
	c) Erdöl	- Betreiber von Erdöl-Fernleitungen
		- Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		- Zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f) der Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
	d) Erdgas	- Versorgungsunternehmen im Sinne des Artikels 2 Nr. 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Verteilernetzbetreiber im Sinne des Artikels 2 Nr. 6 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nr. 4 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Betreiber einer Speicheranlage im Sinne des Artikels 2 Nr. 10 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nr. 12 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Erdgasunternehmen im Sinne des Artikels 2 Nr. 1 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG
		- Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	- Betreiber im Bereich Wasserstofferzeugung, speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	- Luftfahrtunternehmen im Sinne des Artikels 3 Nr. 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002, die für gewerbliche Zwecke genutzt werden

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
		- Flughafenleitungsorgane im Sinne des Artikels 2 Nr. 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte, Flughäfen im Sinne des Artikels 2 Nr. 1 dieser Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		- Flugverkehrskontrolldienste im Sinne des Artikels 2 Nr. 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums
	b) Schienenverkehr	- Infrastrukturbetreiber im Sinne des Artikels 3 Nr. 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums,
		- Eisenbahnunternehmen im Sinne des Artikels 3 Nr. 1 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nr. 12 dieser Richtlinie
	c) Schifffahrt	- Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen für die Schifffahrt bestimmt sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
		- Leitungsorgane von Häfen im Sinne des Artikels 3 Nr. 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen, einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nr. 11 der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		- Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o) der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates
	d) Straßenverkehr	- Straßenverkehrsbehörden im Sinne des Artikels 2 Nr. 12 der Delegierten Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste, die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
		- Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nr. 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern
3. Bankwesen		- Kreditinstitute im Sinne des Artikels 4 Nr. 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012
4. Finanzmarktinfrastrukturen		- Betreiber von Handelsplätzen im Sinne des Artikels 4 Nr. 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
		- Zentrale Gegenparteien im Sinne des Artikels 2 Nr. 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister
5. Gesundheitswesen		- Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g) der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung
		- EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU
		- Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nr. 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel ausüben
		- Einrichtungen, die pharmazeutische Grundstoffe herstellen im Sinne des Anhangs I Abschnitt C Abteilung 21 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik
		- Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
6. Trinkwasser		- Lieferanten von und Unternehmen der Versorgung mit Wasser für den menschlichen Gebrauch im Sinne des Artikels 2 Nr. 1 Buchstabe a) der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch, jedoch unter Ausschluss der 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
7. Abwässer		- Unternehmen, die kommunales Abwasser, häusliches Abwasser oder industrielles Abwasser im Sinne des Artikels 2 Nr. 1, 2 und 3 der Richtlinie 91/271/EWG des Rates vom 21. Mai 1991 über die Behandlung von kommunalem Abwasser sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
8. Digitale Infrastruktur		- Anbieter von Internet-Knoten
		- DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern
		- TLD-Namenregister
		- Anbieter von Cloud-Computing-Diensten
		- Anbieter von Rechenzentrumsdiensten
		- Anbieter von Inhaltszustellnetzen
		- Vertrauensdiensteanbieter
		- Anbieter öffentlicher elektronischer Kommunikationsnetze
		- Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
9. Verwaltung von IKT-Diensten (Business-to-Business)		- Anbieter verwalteter Dienste
		- Anbieter verwalteter Sicherheitsdienste

Anlage I – Sektoren mit hoher Kritikalität		
Sektor	Teilsektor	Art der Einrichtung
10. Öffentliche Verwaltung		- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen
		- Einrichtungen der öffentlichen Verwaltung, die von den föderierten Teilgebieten abhängen und gemäß Artikel 11 § 2 des Gesetzes identifiziert wurden
		- Hilfeleistungszonen im Sinne von Artikel 14 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit oder der "Service d'Incendie et d'Aide médicale urgente de la Région de Bruxelles-Capitale/Brusselse hoofdstedelijke Dienst voor Brandweer en dringende medische Hulp" (Feuerwehrdienst und Dienst für dringende medizinische Hilfe der Region Brüssel-Hauptstadt), geschaffen durch die Ordonnanz vom 19. Juli 1990 "portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale/houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp" (Schaffung des Feuerwehrdienstes und Dienstes für dringende medizinische Hilfe der Region Brüssel-Hauptstadt)
11. Weltraum		- Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Anlage II zum Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit

Anlage II - Sonstige kritische Sektoren		
Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		- Anbieter von Postdiensten im Sinne des Artikels 2 Nr. 1a der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität, einschließlich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		- Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nr. 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über Abfälle und zur Aufhebung bestimmter Richtlinien, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist

Anlage II - Sonstige kritische Sektoren		
Sektor	Teilsektor	Art der Einrichtung
3. Produktion und Herstellung von chemischen Stoffen und Handel mit chemischen Stoffen		- Unternehmen im Sinne des Artikels 3 Nr. 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Agentur für chemische Stoffe, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission, die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nr. 3 der erwähnten Verordnung aus Stoffen oder Gemischen produzieren
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		- Lebensmittelunternehmen im Sinne des Artikels 3 Nr. 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	- Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nr. 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nr. 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission herstellen, mit Ausnahme der unter Anlage I Nr. 5 fünfter Gedankenstrich des vorliegenden Gesetzes aufgeführten Einrichtungen, die Medizinprodukte herstellen

