FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[2024/202344]

26 APRIL 2024. — Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (1)

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

TITEL 1. — *Definities en algemene bepalingen*

HOOFDSTUK 1. — *Onderwerp en toepassingsgebied*

Afdeling 1. — Onderwerp

Artikel 1. Deze wet regelt een materie bedoeld in artikel 74 van de Grondwet.

Art. 2. Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148. Deze richtlijn wordt hierna de "NIS2-richtlijn" genoemd.

Afdeling 2. — Toepassingsgebied

Art. 3. § 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 is deze wet van toepassing op publieke of private entiteiten van een in bijlage I of II bedoelde soort die:

1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of

2° een onderneming die de plafonds overschrijdt zoals bepaald in lid 1 van hetzelfde artikel van deze bijlage.

Artikel 3, lid 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.

§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling nr. 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die zij verleent.

Op basis van het eerste lid beschouwt de nationale cyberbeveiligingsautoriteit een dergelijke entiteit als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.

De Koning kan de criteria bepalen op basis waarvan de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen wordt beoordeeld.

§ 3. Onverminderd artikel 6 is deze wet ook van toepassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen:

1° de diensten worden verleend door:

a) aanbieders van openbare elektronische communicatienetwerken of van openbare elektronische-communicatiediensten;

b) verleners van vertrouwensdiensten;

c) registers voor topleveldomeinnamen en domeinnaamsysteemdienstverleners;

2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;

3° de entiteit is een overheidsinstantie:

a) die van de Federale Staat afhangt;

b) die van de deelgebieden afhangt, geïdentificeerd overeenkomstig artikel 11, § 2;

c) die een hulpverleningszone is in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp in de zin van de ordonnantie van 19 juli 1990 houdende oprichting van

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[2024/202344]

26 AVRIL 2024. — Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (1)

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

TITRE 1er. — *Définitions et dispositions générales*

CHAPITRE 1er. — *Objet et champ d'application*

Section 1re. — Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi vise notamment à transposer la directive européenne (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. Cette directive est dénommée ci-après la "directive NIS2".

Section 2. — Champ d'application

Art. 3. § 1er. Dans les limites de l'article 4 et sans préjudice de l'article 6, la présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II et qui constituent:

1° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou

2° une entreprise qui dépasse les plafonds prévus au paragraphe 1er du même article de cette annexe.

L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.

§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation n° 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit.

Sur base de l'alinéa 1er, l'autorité nationale de cybersécurité considère qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d'indépendance de ladite entité, celle-ci n'aurait pas été considérée comme constituant une entreprise moyenne ou dépassant lesdits plafonds si seules ses propres données avaient été prises en compte.

Le Roi peut déterminer les critères sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.

§ 3. Sans préjudice de l'article 6, la présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans un des cas suivants:

1° les services sont fournis par:

a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;

b) des prestataires de services de confiance;

c) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;

2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;

3° l'entité est une entité de l'administration publique:

a) qui dépend de l'État fédéral;

b) qui dépend des entités fédérées, identifiée conformément à l'article 11, § 2;

c) qui est une zone de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale au sens de l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie

de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.

§ 6. Na raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren en/of deelsectoren toevoegen aan bijlage I of II of de bestaande sectoren en/of deelsectoren uitbreiden.

Art. 4. § 1. Deze wet is van toepassing op de in artikel 3 bedoelde entiteiten die gevestigd zijn in België en die hun diensten verlenen of hun activiteiten verrichten in de Europese Unie.

§ 2. In afwijking van paragraaf 1 is deze wet van toepassing op:

1° aanbieders van openbare elektronische-communicatienetwerken of aanbieders van openbare elektronische-communicatiediensten, wanneer zij deze diensten in België verlenen;

2° DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook op aanbieders van onlinemarktplaatsen, onlinezoekmachines of platformen voor socialenetwerkdiensten, wanneer zij hun hoofdvestiging in België hebben, overeenkomstig de paragrafen 4 en 5.

§ 3. Indien een entiteit bedoeld in paragraaf 2, 2°, niet in de Europese Unie is gevestigd, maar diensten in de Unie aanbiedt, wijst zij een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in een van de lidstaten waar de diensten worden verleend.

§ 4. Voor de toepassing van deze wet hebben de in paragraaf 2, 2°, bedoelde entiteiten hun hoofdvestiging in België wanneer zij er hoofdzakelijk de beslissingen nemen rond maatregelen voor het beheer van cyberbeveiligingsrisico's.

Indien de plaats waar deze beslissingen worden genomen niet kan worden bepaald of zich niet in de Europese Unie bevindt, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben wanneer zij er hun cyberbeveiligingsactiviteiten uitvoeren.

Indien de plaats waar deze activiteiten plaatsvinden niet kan worden bepaald, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben wanneer hun vestiging met het grootste aantal werknemers zich daar bevindt.

§ 5. Voor de toepassing van deze wet worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvestiging in België te hebben, wanneer zij niet gevestigd zijn in de Europese Unie maar hun diensten verlenen in de Unie en hun vertegenwoordiger in de Europese Unie in België gevestigd is.

§ 6. De aanwijzing van een vertegenwoordiger door een entiteit bedoeld in paragraaf 2, 2°, doet geen afbreuk aan juridische stappen die tegen de entiteit zelf kunnen worden ingesteld.

Art. 5. § 1. Deze wet doet geen afbreuk aan de toepassing van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), aan de wettelijke en reglementaire bepalingen die deze verordening aanvullen of verduidelijken of aan de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

§ 2. Deze wet doet geen afbreuk aan de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst en is niet van toepassing op communicatie- en informatiesystemen die zijn goedgekeurd om geclassificeerde informatie in elektronische vorm te gebruiken overeenkomstig de bovengenoemde wet.

§ 3. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op nucleaire documenten in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

et d'aide médicale urgente de la Région de Bruxelles-Capitale.

§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.

§ 6. Après consultation des éventuelles autorités sectorielles concernées et de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs et/ou sous-secteurs à l'annexe I ou II ou élargir les secteurs et/ou sous-secteurs existants.

Art. 4. § 1er. La présente loi s'applique aux entités visées à l'article 3 qui sont établies en Belgique et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

§ 2. Par exception au paragraphe 1er, la présente loi s'applique:

1° aux fournisseurs de réseaux de communications électroniques publics ou aux fournisseurs de services de communications électroniques accessibles au public, lorsqu'ils fournissent ces services en Belgique;

2° aux fournisseurs de services DNS, registres de noms de domaine de premier niveau, entités fournissant des services d'enregistrement de noms de domaine, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, lorsqu'ils ont leur établissement principal en Belgique, conformément aux paragraphes 4 et 5.

§ 3. Si une entité visée au paragraphe 2, 2°, n'est pas établie dans l'Union européenne mais y fournit des services, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres où les services sont fournis.

§ 4. Pour l'application de la présente loi, les entités visées au paragraphe 2, 2°, ont leur établissement principal en Belgique lorsqu'elles y prennent principalement les décisions liées aux mesures de gestion des risques de cybersécurité.

Si l'endroit où ces décisions sont prises ne peut être déterminé ou ne se trouve pas dans l'Union européenne, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsqu'elles y conduisent leurs opérations de cybersécurité.

Si l'endroit où sont conduites ces opérations ne peut être déterminé, les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique lorsque s'y trouve leur établissement avec le plus grand nombre d'employés.

§ 5. Les entités visées au paragraphe 2, 2°, sont réputées avoir leur établissement principal en Belgique, pour l'application de la présente loi, lorsqu'elles ne sont pas établies dans l'Union européenne mais qu'elles fournissent leurs services dans l'Union et que leur représentant dans l'Union européenne est établi en Belgique.

§ 6. La désignation d'un représentant par une entité visée au paragraphe 2, 2°, est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

Art. 5. § 1er. La présente loi ne porte pas préjudice à l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ni aux dispositions légales et réglementaires qui complètent ou précisent ledit règlement ni à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

§ 2. La présente loi est sans préjudice de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé et ne s'applique pas aux systèmes de communication et d'information approuvés pour utiliser des informations classifiées sous forme électronique conformément à la loi précitée.

§ 3. La présente loi est sans préjudice des règles applicables aux documents nucléaires, au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

§ 4. Behoudens de artikelen 8 en 38 en titel 2 is deze wet niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten en de algemene inspectie bedoeld in artikel 2, 2° en 3°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° de netwerk- en informatiesystemen van Belgische diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° de inrichtingen van klasse I in de zin van artikel 3.1 van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen.

In afwijking van het eerste lid, 8°, is deze wet van toepassing op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van elektriciteit.

§ 5. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op:

1° het NCCN;

2° de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16.

§ 6. De paragrafen 4 en 5 zijn niet van toepassing wanneer een van deze entiteiten optreedt als verlener van vertrouwensdiensten.

Art. 6. § 1. Indien een sectorspecifiek rechtsinstrument van de Europese Unie vereist dat entiteiten die tot het toepassingsgebied van deze wet behoren, maatregelen nemen voor het beheer van cyberbeveiligingsrisico's of significante incidenten melden en indien deze eisen ten minste gelijkwaardig zijn aan de in deze wet bepaalde verplichtingen, zijn de relevante bepalingen van deze wet niet van toepassing op deze entiteiten.

Indien een in het eerste lid bedoeld sectorspecifiek rechtsinstrument van de Europese Unie niet op alle entiteiten in een specifieke sector die tot het toepassingsgebied van deze wet behoort, betrekking heeft, zijn de relevante bepalingen van deze wet van toepassing op de entiteiten waarop dit sectorspecifieke rechtsinstrument van de Europese Unie geen betrekking heeft.

§ 2. De in paragraaf 1, eerste lid, bedoelde eisen worden geacht gelijkwaardig te zijn aan de verplichtingen van deze wet wanneer:

1° de maatregelen voor het beheer van cyberbeveiligingsrisico's ten minste gelijkwaardig zijn aan de maatregelen bedoeld in artikel 30; of

2° het sectorspecifieke rechtsinstrument van de Europese Unie in onmiddellijke toegang voorziet, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten voor het nationale CSIRT en wanneer de eisen voor het melden van significante incidenten ten minste gelijkwaardig zijn aan de verplichtingen bedoeld in de artikelen 34 tot 37.

§ 3. De bepalingen van de titels 3 tot 5 zijn niet van toepassing op entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt in de zin van bijlage I die onder het toepassingsgebied vallen van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011, met inbegrip van de activiteit van centrale effectenbewaarinstelling verricht door de Nationale Bank van België.

§ 4. De bepalingen van titel 3, hoofdstuk 1, van titel 4 en van titel 5 zijn niet van toepassing:

1° op de Nationale Bank van België, met uitzondering van haar

§ 4. Sous réserve des articles 8 et 38 ainsi que du titre 2, la présente loi ne s'applique pas:

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au Ministère de la Défense visé à l'article 1er de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police et à l'inspection générale visés à l'article 2, 2° et 3°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le ministère public inclus;

6° au Service public fédéral Justice créé par l'arrêté royal du 23 mai 2001 portant création du Service Public Fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visés au 5°;

7° aux réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° aux établissements de classe I au sens de l'article 3.1 de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants.

Par dérogation à l'alinéa 1er, 8°, la présente loi est applicable aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

§ 5. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas:

1° au NCCN;

2° à l'autorité nationale de cybersécurité visée à l'article 16.

§ 6. Les paragraphes 4 et 5 ne s'appliquent pas lorsqu'une de ces entités agit en tant que prestataire de services de confiance.

Art. 6. § 1er. Lorsqu'un instrument juridique sectoriel de l'Union européenne impose aux entités qui entrent dans le champ d'application de la présente loi d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents significatifs et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions pertinentes de la présente loi ne sont pas applicables à ces entités.

Lorsqu'un instrument juridique sectoriel de l'Union européenne visé à l'alinéa 1er ne couvre pas l'ensemble des entités d'un secteur spécifique entrant dans le champ d'application de la présente loi, les dispositions pertinentes de la présente loi s'appliquent aux entités non couvertes par cet instrument juridique sectoriel de l'Union européenne.

§ 2. Les exigences visées au paragraphe 1er, alinéa 1er, sont considérées comme ayant un effet équivalent aux obligations de la présente loi lorsque:

1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures visées à l'article 30; ou

2° l'instrument juridique sectoriel de l'Union européenne prévoit un accès immédiat, s'il y a lieu automatique et direct, aux notifications d'incidents pour le CSIRT national et lorsque les exigences relatives à la notification des incidents significatifs sont au moins équivalentes aux obligations visées aux articles 34 à 37.

§ 3. Les dispositions des titres 3 à 5 ne s'appliquent pas aux entités relevant des secteurs bancaire et infrastructures des marchés financiers au sens de l'annexe I qui tombent dans le champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, en ce compris l'activité de dépositaire central de titres exercée par la Banque Nationale de Belgique.

