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

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2022/31921]

7 APRIL 2019. — Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. — Officieuze coördinatie in het Duits van uittreksels

De hierna volgende tekst is de officieuze coördinatie in het Duits van de artikelen 1 tot 86, 92 en 96 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (*Belgisch Staatsblad* van 3 mei 2019), zoals ze werd gewijzigd bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie (*Belgisch Staatsblad* van 31 december 2021).

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

SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2022/31921]

7 AVRIL 2019. — Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. — Coordination officieuse en langue allemande d'extraits

Le texte qui suit constitue la coordination officieuse en langue allemande des articles 1 à 86, 92 et 96 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (*Moniteur belge* du 3 mai 2019), telle qu'elle a été modifiée par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques (*Moniteur belge* du 31 décembre 2021).

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

FÖDERALER ÖFFENTLICHER DIENST INNERES

[C − 2022/31921]

7. APRIL 2019 — Gesetz zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit — Inoffizielle Koordinierung in deutscher Sprache von Auszügen

Der folgende Text ist die inoffizielle Koordinierung in deutscher Sprache der Artikel 1 bis 86, 92 und 96 des Gesetzes vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit, so wie es abgeändert worden ist durch das Gesetz vom 21. Dezember 2021 zur Umsetzung des europäischen Kodex für die elektronische Kommunikation und zur Abänderung diverser Bestimmungen im Bereich der elektronischen Kommunikation.

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

FÖDERALER ÖFFENTLICHER DIENST KANZLEI DES PREMIERMINISTERS

7. APRIL 2019 — Gesetz zur Festlegung eines Rahmens für die Sicherheit 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) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, nachstehend "NIS-Richtlinie" genannt.

Abschnitt 2 — Anwendungsbereich

Art. 3 - § 1 - Vorliegendes Gesetz findet Anwendung auf die Betreiber wesentlicher Dienste, wie in Artikel 6 Nr. 11 bestimmt, die mindestens eine Niederlassung auf belgischem Staatsgebiet haben und tatsächlich eine Tätigkeit ausüben, die mit der Bereitstellung mindestens eines wesentlichen Dienstes auf belgischem Staatsgebiet zusammenhängt.

Die Bestimmungen von Titel 1 Artikel 13, 14 und 30 sowie Titel 4 Kapitel 3 sind auf die potenziellen Betreiber wesentlicher Dienste anwendbar.

§ 2 - Vorliegendes Gesetz findet Anwendung auf die Anbieter digitaler Dienste, wie in Artikel 6 Nr. 21 bestimmt, deren Hauptsitz in Belgien liegt. Es wird davon ausgegangen, dass ein Anbieter digitaler Dienste seinen Hauptsitz in Belgien hat, wenn sich sein Gesellschaftssitz dort befindet.

Vorliegendes Gesetz findet ebenfalls Anwendung auf die Anbieter digitaler Dienste, die keine Niederlassung in der Europäischen Union haben, wenn sie in Belgien die in Anlage 2 erwähnten Dienste bereitstellen und ihr Vertreter im Rahmen der NIS-Richtlinie in Belgien niedergelassen ist.

Art. 4 - § 1 - Die in vorliegendem Gesetz vorgesehenen Sicherheits- und Meldeanforderungen sind nicht anwendbar auf Unternehmen, die für ihre Tätigkeiten in Sachen Bereitstellung öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste den in den [Artikeln 107/2 und 107/3] des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation aufgeführten Anforderungen unterliegen, und auf Vertrauensdiensteanbieter, die für ihre Tätigkeiten in Sachen Vertrauensdienste den in Artikel 19 der europäischen 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 aufgeführten Anforderungen unterliegen.

§ 2 - Wird nach Maßgabe eines sektorspezifischen Rechtsakts der Europäischen Union von den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste gefordert, entweder die Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen zu gewährleisten, und sind diese Anforderungen in ihrer Wirkung den in vorliegendem Gesetz enthaltenen Pflichten mindestens gleichwertig, so können die Bestimmungen in Bezug auf die Sicherheit von Netz- und Informationssystemen und die Meldung von Sicherheitsvorfällen jenes Rechtsakts von den Bestimmungen des vorliegenden Gesetzes abweichen.

Der König ist beauftragt, die eventuell gleichwertigen sektorspezifischen Akte, wie in Absatz 1 erwähnt, näher zu bestimmen.

§ 3 - Vorliegendes Gesetz findet keine Anwendung auf Betreiber, die zum Finanzsektor im Sinne von Anlage 1 zu vorliegendem Gesetz gehören, mit Ausnahme der Bestimmungen von Titel 1, Titel 2 Kapitel 1 und Artikel 26.

In Abweichung von Absatz 1 ist Artikel 52 anwendbar auf Betreiber, die zum Finanzsektor im Sinne von Anlage 1 zu vorliegendem Gesetz gehören, mit Ausnahme der Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU.

Die sektorspezifischen Behörden und die Betreiber, die zum Finanzsektor im Sinne von Anlage 1 zu vorliegendem Gesetz gehören, unterliegen den Artikeln 65 bis 73.

In Abweichung von Vorhergehendem sind die Artikel 65 bis 73 nicht auf die betreffende sektorspezifische Behörde anwendbar, wenn diese in den in Artikel 46*bis* des Gesetzes vom 2. August 2002 über die Aufsicht über den Finanzsektor und die Finanzdienstleistungen oder in Artikel 12*quater* des Gesetzes vom 22. Februar 1998 zur Festlegung des Grundlagenstatuts der Belgischen Nationalbank erwähnten Fällen auftritt.

§ 4 - Vorliegendes Gesetz findet keine Anwendung, wenn und soweit aufgrund 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 Maßnahmen für die Sicherheit von Netz- und Informationssystemen bestehen.

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

[Art. 4 § 1 abgeändert durch Art. 257 des G. vom 21. Dezember 2021 (B.S. vom 31. Dezember 2021)]

Art. 5 - § 1 - Vorbehaltlich der Bestimmungen von Titel 6 beeinträchtigt vorliegendes Gesetz weder die Anwendung der Verordnung EU 2016/679 noch die Gesetzes- und Verordnungsbestimmungen, die diese Verordnung ergänzen beziehungsweise näher bestimmen.

§ 2 - Vorliegendes Gesetz beeinträchtigt nicht die Anwendung des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz der kritischen Infrastrukturen, der Artikel 259*bis*, 314*bis*, 380, 382*quinquies*, 383*bis*, 383*bis*/1, 433*septies*, 433*novies*/1, 458*bis*, 550*bis* und 550*ter* des Strafgesetzbuches oder anderer Bestimmungen des belgischen Rechts zur Umsetzung der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates und der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates.

§ 3 - Vorliegendes Gesetz beeinträchtigt nicht die Regeln, die für die Verarbeitung von Informationen, Dokumenten oder Daten, für Ausrüstung, Material oder Stoffe in gleich welcher Form gelten, klassifiziert in Anwendung des Gesetzes vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungnahmen.

§ 4 - 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.

KAPITEL 2 — *Begriffsbestimmungen*

Art. 6 - Für die Anwendung des vorliegenden Gesetzes gelten folgende Begriffsbestimmungen:

1. "nationales CSIRT": vom König bestimmtes nationales Computer-Notfallteam,
2. "sektorspezifische Behörde": durch Gesetz oder vom König durch einen im Ministerrat beratenen Erlass bestimmte öffentliche Behörde,
3. "sektorspezifisches CSIRT": vom König bestimmtes sektorspezifisches Computer-Notfallteam,
4. "Aufsichtsbehörde personenbezogene Daten": Aufsichtsbehörde im Sinne von Artikel 4 Nummer 21 der Verordnung EU 2016/679 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),
5. "Konformitätsbewertungsstelle": Stelle, wie in Artikel I.9 Nr. 7 des Wirtschaftsgesetzbuches erwähnt,
6. "Zertifizierungsaudit": Audit im Rahmen einer in Artikel 22 § 2 erwähnten Zertifizierung,
7. "nationale Akkreditierungsbehörde": vom König in Ausführung von Artikel VIII.30 des Wirtschaftsgesetzbuches eingerichtete Stelle,
8. "Netz- und Informationssystem":
   a) elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nr. 3 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation,
   b) Vorrichtung oder Gruppe ständig oder zeitweilig miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, einschließlich der digitalen, elektronischen oder mechanischen Komponenten dieser Vorrichtung, insbesondere für die Automatisierung des Betriebsablaufs, die Fernsteuerung oder die Erfassung von Echtzeit-Betriebsdaten,
   c) oder digitale Daten, die von den in den Buchstaben *a)* und *b)* genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden,
9. "Sicherheit von Netz- und Informationssystemen": Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder

Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden beziehungsweise zugänglich sind, beeinträchtigen,

10. ″nationale Strategie für die Sicherheit von Netz- und Informationssystemen″: Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen auf nationaler Ebene,

11. ″Betreiber wesentlicher Dienste″: öffentliche oder private Einrichtung, die in Belgien in einem der in Anlage 1 zu vorliegendem Gesetz aufgeführten Sektoren tätig ist, den in Artikel 12 § 1 erwähnten Kriterien entspricht und von der sektorspezifischen Behörde als solcher bestimmt ist,

12. ″potenzieller Betreiber wesentlicher Dienste″: öffentliche oder private Einrichtung, die in Belgien in einem der in Anlage 1 zu vorliegendem Gesetz aufgeführten Sektoren tätig ist, aber nicht als Betreiber wesentlicher Dienste bestimmt worden ist,

13. ″Sicherheitsvorfall″: alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben,

14. ″Bewältigung von Sicherheitsvorfällen″: alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf,

15. ″Risiko″: alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben,

16. ″sektorübergreifendes Kriterium″: Faktor, der allen der in Anlage 1 zu vorliegendem Gesetz erwähnten Sektoren gemeinsam ist und das Ausmaß einer Störung auf die Bereitstellung eines wesentlichen Dienstes im Sinne von Artikel 12 § 1 Buchstabe *c)* bestimmt,

17. ″sektorspezifisches Kriterium″: Faktor, der für einen der in Anlage 1 zu vorliegendem Gesetz erwähnten Sektoren oder Teilsektoren spezifisch ist und das Ausmaß einer Störung auf die Bereitstellung eines wesentlichen Dienstes im Sinne von Artikel 12 § 1 Buchstabe *c)* bestimmt,

18. ″Sicherheitspolitik für Netz- und Informationssysteme (S.P.I.)″: Unterlage, wie in Artikel 21 § 1 erwähnt, mit den von einem Betreiber wesentlicher Dienste ergriffenen Maßnahmen für die Sicherheit der Netz- und Informationssysteme,

19. ″Anlaufstelle für die Sicherheit von Netz- und Informationssystemen″: von dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste bestimmte Kontaktstelle, die für jegliche Fragen in Sachen Sicherheit von Netz- und Informationssystemen, von denen die bereitgestellten wesentlichen Dienste abhängen, als Anlaufstelle für die in Artikel 7 erwähnten Behörden agiert,

20. ″digitaler Dienst″: Dienst im Sinne von Artikel 1 Absatz 1 Buchstabe b) der europäischen 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, der einer in Anlage 2 genannten Art entspricht,

21. ″Anbieter digitaler Dienste″: juristische Person, die einen in Anlage 2 zu vorliegendem Gesetz erwähnten digitalen Dienst anbietet,

22. ″Vertreter eines Anbieters digitaler Dienste″: in Belgien niedergelassene natürliche oder juristische Person, die ausdrücklich bestimmt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich die in Artikel 7 § 1 erwähnte nationale Behörde, die zuständige sektorspezifische Behörde oder der zuständige Inspektionsdienst - statt an den Anbieter digitaler Dienste - hinsichtlich der aus vorliegendem Gesetz hervorgehenden Pflichten dieses Anbieters wenden kann,

23. ″Internet-Knoten (IXP)″: Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr; ein Internet-Knoten dient nur der Zusammenschaltung autonomer Systeme; ein Internet-Knoten setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt,

24. ″Domain-Namen-System″ oder ″DNS″: hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen,

25. ″DNS-Diensteanbieter″: Einrichtung, die DNS-Dienste im Internet anbietet,

26. ″Top-Level-Domain-Name-Registry″: Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt,

27. ″Online-Marktplatz″: digitaler Dienst, der es Verbrauchern im Sinne von Artikel I.1 Absatz 1 Nr. 2 des Wirtschaftsgesetzbuches und/oder Unternehmen im Sinne von Artikel I.8 Nr. 39 desselben Gesetzbuches ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmen entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmens, das von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen,

28. ″Online-Suchmaschine″: digitaler Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können,

29. ″Cloud-Computing-Dienst″: digitaler Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht,

30. ″Gesetz vom 1. Juli 2011″: Gesetz vom 1. Juli 2011 über die Sicherheit und den Schutz der kritischen Infrastrukturen,

31. ″Gesetz vom 11. Dezember 1998″: Gesetz vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungnahmen,

32. ″Gesetz vom 15. April 1994″: Gesetz vom 15. April 1994 über den Schutz der Bevölkerung und der Umwelt gegen die Gefahren ionisierender Strahlungen und über die Föderalagentur für Nuklearkontrolle,

33. ″Verordnung EU 2016/679″: europäische Verordnung 2016/679 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).