Anlage II - Sonstige kritische Sektoren		
Sektor	Teilsektor	Art der Einrichtung
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	- Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Anhangs I Abschnitt C Abteilung 26 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik ausüben
	c) Herstellung von elektrischen Ausrüstungen	- Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Anhangs I Abschnitt C Abteilung 27 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik ausüben
	d) Maschinenbau	- Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Anhangs I Abschnitt C Abteilung 28 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	- Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Anhangs I Abschnitt C Abteilung 29 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik ausüben
	f) Sonstiger Fahrzeugbau	- Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Anhangs I Abschnitt C Abteilung 30 der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik ausüben

Anlage II - Sonstige kritische Sektoren		
Sektor	Teilsektor	Art der Einrichtung
6. Anbieter digitaler Dienste		- Anbieter von Online-Marktplätzen
		- Anbieter von Online-Suchmaschinen
		- Anbieter von Plattformen für Dienste sozialer Netzwerke
7. Forschung		- Forschungseinrichtungen

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2026/007509]

11 DECEMBER 2025. — Wet tot uitvoering van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) 1093/2010 en (EU) 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937, en van verordening (EU) 2023/1113 van het Europees Parlement en de Raad van 31 mei 2023 betreffende bij geldovermakingen en overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van Richtlijn (EU) 2015/849 en houdende diverse financiële bepalingen. — Officieuze coördinatie in het Duits

De hierna volgende tekst is de officieuze coördinatie in het Duits van de wet van 11 december 2025 tot uitvoering van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) 1093/2010 en (EU) 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937, en van verordening (EU) 2023/1113 van het Europees Parlement en de Raad van 31 mei 2023 betreffende bij geldovermakingen en overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van Richtlijn (EU) 2015/849 en houdende diverse financiële bepalingen (*Belgisch Staatsblad* van 24 december 2025), zoals ze werd gewijzigd bij de wet van 22 juli 2026 tot omzetting van Richtlijn (EU) 2024/1619 van het Europees Parlement en de Raad van 31 mei 2024 tot wijziging van Richtlijn 2013/36/EU wat betreft toezichtsbevoegdheden, sancties, bijkantoren uit derde landen en ecologische, sociale en governancerisico's, Richtlijn (EU) 2023/2864 van het Europees Parlement en de Raad van 13 december 2023 tot wijziging van bepaalde richtlijnen wat betreft de oprichting en het functioneren van het Europees centraal toegangspunt, Richtlijn (EU) 2024/2994 van het Europees Parlement en de Raad van 27 november 2024 tot wijziging van de Richtlijnen 2009/65/EG, 2013/36/EU en (EU) 2019/2034 wat betreft de behandeling van het concentratierisico dat voortvloeit uit blootstellingen aan centrale tegenpartijen en het risico van tegenpartijen bij centraal geclearde derivatentransacties, en houdende diverse bepalingen (*Belgisch Staatsblad* van 7 augustus 2026).

Deze officieuze coördinatie in het Duits is opgemaakt door de Centrale dienst voor Duitse vertaling in Malmedy.

SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2026/007509]

11 DECEMBRE 2025. — Loi mettant en œuvre le règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de cryptoactifs, et modifiant les règlements (UE) 1093/2010 et (UE) 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937, et le règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains cryptoactifs, et modifiant la directive (UE) 2015/849 et portant des dispositions financières diverses. — Coordination officieuse en langue allemande

Le texte qui suit constitue la coordination officieuse en langue allemande de la loi du 11 décembre 2025 mettant en œuvre le règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de cryptoactifs, et modifiant les règlements (UE) 1093/2010 et (UE) 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937, et le règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains cryptoactifs, et modifiant la directive (UE) 2015/849 et portant des dispositions financières diverses (*Moniteur belge* du 24 décembre 2025), telle qu'elle a été modifiée par la loi du 22 juillet 2026 visant à assurer la transposition de la directive (UE) 2024/1619 du Parlement européen et du Conseil du 31 mai 2024 modifiant la directive 2013/36/UE en ce qui concerne les pouvoirs de surveillance, les sanctions, les succursales de pays tiers et les risques environnementaux, sociaux et de gouvernance, la directive (UE) 2023/2864 du Parlement européen et du Conseil du 13 décembre 2023 modifiant certaines directives en ce qui concerne l'établissement et le fonctionnement du point d'accès unique européen, la directive (UE) 2024/2994 du Parlement européen et du Conseil du 27 novembre 2024 modifiant les directives 2009/65/CE, 2013/36/UE et (UE) 2019/2034 en ce qui concerne le traitement du risque de concentration découlant d'expositions sur des contreparties centrales et du risque de contrepartie des transactions sur instruments dérivés faisant l'objet d'une compensation centrale, et portant dispositions diverses (*Moniteur belge* du 7 août 2026).

Cette coordination officieuse en langue allemande a été établie par le Service central de traduction allemande à Malmedy.

FÖDERALER ÖFFENTLICHER DIENST INNERES

[C − 2026/007509]

11. DEZEMBER 2025 — Gesetz zur Durchführung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 und zur Durchführung der Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 und zur Festlegung verschiedener finanzieller Bestimmungen — Inoffizielle Koordinierung in deutscher Sprache

Der folgende Text ist die inoffizielle Koordinierung in deutscher Sprache des Gesetzes vom 11. Dezember 2025 zur Durchführung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 und zur Durchführung der Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 und zur Festlegung verschiedener