§ 4. Les dispositions du titre 3, chapitre 1er, du titre 4 et du titre 5 ne s'appliquent pas:

1° à la Banque Nationale de Belgique, exception faite de son activité

activiteit van centrale effectenbewaarinstelling waarop paragraaf 3 van toepassing is;

2° op financiële instellingen die onderworpen zijn aan het toezicht van de Nationale Bank van België krachtens de artikelen 8 en 12*bis* van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België en die niet onder paragraaf 3 vallen.

Art. 7. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad:

1° de gelijkwaardige sectorspecifieke rechtsinstrumenten bedoeld in artikel 6, § 1, eerste lid, nader bepalen;

2° bijzondere regels vaststellen met betrekking tot de coördinatie van de informatie-uitwisseling, met inbegrip van de eisen voor het melden van significante incidenten, tussen de entiteiten bedoeld in artikel 6, § § 3 en 4, de betrokken sectorale overheid, de nationale cyberbeveiligingsautoriteit en de autoriteit belast met het beheer van cyberrisico's.

HOOFDSTUK 2. — *Definities*

Art. 8. Voor de toepassing van deze wet moet worden verstaan onder:

1° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten *a)* en *b)* bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

2° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

3° "cyberbeveiliging": cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), hierna de "cyberbeveiligingsverordening" genoemd;

4° "nationale cyberbeveiligingsstrategie": een samenhangend kader met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en governance om die doelstellingen en prioriteiten in België te verwezenlijken;

5° "incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

6° "bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;

7° "grootschalig cyberbeveiligingsincident": een incident dat leidt tot een verstoringsniveau dat te groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie;

8° "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;

9° "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat een dergelijk incident zich voordoet;

10° "cyberdreiging": een cyberdreiging bedoeld in artikel 2, punt 8), van de cyberbeveiligingsverordening;

de dépositaire central de titres à laquelle s'applique le paragraphe 3;

2° aux établissements financiers soumis à la supervision de la Banque Nationale de Belgique en vertu des articles 8 et 12*bis* de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique qui ne relèvent pas du paragraphe 3.

Art. 7. Le Roi peut, par arrêté délibéré en Conseil des ministres:

1° préciser les instruments juridiques sectoriels équivalents visés à l'article 6, § 1er, alinéa 1er;

2° définir des règles particulières relatives à la coordination de l'échange d'informations, en ce compris des exigences relatives à la notification des incidents significatifs, entre les entités visées à l'article 6, § § 3 et 4, l'autorité sectorielle concernée, l'autorité nationale de cybersécurité et l'autorité chargée de la gestion des risques cyber.

CHAPITRE 2. — *Définitions*

Art. 8. Pour l'application de la présente loi, il faut entendre par:

1° "réseau et système d'information":

a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points *a)* et *b)* en vue de leur fonctionnement, utilisation, protection et maintenance;

2° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

3° "cybersécurité": la cybersécurité au sens de l'article 2, 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), ci-après le "règlement sur la cybersécurité";

4° "stratégie nationale en matière de cybersécurité": le cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser en Belgique;

5° "incident": un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

6° "incident évité": un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite;

7° "incident de cybersécurité majeur": un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre de l'Union européenne concerné ou qui a un impact significatif sur au moins deux États membres de l'Union européenne;

8° "traitement des incidents": toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

9° "risque": le potentiel de perte ou de perturbation à la suite d'un incident, à exprimer comme la combinaison de l'ampleur d'une telle perte ou d'une telle perturbation et de la probabilité qu'un tel incident se produise;

10° "cybermenace": une cybermenace visée à l'article 2, point 8), du règlement sur la cybersécurité;

11° "significante cyberdreiging": een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

12° "ICT-product": een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;

13° "ICT-dienst": een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;

14° "ICT-proces": een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;

15° "kwetsbaarheid": een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;

16° "norm": een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad, hierna "Verordening (EU) nr. 1025/2012";

17° "internetknooppunt": een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;

18° "domeinnaamsysteem" of "DNS": een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;

19° "DNS-dienstverlener": een entiteit die de volgende diensten verleent:

a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers; of

b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers;

20° "register voor topleveldomeinnamen": een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

21° "entiteit die domeinnaamregistratiediensten aanbiedt": een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

22° "digitale dienst": een dienst in de zin van artikel 1, lid 1, punt *b)*, van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

23° "vertrouwensdienst": een vertrouwensdienst in de zin van artikel 3, 16, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna de "eIDAS-verordening" genoemd;

24° "verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten in de zin van artikel 3, 19, van de eIDAS-verordening;

25° "gekwalificeerde vertrouwensdienst": een gekwalificeerde vertrouwensdienst in de zin van artikel 3, 17, van de eIDAS-verordening;

11° "cybermenace importante": une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;

12° "produit TIC": un produit TIC au sens de l'article 2, 12), du règlement sur la cybersécurité;

13° "service TIC": un service TIC au sens de l'article 2, 13), du règlement sur la cybersécurité;

14° "processus TIC": un processus TIC au sens de l'article 2, 14), du règlement sur la cybersécurité;

15° "vulnérabilité": une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;

16° "norme": une norme au sens de l'article 2, 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ci-après le "règlement (UE) n°1025/2012";

17° "point d'échange internet": une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

18° "système de nom de domaine" ou "DNS": un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;

19° "fournisseur de services DNS": une entité qui fournit:

a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou

b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;

20° "registre de noms de domaine de premier niveau": une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

21° "entité fournissant des services d'enregistrement de noms de domaine": un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

22° "service numérique": un service au sens de l'article 1er, paragraphe 1er, point *b)*, de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information;

23° "service de confiance": un service de confiance au sens de l'article 3, 16, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le "règlement eIDAS";

24° "prestataire de services de confiance": un prestataire de services de confiance au sens de l'article 3, 19, du règlement eIDAS;

25° "service de confiance qualifié": un service de confiance qualifié au sens de l'article 3, 17, du règlement eIDAS;

26°"gekwalificeerde verlener van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten in de zin van artikel 3, 20, van de eIDAS-verordening;

27° "onlinemarktplaats": een onlinemarktplaats in de zin van artikel I.8, 41°, van het Wetboek van economisch recht;

28° "onlinezoekmachine": een onlinezoekmachine als bedoeld in artikel 2, 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten;

29° "cloudcomputingdienst": een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;

30° "datacentrumdienst": een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT- en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole;

31° "netwerk voor de levering van inhoud": een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

32° "platform voor socialenetwerkdiensten": een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video's en aanbevelingen;

33° "vertegenwoordiger": een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet;

34° "overheidsinstantie": een administratieve overheid bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

a) zij is niet van industriële of commerciële aard;

b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een andere sector of deelsector van een van de bijlagen;

c) zij is geen privaatrechtelijke rechtspersoon.

35° "openbaar elektronische-communicatienetwerk": een openbaar elektronische-communicatienetwerk als bedoeld in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

36° "elektronische-communicatiedienst": een elektronische-communicatiedienst in de zin van artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

37° "entiteit": een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

38° "aanbieder van beheerde diensten": een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de klanten ter plaatse of op afstand;

39° "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;

26° "prestataire de services de confiance qualifiés": un prestataire de services de confiance qualifié au sens de l'article 3, 20, du règlement eIDAS;

27° "place de marché en ligne": une place de marché en ligne au sens de l'article I.8, 41°, du Code de droit économique;

28° "moteur de recherche en ligne": un moteur de recherche en ligne au sens de l'article 2, 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne;

29° "service d'informatique en nuage": un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

30° "service de centre de données": un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental;

31° "réseau de diffusion de contenu": un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services;

32° "plateforme de services de réseaux sociaux": une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;

33° "représentant": une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union européenne, qui peut être contactée par l'autorité nationale de cybersécurité à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi;

34° "entité de l'administration publique": une autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants:

a) elle n'a pas de caractère industriel ou commercial;

b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi;

c) elle n'est pas une personne morale de droit privé.

35° "réseau de communications électroniques public": un réseau public de communications électroniques au sens de l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques;

36° "service de communications électroniques": un service de communications électroniques au sens de l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques;

37° "entité": une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;

38° "fournisseur de services gérés": une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;

39° "fournisseur de services de sécurité gérés": un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;

40° "onderzoeksorganisatie": een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;

41° "Aanbeveling nr. 2003/361/EG": de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen;

42° "wet van 13 juni 2005": de wet van 13 juni 2005 betreffende de elektronische communicatie;

43° "wet van 1 juli 2011": de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

44° "koninklijk besluit van 18 april 1988": het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering;

45° "nationale cyberbeveiligingsautoriteit": de autoriteit bedoeld in artikel 16;

46° "nationaal CSIRT": het nationale computer security incident response team;

47° "Enisa": het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;

48° "NCCN": het Centrum opgericht door het koninklijk besluit van 18 april 1988;

49° "Verordening (EU) 2016/679": Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

50° "gegevensbeschermingsautoriteit": toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;

51° "nationale accreditatie-instantie": de instantie bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, hierna "Verordening (EG) nr. 765/2008";

52° "beveiligingsbeleid voor de netwerk- en informatiesystemen ("I.B.B.")": het beleid vastgelegd in een document bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen door een essentiële of belangrijke entiteit;

53° "conformiteitsbeoordelingsinstantie": de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

54° "sectorale overheid": de overheid bedoeld in artikel 15, § 2;

55° "CSIRT-netwerk": het netwerk van nationale CSIRT's opgericht bij artikel 15 van de NIS2-richtlijn;

56° "samenwerkingsgroep": de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;

57° "significant incident": elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:

1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of

2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

58° "cybercrisis": elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:

1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;

2° een dringende besluitvorming vereist;

3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt.

59° "Instituut": het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

HOOFDSTUK 3. — *Categorieën van entiteiten*

Art. 9. Zijn essentiële entiteiten:

1° de entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden die zijn bepaald in artikel 2, lid 1, van de bijlage bij Aanbeveling nr. 2003/361/EG;

40° "organisme de recherche": une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement;

41° "recommandation n° 2003/361/CE": la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;

42° "loi du 13 juin 2005": la loi du 13 juin 2005 relative aux communications électroniques;

43° "loi du 1er juillet 2011": la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;

44° "arrêté royal du 18 avril 1988": l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;

45° "autorité nationale de cybersécurité": l'autorité visée à l'article 16;

46° "CSIRT national": le centre national de réponse aux incidents de sécurité informatique;

47° "ENISA": l'Agence de l'Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;

48° "NCCN": le Centre institué par l'arrêté royal du 18 avril 1988;

49° "règlement (UE) 2016/679": le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);

50° "autorité de protection des données": autorité de contrôle au sens de l'article 4, 21°, du règlement (UE) 2016/679;

51° "organisme national d'accréditation": l'organisme visé à l'article 2, point 11, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après le "règlement (CE) n° 765/2008";

52° "politique de sécurité des systèmes et réseaux d'information ("P.S.I.")": la politique consignée dans un document visé à l'article 30, reprenant les mesures de sécurité des réseaux et des systèmes d'information, à adopter par une entité essentielle ou importante;

53° "organisme d'évaluation de la conformité": l'organisme visé à l'article 2, point 13, du règlement (CE) n° 765/2008;

54° "autorité sectorielle": l'autorité visée à l'article 15, § 2;

55° "réseau des CSIRT": le réseau des CSIRT nationaux institué par l'article 15 de la directive NIS2;

56° "groupe de coopération": le groupe de coopération établi par l'article 14 de la directive NIS2;

57° "incident significatif": tout incident ayant un impact significatif sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi et qui:

1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée; ou

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

58° "crise cyber": tout incident de cybersécurité qui, par sa nature ou ses conséquences:

1° menace les intérêts vitaux du pays ou les besoins essentiels de la population;

2° requiert des décisions urgentes;

3° demande une action coordonnée de plusieurs départements et organisations.

59° "Institut": l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

CHAPITRE 3. — *Catégories d'entités*

Art. 9. Sont des entités essentielles:

1° les entités d'un type visé à l'annexe I qui excèdent les plafonds applicables aux moyennes entreprises prévus à l'article 2, paragraphe 1er, de l'annexe de la recommandation n° 2003/361/CE;

2° de gekwalificeerde verleners van vertrouwensdiensten en de registers voor topleveldomeinnamen, alsook de DNS-dienstverleners, ongeacht hun omvang;

3° de aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG;

4° de overheidsinstanties die van de Federale Staat afhangen;

5° de entiteiten bedoeld in artikel 3, § 4;

6° alle andere entiteiten van een in bijlage I of II bedoelde soort die worden geïdentificeerd als essentiële entiteiten overeenkomstig artikel 11.

Art. 10. Zijn belangrijke entiteiten:

1° de entiteiten van een in bijlage I of II bedoelde soort die niet als essentiële entiteiten worden beschouwd op basis van artikel 9;

2° de entiteiten die worden geïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.

HOOFDSTUK 4. — *Identificatie*

Art. 11. § 1. Onverminderd artikel 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief of op voorstel van de eventuele betrokken sectorale overheid, een entiteit als een essentiële of belangrijke entiteit, ongeacht haar omvang, in de volgende gevallen:

1° de entiteit is de enige aanbieder, in België, van minstens één dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, met name in een van de sectoren of deelsectoren van de bijlagen I en II van de wet;

2° een verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

3° een verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

4° de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in België.