KAPITEL 3 — *Zuständige Behörden und Zusammenarbeit auf nationaler Ebene*

Abschnitt 1 — Zuständige Behörden

Art. 7 - § 1 - Der König bestimmt die Behörde, die als nationale Behörde damit beauftragt ist, die Umsetzung des vorliegenden Gesetzes zu begleiten und zu koordinieren.

Die in Absatz 1 erwähnte Behörde ist ebenfalls nationale zentrale Anlaufstelle im Bereich Sicherheit der Netz- und Informationssysteme, und zwar für alle Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, für Belgien in seinen Beziehungen mit der Europäischen Kommission, den Mitgliedstaaten der Europäischen Union, der in Artikel 11 der NIS-Richtlinie erwähnten Kooperationsgruppe und dem CSIRT-Netzwerk. Zu diesem Zweck agiert die Anlaufstelle als Vertreter Belgiens in der Kooperationsgruppe.

§ 2 - Der König bestimmt die Behörde, die damit beauftragt ist, die Rolle des nationalen CSIRT zu übernehmen.

Das nationale CSIRT fungiert als Vertreter Belgiens innerhalb des in Artikel 12 der NIS-Richtlinie erwähnten CSIRT-Netzwerks. Es arbeitet wirksam, effizient und sicher an den Aufträgen des CSIRT-Netzwerks mit.

§ 3 - Der König bestimmt durch einen im Ministerrat beratenen Erlass die sektorspezifischen Behörden, die für ihren jeweiligen Sektor damit beauftragt sind, die Umsetzung der Bestimmungen des vorliegenden Gesetzes zu überwachen.

Der König kann sektorspezifische Behörden einrichten, die sich aus Vertretern des Föderalstaats, der Gemeinschaften und 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 im Gesetz selbst bestimmt.

§ 4 - Der König bestimmt die Behörde, die in Zusammenarbeit mit der in § 1 erwähnten nationalen Behörde damit beauftragt ist, die Ermittlung von Betreibern wesentlicher Dienste zu koordinieren.

§ 5 - Pro Sektor oder gegebenenfalls pro Teilsektor wird ein Inspektionsdienst eingerichtet, der beauftragt ist, die Einhaltung der Bestimmungen des vorliegenden Gesetzes und seiner Ausführungserlasse durch die Betreiber wesentlicher Dienste beziehungsweise die Anbieter digitaler Dienste zu kontrollieren.

Der König bestimmt für einen bestimmten Sektor oder gegebenenfalls pro Teilsektor den für die Kontrolle zuständigen Inspektionsdienst.

In Abweichung von Absatz 2 werden die durch Gesetz eingerichteten und geregelten Inspektionsdienste im Gesetz bestimmt.

Abschnitt 2 — Zusammenarbeit auf nationaler Ebene

Art. 8 - § 1 - Die in Artikel 7 erwähnten Behörden arbeiten eng zusammen, um den in vorliegendem Gesetz aufgeführten Verpflichtungen nachzukommen.

§ 2 - Wie für die Ausführung des Gesetzes erforderlich und gemäß den geltenden Gesetzesbestimmungen arbeiten die in § 1 erwähnten Behörden auf nationaler Ebene ebenfalls mit den Verwaltungsdiensten des Staates, den Verwaltungsbehörden, 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 Aufsichtsbehörden personenbezogene Daten zusammen.

§ 3 - Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und die in Artikel 7 erwähnten Behörden arbeiten ständig durch einen adäquaten Informationsaustausch im Bereich Sicherheit von Netz- und Informationssystemen zusammen.

KAPITEL 4 — *Informationsaustausch*

Art. 9 - § 1 - Vorliegender Artikel beeinträchtigt nicht die Anwendung des Gesetzes vom 11. Dezember 1998, des Gesetzes vom 15. April 1994, 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.

Die in Artikel 7 erwähnten Behörden, Betreiber wesentlicher Dienste, Anbieter digitaler Dienste beziehungsweise ihre Subunternehmer beschränken den Zugriff auf die 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 vorliegendem Gesetz Kenntnis von diesen Informationen und Zugriff auf sie haben müssen.

§ 2 - Personalmitglieder der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste oder ihre Subunternehmer sind an das Berufsgeheimnis gebunden, was Informationen in Bezug auf die Ausführung des vorliegenden Gesetzes betrifft.

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

§ 3 - Informationen, die den in Artikel 7 erwähnten Behörden von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste bereitgestellt werden, dürfen mit den Behörden der Europäischen Union sowie mit belgischen oder ausländischen Behörden ausgetauscht werden, wenn dieser Austausch für die Anwendung von Gesetzesbestimmungen erforderlich ist.

Die auszutauschenden 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 Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste geschützt.

KAPITEL 5 — *Nationale Strategie für die Sicherheit von Netz- und Informationssystemen*

Art. 10 - § 1 - Der König bestimmt durch einen im Ministerrat beratenen Erlass die Behörde, die damit beauftragt ist, die bestehende nationale Strategie für die Sicherheit von Netz- und Informationssystemen fortzuschreiben.

§ 2 - Die in § 1 erwähnte Strategie wird nach Stellungnahme der in Artikel 7 erwähnten Behörden und gegebenenfalls der Aufsichtsbehörden personenbezogene Daten fortgeschrieben. Sie deckt mindestens die in Anlage 1 erwähnten Sektoren und die in Anlage 2 erwähnten Dienste ab.

In dieser Strategie werden angemessene strategische und verordnungsrechtliche Ziele bestimmt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll.

§ 3 - Die nationale Strategie für die Sicherheit von Netz-und Informationssystemen behandelt insbesondere die folgenden Aspekte:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen,

b) einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen betreffenden Akteure,

c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor,

d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen,

e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen,

f) einen Risikobewertungsplan zur Bestimmung von Risiken,

g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind.

TITEL 2 — *Netz- und Informationssysteme der Betreiber wesentlicher Dienste*

KAPITEL 1 — *Ermittlung der Betreiber wesentlicher Dienste*

Art. 11 - § 1 - Die sektorspezifische Behörde ermittelt die Betreiber wesentlicher Dienste für ihren Sektor und berücksichtigt dabei mindestens die in Anlage 1 zu vorliegendem Gesetz aufgeführten Arten von Betreibern.

In den Grenzen ihrer jeweiligen Zuständigkeiten sprechen sich die in Artikel 7 §§ 1 und 4 erwähnten Behörden und die sektorspezifische Behörde ab, um diese Ermittlung vorzunehmen.

Die sektorspezifische Behörde konsultiert gegebenenfalls die betreffenden Regionen beziehungsweise Gemeinschaften sowie die Vertreter der in Anlage 1 erwähnten Einrichtungen.

§ 2 - Nach Konsultierung eines potenziellen Betreibers wesentlicher Dienste teilt die sektorspezifische Behörde diesem Betreiber mit, welche der von ihm bereitgestellten Dienste als wesentlich angesehen werden.

§ 3 - Die sektorspezifische Behörde gewährleistet die ständige Begleitung der Abläufe zur Ermittlung und Bestimmung von Betreibern wesentlicher Dienste und ihrer wesentlichen Dienste gemäß den in vorliegendem Kapitel beschriebenen Verfahren; diese Abläufe finden zum ersten Mal spätestens binnen sechs Monaten nach Inkrafttreten des vorliegenden Gesetzes statt.

Mindestens alle zwei Jahre bewertet die sektorspezifische Behörde die Ermittlung von Betreibern wesentlicher Dienste und ihrer wesentlichen Dienste und aktualisiert sie gegebenenfalls.

Diese Aktualisierungen werden den in Artikel 7 §§ 1 und 4 erwähnten Behörden mitgeteilt.

Art. 12 - § 1 - Zur Ermittlung der in Artikel 11 erwähnten Betreiber wendet die sektorspezifische Behörde folgende Kriterien an:

a) Die Einrichtung stellt einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist.

b) Die Bereitstellung dieses Dienstes ist abhängig von Netz- und Informationssystemen und

c) ein Sicherheitsvorfall würde eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken, wobei die in Artikel 13 erwähnten Kriterien und Inzidenz- beziehungsweise Schwellenwerte berücksichtigt werden.

§ 2 - Außer bei Beweis des Gegenteils wird davon ausgegangen, dass die Bereitstellung eines wesentlichen Dienstes von Netz- und Informationssystemen abhängig ist.

Art. 13 - § 1 - Um das Ausmaß der in Artikel 12 § 1 Buchstabe *c)* erwähnten Störung zu bestimmen, legt die sektorspezifische Behörde sektorspezifische und/oder sektorübergreifende Kriterien, Inzidenz- oder Schwellenwerte für ihren Sektor fest.

Eine erhebliche Störung liegt vor, sobald der potenzielle Betreiber wesentlicher Dienste entweder einen Schwellen- oder einen Inzidenzwert erreicht.

In den Grenzen ihrer jeweiligen Zuständigkeiten sprechen sich die in Artikel 7 §§ 1 und 4 erwähnten Behörden mit der sektorspezifischen Behörde ab, um die Kriterien, Inzidenz- und Schwellenwerte zu bestimmen, gegebenenfalls nach Konsultierung der betreffenden Regionen beziehungsweise Gemeinschaften und der Vertreter der in Anlage 1 erwähnten Einrichtungen.

§ 2 - Die sektorspezifische Behörde berücksichtigt mindestens die folgenden sektorübergreifenden Kriterien auf der Grundlage der verfügbaren Informationen:

a) Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen,

b) Abhängigkeit anderer in Anlage 1 erwähnter Sektoren von dem von dieser Einrichtung angebotenen Dienst,

c) mögliche Auswirkungen von Sicherheitsvorfällen - hinsichtlich Ausmaß und Dauer - auf wirtschaftliche beziehungsweise gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit,

d) Marktanteil dieser Einrichtung,

e) geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte,

f) Bedeutung der Einrichtung für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

§ 3 - Nach Stellungnahme der in Artikel 7 erwähnten Behörden und Konsultierung der betreffenden Regionen und Gemeinschaften kann der König diese sektorübergreifenden Kriterien ergänzen.

Art. 14 - Auf Anfrage einer in Artikel 7 erwähnten Behörde übermitteln potenzielle Betreiber wesentlicher Dienste alle die für ihre eventuelle Ermittlung als Betreiber wesentlicher Dienste nützlichen Informationen, einschließlich jener, die die objektive Feststellung ermöglichen, ob die Bereitstellung des wesentlichen Dienstes von Netz- und Informationssystemen abhängig ist oder nicht.

Die von den potenziellen Betreibern übermittelten relevanten Informationen werden den anderen in Artikel 7 erwähnten Behörden zur Kenntnis gebracht.

Art. 15 - § 1 - Die sektorspezifische Behörde übermittelt den in Artikel 7 §§ 1 und 4 erwähnten Behörden einen mit Gründen versehenen Vorschlag für eine Liste der Betreiber wesentlicher Dienste ihres Sektors zusammen mit dem/den verwendeten Ermittlungskriterien.

Wird für einen Sektor beziehungsweise Teilsektor kein Betreiber wesentlicher Dienste vorgeschlagen, legt die sektorspezifische Behörde schriftlich ihre Gründe dafür dar.

Die in Artikel 7 §§ 1 und 4 erwähnten Behörden geben in den Grenzen ihrer jeweiligen Zuständigkeiten eine Stellungnahme über die mit Gründen versehene vorgeschlagene Liste ab, gegebenenfalls nach Konsultierung der Regionen und Gemeinschaften.

§ 2 - Stellt die sektorspezifische Behörde fest, dass die Einrichtung, die sie als Betreiber wesentlicher Dienste bestimmen möchte, einen oder mehrere wesentliche Dienste in mindestens einem anderen Mitgliedstaat der Europäischen Union bereitstellt, setzt sie die in Artikel 7 §§ 1 und 4 erwähnten Behörden davon in Kenntnis. Diese Behörden organisieren in Zusammenarbeit mit den betreffenden sektorspezifischen Behörden Gespräche mit der/den betreffenden ausländischen nationalen Behörde(n) und gegebenenfalls mit den betreffenden Regionen beziehungsweise Gemeinschaften.

§ 3 - Die sektorspezifische Behörde notifiziert dem Betreiber ihren mit Gründen versehenen Beschluss über seine Bestimmung zum Betreiber wesentlicher Dienste. Diese Notifizierung erfolgt auf gesicherte Weise.

Sie übermittelt ebenfalls eine Kopie dieses Beschlusses an die in Artikel 7 §§ 1 und 4 erwähnten Behörden.

Gegebenenfalls setzt die sektorspezifische Behörde die betreffenden Regionen und/oder Gemeinschaften davon in Kenntnis.