§ 2. Wat betreft de entiteiten die van de deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

§ 3. In het kader van de identificatie bedoeld in de paragrafen 1 en 2 legt de nationale cyberbeveiligingsautoriteit vooraf een ontwerpbeslissing voor aan de betrokken entiteit en vervolgens aan de eventuele betrokken deelgebieden en sectorale overheden, die binnen zestig dagen een niet-gepubliceerd advies uitbrengen.

Indien binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, kan worden voorbijgegaan aan het feit dat geen advies gegeven is.

In geval van een ongunstig advies van een sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, wordt de ontwerpbeslissing samen met het advies voorgelegd aan het Strategisch Comité Inlichtingen en Veiligheid, opgericht bij het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid die een bindend advies uitbrengen.

§ 4. De nationale cyberbeveiligingsautoriteit evalueert en actualiseert, in voorkomend geval, minstens om de twee jaar de identificatie van essentiële en belangrijke entiteiten volgens de modaliteiten bedoeld in de paragrafen 1 tot 3.

De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van essentiële entiteiten naar het NCCN en naar de eventuele betrokken sectorale overheid.

De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van belangrijke entiteiten naar de eventuele betrokken sectorale autoriteit.

§ 5. In de gevallen bedoeld in paragraaf 1 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die geen deel uitmaakt van de in de bijlage bedoelde sectoren, aanwijzen als een essentiële of belangrijke entiteit.

2° les prestataires de services de confiance qualifiés et les registres de noms de domaines de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille;

3° les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent au moins des moyennes entreprises, en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE;

4° les entités de l'administration publique qui dépendent de l'État fédéral;

5° les entités visées à l'article 3, § 4;

6° toute autre entité d'un type visé à l'annexe I ou II qui est identifiée comme entité essentielle conformément à l'article 11.

Art. 10. Sont des entités importantes:

1° les entités d'un type visé à l'annexe I ou II qui ne sont pas qualifiées d'entités essentielles sur la base de l'article 9;

2° les entités identifiées comme entités importantes conformément à l'article 11.

CHAPITRE 4. — *Identification*

Art. 11. § 1er. Sans préjudice de l'article 6, d'initiative ou sur proposition de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité identifie une entité comme entité essentielle ou importante, quelle que soit sa taille, dans les cas suivants:

1° l'entité est le seul prestataire, en Belgique, d'au moins un service essentiel au maintien d'activités sociétales ou économiques critiques, notamment dans l'un des secteurs ou sous-secteurs repris aux annexes I et II de la loi;

2° une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;

3° une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où une telle interruption pourrait avoir un impact transfrontière;

4° l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants, en Belgique.

§ 2. En ce qui concerne les entités qui dépendent des entités fédérées, l'autorité nationale de cybersécurité identifie les administrations publiques qui, à la suite d'une évaluation basée sur les risques, fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

§ 3. Dans le cadre de l'identification visée aux paragraphes 1er et 2, l'autorité nationale de cybersécurité soumet préalablement un projet de décision à l'entité concernée et ensuite aux éventuelles entités fédérées concernées et autorités sectorielles, qui rendent un avis non publié endéans les soixante jours.

En l'absence d'un avis rendu dans le délai visé à l'alinéa 1er, il peut être passé outre à l'absence d'avis.

En cas d'avis défavorable d'une autorité sectorielle et si l'autorité nationale de cybersécurité souhaite maintenir son projet de décision, le projet de décision, accompagné de l'avis, est soumis au Comité stratégique du renseignement et de la sécurité, créé par l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité, qui rend un avis contraignant.

§ 4. L'autorité nationale de cybersécurité évalue et, le cas échéant, met à jour l'identification des entités essentielles et importantes au moins tous les deux ans, selon les modalités visées aux paragraphes 1er à 3.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités essentielles au NCCN et à l'éventuelle autorité sectorielle concernée.

L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités importantes à l'éventuelle autorité sectorielle concernée.

§ 5. Dans les cas visés au paragraphe 1er, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe.

Art. 12. In het kader van de identificatie bedoeld in artikel 11 bezorgt de betrokken entiteit op verzoek van de nationale cyberbeveiligingsautoriteit of de sectorale overheid, alle informatie die nuttig is voor haar eventuele identificatie.

HOOFDSTUK 5. — *Registratie van de entiteiten*

Art. 13. § 1. Binnen vijf maanden na de inwerkingtreding van de wet of de in artikel 11 bedoelde identificatie registreren essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zich bij de nationale cyberbeveiligingsautoriteit volgens de door deze autoriteit vastgestelde praktische modaliteiten en bezorgen haar de volgende informatie:

1° hun naam, alsook hun registratienummer bij de Kruispuntbank van Ondernemingen (KBO) of een gelijkwaardige registratie in de Europese Unie;

2° hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereiken en hun telefoonnummer;

3° indien van toepassing, de relevante sector en deelsector bedoeld in bijlage I of II, en

4° indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen.

De Koning kan deze lijst met informatie aanvullen.

§ 2. In afwijking van paragraaf 1, eerste lid, vervolledigt de in voornoemde paragraaf bedoelde entiteit, wanneer zij krachtens een wettelijke verplichting al een deel van de in voornoemde paragraaf bedoelde informatie meedeelt aan de betrokken sectorale overheid, deze informatie bij deze sectorale overheid.

De in paragraaf 1, eerste lid, bedoelde entiteit bezorgt de informatie binnen vijf maanden na de inwerkingtreding van de wet, volgens de door voornoemde overheid vastgestelde praktische modaliteiten.

§ 3. De in paragraaf 1, eerste lid, bedoelde entiteiten bezorgen onmiddellijk elke wijziging in de informatie die zij op grond van paragraaf 1, eerste lid, en paragraaf 2, eerste lid, hebben ingediend, en in elk geval binnen twee weken na de datum van de wijziging.

§ 4. De betrokken sectorale overheid bezorgt de krachtens de paragrafen 2 en 3 verzamelde informatie aan de nationale cyberbeveiligingsautoriteit.

De nationale cyberbeveiligingsautoriteit neemt de nodige maatregelen om ervoor te zorgen dat de sectorale overheden de meegedeelde gegevens kunnen raadplegen voor de sectoren die hen aangaan.

Art. 14. § 1. Binnen twee maanden na de inwerkingtreding van de wet verstrekken DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten de nationale cyberbeveiligingsautoriteit volgens de modaliteiten bedoeld in artikel 13, § 1, eerste lid, ten minste de volgende informatie:

1° hun naam;

2° hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;

3° het adres van hun hoofdvestiging en hun andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

4° hun actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers en, indien van toepassing, deze van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

5° de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren; en

6° hun IP-bereiken.

§ 2. De in paragraaf 1 bedoelde entiteiten stellen de nationale cyberbeveiligingsautoriteit onverwijld en in elk geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis van eventuele wijzigingen in de gegevens die zij op grond van paragraaf 1 hebben ingediend.

§ 3. In afwijking van paragraaf 1 worden de in diezelfde paragraaf bedoelde gegevens met betrekking tot gekwalificeerde verleners van vertrouwensdiensten in België, die al zijn verstrekt aan het in artikel 17

Art. 12. Dans le cadre de l'identification visée à l'article 11, l'entité concernée transmet toutes les informations utiles à son éventuelle identification, à la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle.

CHAPITRE 5. — *Enregistrement des entités*

Art. 13. § 1er. Dans les cinq mois suivant l'entrée en vigueur de la loi ou l'identification visée à l'article 11, les entités essentielles, les entités importantes et les entités fournissant des services d'enregistrement de noms de domaine s'enregistrent auprès de l'autorité nationale de cybersécurité selon les modalités pratiques fixées par cette autorité et lui communiquent les informations suivantes:

1° leur dénomination ainsi que leur numéro d'enregistrement auprès de la Banque-carrefour des entreprises (BCE) ou un enregistrement équivalent dans l'Union européenne;

2° leur adresse et leurs coordonnées actualisées, y compris leur adresse de courrier électronique, leurs plages d'IP et leur numéro de téléphone;

3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et

4° le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente loi.

Le Roi peut compléter cette liste d'informations.

§ 2. Par dérogation au paragraphe 1er, alinéa 1er, lorsque l'entité visée au paragraphe précité communique déjà à l'autorité sectorielle concernée certaines des informations visées au paragraphe précité, en vertu d'une obligation légale, l'entité complète ces informations auprès de cette autorité sectorielle.

L'entité visée au paragraphe 1er, alinéa 1er, communique les informations dans les cinq mois suivant l'entrée en vigueur de la loi, selon les modalités pratiques fixées par l'autorité précitée.

§ 3. Les entités visées au paragraphe 1er, alinéa 1er, communiquent sans tarder toute modification des informations qu'elles ont communiquées conformément au paragraphe 1er, alinéa 1er, et paragraphe 2, alinéa 1er, et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

§ 4. L'autorité sectorielle concernée communique les informations collectées en vertu des paragraphes 2 et 3 à l'autorité nationale de cybersécurité.

L'autorité nationale de cybersécurité prend les mesures nécessaires pour que les autorités sectorielles puissent consulter, pour les secteurs qui les concernent, les données communiquées.

Art. 14. § 1er. Dans les deux mois suivant l'entrée en vigueur de la loi, les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux communiquent à l'autorité nationale de cybersécurité, selon les modalités visées à l'article 13, § 1er, alinéa 1er, au moins les informations suivantes:

1° leur nom;

2° leur secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant;

3° l'adresse de leur établissement principal et de leurs autres établissements légaux dans l'Union ou, s'ils ne sont pas établis dans l'Union, de leur représentant désigné conformément à l'article 4, § 3;

4° leurs coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone et, le cas échéant, celles de leur représentant désigné conformément à l'article 4, § 3;

5° les États membres dans lesquels ils fournissent leurs services relevant du champ d'application de la présente loi; et

6° leurs plages d'IP.

§ 2. Les entités visées au paragraphe 1er notifient à l'autorité nationale de cybersécurité toute modification des informations qu'elles ont communiquées en vertu du paragraphe 1er sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

§ 3. Par dérogation au paragraphe 1er, les données visées au même paragraphe, relatives aux prestataires de services de confiance qualifiés en Belgique, qui ont déjà été communiquées à l'organe de contrôle visé

van de eIDAS-verordening bedoelde toezichthoudende orgaan, door dat orgaan doorgestuurd naar de nationale cyberbeveiligingsautoriteit, volgens de door de Koning vastgestelde modaliteiten.

TITEL 2. — *Bevoegde autoriteiten en samenwerking op nationaal niveau*

HOOFDSTUK 1. — *Bevoegde autoriteiten*

Afdeling 1. — Aanwijzing van de bevoegde autoriteiten

Art. 15. § 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.

§ 2. Na advies van de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een sectorale overheid en, in voorkomend geval, een sectorale inspectiedienst aanwijzen die voor een specifieke sector of deelsector belast is met het toezicht op de uitvoering van de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33.

In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van de in het kader van de wet van 1 juli 2011 aangewezen sectorale overheden en sectorale inspectiediensten.

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.

Afdeling 2. — De nationale cyberbeveiligingsautoriteit

Art. 16. De nationale cyberbeveiligingsautoriteit is belast met de opvolging en coördinatie van de uitvoering van deze wet, het toezicht op de uitvoering ervan door de essentiële en belangrijke entiteiten, alsook met het beheer van cybercrises en cyberbeveiligingsincidenten overeenkomstig artikel 18.

Daartoe vervult de nationale cyberbeveiligingsautoriteit de taken van bevoegde autoriteit voor essentiële en belangrijke entiteiten, van nationaal CSIRT, van centraal nationaal contactpunt voor de uitvoering van deze wet, en vertegenwoordigt zij België in de samenwerkingsgroep, het CSIRT-netwerk en het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) bedoeld in artikel 16 van de NIS2-richtlijn.

Onderafdeling 1. — Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging

Art. 17. De nationale cyberbeveiligingsautoriteit heeft de volgende taken:

1° het zorgen voor coördinatie tussen de bevoegde autoriteiten in het kader van de toepassing van deze wet, alsook tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberbeveiliging in België;

2° het opvolgen en coördineren van en toezien op de uitvoering van de nationale cyberbeveiligingsstrategie bedoeld in artikel 28;

3° het identificeren van de essentiële en belangrijke entiteiten overeenkomstig artikel 11;

4° het toezien op de uitvoering van de wet door de essentiële en belangrijke entiteiten overeenkomstig titel 4;

5° het zorgen voor coördinatie tussen de overheden en de private sector of de wetenschappelijke wereld;

6° het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader op het vlak van cyberbeveiliging;

7° het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor de cyberbeveiliging van de verschillende soorten informatiesystemen;

8° het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberbeveiliging, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;

9° het fungeren als centraal contactpunt dat een verbindingsfunctie vervult om, in het kader van de toepassing van deze wet, te zorgen voor grensoverschrijdende samenwerking van de Belgische autoriteiten met de bevoegde autoriteiten van andere lidstaten van de Europese Unie en in voorkomend geval met de Europese Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde Belgische autoriteiten;

à l'article 17 du règlement eIDAS sont transmises par cet organe à l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi.