Art. 16 - Binnen drei Monaten nach seiner Bestimmung übermittelt der Betreiber wesentlicher Dienste der sektorspezifischen Behörde eine Beschreibung der Netz- und Informationssysteme, von denen die Bereitstellung des/der betreffenden wesentlichen Dienste(s) abhängig ist.

Die sektorspezifische Behörde leitet diese Beschreibung an die in Artikel 7 § 1 erwähnte Behörde weiter.

Art. 17 - Unbeschadet der eventuellen Anwendung des Gesetzes vom 11. Dezember 1998 gelten die Verwaltungsunterlagen in Bezug auf die Anwendung des vorliegenden Kapitels als Verwaltungsunterlagen im Bereich Sicherheit der Bevölkerung, öffentliche Ordnung und Sicherheit im Sinne von Artikel 6 § 1 des Gesetzes vom 11. April 1994 über die Öffentlichkeit der Verwaltung und dürfen für die Öffentlichkeit nicht eingesehen, erläutert oder in Form einer Abschrift mitgeteilt werden.

Art. 18 - § 1 - In Abweichung von Artikel 11 bestimmt die sektorspezifische Behörde die Betreiber kritischer Infrastrukturen, wie aufgrund von Artikel 8 des Gesetzes vom 1. Juli 2011 und Artikel 6 des Königlichen Erlasses vom 2. Dezember 2011 über die kritischen Infrastrukturen im Teilsektor des Luftverkehrs ausgewiesen, als Betreiber wesentlicher Dienste, wenn ihr Sektor in Anlage 1 zu vorliegendem Gesetz aufgeführt ist und die Bereitstellung ihrer wesentlichen Dienste von Netz- und Informationssystemen abhängt.

Diese Bestimmung erfolgt in Absprache mit den in Artikel 7 §§ 1 und 4 erwähnten Behörden in den Grenzen ihrer jeweiligen Zuständigkeiten.

§ 2 - Außer bei Beweis des Gegenteils wird davon ausgegangen, dass der Betrieb einer kritischen Infrastruktur von Netz- und Informationssystemen abhängig ist.

§ 3 - Auf Anfrage der sektorspezifischen Behörde oder einer in Artikel 7 §§ 1 und 4 erwähnten Behörde übermittelt der Betreiber der sektorspezifischen Behörde alle die für seine eventuelle Ermittlung als Betreiber wesentlicher Dienste nützlichen Informationen, einschließlich jener, die die objektive Feststellung ermöglichen, ob er von Netz- und Informationssystemen abhängig ist oder nicht.

Die sektorspezifische Behörde leitet die vom Betreiber übermittelten relevanten Informationen an die in Artikel 7 §§ 1 und 4 erwähnten Behörden weiter.

§ 4 - Artikel 15 § 3 findet Anwendung auf den mit Gründen versehenen Beschluss zur Bestimmung eines Betreibers einer kritischen Infrastruktur zum Betreiber wesentlicher Dienste.

Art. 19 - Der König kann der Anlage 1 zu vorliegendem Gesetz durch einen im Ministerrat beratenen Erlass weitere Sektoren oder Arten von Betreibern hinzufügen.

KAPITEL 2 — *Sicherheitsmaßnahmen*

Art. 20 - Betreiber wesentlicher Dienste ergreifen geeignete und verhältnismäßige technische und organisatorische Maßnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, von denen ihre wesentlichen Dienste abhängen, zu bewältigen.

Diese Maßnahmen gewährleisten unter Berücksichtigung des Stands der Technik ein physisches und logisches Sicherheitsniveau der Netz- und Informationssysteme, das den bestehenden Risiken angemessen ist.

Betreiber ergreifen ebenfalls geeignete Maßnahmen, um Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise deren Auswirkungen so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

Art. 21 - § 1 - Betreiber wesentlicher Dienste arbeiten eine Sicherheitspolitik für ihre Netz- und Informationssysteme (nachstehend "S.P.I." genannt) aus, die mindestens die in Artikel 20 erwähnten konkreten Sicherheitszielsetzungen und -maßnahmen umfasst.

§ 2 - Betreiber wesentlicher Dienste arbeiten ihre S.P.I. spätestens binnen zwölf Monaten nach Notifizierung ihrer Bestimmung aus. Spätestens binnen vierundzwanzig Monaten nach Notifizierung ihrer Bestimmung setzen sie die in ihrer S.P.I. vorgesehenen Maßnahmen um.

Die zuständige sektorspezifische Behörde kann diese Frist für einen bestimmten Sektor oder gegebenenfalls pro Teilsektor je nach Art der in der S.P.I. vorgesehenen Maßnahmen anpassen.

§ 3 - Nach Stellungnahme der in Artikel 7 erwähnten Behörden und gegebenenfalls nach Konsultierung der betreffenden Regionen beziehungsweise Gemeinschaften kann der König den Betreibern wesentlicher Dienste eines oder mehrerer Sektoren bestimmte Sicherheitsmaßnahmen auferlegen.

§ 4 - In Absprache mit der in Artikel 7 § 1 erwähnten Behörde und gegebenenfalls nach Konsultierung der Regionen und Gemeinschaften kann die sektorspezifische Behörde durch einen individuellen Verwaltungsbeschluss zusätzliche Sicherheitsmaßnahmen auferlegen.

§ 5 - Die Maßnahmen für die physische und logische Sicherheit der Netz- und Informationssysteme, die in dem in Artikel 13 des Gesetzes vom 1. Juli 2011 und Artikel 11 des Königlichen Erlasses vom 2. Dezember 2011 über die kritischen Infrastrukturen im Teilsektor des Luftverkehrs erwähnten Sicherheitsplan des Betreibers (SPB) aufgenommen sind, werden der S.P.I. gleichgesetzt, wenn dort alle in § 2 erwähnten Informationen aufgeführt sind.

Art. 22 - § 1 - Die in Artikel 21 § 1 erwähnte S.P.I. gilt bis zum Beweis des Gegenteils als den in Artikel 20 erwähnten Sicherheitsanforderungen entsprechend, wenn die Sicherheitsmaßnahmen, die sie umfasst, den Anforderungen der Norm ISO/IEC 27001 beziehungsweise einer nationalen, ausländischen oder internationalen Norm entspricht, die der König durch einen im Ministerrat beratenen Erlass als gleichwertig anerkennt.

Der in Absatz 1 erwähnte Erlass ergeht nach Stellungnahme der nationalen Akkreditierungsbehörde, der sektorspezifischen Behörde und der in Artikel 7 § 1 erwähnten Behörde.

§ 2 - Die Einhaltung der in § 1 erwähnten Anforderungen wird durch eine Bescheinigung nachgewiesen, die von einer Konformitätsbewertungsstelle ausgestellt wird, die gemäß der Norm ISO/IEC 17021 oder ISO/IEC 17065 von der nationalen Akkreditierungsbehörde oder einer Einrichtung akkreditiert ist, die Mitunterzeichner der Anerkennungsabkommen der "European Cooperation for Accreditation" ist.

Diese Bescheinigung muss sich auf den Zertifizierungsbereich beziehen, für den die Konformitätsbewertungsstelle akkreditiert ist, und den gesamten Inhalt der S.P.I. betreffen.

Art. 23 - § 1 - Betreiber wesentlicher Dienste bestimmen eine Anlaufstelle für die Sicherheit ihrer Netz- und Informationssysteme und übermitteln der zuständigen sektorspezifischen Behörde die diesbezüglichen Angaben, und zwar binnen drei Monaten nach Notifizierung ihrer Bestimmung als Betreiber wesentlicher Dienste und unverzüglich nach jeder Aktualisierung dieser Angaben.

Die sektorspezifische Behörde stellt diese Angaben den in Artikel 7 §§ 1 und 4 erwähnten Behörden zur Verfügung.

§ 2 - Wenn aufgrund nationaler oder internationaler Bestimmungen, die auf einen Sektor oder einen Teilsektor anwendbar sind, bereits eine Anlaufstelle im Bereich Sicherheit besteht, übermittelt der betreffende Betreiber wesentlicher Dienste der sektorspezifischen Behörde die entsprechenden Angaben binnen der in § 1 erwähnten Fristen.

§ 3 - Die in § 1 erwähnte Anlaufstelle für die Sicherheit von Netz- und Informationssystemen ist jederzeit verfügbar.

KAPITEL 3 — *Meldung von Sicherheitsvorfällen*

Art. 24 - § 1 - Betreiber wesentlicher Dienste melden unverzüglich alle Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität von Netz- und Informationssystemen haben, von denen der beziehungsweise die von ihnen bereitgestellten wesentlichen Dienste abhängen.

§ 2 - Nach Stellungnahme des nationalen CSIRT, der in Artikel 7 § 4 erwähnten Behörde, der sektorspezifischen Behörde und gegebenenfalls der betreffenden Regionen beziehungsweise Gemeinschaften kann der König pro Sektor oder Teilsektor Inzidenz- und/oder Schwellenwerte festlegen, die mindestens erhebliche Auswirkungen im Sinne von § 1 haben.

§ 3 - Sind keine Inzidenz- und/oder Schwellenwerte, wie in § 2 erwähnt, bestimmt, meldet der Betreiber alle Sicherheitsvorfälle, die Auswirkungen auf die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität von Netz- und Informationssystemen haben, von denen der beziehungsweise die von ihm bereitgestellten wesentlichen Dienste abhängen.

§ 4 - Der König kann je nach Ausmaß der Auswirkungen des Sicherheitsvorfalls verschiedene Meldekategorien bestimmen.

Art. 25 - Die in Artikel 24 erwähnte Meldung erfolgt gleichzeitig an das nationale CSIRT, die sektorspezifische Behörde beziehungsweise ihr sektorspezifisches CSIRT und die in Artikel 7 § 4 erwähnte Behörde.

Die Meldepflicht gilt selbst dann, wenn der Betreiber wesentlicher Dienste nur über einen Teil der relevanten Informationen verfügt, um zu bewerten, ob der Sicherheitsvorfall erhebliche Auswirkungen hat.

Art. 26 - § 1 - Vorliegendes Kapitel findet Anwendung auf Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU.

§ 2 - Betreiber, die zum Finanzsektor im Sinne von Anlage 1 zu vorliegendem Gesetz gehören, mit Ausnahme der Betreiber von Handelsplätzen, melden der Belgischen Nationalbank (BNB) unverzüglich alle Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität von Netz- und Informationssystemen haben, von denen der beziehungsweise die von ihnen bereitgestellten wesentlichen Dienste abhängen. Die Belgische Nationalbank bestimmt die in vorliegendem Absatz erwähnten erheblichen Auswirkungen.

Danach leitet die BNB die Meldung unverzüglich an das nationale CSIRT und die in Artikel 7 § 4 erwähnte Behörde weiter.

Art. 27 - Ein Unternehmen, das einem Betreiber wesentlicher Dienste einen digitalen Dienst bereitstellt und dem vorliegenden Gesetz unterliegt, meldet ihm unverzüglich alle Sicherheitsvorfälle, die im Sinne von Artikel 24 erhebliche Auswirkungen auf die Verfügbarkeit der von diesem Betreiber bereitgestellten wesentlichen Dienste haben.

Anschließend meldet der Betreiber wesentlicher Dienste den Vorfall gemäß den in vorliegendem Kapitel beschriebenen Verfahren.

Art. 28 - § 1 - Wenn ein Betreiber wesentlicher Dienste von einem Sicherheitsvorfall betroffen ist, der erhebliche Auswirkungen im Sinne von Artikel 24 hat, ist er verpflichtet, den Vorfall zu bewältigen und reaktive Maßnahmen zu seiner Behebung zu ergreifen.

Der Betreiber wesentlicher Dienste bleibt für die Bewältigung des Sicherheitsvorfalls verantwortlich.

§ 2 - Betreiber wesentlicher Dienste prüfen die Sicherheitsvorfälle oder verdächtigen Ereignisse, die ihnen von dem nationalen CSIRT, der sektorspezifischen Behörde oder der in Artikel 7 § 4 erwähnten Behörde gemeldet werden.

Art. 29 - Auf der Grundlage der in der Meldung durch den Betreiber wesentlicher Dienste bereitgestellten Informationen unterrichtet das nationale CSIRT die anderen betroffenen Mitgliedstaaten der Europäischen Union, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesen Mitgliedstaaten hat.

Dabei wahrt das nationale CSIRT im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Betreibers wesentlicher Dienste sowie die Vertraulichkeit der in dessen Meldung bereitgestellten Informationen.

Das nationale CSIRT leitet die in Absatz 1 erwähnten Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

Art. 30 - § 1 - Potenzielle Betreiber wesentlicher Dienste können auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen in Belgien bereitgestellten Dienste haben.

Eine freiwillige Meldung darf nicht dazu führen, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte.

§ 2 - Bei der Bearbeitung von Meldungen können das nationale CSIRT, die sektorspezifische Behörde beziehungsweise ihr sektorspezifisches CSIRT und die in Artikel 7 § 4 erwähnte Behörde die durch vorliegendes Gesetz auferlegten Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten.

Freiwillige Meldungen werden nur bearbeitet, wenn diese Bearbeitung keinen unverhältnismäßigen oder unzumutbaren Aufwand für das nationale CSIRT, die sektorspezifische Behörde beziehungsweise ihr sektorspezifisches CSIRT und die in Artikel 7 § 4 erwähnte Behörde darstellt.

Art. 31 - § 1 - Der König ist damit beauftragt, die Modalitäten für die Meldung von Sicherheitsvorfällen und die diesbezügliche Berichterstattung zu bestimmen und eine gesicherte Meldeplattform zu schaffen.

Über diese Plattform können Betreiber wesentlicher Dienste den Aufsichtsbehörden ebenfalls Verletzungen des Schutzes personenbezogener Daten melden, wie durch Artikel 33 Absatz 1 der Verordnung EU 2016/679 auferlegt.

§ 2 - Nach Anhörung des meldenden Betreibers und der zuständigen sektorspezifischen Behörde kann das nationale CSIRT die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist. Diese Unterrichtung betrifft ausschließlich allgemeine Informationen über den Sicherheitsvorfall.

TITEL 3 — *Netz- und Informationssysteme der Anbieter digitaler Dienste*

KAPITEL 1 — *Anwendungsbereich*

Art. 32 - Vorliegender Titel findet keine Anwendung auf Kleinstunternehmen und kleine Unternehmen, wie in der Empfehlung der Europäischen Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2006/361/EG) bestimmt.

KAPITEL 2 — *Sicherheitsanforderungen*

Art. 33 - § 1 - Anbieter digitaler Dienste ermitteln die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung der in Anlage 2 aufgeführten Dienste innerhalb der Union nutzen, und ergreifen geeignete und verhältnismäßige technische und organisatorische Maßnahmen, um diese Risiken zu bewältigen.

Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Business Continuity Management,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

§ 2 - Anbieter digitaler Dienste treffen ebenfalls Maßnahmen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit ihrer Netz- und Informationssysteme beeinträchtigen, auf die in Anlage 2 zu vorliegendem Gesetz erwähnten, innerhalb der Europäischen Union erbrachten Dienste vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

Art. 34 - Anbieter digitaler Dienste bestimmen eine Anlaufstelle für die IT-Sicherheit und übermitteln der für die Anbieter digitaler Dienste zuständigen sektorspezifischen Behörde die diesbezüglichen Angaben sowie nach jeder Aktualisierung dieser Angaben. Die sektorspezifische Behörde leitet diese Informationen an die in Artikel 7 § 1 erwähnte nationale Behörde weiter.

KAPITEL 3 — *Meldung von Sicherheitsvorfällen*

Art. 35 - § 1 - Anbieter digitaler Dienste melden unverzüglich jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines der in Anlage 2 erwähnten, von ihnen innerhalb der Europäischen Union erbrachten Dienste hat.

Die Meldung erfolgt gleichzeitig an das nationale CSIRT, die sektorspezifische Behörde beziehungsweise ihr sektorspezifisches CSIRT und die in Artikel 7 § 4 erwähnte Behörde, und zwar über die in Artikel 31 erwähnte Meldeplattform.

§ 2 - Die Meldung erfolgt gemäß den Durchführungsverordnungen der Europäischen Kommission, unter anderem der Durchführungsverordnung (EU) 2018/151 vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls.

Die Meldungen müssen die Informationen enthalten, die es ermöglichen, das Ausmaß etwaiger grenzübergreifender Auswirkungen des Sicherheitsvorfalls festzustellen. Mit der Meldung wird keine höhere Haftung der meldenden Partei begründet.

§ 3 - Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu den Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls vollständig oder teilweise zu bewerten.

Art. 36 - § 1 - Diese Meldung erfolgt gemäß den vom König vorgesehenen Modalitäten und über die in Artikel 31 erwähnte Plattform.

§ 2 - Über die in Artikel 31 erwähnte Plattform können Anbieter digitaler Dienste den Aufsichtsbehörden ebenfalls Verletzungen des Schutzes personenbezogener Daten melden, wie durch Artikel 33 Absatz 1 der Verordnung EU 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr auferlegt.

Art. 37 - § 1 - Gegebenenfalls und insbesondere, wenn der in Artikel 35 § 1 erwähnte Sicherheitsvorfall mindestens einen anderen Mitgliedstaat der Europäischen Union betrifft, unterrichtet das nationale CSIRT den beziehungsweise die anderen betroffenen Mitgliedstaaten. Dabei wahrt das nationale CSIRT im Einklang mit dem nationalen Recht und dem Unionsrecht die Sicherheit und das wirtschaftliche Interesse des Anbieters digitaler Dienste sowie die Vertraulichkeit der bereitgestellten Informationen.

§ 2 - Nach Anhörung des betreffenden Anbieters digitaler Dienste, der sektorspezifischen Behörde und gegebenenfalls der Behörden oder der CSIRTs anderer betroffener Mitgliedstaaten der Europäischen Union kann das nationale CSIRT die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt. Diese Unterrichtung kann insbesondere erforderlich sein, wenn die Sensibilisierung der Öffentlichkeit die Verhütung von Sicherheitsvorfällen oder die Bewältigung aktueller Sicherheitsvorfälle ermöglicht oder wenn die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

TITEL 4 — *Kontrolle und Sanktionen*

KAPITEL 1 — *Kontrolle der Betreiber wesentlicher Dienste*

Abschnitt 1 — Audits

Art. 38 - § 1 - Betreiber wesentlicher Dienste führen jährlich und auf eigene Kosten ein internes Audit über die Netz- und Informationssysteme durch, von denen die von ihnen bereitgestellten wesentlichen Dienste abhängen. Durch dieses interne Audit müssen sie sich vergewissern können, dass die in ihrer S.P.I. bestimmten Maßnahmen und Abläufe richtig angewandt werden und regelmäßigen Kontrollen unterliegen.

Die Berichte über interne Audits übermitteln die Betreiber wesentlicher Dienste binnen dreißig Tagen der sektorspezifischen Behörde.

§ 2 - Betreiber wesentlicher Dienste lassen mindestens alle drei Jahre und auf eigene Kosten von einer Konformitätsbewertungsstelle, die von der nationalen Akkreditierungsbehörde oder einer Einrichtung akkreditiert ist, die Mitunterzeichner der Anerkennungsabkommen der "European Cooperation for Accreditation" ist, ein externes Audit durchführen.

Die Berichte über externe Audits übermitteln die Betreiber wesentlicher Dienste binnen dreißig Tagen der sektorspezifischen Behörde.

§ 3 - Spätestens drei Monate nach Ausarbeitung ihrer S.P.I. führen Betreiber wesentlicher Dienste ihr erstes internes Audit durch. Ihr erstes externes Audit führen sie spätestens vierundzwanzig Monate nach Durchführung ihres ersten internen Audits durch.

Art. 39 - § 1 - Nach Stellungnahme der sektorspezifischen Behörde und der in Artikel 7 § 1 erwähnten Behörde bestimmt der König:

1. die allgemeinen Akkreditierungsbedingungen auf der Grundlage der Anforderungen der Normen ISO/IEC 17021 oder 17065,
2. die zusätzlichen sektorspezifischen Anforderungen, denen die Konformitätsbewertungsstelle unterliegen kann,
3. die für das interne Audit geltenden Regeln,
4. die für das externe Audit geltenden Regeln.

§ 2 - Durch einen im Ministerrat beratenen Erlass sowie nach Stellungnahme der sektorspezifischen Behörde und der in Artikel 7 § 1 erwähnten Behörde kann der König ebenfalls die Bedingungen für eine eventuelle Zulassung festlegen, die die sektorspezifische Behörde einer Konformitätsbewertungsstelle erteilt.

§ 3 - Die Liste der akkreditierten beziehungsweise zugelassenen Konformitätsbewertungsstellen ist bei der sektorspezifischen Behörde verfügbar, die sie fortschreibt.

Art. 40 - § 1 - Zertifizierungsaudits können vom Inspektionsdienst oder von der sektorspezifischen Behörde dem in Artikel 39 § 1 erwähnten obligatorischen internen Audit, das jährlich durchzuführen ist, gleichgesetzt werden. Die Berichte über diese Audits übermitteln die Betreiber wesentlicher Dienste binnen dreißig Tagen der sektorspezifischen Behörde.

§ 2 - Zertifizierungsaudits können vom Inspektionsdienst oder von der sektorspezifischen Behörde dem in Artikel 39 § 2 erwähnten obligatorischen externen Audit gleichgesetzt werden. Die Berichte über diese Audits übermitteln die Betreiber wesentlicher Dienste binnen dreißig Tagen der sektorspezifischen Behörde.

Art. 41 - Die in Artikel 7 § 1 erwähnte Behörde kann bei der sektorspezifischen Behörde beziehungsweise dem Inspektionsdienst einen mit Gründen versehenen Antrag auf Übermittlung der Zertifizierungs- beziehungsweise Auditberichte eines Betreibers wesentlicher Dienste einreichen.

Abschnitt 2 — Inspektionsdienst

Art. 42 - § 1 - Inspektionsdienste können jederzeit Kontrollen im Bereich Einhaltung der Sicherheitsmaßnahmen und der Regeln zur Meldung von Sicherheitsvorfällen durch die Betreiber wesentlicher Dienste vornehmen.

§ 2 - Die in Artikel 7 § 1 erwähnte Behörde beziehungsweise die sektorspezifische Behörde kann einem Inspektionsdienst mit entsprechender Begründung die Durchführung von Kontrollen empfehlen.

Nach Stellungnahme der sektorspezifischen Behörde und der in Artikel 7 § 1 erwähnten Behörde kann der König die eventuellen sektorspezifischen praktischen Kontrollmodalitäten festlegen.

§ 3 - Bei der Anforderung von Informationen oder Nachweisen nennt der Inspektionsdienst den Zweck des Ersuchens und gibt an, binnen welcher Frist die Informationen oder Nachweise übermittelt werden müssen.

Der Inspektionsdienst kann Sachverständige hinzuziehen.

Art. 43 - Wenn sich die Netz- und Informationssysteme eines Betreibers wesentlicher Dienste außerhalb des belgischen Staatsgebiets befinden, kann der Inspektionsdienst in Absprache mit der in Artikel 7 § 1 erwähnten Behörde die zuständigen Aufsichtsbehörden dieser anderen Staaten um Zusammenarbeit und Unterstützung ersuchen. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch und das Ersuchen umfassen, Überwachungsmaßnahmen zu ergreifen.

Art. 44 - § 1 - Die Mitglieder des Inspektionsdienstes verfügen über eine Legitimationskarte, deren Muster der König pro Sektor oder gegebenenfalls pro Teilsektor festlegt.

§ 2 - Die Mitglieder des Inspektionsdienstes oder die Sachverständigen, die für die Inspektion hinzugezogen werden, dürfen in den 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.

§ 3 - Unbeschadet der in Artikel 8 des Strafprozessgesetzbuches vorgesehenen Zuständigkeiten der Gerichtspolizeioffiziere verfügen die vereidigten Mitglieder des Inspektionsdienstes bei der Ausführung ihres Auftrags sowohl im Rahmen von Verwaltungshandlungen als auch im Rahmen der Feststellung von Verstößen mittels Protokoll jederzeit über folgende Kontrollbefugnisse:

1. ohne vorherige Ankündigung auf Vorlage ihrer Legitimationskarte alle Orte betreten, die der Betreiber wesentlicher Dienste nutzt; zu bewohnten Räumlichkeiten haben sie nur Zugang mit der vorherigen Ermächtigung des Untersuchungsrichters,
2. vor Ort die S.P.I., Auditberichte und alle für die Ausführung ihres Auftrags notwendigen Urkunden, Unterlagen und anderen Informationsquellen einsehen und eine Kopie davon erhalten,
3. alle Untersuchungen, Kontrollen und Vernehmungen vornehmen und alle Informationen anfordern, die sie für die Ausübung ihres Auftrags für notwendig erachten,
4. die Personalien der Personen aufnehmen, die sich an den Orten, die der Betreiber wesentlicher Dienste nutzt, befinden und deren Vernehmung sie für die Ausführung ihres Auftrags für notwendig erachten. Zu diesem Zweck können sie von diesen Personen die Vorlegung offizieller Identifizierungsdokumente fordern,
5. die Unterstützung der Dienste der föderalen oder lokalen Polizei anfordern,
6. bei den in Artikel 9 des Gesetzes vom 15. April 1994 erwähnten Personalmitgliedern Informationen zur Ausführung der Bestimmungen des vorliegenden Gesetzes und des Gesetzes vom 1. Juli 2011 anfordern.

§ 4 - Um eine Ermächtigung zum Betreten bewohnter Räumlichkeiten zu erhalten, richten die Personalmitglieder des Inspektionsdienstes einen mit Gründen versehenen Antrag an den Untersuchungsrichter. Dieser Antrag enthält mindestens:

1. die Angabe der bewohnten Räumlichkeiten, zu denen die Personalmitglieder des Inspektionsdienstes beziehungsweise der sektorspezifischen Behörde 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 48 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 kann gegen die Verweigerungsentscheidung oder das Ausbleiben einer Entscheidung binnen 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.