TITRE 2. — *Autorités compétentes et coopération au niveau national*

CHAPITRE 1er. — *Autorités compétentes*

Section 1re. — Désignation des autorités compétentes

Art. 15. § 1er. Le Roi désigne l'autorité nationale de cybersécurité.

§ 2. Après avis de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner une autorité sectorielle et, le cas échéant, un service d'inspection sectoriel chargé, pour un secteur ou sous-secteur spécifique, de la supervision de la mise en œuvre des mesures sectorielles ou sous-sectorielles supplémentaires de gestion des risques en matière de cybersécurité visées à l'article 33.

Dans le cadre de la désignation visée à l'alinéa 1er, le Roi tient compte de l'identité des autorités sectorielles et services d'inspection sectoriels désignées dans le cadre de la loi du 1er juillet 2011.

Le Roi peut, par arrêté délibéré en Conseil des ministres, créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92ter de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Par dérogation à l'alinéa 1er, la présente loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régis par la loi.

Section 2. — L'autorité nationale de cybersécurité

Art. 16. L'autorité nationale de cybersécurité est chargée du suivi et de la coordination de la mise en œuvre de la présente loi, de veiller à la mise en œuvre de la présente loi par les entités essentielles et importantes ainsi que de la gestion des crises cyber et incidents de cybersécurité conformément à l'article 18.

À ce titre, l'autorité nationale de cybersécurité assure les tâches d'autorité compétente pour les entités essentielles et importantes, de CSIRT national, de point de contact national unique pour l'exécution de la présente loi et de représentation de la Belgique au sein du groupe de coopération, du réseau des CSIRT et du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) visé à l'article 16 de la directive NIS2.

Sous-section 1re. — Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité

Art. 17. Les tâches de l'autorité nationale de cybersécurité sont les suivantes:

1° assurer la coordination entre les autorités compétentes dans le cadre de l'application de la présente loi, ainsi qu'entre les différents services et autorités concernés par la cybersécurité en Belgique;

2° superviser, coordonner et veiller à la mise en œuvre de la stratégie nationale en matière de cybersécurité visée à l'article 28;

3° identifier des entités essentielles et importantes conformément à l'article 11;

4° superviser la mise en œuvre de la loi par les entités essentielles et importantes conformément au titre 4;

5° assurer la coordination entre les autorités publiques et le secteur privé ou le monde scientifique;

6° formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;

7° élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes pour la cybersécurité des différents types de systèmes d'information;

8° coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière;

9° servir de point de contact unique exerçant une fonction de liaison visant à assurer, dans le cadre de l'application de la présente loi, la coopération transfrontière des autorités belges avec les autorités compétentes des autres États membres de l'Union européenne et, le cas échéant, avec la Commission européenne et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes belges;

10° het coördineren van de evaluatie en certificering van de beveiliging van informatie- en communicatiesystemen;

11° het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen;

12° het toekennen van subsidies voor projecten en activiteiten rond cyberbeveiliging, binnen de grenzen van haar begrotingskredieten en volgens de voorwaarden bepaald door de Koning;

13° het faciliteren en aanmoedigen van de organisatie van opleidingen rond cyberbeveiliging voor personeelsleden van essentiële of belangrijke entiteiten;

14° het opstellen van een lijst van essentiële en belangrijke entiteiten, alsook van entiteiten die domeinnaamregistratiediensten verlenen. Vervolgens het regelmatig en ten minste om de twee jaar evalueren en, in voorkomend geval, actualiseren van die lijst.

Onderafdeling 2. — Taken met betrekking tot het cybercrisisbeheer

Art. 18. Onverminderd de artikelen 8 en 9 van de wet van 15 mei 2007 betreffende de civiele veiligheid en de uitvoeringsbesluiten ervan en onverminderd de bevoegdheden van het NCCN vervult de nationale cyberbeveiligingsautoriteit de volgende taken met betrekking tot het cybercrisisbeheer:

1° in samenwerking met het NCCN, het vaststellen van de capaciteiten, middelen en procedures die in geval van een cybercrisis kunnen worden ingezet;

2° het opvolgen van de opmaak, actualisering en operationalisering van het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons bedoeld in artikel 29, in samenwerking met het NCCN;

3° het vervullen van de rol van coördinator bij het beheer van cybercrises en cyberbeveiligingsincidenten, in voorkomend geval overeenkomstig het in 2° bedoelde plan.

Onderafdeling 3. — Taken en voorschriften met betrekking tot de rol van nationaal CSIRT

Art. 19. § 1. Het nationale CSIRT heeft de volgende taken:

1° het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen;

2° het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;

3° het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;

4° het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;

5° op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;

6° het deelnemen aan het CSIRT-netwerk, het doeltreffend, efficiënt en veilig samenwerken in dit netwerk en, in overeenstemming met zijn capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van dit netwerk op hun verzoek;

7° indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 22 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;

8° het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie;

9° het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen als deze scan wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren en deze geen negatieve gevolgen heeft voor de werking van de diensten van de entiteiten;

10° het opsporen, observeren en analyseren van computerbeveiligingsproblemen;

11° het tot stand brengen van samenwerkingsrelaties met relevante belanghebbenden in de private sector, teneinde de doelstellingen van deze wet te verwezenlijken;

10° coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;

11° informer et sensibiliser les utilisateurs des systèmes d'information et de communication;

12° accorder des subventions pour des projets et activités relatifs à la cybersécurité, dans les limites de ses crédits budgétaires et selon les conditions établies par le Roi;

13° faciliter et encourager l'organisation de formations en matière de cybersécurité pour les membres du personnel des entités essentielles ou importantes;

14° établir une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Par la suite, réexaminer cette liste et, le cas échéant, la mettre à jour régulièrement et au moins tous les deux ans.

Sous-section 2. — Tâches relatives au rôle de gestion des crises cyber

Art. 18. Sans préjudice des articles 8 et 9 de la loi du 15 mai 2007 relative à la sécurité civile et de leurs arrêtés d'exécution et sans préjudice des compétences du NCCN, les tâches de l'autorité nationale de cybersécurité relatives au rôle de gestion des crises cyber sont les suivantes:

1° en collaboration avec le NCCN, recenser les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise cyber;

2° superviser, en collaboration avec le NCCN, la rédaction, l'actualisation et l'opérationnalisation du plan national de réaction aux crises cyber et incidents de cybersécurité visé à l'article 29;

3° assurer le rôle de coordinateur dans la gestion des crises cyber et incidents de cybersécurité, le cas échéant conformément au plan visé au 2°.

Sous-section 3. — Tâches et obligations relatives au rôle de CSIRT national

Art. 19. § 1er. Les tâches du CSIRT national sont les suivantes:

1° surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information;

2° activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant;

4° rassembler et analyser des données forensiques, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité;

5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif des réseaux et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;

6° participer au réseau des CSIRT, coopérer de manière effective, efficace et sécurisée au sein de ce réseau et apporter une assistance mutuelle en fonction de ses capacités et de ses compétences aux autres membres du réseau des CSIRT à leur demande;

7° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 22;

8° contribuer au déploiement d'outils sécurisés de partage d'informations;

9° procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public lorsque ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées et qu'il n'a pas d'effet négatif sur le fonctionnement des services des entités;

10° détecter, observer et analyser des problèmes de sécurité informatique;

11° établir des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente loi;

12° het vergemakkelijken van de in punt 11° bedoelde samenwerking door de invoering en het gebruik te bevorderen van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot:

a) procedures voor de incidentenbehandeling;

b) crisisbeheer; en

c) de gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 22;

13° het samenwerken en in voorkomend geval uitwisselen van relevante informatie overeenkomstig artikel 27 met de in datzelfde artikel bedoelde gemeenschappen;

14° het deelnemen aan de overeenkomstig artikel 19 van de NIS2-richtlijn georganiseerde collegiale toetsingen.

Na advies van het nationale CSIRT kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, dit CSIRT bijkomende taken toevertrouwen.

§ 2. Bij de uitvoering van de in paragraaf 1 bedoelde taken kan het nationale CSIRT, op grond van een risicogebaseerde benadering, prioriteit geven aan bepaalde taken.

Art. 20. De voorschriften voor het nationale CSIRT omvatten het volgende:

1° beschikken over een passende, veilige en weerbare communicatie- en informatie-infrastructuur waardoor informatie kan worden uitgewisseld met essentiële en belangrijke entiteiten en andere relevante belanghebbenden;

2° een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten te voorkomen en te allen tijde te beschikken over diverse kanalen waarlangs ze gecontacteerd kunnen worden en contact met anderen kunnen opnemen; de communicatiekanalen duidelijk specificeren en meedelen aan de gebruikersgroep en de samenwerkingspartners;

3° beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden;

4° uitgerust zijn met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op doeltreffende en efficiënte overdrachten;

5° de vertrouwelijkheid en betrouwbaarheid van zijn activiteiten waarborgen;

6° beschikken over voldoende personeel om te allen tijde de beschikbaarheid van zijn diensten te garanderen, en ervoor zorgen dat zijn personeel naar behoren wordt opgeleid;

7° uitgerust zijn met redundante systemen en reservewerkruimten om de continuïteit van zijn diensten te waarborgen.

Art. 21. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 19 en 20 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen, en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 19, § 1, 1° tot 5°, kan het nationale CSIRT identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronischecommunicatiemetagegevens bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 verkrijgen van een operator in de zin van artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.

Zonder afbreuk te doen aan of zich in te mengen in de bevoegdheden van personen die de gerechtelijke politie uitoefenen en de gerechtelijke autoriteiten, worden met voornoemde taken de volgende doeleinden nagestreefd:

1° zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronischecommunicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

3° het onderzoeken van beveiligingsproblemen bij elektronischecommunicatienetwerken of -diensten of informatiesystemen.

Het nationale CSIRT kan bepalen binnen welke termijn de operator op zijn verzoek moet reageren, naargelang de dringendheid hiervan.

12° faciliter la coopération visée au 11° en encourageant l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne:

a) les procédures de gestion des incidents;

b) la gestion de crise; et

c) la divulgation coordonnée des vulnérabilités en vertu de l'article 22;

13° coopérer et, le cas échéant, échanger des informations pertinentes conformément à l'article 27 avec les communautés visées au même article;

14° participer aux évaluations par les pairs organisées conformément à l'article 19 de la directive NIS2.

Après avis du CSIRT national, le Roi peut, par arrêté délibéré en Conseil des ministres, lui confier des tâches supplémentaires.

§ 2. Lorsqu'il exécute les tâches visées au paragraphe 1er, le CSIRT national peut donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

Art. 20. Les obligations du CSIRT national sont les suivantes:

1° disposer d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente lui permettant d'échanger des informations avec les entités essentielles et importantes et les autres parties prenantes;

2° veiller à un niveau élevé de disponibilité de ses canaux de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contacté et contacter autrui à tout moment; spécifier clairement les canaux de communication et les faire connaître aux partenaires et collaborateurs;

3° disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés;

4° être doté d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

5° garantir la confidentialité et la fiabilité de ses opérations;

6° être doté des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de ses services et veiller à ce que son personnel reçoive une formation appropriée;

7° être doté de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de ses services.

Art. 21. § 1er. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 19 et 20. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 19, § 1er, 1° à 5°, le CSIRT national peut obtenir d'un opérateur visé à l'article 2, 11°, de la loi du 13 juin 2005, des données d'identification visées à l'article 2, alinéa 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.

Sans porter atteinte aux, ou sans s'immiscer dans les compétences des personnes exerçant la police judiciaire ni des autorités judiciaires, les finalités poursuivies par les tâches précitées sont:

1° sans finalité à caractère pénal, la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave;

2° la prévention de menaces graves contre la sécurité publique;

3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information.

Le CSIRT national peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci.

§ 3. Indien het nationale CSIRT een operator een verzoek om identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.

§ 4. Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegevens in de zin van artikel 2, 93°, van de wet van 13 juni 2005 die geen in paragraaf 3 bedoelde gegevens zijn, stuurt, wordt dat verzoek vooraf gecontroleerd door de gegevensbeschermingsautoriteit.

In dringende en naar behoren met redenen omklede gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het eerste lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het eerste lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.

Indien de gegevensbeschermingsautoriteit, na de in het tweede lid bedoelde controle, weigert de geldigheid van het in het eerste lid bedoelde verzoek om elektronische-communicatiemetagegevens te bevestigen, stelt het nationale CSIRT de betrokken operator daarvan onverwijld in kennis en verwijdert het de ontvangen metagegevens.

§ 5. De directeur-generaal van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om de in dit artikel bedoelde elektronische-communicatiegegevens te verwerken.

§ 6. Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.