§ 5 - 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 belasten zu müssen.

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.

Die Personalmitglieder des Inspektionsdienstes, die eine Person befragen, informieren sie darüber, dass sie eine Kopie des Textes ihrer Vernehmung beantragen darf. Diese Kopie wird ihr kostenlos ausgehändigt.

§ 6 - Die Mitglieder des 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 die Mitglieder des Inspektionsdienstes das Datenverarbeitungssystem und die darin enthaltenen Daten gegen Empfangsbestätigung mit Beschlagnahmeverzeichnis beschlagnahmen.

§ 7 - Um die auf der Grundlage von § 6 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 einen Untersuchungsrichter darum ersuchen einzugreifen.

Art. 45 - § 1 - Nach jeder Inspektion erstellen die Mitglieder des Inspektionsdienstes einen Bericht und übermitteln dem inspizierten Betreiber wesentlicher Dienste und der zuständigen sektorspezifischen Behörde eine Kopie davon.

§ 2 - Die in Artikel 7 § 1 erwähnte Behörde und die sektorspezifische Behörde können bei dem Inspektionsdienst einen mit Gründen versehenen Antrag auf Übermittlung seiner Inspektionsberichte einreichen.

Art. 46 - § 1 - Der betreffende Betreiber wesentlicher Dienste gewährt den Mitgliedern des Inspektionsdienstes bei der Ausübung ihrer Aufgaben seine volle Mitwirkung, insbesondere um sie bestmöglich über alle bestehenden Sicherheitsmaßnahmen zu informieren.

Falls erforderlich stellt der Betreiber wesentlicher Dienste den Mitgliedern des Inspektionsdienstes oder der sektorspezifischen Behörde das erforderliche Sicherheitsmaterial zur Verfügung, damit sie die Sicherheitsvorschriften bei den Inspektionen einhalten können.

§ 2 - Für jeden Sektor oder Teilsektor kann der König durch einen im Ministerrat beratenen Erlass und nach Stellungnahme der sektorspezifischen Behörde Gebühren für Inspektionsleistungen bestimmen. Diese Gebühren gehen zu Lasten der Betreiber wesentlicher Dienste. Der König legt die Berechnungs- und Zahlungsmodalitäten fest.

KAPITEL 2 — *Kontrolle der Anbieter digitaler Dienste*

Art. 47 - § 1 - Die praktischen Modalitäten für die Kontrolle der Anbieter digitaler Dienste werden vom König festgelegt.

§ 2 - Anbieter digitaler Dienste sind insbesondere verpflichtet:

a) dem zuständigen Inspektionsdienst binnen der gesetzten Frist die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der nachweislichen Maßnahmen ihrer Sicherheitspolitik, zur Verfügung zu stellen,

b) bei jedem Fall von Nichteinhaltung der Sicherheitsanforderungen und der Anforderungen in Sachen Meldung von Sicherheitsvorfällen Abhilfe zu schaffen.

§ 3 - Gemäß den vom König festgelegten Regeln kann der Inspektionsdienst erforderlichenfalls im Wege von Ex-post-Überwachungsmaßnahmen tätig werden, wenn ihm Nachweise dafür vorgelegt werden, dass ein Anbieter digitaler Dienste die Sicherheitsanforderungen beziehungsweise die Anforderungen in Sachen Meldung von Sicherheitsvorfällen nicht einhält. Derartige Nachweise können von der zuständigen Behörde eines anderen Mitgliedstaats der Europäischen Union, in dem der Dienst bereitgestellt wird, vorgelegt werden.

§ 4 - Im Rahmen seiner Ex-Post-Kontrollen hat der Inspektionsdienst dieselben Befugnisse, wie in Artikel 44 vorgesehen.

§ 5 - Hat ein Anbieter digitaler Dienste seine Hauptniederlassung oder einen Vertreter in Belgien, aber seine Netz- und Informationssysteme befinden sich in einem oder mehreren anderen Staaten, so kann der Inspektionsdienst in Absprache mit der in Artikel 7 § 1 erwähnten Behörde die zuständigen Aufsichtsbehörden dieser anderen Staaten um Zusammenarbeit und Unterstützung ersuchen. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch und das Ersuchen umfassen, Überwachungsmaßnahmen zu ergreifen.

§ 6 - Gemäß den vom König festgelegten Regeln kann der Inspektionsdienst die in vorliegendem Artikel vorgesehenen Befugnisse ebenfalls auf Ersuchen der zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union ausüben.

§ 7 - Die in Artikel 7 § 1 erwähnte Behörde kann beim Inspektionsdienst die Übermittlung der Inspektionsberichte in Bezug auf einen Anbieter digitaler Dienste beantragen.

§ 8 - Der König kann durch einen im Ministerrat beratenen Erlass und nach Stellungnahme der sektorspezifischen Behörde Gebühren für Kontrollleistungen bestimmen. Diese Gebühren gehen zu Lasten der Anbieter digitaler Dienste. Der König legt die Berechnungs- und Zahlungsmodalitäten fest.

KAPITEL 3 — *Sanktionen*

Abschnitt 1 — Verfahren

Art. 48 - § 1 - Werden ein oder mehrere Fälle von Nichteinhaltung der Anforderungen festgestellt, die durch das Gesetz, seine Ausführungserlasse oder individuelle diesbezügliche Verwaltungsbeschlüsse auferlegt werden, so setzt der Inspektionsdienst den betreffenden Betreiber wesentlicher Dienste beziehungsweise Anbieter digitaler Dienste in Verzug und fordert ihn auf, seinen Verpflichtungen binnen einer vom Inspektionsdienst festzulegenden Frist nachzukommen.

Die Frist wird unter Berücksichtigung der Betriebsbedingungen des Betreibers wesentlicher Dienste beziehungsweise des Anbieters digitaler Dienste und der zu ergreifenden Maßnahmen bestimmt.

§ 2 - Der Inspektionsdienst informiert den Zuwiderhandelnden vorab unter Angabe von Gründen über seine Absicht, ihm eine Inverzugsetzung zu übermitteln, und weist ihn auf sein Recht hin, binnen fünfzehn Tagen ab Erhalt dieser Information schriftlich seine Verteidigungsmittel einzureichen oder um Anhörung zu ersuchen. Es wird davon ausgegangen, dass der Zuwiderhandelnde die Information am sechsten Tag nach ihrer Versendung durch den Inspektionsdienst erhalten hat.

§ 3 - Auf der Grundlage der ihr zur Verfügung stehenden Sachverhalte kann die in Artikel 7 § 1 erwähnte Behörde dem Inspektionsdienst mit entsprechender Begründung ebenfalls empfehlen, einen Betreiber wesentlicher Dienste beziehungsweise Anbieter digitaler Dienste in Verzug zu setzen.

Art. 49 - § 1 - Stellt der Inspektionsdienst fest, dass der Betreiber wesentlicher Dienste beziehungsweise der Anbieter digitaler Dienste der Inverzugsetzung nicht fristgerecht nachgekommen ist, wird der Sachverhalt in einem von den vereidigten Mitgliedern des Inspektionsdienstes erstellten Protokoll festgehalten. Dieses Protokoll wird der zuständigen sektorspezifischen Behörde übermittelt.

§ 2 - Die Tatsache, dass jemand die Ausführung einer Kontrolle durch die Mitglieder des 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 in einem Protokoll festgehalten.

§ 3 - Die Paragraphen 1 und 2 finden ebenfalls Anwendung auf potenzielle Betreiber wesentlicher Dienste oder Betreiber einer kritischen Infrastruktur, die der in Artikel 14 oder 18 § 3 erwähnten Informationspflicht nicht nachkommen.

§ 4 - Die von den vereidigten Mitgliedern des Inspektionsdienstes erstellten Protokolle haben Beweiskraft bis zum Beweis des Gegenteils.

Art. 50 - Verstöße gegen das vorliegende Gesetz oder seine Ausführungserlasse können mit strafrechtlichen Sanktionen oder Verwaltungssanktionen geahndet werden.

Abschnitt 2 — Strafrechtliche Sanktionen

Art. 51 - § 1 - Mit einer Gefängnisstrafe von acht Tagen bis zu einem Jahr und einer Geldbuße von 26 bis zu 20.000 EUR oder mit nur einer dieser Strafen wird belegt, wer einer der in Artikel 24 oder 35 erwähnten Verpflichtungen in Sachen Meldung von Sicherheitsvorfällen nicht nachkommt.

§ 2 - Mit einer Gefängnisstrafe von acht Tagen bis zu einem Jahr und einer Geldbuße von 26 bis zu 30.000 EUR oder mit nur einer dieser Strafen wird belegt, wer einer der Sicherheitsverpflichtungen, die der König oder die sektorspezifische Behörde aufgrund von Artikel 21 oder 33 auferlegt, nicht nachkommt.

§ 3 - Mit einer Gefängnisstrafe von acht Tagen bis zu einem Jahr und einer Geldbuße von 26 bis zu 50.000 EUR oder mit nur einer dieser Strafen wird belegt, wer einer der in Titel 4 Kapitel 1 und 2 erwähnten Kontrollpflichten nicht nachkommt.

§ 4 - Mit einer Gefängnisstrafe von acht Tagen bis zu einem Jahr und einer Geldbuße von 26 bis zu 50.000 EUR oder mit nur einer dieser Strafen wird belegt, wer einer der in Artikel 14 oder 18 § 3 erwähnten Informationspflichten nicht nachkommt.

§ 5 - Mit einer Gefängnisstrafe von acht Tagen bis zu zwei Jahren und einer Geldbuße von 26 bis zu 75.000 EUR oder mit nur einer dieser Strafen wird belegt, wer die Ausführung der Kontrolle durch die Mitglieder des Inspektionsdienstes vorsätzlich verhindert oder behindert, sich weigert, die anlässlich dieser Kontrolle von ihm verlangten Informationen zu übermitteln, oder wissentlich falsche oder unvollständige Angaben macht.

§ 6 - Bei Rückfälligkeit aufgrund der gleichen Verstöße binnen einer Frist von drei Jahren wird die Geldbuße verdoppelt und der Zuwiderhandelnde wird mit einer Gefängnisstrafe von fünfzehn Tagen bis zu drei Jahren belegt.

§ 7 - Die Bestimmungen von Buch I des Strafgesetzbuches einschließlich Kapitel VII und Artikel 85 finden Anwendung auf die in vorliegendem Artikel erwähnten Verstöße.

Die Artikel 269 bis 274 und 276 des Strafgesetzbuches sind anwendbar auf Mitglieder des Inspektionsdienstes, die in Rahmen der Ausübung ihrer Aufgaben handeln.

§ 8 - Verstöße gegen Artikel 9 §§ 2 und 3 des vorliegenden Gesetzes werden mit den in Artikel 458 des Strafgesetzbuches vorgesehenen Strafen geahndet.

Abschnitt 3 — Verwaltungssanktionen

Art. 52 - § 1 - Jeder Verstoß gegen das vorliegende Gesetz, seine Ausführungserlasse oder aufgrund dieses Gesetzes gefasste Verwaltungsbeschlüsse kann mit einer Verwaltungssanktion geahndet werden.

§ 2 - Mit einer Geldbuße von 500 bis zu 75.000 EUR wird belegt, wer den in Artikel 24 oder 35 erwähnten Verpflichtungen in Sachen Meldung von Sicherheitsvorfällen nicht nachkommt.

§ 3 - Mit einer Geldbuße von 500 bis zu 100.000 EUR wird belegt, wer den Sicherheitsverpflichtungen, die der König oder die sektorspezifische Behörde aufgrund von Artikel 21 oder 33 auferlegt, nicht nachkommt.

§ 4 - Mit einer Geldbuße von 500 bis zu 125.000 EUR wird belegt, wer den in Artikel 14 oder 18 § 3 erwähnten Informationspflichten nicht nachkommt.

§ 5 - Mit einer Geldbuße von 500 bis zu 200.000 EUR wird belegt, wer den in Titel 4 Kapitel 1 und 2 erwähnten Kontrollpflichten nicht nachkommt.

§ 6 - Jede Handlung, durch die eine Person, die im Namen eines Betreibers wesentlicher Dienste oder eines Anbieters digitaler Dienste handelt, nachteilige Folgen dadurch erfährt, dass sie in gutem Glauben und im Rahmen ihrer Aufgaben die sich aus vorliegendem Gesetz ergebenden Verpflichtungen erfüllt, wird mit einer Geldbuße von 500 bis zu 200.000 EUR geahndet.

Art. 53 - Der Inspektionsdienst übermittelt dem Prokurator des Königs das Original des Protokolls.

Gleichzeitig wird dem Zuwiderhandelnden eine Kopie des Protokolls zugestellt.

Art. 54 - Ab dem Tag des Empfangs des Protokolls verfügt der Prokurator des Königs über eine zweimonatige Frist, um die sektorspezifische Behörde davon in Kenntnis zu setzen, dass eine Strafverfolgung eingeleitet worden ist.