§ 7. Onverminderd de artikelen 28quinquies, § 1, en 57, § 1, van het Wetboek van strafvordering mag het nationale CSIRT, om die doelstellingen te verwezenlijken, alle beschikbare gegevens bezitten, onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 8. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid, waarbij er steeds bij voorrang voor wordt gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 22. § 1. In zijn rol van coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden treedt het nationale CSIRT op als betrouwbare tussenpersoon en vergemakkelijkt het, waar nodig, de interactie tussen de natuurlijke of rechtspersoon die een mogelijke kwetsbaarheid meldt enerzijds en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten anderzijds, op verzoek van een van beide partijen.

In dat kader omvatten de taken van het nationale CSIRT met name:

1° het identificeren van en contact opnemen met de betrokken entiteiten;

2° het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden; en

3° het onderhandelen over tijdschema's voor de bekendmaking, en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.

§ 2. Iedere natuurlijke of rechtspersoon kan, zelfs desgevraagd anoniem, aan het nationale CSIRT het bestaan van een mogelijke kwetsbaarheid melden.

De melding gebeurt schriftelijk, volgens de procedure die op de website van het nationale CSIRT beschreven is.

Deze melding doet geen afbreuk aan de toepassing van de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector of van wettelijke bepalingen betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de overheidssector.

§ 3. Het nationale CSIRT ziet erop toe dat de gemelde kwetsbaarheid zorgvuldig wordt opgevolgd en waarborgt de anonimiteit van de natuurlijke of rechtspersoon die de kwetsbaarheid meldt, voor zover deze persoon hierom verzoekt en de in artikel 23 bedoelde voorwaarden naleeft.

§ 3. Lorsque le CSIRT national adresse à un opérateur une demande de données d'identification visées à l'article 2, alinéa 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

§ 4. Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi du 13 juin 2005 autres que celles visées au paragraphe 3, cette demande fait l'objet d'un contrôle préalable par l'autorité de protection des données.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 1er et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 1er pour permettre un contrôle ultérieur.

Lorsqu'à la suite du contrôle visé à l'alinéa 2, l'autorité de protection des données refuse de confirmer la validité de la demande de métadonnées de communications électroniques visée à l'alinéa 1er, le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 5. Le directeur général du CSIRT national désigne expressément les personnes habilitées à traiter les données de communications électroniques visées au présent article.

§ 6. Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.

§ 7. Sans préjudice des articles 28quinquies, § 1er, et 57, § 1er, du Code d'instruction criminelle, pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 8. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 22. § 1er. Dans son rôle de coordinateur aux fins de la divulgation coordonnée des vulnérabilités, le CSIRT national fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une potentielle vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties.

Dans ce cadre, les tâches du CSIRT national consistent notamment à:

1° identifier et contacter les entités concernées;

2° apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et

3° négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

§ 2. Toute personne physique ou morale peut signaler, même de manière anonyme lorsqu'elle le demande, au CSIRT national l'existence d'une potentielle vulnérabilité.

Le signalement est effectué par écrit, selon la procédure détaillée sur le site internet du CSIRT national.

Ce signalement est sans préjudice de l'application de la loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé ou des dispositions légales sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur public.

§ 3. Le CSIRT national veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité, pour autant que cette personne le demande et respecte les conditions visées à l'article 23.

Het nationale CSIRT waarborgt de volledigheid, integriteit, duurzame opslag en geheimhouding van de informatie die via de melding wordt overgemaakt.

De toegang tot deze informatie wordt beperkt tot personen die daartoe door de directeur-generaal van het nationale CSIRT gemachtigd zijn, behalve indien het delen van deze informatie noodzakelijk is voor de uitvoering van de taken opgesomd in dit artikel.

§ 4. Met inachtneming van de voorwaarden opgesomd in artikel 21, § § 1 en 4, kan het nationale CSIRT de beveiliging van een netwerk- en informatiesysteem observeren, onderzoeken en testen om te bepalen of er sprake is van een mogelijke kwetsbaarheid of om de door de melder gebruikte methoden na te gaan.

§ 5. Wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat, werkt het nationale CSIRT, in voorkomend geval, samen met andere als coördinator aangewezen CSIRT's binnen het CSIRT-netwerk.

§ 6. De directeur-generaal van het nationale CSIRT zorgt voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werkt hij interne procedures uit.

Art. 23. § 1. In het kader van de procedure bedoeld in artikel 22 plegen melders geen inbreuk op de artikelen 314*bis*, 458, 550*bis* en 550ter van het Strafwetboek en op artikel 145 van de wet van 13 juni 2005, op voorwaarde dat:

1° zij zonder bedrieglijk opzet of het oogmerk om te schaden hebben gehandeld;

2° zij onverwijld en uiterlijk binnen vierentwintig uur na de ontdekking van een mogelijke kwetsbaarheid een vereenvoudigde kennisgeving met de identificatie van het betrokken systeem en een eenvoudige beschrijving van de mogelijke kwetsbaarheid hebben gestuurd naar de organisatie die verantwoordelijk is voor het systeem en naar het nationale CSIRT;

3° zij onverwijld en uiterlijk binnen tweeënzeventig uur na de ontdekking van een mogelijke kwetsbaarheid een volledige kennisgeving hebben gestuurd naar de organisatie die verantwoordelijk is voor het systeem, in voorkomend geval met inachtneming van de door deze organisatie vastgestelde meldingsmodaliteiten, en naar het nationale CSIRT, overeenkomstig de in artikel 22, § 2, bedoelde procedure;

4° zij niet verder zijn gegaan dan nodig en evenredig was om het bestaan van een kwetsbaarheid na te gaan en die te melden;

5° zij de informatie over de ontdekte kwetsbaarheid en de kwetsbare systemen niet openbaar hebben gemaakt zonder de toestemming van het nationale CSIRT;

6° zij, wat betreft de netwerken en systemen van de in artikel 5, § § 4 en 5, bedoelde organisaties en van de rechterlijke instanties, en de informatie die door hen of namens hen wordt verwerkt, vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde dienst over de te hanteren modaliteiten en methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden.

§ 2. Personen die informatie melden over een mogelijke kwetsbaarheid waarvan zij in het kader van hun beroep kennis hebben gekregen, worden niet geacht hun beroepsgeheim te hebben geschonden en kunnen op generlei wijze aansprakelijk worden gesteld voor de overdracht van informatie die noodzakelijk was om een mogelijke kwetsbaarheid aan het nationale CSIRT te melden.

§ 3. Voor elke andere mogelijke aansprakelijkheid van melders die voortvloeit uit handelingen of nalatigheden die niet noodzakelijk zijn voor de uitvoering van de in artikel 22 bedoelde procedure en die niet voldoen aan de voorwaarden van paragraaf 1, blijft het toepasselijke recht gelden.

Afdeling 3. — De eventuele sectorale overheden

Art. 24. Onverminderd de andere bepalingen kan de sectorale overheid:

1° sectorale oefeningen organiseren, coördineren of eraan deelnemen, voor wat betreft de maatregelen bedoeld in de artikelen 30 en 33;

2° de gevolgen van een incident voor de sector analyseren en beheren;

3° deelnemen aan de werkzaamheden van de samenwerkingsgroep voor de onderwerpen die betrekking hebben op haar bevoegdheden;

4° de entiteiten die onder haar sector vallen sensibiliseren.

HOOFDSTUK 2. — *Samenwerking op nationaal niveau*

Art. 25. § 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.

Le CSIRT national préserve l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement.

L'accès à ces informations est limité aux personnes habilitées par le directeur général du CSIRT national, sauf lorsque le partage de ces informations s'avère nécessaire à l'exécution des tâches énumérées au présent article.

§ 4. Tout en respectant les conditions énumérées à l'article 21, § § 1er et 4, le CSIRT national peut observer, étudier ou tester la sécurité d'un réseau et système d'information afin de déterminer l'existence d'une vulnérabilité potentielle ou de vérifier les méthodes utilisées par l'auteur de signalement.

§ 5. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact significatif sur des entités dans plusieurs États membres, le CSIRT national coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT.

§ 6. Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.

Art. 23. § 1er. Dans le cadre de la procédure visée à l'article 22, les auteurs de signalement ne commettent pas d'infraction aux articles 314*bis*, 458, 550*bis*, 550ter du Code pénal et de l'article 145 de la loi du 13 juin 2005 à condition:

1° qu'ils aient agi sans intention frauduleuse, ni dessein de nuire;

2° qu'ils aient adressé une notification simplifiée qui reprend l'identification du système concerné et une description simple de la vulnérabilité potentielle, sans délai et au plus tard dans les vingt-quatre heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système et au CSIRT national;

3° qu'ils aient adressé une notification complète, sans délai et au plus tard dans les septante-deux heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système, le cas échéant dans le respect des modalités de signalement établis par cette organisation, et au CSIRT national, conformément à la procédure visée à l'article 22, § 2;

4° qu'ils n'aient pas agi au-delà de ce qui était nécessaire et proportionné pour vérifier l'existence d'une vulnérabilité et pour la rapporter;

5° qu'ils n'aient pas publiquement divulgué les informations relatives à la vulnérabilité découverte et aux systèmes vulnérables, sans l'accord du CSIRT national;

6° en ce qui concerne les réseaux et systèmes des organisations visées à l'article 5, § § 4 et 5, et des organes judiciaires ainsi que les informations traitées par eux ou pour leur compte, qu'ils aient, avant la commission de ces actes, conclu un accord écrit avec le service compétent sur les modalités et la méthodologie à utiliser dans le cadre de la recherche de potentielles vulnérabilités.

§ 2. Lorsque des personnes signalent des informations sur une potentielle vulnérabilité dont ils ont eu connaissance dans leur contexte professionnel, elles ne sont pas considérées comme ayant enfreint leur obligation de secret professionnel et n'encourent aucune responsabilité d'aucune sorte concernant la transmission d'informations nécessaires pour signaler une potentielle vulnérabilité au CSIRT national.

§ 3. Toute autre responsabilité éventuelle des auteurs de signalement découlant d'actes ou d'omissions qui ne sont pas nécessaires à l'accomplissement de la procédure visée à l'article 22 et ne respectent pas les conditions du paragraphe 1er continue d'être régie par le droit applicable.

Section 3. — Les éventuelles autorités sectorielles

Art. 24. Sans préjudice des autres dispositions, l'autorité sectorielle peut:

1° organiser des exercices sectoriels, les coordonner ou y participer, pour ce qui concerne les mesures visées aux articles 30 et 33;

2° analyser et gérer les conséquences d'un incident pour le secteur;

3° participer aux travaux du groupe de coopération pour ce qui concerne les sujets qui touchent à ses compétences;

4° sensibiliser les entités relevant de son secteur.

CHAPITRE 2. — *Coopération au niveau national*

Art. 25. § 1er. Les autorités visées au chapitre 1er du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.

§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening (EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de wet van 1 juli 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten.

§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.

§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de wet van 1 juli 2011 bevoegde autoriteiten werken samen en wisselen regelmatig informatie uit inzake het als kritiek aanmerken van infrastructuren, over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.

§ 5. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de autoriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 en de wet van 13 juni 2005, wisselen regelmatig relevante informatie uit, onder meer met betrekking tot relevante incidenten en cyberdreigingen.

§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform op dat de in artikel 15 bedoelde autoriteiten en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van deze wet op elkaar af te stemmen.

HOOFDSTUK 3. — *Vertrouwelijkheid en informatie-uitwisseling*

Art. 26. § 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of andere wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de nationale openbare veiligheid waarborgen.

§ 2. Eenieder die beroepshalve zijn medewerking dient te verlenen aan de conformiteitsbeoordeling of het toezicht is tot geheimhouding verplicht. Diegene die dit geheim schendt, wordt gestraft met de straffen bepaald in artikel 458 van het Strafwetboek.

Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet.

Deze personen verkrijgen het akkoord van de autoriteiten bedoeld in artikel 5, § 4, wanneer deze autoriteiten bij het geheim betrokken zijn.

§ 3. De autoriteiten bedoeld in hoofdstuk 1 van deze titel en de essentiële of belangrijke entiteiten, of hun onderaannemers, beperken de toegang tot de informatie in het kader van deze wet tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

§ 4. De informatie die door essentiële of belangrijke entiteiten aan de autoriteiten bedoeld in hoofdstuk 1 van deze titel wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1er coopèrent également, au niveau national, avec le NCCN, les services administratifs de l'État, les autorités administratives, en ce compris les autorités nationales en vertu des règlements (CE) nº 300/2008 et nº 2018/1139, les organes de contrôle au titre du règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque Nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi du 1er juillet 2011, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de protection des données.

§ 3. Les entités essentielles et importantes et les autorités visées au chapitre 1er du présent titre collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

§ 4. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes dans le cadre de la loi du 1er juillet 2011 coopèrent et échangent régulièrement des informations sur le recensement des infrastructures critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les exploitants d'infrastructures recensées en tant qu'infrastructures critiques en vertu de la loi du 1er juillet 2011 et sur les mesures prises pour faire face à ces risques, menaces et incidents.

§ 5. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu du règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 et de la loi du 13 juin 2005, échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

§ 6. L'autorité nationale de cybersécurité crée une plateforme de coordination et d'évaluation afin que les autorités visées à l'article 15 et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la présente loi.

CHAPITRE 3. — *Confidentialité et échanges d'information*

Art. 26. § 1er. Le présent article ne porte pas préjudice à l'application de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, de la loi du 11 avril 1994 relative à la publicité de l'administration ou d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.

§ 2. Toute personne qui est appelée à prêter son concours professionnel à l'évaluation de la conformité ou à la supervision est tenue au secret. Celui qui viole ce secret est puni des peines prévues à l'article 458 du Code pénal.

Les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie sont autorisées à faire connaître ces secrets pour l'exécution de la présente loi.

Ces personnes obtiennent l'accord des autorités visées à l'article 5, § 4, lorsque ces autorités sont concernées par le secret.

§ 3. Les autorités visées au chapitre 1er du présent titre, les entités essentielles ou importantes, ou leurs sous-traitants, limitent l'accès aux informations dans le cadre de la présente loi aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la présente loi.

§ 4. Les informations fournies aux autorités visées au chapitre 1er du présent titre par les entités essentielles ou importantes, peuvent être échangées avec des autorités de l'Union européenne, avec des autorités belges ou étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening (EU) 2016/679. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de beveiligings- en commerciële belangen van essentiële of belangrijke entiteiten beschermd.

Art. 27. § 1. Binnen het toepassingsgebied van deze wet vallende entiteiten en, indien van toepassing, andere entiteiten die niet binnen het toepassingsgebied van deze wet vallen, kunnen op vrijwillige basis onderling, binnen gemeenschappen, relevante informatie over cyberbeveiliging uitwisselen, met inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden, technieken en procedures, indicatoren voor aantasting, vijandige tactieken, dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen te detecteren, wanneer dat uitwisselen van informatie:

1° beoogt incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;

2° het niveau van de cyberbeveiliging verhoogt, met name door de bewustwording met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beperken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en openbaarmaking van kwetsbaarheden, het opsporen van dreigingen, beheersings- en preventietechnieken, beperkingsstrategieën of respons- en herstelfasen te ondersteunen of gezamenlijk onderzoek naar cyberdreigingen door publieke en private entiteiten te bevorderen.

§ 2. De informatie-uitwisseling bedoeld in paragraaf 1 wordt uitgevoerd door middel van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie.

§ 3. De nationale cyberbeveiligingsautoriteit faciliteert de vaststelling van de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging. In dergelijke regelingen kunnen de operationele elementen, met inbegrip van het gebruik van specifieke ICT-platforms en automatiseringshulpmiddelen, de inhoud en de voorwaarden van de informatie-uitwisselingsregelingen worden gespecificeerd. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden kunnen voorwaarden opleggen aan het gebruik van de informatie die zij ter beschikking stellen van de gemeenschappen bedoeld in paragraaf 1.

§ 4. De essentiële en belangrijke entiteiten stellen de nationale cyberbeveiligingsautoriteit in kennis van hun deelname aan de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

HOOFDSTUK 4. — *Nationale cyberbeveiligingsstrategie*

Art. 28. § 1. De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de vijf jaar bij op basis van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN en, in voorkomend geval, de gegevensbeschermingsautoriteiten.

Deze strategie bepaalt de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.

§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:

1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;

2° een governancekader om de in punt 1° bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van de taken en verantwoordelijkheden van de overheid en de andere belanghebbenden alsook van het in paragraaf 3 bedoelde beleid;

3° een governancekader dat de taken en verantwoordelijkheden van de belanghebbenden in België verduidelijkt, ter onderbouwing van de samenwerking en coördinatie, in België, tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel, alsook van de samenwerking en coördinatie tussen die autoriteiten en uit hoofde van sectorspecifieke rechtsinstrumenten van de Europese Unie bevoegde autoriteiten;

4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;

Les informations échangées se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect du règlement (UE) 2016/679. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

Art. 27. § 1er. À titre volontaire, les entités relevant du champ d'application de la présente loi et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente loi peuvent échanger, entre elles, au sein de communautés, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

1° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;

2° renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

§ 2. L'échange d'informations visé au paragraphe 1er est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

§ 3. L'autorité nationale de cybersécurité facilite la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. L'autorité nationale de cybersécurité et les éventuelles autorités sectorielles peuvent imposer des conditions d'utilisation des informations qu'elles mettent à disposition des communautés visées au paragraphe 1er.

§ 4. Les entités essentielles et importantes notifient à l'autorité nationale de cybersécurité leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

CHAPITRE 4. — *Stratégie nationale en matière de cybersécurité*

Art. 28. § 1er. Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les cinq ans, sur la base d'indicateurs de performance, après avis du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN et, le cas échéant, des autorités de protection des données.

Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et règlementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.

§ 2. La stratégie nationale en matière de cybersécurité comprend, entre autres:

1° les objectifs et les priorités de la stratégie nationale en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;

2° un cadre de gouvernance visant à atteindre les objectifs et les priorités visés au 1°, y compris les tâches et les responsabilités des autorités publiques et des autres acteurs concernés ainsi que les politiques visées au paragraphe 3;

3° un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes en Belgique, et sur lequel reposent la coopération et la coordination, en Belgique, entre les autorités visées au chapitre 1er du présent titre ainsi que la coopération et la coordination entre ces autorités et les autorités compétentes en vertu d'instruments juridiques sectoriels de l'Union européenne;

4° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;

5° een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de private sector;

6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;

7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;

8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;

9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;

10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.

§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale cyberbeveiligingsstrategie:

1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;

2° inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;

3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 22;

4° inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;

5° voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;

6° voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligingsvaardigheden, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiëne, gericht op burgers, belanghebbenden en entiteiten;

7° voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;

8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillig delen van cyberbeveiligingsinformatie tussen entiteiten;

9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiëne van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze wet zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;

10° voor het bevorderen van actieve cyberbescherming.

HOOFDSTUK 5. — *Het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons*

Art. 29. § 1. De Koning stelt, bij besluit vastgesteld na overleg in de Ministerraad, een nationaal plan voor cyberbeveiligingsincidenten en cybercrisisrespons op. Dit plan is een nationaal plan in de zin van artikel 9, § 2, van de wet van 15 mei 2007 betreffende de civiele veiligheid.

§ 2. Onverminderd de elementen die moeten worden opgenomen in de nationale plannen, bevat het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons ten minste:

1° de doelstellingen van de nationale paraatheidsmaatregelen en -activiteiten;

2° de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

5° un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;

6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;

7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu de la loi du 1er juillet 2011 aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;

8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;

9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;

10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.

§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont adoptées et portent sur les éléments suivants:

1° la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services;

2° l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes;

3° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;

4° le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;

5° la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;

6° la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et de développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;

7° le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;

8° la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités;

9° le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;

10° la promotion d'une cyberprotection active.

CHAPITRE 5. — *Le plan national de réaction aux crises cyber et incidents de cybersécurité*

Art. 29. § 1er. Le Roi établit, par arrêté délibéré en Conseil des ministres, un plan national de réaction aux crises cyber et incidents de cybersécurité. Ce plan constitue un plan national au sens de l'article 9, § 2, de la loi du 15 mai 2007 relative à la sécurité civile.

§ 2. Sans préjudice des éléments devant être contenus dans les plans nationaux, le plan national de réaction aux crises cyber et incidents de cybersécurité contient au moins les éléments suivants:

1° les objectifs des mesures et activités nationales de préparation;

2° les tâches et responsabilités des autorités de gestion des crises cyber;

3° de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;

4° de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

5° de relevante publieke en private belanghebbenden en betrokken infrastructuur;

6° de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van België aan het gecoördineerde beheer van cybercrises en cyberbeveiligingsincidenten op het niveau van de Europese Unie en de ondersteuning daarvan te waarborgen.

TITEL 3. — *Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen*

HOOFDSTUK 1. — *Maatregelen voor het beheer van cyberbeveiligingsrisico's*

Art. 30. § 1. De essentiële en belangrijke entiteiten nemen passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun activiteiten of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

§ 2. Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in paragraaf 1 bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

§ 3. De in paragraaf 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en hebben ten minste betrekking op het volgende:

1° beleid inzake risicoanalyse en beveiliging van informatiesystemen;

2° incidentenbehandeling;

3° bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;

4° de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

5° beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

6° beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

7° basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

8° beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

9° beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

10° wanneer gepast, het gebruik van multifactorauthenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;

11° een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

§ 4. Wanneer essentiële en belangrijke entiteiten nagaan welke maatregelen bedoeld in paragraaf 3, 4°, passend zijn, houden zij rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.

Deze maatregelen moeten passend zijn in het licht van de resultaten van de op het niveau van de Europese Unie gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

3° les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations;

4° les mesures de préparation nationales, y compris des exercices et des activités de formation;

5° les parties prenantes et les infrastructures des secteurs public et privé concernées;

6° les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de la Belgique à la gestion coordonnée des crises cyber et incidents de cybersécurité au niveau de l'Union européenne.

TITRE 3. — *Mesures de gestion des risques en matière de cybersécurité et obligations d'information*

CHAPITRE 1. — *Mesures de gestion des risques en matière de cybersécurité*

Art. 30. § 1er. Les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

§ 2. Les mesures visées au paragraphe 1er garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

§ 3. Les mesures visées au paragraphe 1er sont fondées sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles portent au moins sur:

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

2° la gestion des incidents;

3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

4° la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

5° la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

10° l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins;

11° une politique de divulgation coordonnée des vulnérabilités.

§ 4. Lorsque les entités essentielles et importantes examinent lesquelles des mesures visées au paragraphe 3, 4°, sont appropriées, elles tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.

Ces mesures doivent être appropriées au regard des résultats des évaluations coordonnées au niveau de l'Union européenne des risques pour la sécurité des chaînes d'approvisionnement critiques.

§ 5. Iedere essentiële en belangrijke entiteit voert een risicoanalyse uit gebaseerd op een benadering die alle gevaren omvat en tot doel heeft de netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen en werkt, op basis daarvan, een I.B.B. uit dat minstens de in paragraaf 3 bedoelde aspecten bevat.

§ 6. Een essentiële of belangrijke entiteit die vaststelt dat zij niet voldoet aan de in paragraaf 3 bedoelde maatregelen, neemt onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen.

Art. 31. § 1. De bestuursorganen van essentiële en belangrijke entiteiten keuren de maatregelen voor het beheer van cyberbeveiligingsrisico's goed die deze entiteiten nemen om te voldoen aan artikel 30, zien toe op de uitvoering ervan en zijn aansprakelijk voor inbreuken door deze entiteiten op dat artikel.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

§ 2. De leden van de bestuursorganen van essentiële en belangrijke entiteiten volgen een opleiding zodat ze over voldoende kennis en vaardigheden beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Art. 32. De essentiële of belangrijke entiteit is verantwoordelijk voor de uitgevoerde risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen bedoeld in artikel 30, § 1.

Art. 33. Na raadpleging van de nationale cyberbeveiligingsautoriteit, de eventuele betrokken sectorale overheid en deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, passende en evenredige bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's opleggen.

HOOFDSTUK 2. — *Melding van incidenten*

Afdeling 1. — Verplichte melding

Art. 34. § 1. De essentiële en belangrijke entiteiten melden elk significant incident onverwijld aan het nationale CSIRT, volgens de modaliteiten bepaald in een protocol gesloten tussen het nationale CSIRT en het NCCN. Deze entiteiten rapporteren onder meer alle informatie die het nationale CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van de diensten betreffende de sectoren of deelsectoren van de bijlagen I en II.

Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

§ 2. Indien van toepassing delen de betrokken entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stellen de entiteiten die ontvangers ook in kennis van de significante cyberdreiging zelf.

§ 3. Na raadpleging van de nationale cyberbeveiligingsautoriteit, de sectorale overheden, het NCCN en de deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, precieze meldingsdrempels bepalen naargelang de impact of dringendheid van het incident.

§ 4. Een melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.

Art. 35. § 1. Voor de in artikel 34, § 1, eerste lid, bedoelde melding bezorgen de betrokken entiteiten het nationale CSIRT:

1° onverwijld en in elk geval binnen vierentwintig uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben;

2° onverwijld en in elk geval binnen tweeënzeventig uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding met, indien van toepassing, een update van de in 1° bedoelde informatie, een initiële beoordeling van het significante incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting;

§ 5. Chaque entité essentielle et importante effectue une analyse des risques fondée sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents et élabore, sur la base de cette analyse, une P.S.I. reprenant au moins les aspects visés au paragraphe 3.

§ 6. Lorsqu'une entité essentielle ou importante constate qu'elle ne se conforme pas aux mesures visées au paragraphe 3, elle prend, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

Art. 31. § 1er. Les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité que ces entités prennent afin de se conformer à l'article 30, supervisent leur mise en œuvre et sont responsables de la violation dudit article par ces entités.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

§ 2. Les membres des organes de direction des entités essentielles et importantes suivent une formation pour que leurs connaissances et compétences soient suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Art. 32. L'entité essentielle ou importante est responsable de l'analyse des risques effectuée ainsi que du choix et de la mise en œuvre des mesures visées à l'article 30, § 1er.