Die sektorspezifische Behörde darf das Verfahren zur Auferlegung einer administrativen Geldbuße nicht vor Ablauf der vorerwähnten Frist einleiten, außer wenn der Prokurator des Königs vorher mitteilt, dass er die Tat nicht weiterverfolgt.

Falls der Prokurator des Königs es versäumt, seine Entscheidung binnen der festgelegten Frist zu notifizieren, oder auf eine Strafverfolgung verzichtet, kann die sektorspezifische Behörde beschließen, das Verwaltungsverfahren einzuleiten.

Art. 55 - § 1 - Der Beschluss, eine administrative Geldbuße aufzuerlegen, wird mit Gründen versehen. Der Betrag der administrativen Geldbuße und die erwähnten Verstöße werden ebenfalls darin vermerkt.

§ 2 - Die sektorspezifische Behörde übermittelt dem Zuwiderhandelnden vorab ihren mit Gründen versehenen Vorschlag einer Verwaltungssanktion und weist ihn auf sein Recht hin, binnen fünfzehn Tagen ab Erhalt dieses Vorschlags schriftlich seine Verteidigungsmittel einzureichen oder um Anhörung zu ersuchen. Es wird davon ausgegangen, dass der Zuwiderhandelnde den Vorschlag am sechsten Tag nach seiner Versendung durch die sektorspezifische Behörde erhalten hat.

§ 3 - Unter Berücksichtigung der Verteidigungsmittel, die binnen der in § 2 erwähnten Frist vorgebracht worden sind, oder wenn der Zuwiderhandelnde binnen dieser selben Frist nicht reagiert, kann die sektorspezifische Behörde eine in Artikel 52 erwähnte Verwaltungssanktion auferlegen.

§ 4 - Die administrative Geldbuße steht im Verhältnis zu der Schwere, der Dauer, den eingesetzten Mitteln, dem verursachten Schaden und den Umständen der Verstöße.

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

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

Art. 56 - Der Beschluss wird dem Zuwiderhandelnden per Einschreiben notifiziert.

Dem Beschluss wird eine Aufforderung zur Zahlung der Geldbuße binnen einer einmonatigen Frist beigefügt.

Art. 57 - Der Zuwiderhandelnde kann den Beschluss der sektorspezifischen Behörde vor dem in Artikel 101 des Gerichtsgesetzbuches erwähnten Märktegerichtshof anfechten.

Zur Vermeidung des Verfalls werden Klagen binnen sechzig Tagen nach Notifizierung des Beschlusses der sektorspezifischen Behörde durch kontradiktorische Antragschrift eingereicht.

Die Sache wird wie im Eilverfahren gemäß den Artikeln 1035 bis 1038, 1040 und 1041 des Gerichtsgesetzbuches behandelt.

Durch diese Beschwerde wird die Ausführung des Beschlusses nicht ausgesetzt.

Art. 58 - § 1 - Versäumt es der Zuwiderhandelnde, die administrative Geldbuße innerhalb der vorgegebenen Frist zu bezahlen, ist der Beschluss zur Auferlegung einer administrativen Geldbuße vollstreckbar und kann die sektorspezifische Behörde einen Zwangsbefehl erlassen.

Zwangsbefehle werden von dem gesetzlichen Vertreter der 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 vierundzwanzig Stunden zu zahlen, sowie 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 der Zustellung des Zwangsbefehls durch eine Ladung an die 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 Schuldforderung aus, bis über die Begründetheit des Einspruchs befunden worden ist. Die bereits zu einem früheren Zeitpunkt durchgeführten Pfändungen behalten ihre sichernde Wirkung.

§ 4 - Die 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 - Die Kosten für die Zustellung des Zwangsbefehls und die 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. 59 - Die sektorspezifische Behörde kann nach Ablauf einer Frist von drei Jahren ab dem Tag, an dem die Tat begangen worden ist, keine administrative Geldbuße auferlegen.

Mit der Zahlung gemäß dem Verwaltungsverfahren erlischt zudem die Möglichkeit, eine Strafverfolgung wegen der erwähnten Taten einzuleiten.

TITEL 5 — *CSIRT*

KAPITEL 1 — *Nationales CSIRT*

Abschnitt 1 — Aufgaben des nationalen CSIRT

Art. 60 - Die Aufgaben des nationalen CSIRT umfassen mindestens Folgendes:

a) Überwachung von Sicherheitsvorfällen auf nationaler und internationaler Ebene, einschließlich Verarbeitung personenbezogener Daten im Zusammenhang mit der Überwachung solcher Vorfälle,

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interesse habenden Parteien,

c) Reaktion auf Sicherheitsvorfälle,

d) dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung,

e) Erkennung, Beobachtung und Analyse von IT-Sicherheitsproblemen,

f) Förderung der Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken sowie für Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen,

g) Aufbau von Kooperationsbeziehungen zum Privatsektor sowie zu anderen Verwaltungsdiensten oder öffentlichen Behörden,

h) Beteiligung an dem in Artikel 12 der NIS-Richtlinie erwähnten CSIRT-Netzwerk.

Nach Stellungnahme des nationalen CSIRT kann der König diesem CSIRT zusätzliche Aufgaben anvertrauen.

Abschnitt 2 — Anforderungen an das nationale CSIRT

Art. 61 - Die Anforderungen an das nationale CSIRT umfassen mindestens Folgendes:

a) Gewährleistung eines hohen Grades der Verfügbarkeit seiner Kommunikationsdienste, indem es punktuellen Ausfällen vorbeugt und mehrere Kanäle bereitstellt, damit es jederzeit erreichbar bleibt und selbst Kontakt aufnehmen kann,

b) Verfügbarkeit von Räumlichkeiten und Informationssystemen an sicheren Standorten,

c) Gewährleistung der Betriebskontinuität mit einem geeigneten System zur Verwaltung und Weiterleitung von Anfragen, um Übergaben zu erleichtern,

d) Beteiligung an Versammlungen des in Artikel 12 der NIS-Richtlinie erwähnten CSIRT-Netzwerks,

e) Stützung auf eine Infrastruktur, deren Verfügbarkeit sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen,

f) Sicherstellung, dass seine Kommunikationskanäle genau spezifiziert und seinen Partnern wohlbekannt sind.

Art. 62 - Im Rahmen der Ausübung seiner Befugnisse ergreift das nationale CSIRT alle geeigneten Maßnahmen, um die in den Artikeln 60 und 61 bestimmten Ziele umzusetzen. Diese Maßnahmen müssen in einem angemessenen Verhältnis zu den Zielen stehen und die Grundsätze der Objektivität, Transparenz und Nichtdiskriminierung beachten.

Um diese Ziele zu erreichen, darf das nationale CSIRT alle verfügbaren Informationen für sich behalten, 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.

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.

Die leitenden Beamten des nationalen CSIRT gewährleisten die Einhaltung der in vorliegendem Artikel erwähnten Bedingungen. Dazu werden interne Verfahren ausgearbeitet.

KAPITEL 2 — *Sektorspezifisches CSIRT*

Abschnitt 1 — Aufgaben des sektorspezifischen CSIRT

Art. 63 - Die Aufgaben eines sektorspezifischen CSIRT umfassen in Zusammenarbeit mit dem nationalen CSIRT mindestens Folgendes:

a) Überwachung sektorspezifischer Sicherheitsvorfälle,

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interesse habenden Parteien des Sektors,

c) Reaktion auf sektorspezifische Sicherheitsvorfälle,

d) dynamische Analyse von sektorspezifischen Risiken und Vorfällen und Lagebeurteilung,

e) Aufbau von Kooperationsbeziehungen zu den Betreibern seines Sektors,

f) mögliche Beteiligung an Versammlungen des in Artikel 12 der NIS-Richtlinie erwähnten CSIRT-Netzwerks, die seinen Sektor betreffen.

Nach Stellungnahme des sektorspezifischen CSIRT kann der König diesem CSIRT zusätzliche Aufgaben anvertrauen.

Abschnitt 2 — Anforderungen an ein sektorspezifisches CSIRT

Art. 64 - Die Anforderungen an ein sektorspezifisches CSIRT umfassen Folgendes:

a) Gewährleistung eines hohen Grades der Verfügbarkeit seiner Kommunikationskanäle, indem es punktuellen Ausfällen vorbeugt und mehrere Kanäle bereitstellt, damit es jederzeit erreichbar bleibt und selbst Kontakt aufnehmen kann,

b) Verfügbarkeit von Räumlichkeiten und Informationssystemen an sicheren Standorten,

c) Gewährleistung der Betriebskontinuität mit einem geeigneten System zur Verwaltung und Weiterleitung von Anfragen, um Übergaben zu erleichtern,

d) Stützung auf eine Infrastruktur, deren Verfügbarkeit sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen,

f) Sicherstellung, dass seine Kommunikationskanäle genau spezifiziert und seinen Partnern wohlbekannt sind.

TITEL 6 — *Verarbeitung personenbezogener Daten*

KAPITEL 1 — *Grundsätze in Sachen Verarbeitung, Rechtsgrundlage und Zwecke*

Art. 65 - § 1 - Gemäß Artikel 5 Absatz 1 Buchstabe c der Verordnung EU 2016/679 gewährleistet der für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten im Rahmen der Ausführung des vorliegenden Gesetzes, dass die Verarbeitung auf das notwendige Maß beschränkt bleibt und dem verfolgten Zweck angemessen ist.

§ 2 - In Übereinstimmung mit diesem Grundsatz können die verarbeiteten personenbezogenen Daten alle Arten von Daten in Bezug auf die Sicherheit von Netz- und Informationssystemen sein, das heißt gegebenenfalls namentliche Informationen, Daten über Mitarbeiter einer Organisation oder externe Personen, Verbindungsdaten oder -kennungen, Geolokalisierungsdaten, Identifizierungs- oder Authentifizierungsdaten, gegebenenfalls mithilfe gesicherter Systeme.

§ 3 - Die wichtigsten Verarbeitungen personenbezogener Daten im Rahmen des vorliegenden Gesetzes können wie folgt zusammengefasst werden:

— allgemeiner Informationsaustausch zwischen den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste einerseits und den in Artikel 7 erwähnten Behörden andererseits,

— Verarbeitung spezifischer Informationen zwischen den im ersten Gedankenstrich erwähnten Einrichtungen im Rahmen der Meldung von Sicherheitsvorfällen oder eines anderen spezifischen Austauschs,

— Verarbeitung durch die Inspektionsdienste gemäß Titel 4,

— Verarbeitung durch Gerichtshöfe und Gerichte oder sektorspezifische Behörden im Rahmen der Umsetzung des Gesetzes und insbesondere der Ermittlung, Verfolgung und Ahndung von Verstößen,

— Austausch und sonstige Verarbeitung von Informationen durch das nationale und das sektorspezifische CSIRT im Rahmen ihrer in den Artikeln 60 bis 62 beziehungsweise 63 und 64 erwähnten Aufträge.

Art. 66 - § 1 - Sofern möglich werden die verarbeiteten Daten pseudonymisiert beziehungsweise aggregiert, sodass das Risiko vermindert wird, personenbezogene Daten auf eine Weise zu verwenden, die mit der Verordnung EU 2016/679 oder den Gesetzen und Verordnungen, die diese Verordnung ergänzen oder näher bestimmen, unvereinbar ist.

§ 2 - Die besonderen Datenkategorien im Sinne der Artikel 9 und 10 der Verordnung EU 2016/679 werden in Übereinstimmung mit dieser Verordnung sowie den Gesetzen und Verordnungen verarbeitet, die sie ergänzen beziehungsweise näher bestimmen.

§ 3 - Für die Verarbeitung verantwortlich können entweder eine der in Artikel 7 erwähnten Behörden, die Betreiber wesentlicher Dienste beziehungsweise Anbieter digitaler Dienste oder die Polizei- oder Gerichtsbehörden sein.

§ 4 - Empfänger personenbezogener Daten können alle Personen sein, die an der Ausführung der Bestimmungen des Gesetzes beteiligt sind, soweit dies für den im Gesetz vorgesehenen Informationsaustausch erforderlich ist.

Art. 67 - Gemäß Artikel 6 Absatz 1 Buchstabe c und e der Verordnung EU 2016/679 müssen die in Artikel 65 § 3 erwähnten Verarbeitungen zur Erfüllung einer rechtlichen Verpflichtung des für die Verarbeitung Verantwortlichen oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt und dem Verantwortlichen übertragen wurde, weiterhin erforderlich sein. Diese Verarbeitungen müssen lediglich im Hinblick auf diese Rechtsgrundlage erforderlich sein und auf das zu ihrer Erfüllung erforderliche Maß beschränkt bleiben.

Art. 68 - § 1 - Die in Artikel 65 § 3 erwähnten Verarbeitungen müssen auf die von dem für die Verarbeitung Verantwortlichen bestimmten Zwecke beschränkt sein und mit diesen vereinbar bleiben.