Art. 33. Après consultation de l'autorité nationale de cybersécurité, de l'éventuelle autorité sectorielle concernée et des entités fédérées concernées, le Roi peut, par arrêté délibéré en Conseil des ministres, imposer des mesures supplémentaires de gestion des risques en matière de cybersécurité appropriées et proportionnées.

CHAPITRE 2. — *Notification d'incidents*

Section 1re. — Notification obligatoire

Art. 34. § 1er. Les entités essentielles et importantes notifient tout incident significatif sans retard injustifié au CSIRT national, selon les modalités établies dans un protocole conclu entre lui et le NCCN. Ces entités signalent, entre autres, toute information permettant au CSIRT national de déterminer si l'incident a un impact transfrontière.

Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents significatifs susceptibles de nuire à la fourniture des services relatifs aux secteurs ou sous-secteurs repris à l'annexe I et II.

Le CSIRT national communique immédiatement les notifications visées à l'alinéa 1er aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

§ 2. Le cas échéant, les entités concernées communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

§ 3. Après consultation de l'autorité nationale de cybersécurité, des autorités sectorielles, du NCCN et des entités fédérées, le Roi peut déterminer, par arrêté délibéré en Conseil des ministres, des seuils précis de notification en fonction du degré d'impact ou d'urgence de l'incident.

§ 4. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Art. 35. § 1er. Aux fins de la notification visée à l'article 34, § 1er, alinéa 1er, les entités concernées soumettent au CSIRT national:

1° sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif, une alerte précoce qui, le cas échéant, indique si l'on suspecte que l'incident significatif a été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière;

2° sans retard injustifié et en tout état de cause dans les septante-deux heures après avoir eu connaissance de l'incident significatif, une notification d'incident qui, le cas échéant, met à jour les informations visées au 1° et fournit une évaluation initiale de l'incident significatif, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

3° op verzoek van het nationale CSIRT of van de eventuele betrokken sectorale overheid, een tussentijds verslag over relevante updates van de situatie;

4° uiterlijk één maand na de indiening van de in 2° bedoelde incidentmelding, een eindverslag waarin het volgende is opgenomen:

a) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;

b) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

c) toegepaste en lopende risicobeperkende maatregelen;

d) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;

5° indien het incident nog aan de gang is op het moment dat het in 4° bedoelde eindverslag moet worden ingediend, dienen de betrokken entiteiten op dat moment een voortgangsverslag in, en binnen één maand nadat zij het incident definitief hebben afgehandeld, een eindverslag.

§ 2. In afwijking van paragraaf 1, 2°, meldt een verlener van vertrouwensdiensten significante incidenten die gevolgen hebben voor de verlening van zijn vertrouwensdiensten onverwijld, en in elk geval binnen vierentwintig uur nadat hij er kennis van heeft gekregen, aan het nationale CSIRT.

§ 3. Het nationale CSIRT bezorgt de in de paragrafen 1 en 2 bedoelde meldingen onmiddellijk aan de eventuele bevoegde sectorale overheden. Meldingen van essentiële entiteiten worden ook doorgestuurd naar het NCCN.

Art. 36. § 1. Het nationale CSIRT verstrekt onverwijld en zo mogelijk binnen vierentwintig uur na ontvangst van de in artikel 35, § 1, 1°, bedoelde vroegtijdige waarschuwing een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het significante incident en, op verzoek van de entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen.

§ 2. Het nationale CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat het significante incident van criminele aard is, geeft het nationale CSIRT ook richtsnoeren voor het melden van het significante incident aan de rechtshandhavingsinstanties.

Art. 37. § 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig artikel 35 is ontvangen. Daarbij beschermt het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie.

§ 2. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entiteit, het NCCN, de eventuele betrokken sectorale overheid en de betrokken minister, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.

§ 3. De nationale cyberbeveiligingsautoriteit stuurt, op verzoek van de eventuele betrokken sectorale overheid, de op grond van artikel 34, § 1, eerste lid, ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.

§ 4. De nationale cyberbeveiligingsautoriteit dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld.

§ 5. Het nationale CSIRT verstrekt de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld door exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn geïdentificeerd.

Afdeling 2. — Vrijwillige melding

Art. 38. § 1. Naast de in artikel 34 bedoelde meldingsverplichtingen kunnen vrijwillig aan het nationale CSIRT worden gemeld door:

1° essentiële en belangrijke entiteiten: incidenten, cyberdreigingen en bijna-incidenten;

3° à la demande du CSIRT national ou de l'éventuelle autorité sectorielle concernée, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au 2°, comprenant les éléments suivants:

a) une description détaillée de l'incident, y compris de sa gravité et de son impact;

b) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

c) les mesures d'atténuation appliquées et en cours;

d) le cas échéant, l'impact transfrontière de l'incident;

5° en cas d'incident en cours au moment de la présentation du rapport final visé au 4°, les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter du traitement définitif de l'incident.

§ 2. Par dérogation au paragraphe 1er, 2°, un prestataire de services de confiance notifie au CSIRT national les incidents significatifs qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident significatif.

§ 3. Le CSIRT national communique, immédiatement, les notifications visées aux paragraphes 1er et 2 aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.

Art. 36. § 1er. Le CSIRT national fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de l'alerte précoce visée à l'article 35, § 1er, 1°, une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident significatif et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

§ 2. Le CSIRT national fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT national fournit également des orientations sur les modalités de notification de l'incident significatif aux autorités répressives.

Art. 37. § 1er. Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard injustifié les autres États membres touchés et l'ENISA de l'incident significatif. Sont alors partagées des informations du type de celles reçues conformément à l'article 35. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

§ 2. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou lorsque la divulgation de l'incident significatif est par ailleurs dans l'intérêt public, le CSIRT national peut, après avoir consulté l'entité concernée, le NCCN, l'éventuelle autorité sectorielle concernée et le ministre concerné, informer le public de l'incident significatif ou exiger de l'entité qu'elle le fasse.

§ 3. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1er, alinéa 1er, aux points de contact uniques des autres États membres touchés.

§ 4. L'autorité nationale de cybersécurité soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er.

§ 5. Le CSIRT national fournit aux autorités compétentes en vertu de la loi du 1er juillet 2011 des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er, par les exploitants d'infrastructures identifiées comme infrastructures critiques en vertu de la loi du 1er juillet 2011.

Section 2. — Notification volontaire

Art. 38. § 1er. Outre les obligations de notification visées à l'article 34, peuvent être notifiés à titre volontaire au CSIRT national par:

1° les entités essentielles et importantes, les incidents, les cybermenaces et les incidents évités;

2° andere dan in 1° bedoelde entiteiten, ongeacht of zij tot het toepassingsgebied van deze wet behoren: significante incidenten, cyberdreigingen en bijna-incidenten.

§ 2. De in paragraaf 1 bedoelde vrijwillige meldingen worden op dezelfde wijze verwerkt als de verplichte meldingen bedoeld in afdeling 1 van dit hoofdstuk.

Er kan evenwel voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.

Onverminderd het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten, mag een vrijwillige melding er niet direct toe leiden dat een inspectie volgens artikel 44 wordt opgestart of dat er bijkomende verplichtingen worden opgelegd aan de meldende entiteit waaraan zij niet zou zijn onderworpen indien zij de melding niet had ingediend.

TITEL 4. — *Toezicht en sancties*

HOOFDSTUK 1. — *Toezicht*

Afdeling 1. — Regelmatige conformiteitsbeoordeling

Art. 39. Essentiële entiteiten onderwerpen zich aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, op basis van de door de Koning bepaalde modaliteiten en referentiekaders:

1° ofwel opteren zij voor een in artikel 40 bedoelde regelmatige conformiteitsbeoordeling, op basis van een van de door de Koning bepaalde referentiekaders;

2° ofwel onderwerpen zij zich aan een inspectie door de nationale cyberbeveiligingsautoriteit, op basis van de door de Koning bepaalde nadere regels.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden de in het eerste lid, 2°, bedoelde inspecties gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit of worden gedelegeerd aan de eventuele betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

Indien de Koning meerdere referentiekaders bepaalt, kiezen essentiële entiteiten aan welk referentiekader zij zich onderwerpen.

Art. 40. § 1. De in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling wordt verricht door een conformiteitsbeoordelingsinstantie die erkend is door de nationale cyberbeveiligingsautoriteit volgens de door de Koning bepaalde voorwaarden.

Voor het toezicht op entiteiten die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit kan op elk ogenblik nagaan of de conformiteitsbeoordelingsinstanties de in paragraaf 1 bedoelde erkenningsvoorwaarden naleven, overeenkomstig de bepalingen van dit hoofdstuk.

Art. 41. Belangrijke entiteiten kunnen zich vrijwillig onderwerpen aan een regelmatige conformiteitsbeoordeling bedoeld in artikel 39, eerste lid, 1°, van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 30, § 3, op basis van de door de Koning bepaalde modaliteiten en referentiekaders.

Art. 42. Essentiële en belangrijke entiteiten die zich aan een regelmatige conformiteitsbeoordeling bedoeld in artikel 39, eerste lid, 1°, onderwerpen, respectievelijk overeenkomstig artikel 39 en 41, worden tot bewijs van het tegendeel geacht de in artikel 30 bedoelde verplichtingen na te leven.

Art. 43. Een lijst van de conformiteitsbeoordelingsinstanties die overeenkomstig artikel 40 erkend zijn door de nationale cyberbeveiligingsautoriteit, is beschikbaar bij laatstgenoemde autoriteit, die ze actueel houdt.

Afdeling 2. — Algemene bepalingen betreffende de inspectiedienst

Art. 44. § 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit voert controles uit om na te gaan of de essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

In afwijking van het eerste lid en op verzoek van de betrokken sectorale overheid worden deze controles gezamenlijk uitgevoerd, onder leiding van de nationale cyberbeveiligingsautoriteit, of gedelegeerd aan de eventuele betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.

2° les entités autres que celles visées au 1°, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente loi, les incidents significatifs, les cybermenaces et les incidents évités.

§ 2. Les notifications volontaires visées au paragraphe 1er sont traitées de la même manière que les notifications obligatoires visées à la section 1re du présent chapitre.

Les notifications obligatoires peuvent néanmoins être traitées de manière prioritaire par rapport aux notifications volontaires.

Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet direct de lancer une inspection visée à l'article 44 ou d'imposer à l'entité ayant effectué la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

TITRE 4. — *Supervision et sanctions*

CHAPITRE 1er. — *Supervision*

Section 1re. — Évaluation périodique de la conformité

Art. 39. Les entités essentielles se soumettent à une évaluation périodique de la conformité de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, sur base des modalités et des cadres de référence déterminés par le Roi:

1° Soit en choisissant une évaluation périodique de la conformité visée à l'article 40, sur base de l'un des cadres de référence déterminé par le Roi;

2° Soit en se soumettant à une inspection par l'autorité nationale de cybersécurité, sur base des modalités déterminées par le Roi.

Par dérogation à l'alinéa 1er, et à la demande de l'autorité sectorielle concernée, les inspections visées à l'alinéa 1er, 2°, sont effectuées de manière conjointe, sous la direction de l'autorité nationale de cybersécurité ou sont déléguées à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

Lorsque le Roi détermine plusieurs cadres de référence, les entités essentielles choisissent le cadre de référence auquel ils se soumettent.

Art. 40. § 1er. L'évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°, est effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité selon les conditions fixées par le Roi.

Pour le contrôle des entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 et des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui évaluent la conformité disposent d'une habilitation de sécurité.

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité peut à tout moment vérifier le respect des conditions d'agrément visées au paragraphe 1er par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.

Art. 41. Les entités importantes peuvent, de manière volontaire, se soumettre à une évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°, de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité visées à l'article 30, § 3, sur base des modalités et des cadres de référence déterminés par le Roi.

Art. 42. Les entités essentielles et importantes qui se soumettent à une évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°, respectivement conformément à l'article 39 et 41 sont, jusqu'à preuve du contraire, présumées respecter les obligations visées à l'article 30.

Art. 43. Une liste des organismes d'évaluation de la conformité agréés par l'autorité nationale de cybersécurité conformément à l'article 40 est disponible auprès de l'autorité nationale de cybersécurité, qui la tient à jour.

Section 2. — Dispositions générales relatives au service d'inspection

Art. 44. § 1er. Le service d'inspection de l'autorité nationale de cybersécurité réalise des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité et des règles de notification des incidents.

Par dérogation à l'alinéa 1er, et à la demande de l'autorité sectorielle concernée, ces contrôles sont effectués de manière conjointe, sous la direction de l'autorité nationale de cybersécurité, ou sont délégués à l'éventuel service d'inspection concerné moyennant l'accord de l'autorité nationale de cybersécurité.

De bevoegde sectorale overheid of sectorale inspectiedienst of, indien geen sectorale inspectiedienst is aangewezen door de wet of de Koning, de inspectiedienst van de nationale cyberbeveiligingsautoriteit kan controles uitvoeren om na te gaan of de essentiële en belangrijke entiteiten de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33 naleven.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermelden de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt.