§ 2 - Diese Zwecke können insbesondere sein: ein besserer Schutz der Netz- und Informationssysteme, eine verstärkte Präventions- und Sicherheitspolitik, die Vorbeugung von Sicherheitsvorfällen, die Verfügbarkeit der in vorliegendem Gesetz erwähnten wesentlichen beziehungsweise digitalen Dienste, die Kontrolle von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste, die Zusammenarbeit auf nationaler und internationaler Ebene, die Beurteilung der Umsetzung des Gesetzes, die Vorbereitung, Organisation, Verwaltung und Weiterverfolgung von Ermittlungen beziehungsweise Strafverfolgungen sowie die sonstigen Aufträge, die den verschiedenen betreffenden Behörden durch das Gesetz zugewiesen sind.

§ 3 - In Bezug auf die relevanten Zwecke und Teilzwecke bestimmt jeder für die Verarbeitung Verantwortliche die betreffenden Daten- und Personenkategorien, die Empfänger beziehungsweise Kategorien von Empfängern von Daten, die Speicherfristen und andere eventuelle Merkmale der Verarbeitung sowie die Regeln und Modalitäten für die Einhaltung der geltenden Vorschriften.

KAPITEL 2 — *Speicherfrist*

Art. 69 - § 1 - Unbeschadet der Speicherung, die für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 der Verordnung EU 2016/679 erforderlich ist, werden die in Ausführung des Gesetzes verarbeiteten personenbezogenen Daten von den in Artikel 7 erwähnten Behörden nicht länger gespeichert, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

§ 2 - In Übereinstimmung mit § 1 kann der König die Höchstdauer, für die dieselben Daten gespeichert werden, durch einen im Ministerrat beratenen Erlass festlegen.

KAPITEL 3 — *Datenschutzbeauftragter*

Art. 70 - Jeder Betreiber wesentlicher Dienste, jeder Anbieter digitaler Dienste und jede in Artikel 7 des Gesetzes erwähnte Behörde, der/die personenbezogene Daten verarbeitet, bestimmt einen Datenschutzbeauftragten.

KAPITEL 4 — *Beschränkung der Rechte der betroffenen Personen*

Art. 71 - § 1 - In Anwendung von Artikel 23 Absatz 1 Buchstabe a, b, c, d, 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 - Die Artikel 12 bis 22 der vorerwähnten Verordnung finden keine Anwendung auf die Verarbeitung personenbezogener Daten durch einen Betreiber wesentlicher Dienste, einen Anbieter digitaler Dienste oder eine in Artikel 7 erwähnte Behörde, die in Übereinstimmung mit vorliegendem Gesetz und zur Erfüllung der durch dieses Gesetz auferlegten Verpflichtungen in Bezug auf die Meldung von Sicherheitsvorfällen, wie in Titel 2 Kapitel 3 und Titel 3 Kapitel 3 erwähnt, und Kontrollen, wie in Titel 4 erwähnt, erfolgt. Die Befreiung gilt nur, wenn und soweit eine solche Verarbeitung für die oben bestimmten Zwecke erforderlich ist, insbesondere soweit die Anwendung der Rechte, die in vorerwähnter Verordnung vorgesehen sind, den Zwecken der Kontrolle, der Untersuchung oder der vorbereitenden Verrichtungen schaden würde beziehungsweise die Vertraulichkeit der strafrechtlichen Ermittlung zu verletzen oder die Sicherheit von Personen zu beeinträchtigen droht.

§ 3 - Bei den für die Verarbeitung Verantwortlichen, die die in § 2 erwähnte Befreiung in Anspruch nehmen können, handelt es sich entweder um Betreiber wesentlicher Dienste, Anbieter digitaler Dienste oder in Artikel 7 erwähnte Behörden, und zwar jeweils in Bezug auf die Daten, über die sie im Rahmen der in § 2 erwähnten Aufträge verfügen.

§ 4 - Die Befreiung gilt vorbehaltlich des Grundsatzes der Verhältnismäßigkeit und gegebenenfalls der Datenminimierung für alle Kategorien personenbezogener Daten, soweit die Verarbeitung dieser Daten in Übereinstimmung mit den in § 2 erwähnten Zwecken erfolgt. Diese Befreiung gilt ebenfalls für vorbereitende Verrichtungen oder Verfahren im Hinblick auf die eventuelle Anwendung einer Verwaltungssanktion.

§ 5 - Personenbezogene Daten, die aus der in § 2 erwähnten Befreiung hervorgehen, werden nicht länger gespeichert, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, wobei die Höchstdauer, für die sie gespeichert werden, die Dauer der Verjährungsfrist in Bezug auf eventuelle, in Artikel 51 und 52 erwähnte Verstöße gemäß den anwendbaren Rechtsvorschriften nicht überschreiten darf.

§ 6 - Für die Verarbeitung Verantwortliche, die nicht alle Bestimmungen des Gesetzes und insbesondere von Artikel 72 einhalten, können die Befreiung nicht in Anspruch nehmen.

§ 7 - Jeder für die Verarbeitung Verantwortliche ist zudem verpflichtet, die Vertraulichkeit der personenbezogenen Daten, die Gegenstand der Befreiung sind, zu wahren und sicherzustellen, dass sie nur denjenigen zugänglich sind, die sie für die Ausführung der Bestimmungen des vorliegenden Gesetzes benötigen. Ferner muss jeder betreffende für die Verarbeitung Verantwortliche der Datenschutzbehörde mindestens einmal pro Jahr schriftlich eine Liste der Anträge auf Ausübung der in den Artikeln 12 bis 22 der Verordnung erwähnten Rechte zukommen lassen, die nach Ansicht dieses Verantwortlichen unter die Befreiung fallen. Unbeschadet der Bestimmungen des vorliegenden Gesetzes ist jeder

betreffende für die Verarbeitung Verantwortliche darüber hinaus verpflichtet, alle sonstigen angemessenen Maßnahmen zu ergreifen, um jegliche Form des Missbrauchs, des unrechtmäßigen Zugangs oder der unrechtmäßigen Übermittlung personenbezogener Daten, die unter die Befreiung fallen, zu verhindern, insbesondere und ohne Beschränkung der in Artikel 32 der Verordnung EU 2016/679 vorgesehenen Maßnahmen.

Art. 72 - § 1 - Betreffende können einen Antrag in Bezug auf ihre in den Artikeln 12 bis 22 der Verordnung EU 2016/679 vorgesehenen Rechte an den Datenschutzbeauftragten richten, der den Eingang bestätigt.

§ 2 - Der Datenschutzbeauftragte des für die Verarbeitung Verantwortlichen informiert die betroffene Person unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, schriftlich über jede Verweigerung oder Einschränkung ihrer in den Artikeln 12 bis 22 der Verordnung EU 2016/679 vorgesehenen Rechte sowie über die Gründe für diese Verweigerung oder Einschränkung. Die Information über die Verweigerung oder Einschränkung kann weggelassen werden, wenn ihre Mitteilung einen der in Artikel 71 § 2 erwähnten Zwecke zu gefährden droht. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl Anträge erforderlich ist. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über diese Fristverlängerung und die Gründe für die Verzögerung.

§ 3 - Der Datenschutzbeauftragte des für die Verarbeitung Verantwortlichen unterrichtet die betroffene Person über die Möglichkeiten, bei der Datenschutzbehörde Beschwerde einzureichen und eine gerichtliche Beschwerde einzulegen.

Der Datenschutzbeauftragte des für die Verarbeitung Verantwortlichen hält die tatsächlichen oder rechtlichen Gründe fest, auf die sich sein Beschluss stützt. Diese Informationen werden der Datenschutzbehörde zur Verfügung gestellt.

§ 4 - Der betreffende für die Verarbeitung Verantwortliche gewährt der betroffenen Person jedoch 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.

§ 5 - Die Verweigerung oder Einschränkung der in den Artikeln 12 bis 22 der Verordnung EU 2016/679 vorgesehenen Rechte muss aufgehoben werden:

— für Maßnahmen, die durch die Pflichten in Bezug auf die Meldung von Sicherheitsvorfällen gerechtfertigt sind, wenn die Bearbeitung eines Vorfalls durch die in Artikel 24 oder 34 erwähnten Behörden beendet ist,

— für Maßnahmen, die durch die Pflichten aufgrund von Titel 4 gerechtfertigt sind, wenn die Kontrolle, die Untersuchung oder die vorbereitenden Verrichtungen dazu durch den Inspektionsdienst beendet sind, und während des Zeitraums, in dem die sektorspezifische Behörde Dokumente des Inspektionsdienstes im Hinblick auf eine Verfolgung bearbeitet,

— spätestens ein Jahr nach Eingang des Antrags in Anwendung der Artikel 12 bis 22 der europäischen Verordnung EU 2016/679, es sei denn, eine Kontrolle beziehungsweise Untersuchung läuft gerade.

§ 6 - Der betreffende für die Verarbeitung Verantwortliche hebt die Verweigerung oder Einschränkung der in den Artikeln 12 bis 22 der Verordnung EU 2016/679 vorgesehenen Rechte ebenfalls auf, sobald eine solche Maßnahme für einen der in Artikel 68 § 2 erwähnten Zwecke nicht mehr erforderlich ist.

§ 7 - In allen Fällen, in denen die Paragraphen 5 und 6 Anwendung finden, unterrichtet der Datenschutzbeauftragte die betroffene(n) Person(en) schriftlich über die Aufhebung der Verweigerung beziehungsweise Einschränkung.

KAPITEL 5 — *Einschränkungen der Pflichten in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten*

Art. 73 - Der betreffende für die Verarbeitung Verantwortliche ist vorbehaltlich der Genehmigung der in Artikel 7 § 1 erwähnten Behörde 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 71 § 2 erwähnten Zwecke zu gefährden droht.

TITEL 7 — *Schlussbestimmungen*

KAPITEL 1 — *Abänderungen des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz der kritischen Infrastrukturen*

Art. 74 - Artikel 2 des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz der kritischen Infrastrukturen wird durch einen Absatz mit folgendem Wortlaut ergänzt:

"Durch vorliegendes Gesetz wird die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union teilweise umgesetzt."

Art. 75 - Artikel 3 desselben Gesetzes, abgeändert durch die Gesetze vom 25. April 2014 und 15. Juli 2018, wird wie folgt abgeändert:

1. In Nr. 3 werden die Buchstaben *c)* und *d)* wie folgt ersetzt:

"*c)* für den Finanzsektor, mit Ausnahme der Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU: die Belgische Nationalbank (BNB),

d) für die Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU: die Autorität Finanzielle Dienste und Märkte (FSMA),"

2. Nummer 3 wird durch die Buchstaben *e)* bis *g)* mit folgendem Wortlaut ergänzt:

"*e)* für die Sektoren elektronische Kommunikation und digitale Infrastruktur: das Belgische Institut für Post- und Fernmeldewesen (BIPF),

f) für den Gesundheitssektor: die vom König durch einen im Ministerrat beratenen Erlass bestimmte öffentliche Behörde,

g) für den Sektor der Trinkwasserversorgung: die vom König durch einen im Ministerrat beratenen Erlass bestimmte Behörde,".

3. Der Artikel wird durch die Nummern 13 bis 17 mit folgendem Wortlaut ergänzt:

"13. "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,

14. "Sicherheit von Netz- und Informationssystemen": Sicherheit von Netz- und Informationssystemen im Sinne von Artikel 6 Nr. 8 und 9 des Gesetzes vom 7. April 2019,

15. "Sektor der digitalen Infrastruktur": Sektor, wie in Punkt 6 von Anlage 1 zum Gesetz vom 7. April 2019 erwähnt,

16. "Sektor der Trinkwasserversorgung": Sektor, wie in Punkt 5 von Anlage 1 zum Gesetz vom 7. April 2019 erwähnt,

17. "Gesundheitssektor": Sektor, wie in Punkt 4 von Anlage 1 zum Gesetz vom 7. April 2019 erwähnt."

Art. 76 - In Artikel 4 desselben Gesetzes, abgeändert durch das Gesetz vom 15. Juli 2018, wird § 4 wie folgt ersetzt:

"§ 4 - Vorliegendes Kapitel findet Anwendung auf den Finanzsektor, einschließlich der in Artikel 3 Nr. 3 Buchstabe *d)* erwähnten Betreiber von Handelsplätzen, den Sektor der elektronischen Kommunikation, den Sektor der digitalen Infrastruktur, den Gesundheitssektor und den Sektor der Trinkwasserversorgung in Bezug auf die Sicherheit und den Schutz der nationalen kritischen Infrastrukturen."

Art. 77 - Artikel 5 desselben Gesetzes, abgeändert durch das Gesetz vom 15. Juli 2018, wird durch einen Paragraphen 3 mit folgendem Wortlaut ergänzt:

"§ 3 - Während des gesamten in vorliegendem Abschnitt erwähnten Identifizierungsverfahrens wird die in Artikel 7 § 1 des Gesetzes vom 7. April 2019 erwähnte Behörde in die nationalen und internationalen Konzertierungen einbezogen, die von den sektorspezifischen Behörden und der GDKZ in Bezug auf die Identifizierung kritischer Infrastrukturen im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen durchgeführt werden."

Art. 78 - Artikel 13 desselben Gesetzes, abgeändert durch die Gesetze vom 25. April 2014 und 15. Juli 2018, wird wie folgt abgeändert:

1. In § 5*bis* werden zwischen den Wörtern "des Finanzsektors" und den Wörtern "werden Sicherheitsmaßnahmen" die Wörter ", mit Ausnahme der von Betreibern von Handelsplätzen betriebenen Infrastrukturen," eingefügt.

2. In § 6 Absatz 1 werden zwischen den Wörtern "den Finanzsektor" und den Wörtern "werden Übungen" die Wörter ", mit Ausnahme der von Betreibern von Handelsplätzen betriebenen kritischen Infrastrukturen," eingefügt.

Art. 79 - In Artikel 14 desselben Gesetzes, abgeändert durch das Gesetz vom 15. Juli 2018, wird § 2 durch die Wörter ", und gegebenenfalls die in Artikel 7 § 1 des Gesetzes vom 7. April 2019 erwähnte Behörde in Bezug auf die Sicherheit von Netz- und Informationssystemen" ergänzt.

Art. 80 - In Artikel 18 desselben Gesetzes, abgeändert durch das Gesetz vom 15. Juli 2018, werden die Wörter "Die GDKZ, die Polizeidienste und das KOBA" durch die Wörter "Die GDKZ, die Polizeidienste, das KOBA und gegebenenfalls die in Artikel 7 § 1 des Gesetzes vom 7. April 2019 erwähnte Behörde, was die Sicherheit von Netz- und Informationssystemen betrifft," ersetzt.

Art. 81 - In Artikel 19 desselben Gesetzes werden die Wörter "Der Betreiber, die Kontaktstelle für die Sicherheit, die sektorspezifische Behörde, die GDKZ, das KOBA und die Polizeidienste" durch die Wörter "Der Betreiber, die Kontaktstelle für die Sicherheit, die sektorspezifische Behörde, die GDKZ, das KOBA, die Polizeidienste und gegebenenfalls die in Artikel 7 § 1 des Gesetzes vom 7. April 2019 erwähnte Behörde, was die Sicherheit von Netz- und Informationssystemen betrifft," ersetzt.

Art. 82 - In Artikel 22 desselben Gesetzes, ersetzt durch das Gesetz vom 15. Juli 2018, werden die Wörter "Die sektorspezifische Behörde, die GDKZ, das KOBA und die Polizeidienste" durch die Wörter "Die sektorspezifische Behörde, die GDKZ, das KOBA, die Polizeidienste und die in Artikel 7 § 1 des Gesetzes vom 7. April 2019 erwähnte Behörde" ersetzt.

Art. 83 - Artikel 22*bis* desselben Gesetzes, eingefügt durch das Gesetz vom 25. April 2004, wird wie folgt abgeändert:

1. In Absatz 1 werden die Wörter "Finanzsektor teilt die Belgische Nationalbank dem Minister der Finanzen einen Bericht über die Aufgaben" durch die Wörter "Finanzsektor, mit Ausnahme des Teilsektors der Betreiber von Handelsplätzen, teilt die Belgische Nationalbank dem Minister der Finanzen einen Bericht über die Aufgaben mit" ersetzt.

2. Der Artikel wird durch einen Absatz mit folgendem Wortlaut ergänzt:

"Für die Betreiber von Handelsplätzen teilt die FSMA dem Minister der Finanzen einen Bericht über die Aufgaben mit, die sie aufgrund des vorliegenden Gesetzes erfüllt, gemäß einer angepassten Periodizität von höchstens drei Jahren. Die FSMA benachrichtigt den Minister jedoch unverzüglich über jede konkrete und unmittelbare Bedrohung für eine kritische Infrastruktur, die zu seinem Sektor gehört."

Art. 84 - Artikel 24 desselben Gesetzes, abgeändert durch die Gesetze vom 25. April 2014 und 15. Juli 2018, wird wie folgt abgeändert:

1. In § 2 Absatz 3 werden zwischen den Wörtern "den Finanzsektor" und den Wörtern "wird die Belgische Nationalbank" die Wörter ", mit Ausnahme des Teilsektors der Betreiber von Handelsplätzen," eingefügt.

2. Paragraph 2 wird durch einen Absatz mit folgendem Wortlaut ergänzt:

"Für die Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU wird die Autorität Finanzielle Dienste und Märkte als Inspektionsdienst bestimmt, der mit der Kontrolle der Anwendung der Bestimmungen des vorliegenden Gesetzes und seiner Ausführungserlasse beauftragt ist. Vorliegender Artikel beeinträchtigt nicht die Möglichkeit der FSMA, zur Ausführung der ihr durch vorliegendes Gesetz anvertrauten Aufträge einen spezialisierten externen Dienstleister mit der Durchführung bestimmter Aufgaben zu beauftragen beziehungsweise die Unterstützung eines solchen Dienstleisters in Anspruch zu nehmen."

KAPITEL 2 — *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. 85 - 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 13. Dezember 2017, wird wie folgt ergänzt:

"- 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."

Art. 86 - In Kapitel III Abschnitt 1 desselben Gesetzes wird ein Artikel 15*ter* mit folgendem Wortlaut eingefügt:

"Art. 15*ter* - Die Agentur wird als Inspektionsdienst im Sinne von Artikel 42 des Gesetzes vom 7. April 2019 bestimmt und ist mit der Kontrolle der Anwendung der Bestimmungen dieses Gesetzes und seiner Ausführungserlasse durch die Betreiber wesentlicher Dienste, die aufgrund des vorerwähnten Gesetzes ermittelt wurden, beauftragt, und zwar in Bezug auf die zur Übertragung von Elektrizität verwendeten Komponenten einer kerntechnischen Anlage für industrielle Stromerzeugung.

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

(...)

KAPITEL 5 — *Abänderungen des Gesetzes vom 2. August 2002 über die Aufsicht über den Finanzsektor und die Finanzdienstleistungen*

Art. 92 - Artikel 75 § 1 Nr. 15 des Gesetzes vom 2. August 2002 über die Aufsicht über den Finanzsektor und die Finanzdienstleistungen, aufgehoben durch das Gesetz vom 5. Dezember 2017 zur Festlegung verschiedener finanzieller Bestimmungen, wird mit folgendem Wortlaut wieder eingesetzt:

"15. in den Grenzen des Rechts der Europäischen Union den in Artikel 7 des Gesetzes vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit erwähnten Behörden zur Ausführung der Bestimmungen dieses Gesetzes und des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz der kritischen Infrastrukturen,".

(...)

KAPITEL 7 — *Inkrafttreten*

Art. 96 - Vorliegendes Gesetz tritt am Tag seiner Veröffentlichung im *Belgischen Staatsblatt* in Kraft.

Wir fertigen das vorliegende Gesetz aus und ordnen an, dass es mit dem Staatssiegel versehen und durch das *Belgische Staatsblatt* veröffentlicht wird.

Gegeben zu Brüssel, den 7. April 2019

PHILIPPE

Von Königs wegen:

Der Premierminister
Ch. MICHEL

Der Minister der Sicherheit und des Innern
P. DE CREM

Mit dem Staatssiegel versehen:

Der Minister der Justiz
K. GEENS

Anlage 1 zum Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit

Arten von Betreibern wesentlicher Dienste, wie in Artikel 11 § 1 erwähnt

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	Elektrizitätsunternehmen im Sinne von Artikel 2 Nr. 15*ter* des Gesetzes vom 29. April 1999 über die Organisation des Elektrizitätsmarktes
		Verteilernetzbetreiber im Sinne von Artikel 2 Nr. 11 des Gesetzes vom 29. April 1999 über die Organisation des Elektrizitätsmarktes
		Netzbetreiber im Sinne von Artikel 2 Nr. 8 des Gesetzes vom 29. April 1999 über die Organisation des Elektrizitätsmarktes
	b) Erdöl	Betreiber von Erdöl-Fernleitungen
		Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
	c) Erdgas	Erdgasunternehmen im Sinne von Artikel 1 Nr. 5*bis* des Gesetzes vom 12. April 1965 über den Transport gasförmiger und anderer Produkte durch Leitungen

Sektor	Teilsektor	Art der Einrichtung
		Verteilernetzbetreiber im Sinne von Artikel 1 Nr. 13 des Gesetzes vom 12. April 1965 über den Transport gasförmiger und anderer Produkte durch Leitungen
		Betreiber des Erdgas-Fernleitungsnetzes im Sinne von Artikel 1 Nr. 31 des Gesetzes vom 12. April 1965 über den Transport gasförmiger und anderer Produkte durch Leitungen
		Betreiber von Speicheranlagen im Sinne von Artikel 1 Nr. 33 des Gesetzes vom 12. April 1965 über den Transport gasförmiger und anderer Produkte durch Leitungen
		Betreiber von LNG-Anlagen im Sinne von Artikel 1 Nr. 35 des Gesetzes vom 12. April 1965 über den Transport gasförmiger und anderer Produkte durch Leitungen
		Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
2. Verkehr	a) Luftverkehr	Luftfahrtunternehmen im Sinne von Artikel 3 Nummer 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
		Flughafenleitungsorgane im Sinne von Artikel 2 Nr. 2 des Königlichen Erlasses vom 6. November 2010 über den Zugang zum Markt der Bodenabfertigungsdienste auf dem Flughafen Brüssel-National, Flughäfen im Sinne von Artikel 2 Nummer 1 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		Flugsicherungsdienste im Sinne von Artikel 2 Nummer 4 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 (”Rahmenverordnung”)
		Netzmanager im Sinne von Artikel 2 Nummer 22 der Verordnung (EU) Nr. 677/2011 der Kommission vom 7. Juli 2011 zur Festlegung von Durchführungsbestimmungen für die Funktionen des Flugverkehrsmanagementnetzes und zur Änderung der Verordnung (EU) Nr. 691/2010
	b) Schienenverkehr	Infrastrukturbetreiber im Sinne von Artikel 3 Nr. 29 des Eisenbahngesetzbuches
		Eisenbahnunternehmen im Sinne von Artikel 3 Nr. 27 des Eisenbahngesetzbuches
	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 für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		Leitungsorgane von Häfen im Sinne von Artikel 5 Nr. 7 des Gesetzes vom 5. Februar 2007 über die Gefahrenabwehr im Seeverkehr, einschließlich ihrer Hafenanlagen im Sinne von Artikel 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		Betreiber von Schiffsverkehrsdiensten (VTS) im Sinne von Artikel 1 Nr. 12 des Königlichen Erlasses vom 17. September 2005 zur Umsetzung der Richtlinie 2002/59/EG vom 27. Juni 2002
	d) Straßenverkehr	Straßenverkehrsbehörden im Sinne von Artikel 2 Nummer 12 der delegierten Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste, die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind
		Betreiber intelligenter Verkehrssysteme im Sinne von Artikel 3 Nr. 1 des Gesetzes vom 17. August 2013 zur Schaffung des Rahmens für die Einführung intelligenter Verkehrssysteme und zur Abänderung des Gesetzes vom 10. April 1990 zur Regelung der privaten und besonderen Sicherheit (nachstehend: ”IVS-Rahmengesetz”)

Sektor	Teilsektor	Art der Einrichtung
3. Finanzen	a) Finanzinstitute	Kreditinstitute im Sinne von Artikel 4 Nummer 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
		Zentrale Gegenparteien im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister
		Finanzinstitute (weder Kreditinstitute noch zentrale Gegenparteien), die aufgrund der Artikel 8 und 12*bis* des Gesetzes vom 22. Februar 1998 zur Festlegung des Grundlagenstatuts der Belgischen Nationalbank der Aufsicht durch die Belgische Nationalbank unterliegen
	b) Finanzhandelsplätze	Betreiber von Handelsplätzen im Sinne von Artikel 3 Nr. 6 des Gesetzes vom 21. November 2017 über die Infrastrukturen der Märkte für Finanzinstrumente und zur Umsetzung der Richtlinie 2014/65/EU
4. Gesundheit	Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäuser und Privatkliniken)	Gesundheitsdienstleister im Sinne von Artikel 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
5. Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit "Wasser für den menschlichen Gebrauch" im Sinne von Artikel 2 Nummer 1 Buchstabe a der Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch, jedoch unter Ausschluss der Versorger, für die die Versorgung mit Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Versorgung mit anderen Rohstoffen und Gütern ist, die nicht als wesentliche Dienste eingestuft werden
6. Digitale Infrastruktur		IXP
		DNS-Diensteanbieter
		TLS-Name-Registries

Gesehen, um dem Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit beigefügt zu werden.

PHILIPPE

Von Königs wegen:

Der Premierminister
Ch. MICHEL

Der Minister der Sicherheit und des Innern
P. DE CREM

Anlage 2 zum Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit

Arten digitaler Dienste

1. Online-Marktplatz
2. Online-Suchmaschine
3. Cloud-Computing-Dienst

Gesehen, um dem Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit beigefügt zu werden.

PHILIPPE

Von Königs wegen:

Der Premierminister
Ch. MICHEL

Der Minister der Sicherheit und des Innern
P. DE CREM