De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen een beroep doen op experten.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten kunnen prioriteit geven aan de in deze titel bedoelde toezichtstaken volgens een risicogebaseerde benadering.

§ 4. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12), van Verordening (EU) 2016/679, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectiediensten nauw samen met de gegevensbeschermingsautoriteiten, onverminderd de bevoegdheid en taken van deze laatsten.

Art. 45. § 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de wet van 1 juli 2011 de bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een exploitant van een infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur wordt geïdentificeerd, voldoet aan deze wet. In voorkomend geval kunnen de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een exploitant van een infrastructuur die is geïdentificeerd als kritieke infrastructuur uit hoofde van de wet van 1 juli 2011.

§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst werken samen met de relevante autoriteiten die bevoegd zijn uit hoofde van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen met name het oversightforum dat is opgericht op grond van artikel 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële of belangrijke entiteit die op grond van artikel 31 van bovengenoemde verordening als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze wet.

Art. 46. § 1. Wanneer de netwerk- en informatiesystemen van een entiteit zich buiten het Belgische grondgebied bevinden, kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, in overleg met de nationale cyberbeveiligingsautoriteit, de bevoegde toezichthoudende autoriteiten van andere lidstaten om samenwerking en bijstand verzoeken.

In het kader van het verzoek bedoeld in het eerste lid:

1° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten verzoeken om toezichts- of handhavingsmaatregelen te nemen;

2° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten op een met redenen omklede wijze om wederzijdse bijstand verzoeken, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

L'autorité sectorielle ou le service d'inspection sectoriel compétents, ou, lorsqu'aucun service d'inspection sectoriel n'a été désigné par la loi ou par le Roi, le service d'inspection de l'autorité nationale de cybersécurité peut réaliser des contrôles du respect par les entités essentielles et importantes des mesures de gestion des risques en matière de cybersécurité sectorielles ou sous-sectorielles supplémentaires visées à l'article 33.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents mentionnent la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies.

Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent faire appel à des experts.

§ 3. Le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels peuvent fixer des priorités en ce qui concerne les tâches de supervision visées au présent titre selon une approche basée sur les risques.

§ 4. Lorsqu'ils traitent des incidents donnant lieu à des violations de données à caractère personnel telles que définies à l'article 4, point 12), du règlement (UE) 2016/679, le service d'inspection de l'autorité nationale de cybersécurité ainsi que les éventuels autorités sectorielles et services d'inspection sectoriels coopèrent étroitement avec les autorités de protection des données, sans préjudice de la compétence et des missions de ces dernières.

Art. 45. § 1er. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent les autorités compétentes en vertu de la loi du 1er juillet 2011 lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'un exploitant d'une infrastructure identifiée comme critique en vertu de la loi du 1er juillet 2011 respecte la présente loi. Le cas échéant, les autorités compétentes en vertu de la loi du 1er juillet 2011 peuvent demander au service d'inspection de l'autorité nationale de cybersécurité et à l'éventuelle autorité sectorielle ou à l'éventuel service d'inspection sectoriel compétents d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'un exploitant d'une infrastructure qui est identifiée comme infrastructure critique en vertu de la loi du 1er juillet 2011.

§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents coopèrent avec les autorités compétentes pertinentes en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, dudit règlement lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle ou importante qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.

Art. 46. § 1er. Lorsque les réseaux et les systèmes d'information d'une entité sont situés en dehors du territoire belge, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents, en concertation avec l'autorité nationale de cybersécurité, peuvent solliciter la coopération et l'assistance des autorités de contrôle compétentes d'autres États membres.

Dans le cadre de la sollicitation visée à l'alinéa 1er:

1° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents peuvent demander aux autorités de contrôle compétentes d'autres États membres de prendre des mesures de supervision ou d'exécution;

2° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents peuvent demander, de manière motivée, aux autorités de contrôle compétentes d'autres États membres une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

De wederzijdse bijstand bedoeld in het tweede lid, 2°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

§ 2. In verhouding tot hun middelen en voor zover dit binnen hun bevoegdheden valt, werken de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst samen met de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten en verlenen ze bijstand aan deze autoriteiten die daarom verzoeken, wanneer de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden.

In het kader van het verzoek bedoeld in het eerste lid:

1° centraliseert de nationale cyberbeveiligingsautoriteit de informatie en raadplegingen met betrekking tot de toezichts- en handhavingsmaatregelen die zijzelf of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst heeft genomen, en deelt deze mee aan de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten;

2° kan dit verzoek betrekking hebben op toezichts- of handhavingsmaatregelen;

3° kan dit verzoek, op een met redenen omklede wijze, betrekking hebben op wederzijdse bijstand, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

De wederzijdse bijstand bedoeld in het tweede lid, 3°, kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse, toezicht elders of gerichte beveiligingsaudits uit te voeren.

De autoriteit waaraan een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij wordt vastgesteld dat zij niet bevoegd is om de gevraagde bijstand te verlenen, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van deze autoriteit, of het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indien ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of de defensie van België. Alvorens een dergelijk verzoek af te wijzen, raadpleegt voornoemde autoriteit de andere betrokken bevoegde autoriteiten alsook, op verzoek van een van de betrokken lidstaten, de Europese Commissie en Enisa.

§ 3. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen in onderlinge overeenstemming gezamenlijke toezichtsacties uitvoeren, en dit onderling en/of met de bevoegde toezichthoudende autoriteiten van andere lidstaten.

§ 4. Dit artikel is niet van toepassing op diplomatieke en consulaire missies.

Art. 47. § 1. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst en de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarvoor zij met het toezicht belast zijn, waardoor hun objectiviteit in het gedrang zou kunnen komen. Zij leggen de eed af bij de leidend ambtenaar van hun dienst.

De autoriteiten bedoeld in artikel 44, § 1, nemen de nodige maatregelen om, bij de uitvoering van hun taken, de onafhankelijkheid van hun personeelsleden te garanderen en om belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een personeelslid van de autoriteiten bedoeld in artikel 44, § 1, rechtstreeks of onrechtstreeks financiële, economische of andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 3. De personeelsleden van de autoriteiten bedoeld in artikel 44, § 1, krijgen noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze instructies van derden.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

L'assistance mutuelle visée à l'alinéa 2, 2°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

§ 2. De manière proportionnée à leurs ressources et pour autant que cela rentre dans le cadre de leurs compétences, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents coopèrent et apportent leur assistance aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres qui en font la demande, lorsque les réseaux et les systèmes d'information de l'entité concernée sont situés dans le territoire belge.

Dans le cadre de la demande visée à l'alinéa 1er:

1° l'autorité nationale de cybersécurité centralise les informations et consultations en ce qui concerne les mesures de supervision et d'exécution prises par elle-même, par l'éventuelle autorité sectorielle et par l'éventuel service d'inspection sectoriel compétents et les communique aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres;

2° ladite demande peut porter sur des mesures de supervision ou d'exécution;

3° ladite demande peut, de manière motivée, porter sur une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée à l'alinéa 2, 3°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés.

L'autorité à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que ladite autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de ladite autorité ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de la Belgique. Avant de refuser une telle demande, ladite autorité consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission européenne et l'ENISA.

§ 3. D'un commun accord, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents peuvent mener à bien des actions communes de supervision entre elles et/ou avec les autorités de contrôle compétentes d'autres États membres.

§ 4. Le présent article n'est pas applicable aux missions diplomatiques et consulaires.

Art. 47. § 1er. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent et les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

Les autorités visées à l'article 44, § 1er, prennent les mesures nécessaires afin d'assurer l'indépendance des membres de leur personnel et de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de leurs tâches.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel des autorités visées à l'article 44, § 1er, a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 3. Les membres du personnel des autorités visées à l'article 44, § 1er, ne reçoivent ni ne cherchent pas, dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne tierce.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

De Koning kan ook andere situaties benoemen als belangenconflicten.

Afdeling 3. — Het door de inspectiedienst uitgeoefende toezicht op de entiteiten

Art. 48. § 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de beëdigde leden van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun toezichtsopdracht over de volgende toezichtsbevoegdheden, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken op deze wet:

1° toegang vragen tot alle documenten of informatie die nodig zijn voor de uitoefening van hun toezichtsopdracht en hiervan een kopie verkrijgen, met name de bewijzen van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van conformiteitsbeoordelingen en van beveiligingsaudits of de respectieve onderliggende bewijzen;

2° overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;

3° essentiële entiteiten onderwerpen aan regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie, gebaseerd op door de betrokken inspectiedienst of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie;

4° alle informatie inwinnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's, met name betreffende het gedocumenteerde cyberbeveiligingsbeleid, de naleving van de verplichting om informatie in te dienen bij de nationale cyberbeveiligingsautoriteit of bij de eventuele sectorale overheid overeenkomstig titel 1 en de uitvoering van deze wet;

5° een ad-hocaudit uitvoeren, met name in gevallen waarin dat gerechtvaardigd is vanwege een significant incident of een inbreuk op deze wet;

6° beveiligingsscans uitvoeren op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

7° de identiteit opnemen van de personen die zich op de door de entiteit gebruikte plaatsen bevinden en van wie ze het verhoor nodig achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze officiële identificatiedocumenten voorleggen;

8° in voorkomend geval, de bijstand vragen van de federale of lokale politiediensten in het kader van het gebruik van geweld;

9° informatie inwinnen bij de personeelsleden bedoeld in artikel 9 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, voor de uitvoering van de bepalingen van deze wet;

10° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle door de entiteit gebruikte plaatsen betreden; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter.

§ 2. In het kader van de inspectie van belangrijke entiteiten worden de toezichtsbevoegdheden bedoeld in paragraaf 1 achteraf ("ex post") uitgeoefend op basis van bewijzen, aanwijzingen of informatie waaruit blijkt dat een belangrijke entiteit deze wet niet naleeft.

§ 3. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben;

2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum achtenveertig uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

Section 3. — La supervision des entités par le service d'inspection

Art. 48. § 1er. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité et les membres assermentés de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents disposent, dans l'exercice de leur mission de supervision, des compétences de contrôle suivantes, tant dans le cadre de démarches administratives que dans le cadre de la constatation de violations de la présente loi:

1° demander l'accès à et obtenir une copie de tout document ou toute information nécessaire à l'exercice de leur mission de supervision, notamment les preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des évaluations de la conformité ou des audits de sécurité ou les éléments de preuve sous-jacents correspondants;

2° procéder, sur place ou à distance, à tout examen, contrôle et audition, y compris des contrôles aléatoires effectués par des professionnels formés;

3° soumettre les entités essentielles à des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant, basés sur des évaluations des risques effectuées par le service d'inspection concerné ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques;

4° requérir toutes les informations qu'ils estiment nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, du respect de l'obligation de soumettre des informations à l'autorité nationale de cybersécurité ou à l'éventuelle autorité sectorielle conformément au titre 1er et de la mise en œuvre de la présente loi;

5° réaliser un audit ad hoc, notamment lorsqu'il est justifié en raison d'un incident significatif ou d'une violation de la présente loi;

6° effectuer des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

7° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'entité et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. À cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

8° le cas échéant, demander l'assistance des services de la police fédérale ou locale dans le cadre de l'usage de la force;

9° solliciter des informations auprès des membres du personnel visés à l'article 9 de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, pour les besoins de l'exécution des dispositions de la présente loi;

10° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'entité; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction.

§ 2. Dans le cadre de l'inspection des entités importantes, les compétences de contrôle visées au paragraphe 1er s'effectuent de manière ex post, sur base d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecte pas la présente loi.

§ 3. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels ils souhaitent avoir accès;

2° les manquements éventuels qui font l'objet du contrôle;

3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire.

Le juge d'instruction décide dans un délai de quarante-huit heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans le délai

beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.

§ 4. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 5. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 6. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 5 werd opgestart uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een onderzoeksrechter vragen om op te treden.

§ 7. Wanneer de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst er in het kader van het toezicht of de handhaving kennis van krijgen dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 30 en 34 tot 37 vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens in de zin van artikel 4, punt 12, van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

Wanneer de bevoegde gegevensbeschermingsautoriteit in een andere lidstaat dan België gevestigd is, stelt de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de in België gevestigde bevoegde gegevensbeschermingsautoriteit in kennis van de in het eerste lid bedoelde potentiële inbreuk in verband met persoonsgegevens.

§ 8. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de beëdigde leden van de autoriteiten bedoeld in artikel 44, § 1, ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor dit toezicht.

prescrit, la visite des lieux est réputée être refusée. Le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

§ 4. Au début de toute audition, il est communiqué à la personne interrogée:

1° que ses déclarations peuvent être utilisées comme preuve en justice;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou lors d'une partie de celle-ci.

À la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées.

Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 5. Les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 6. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 5, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents peut solliciter l'intervention d'un juge d'instruction.

§ 7. Lorsque le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents prend connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 30 et 34 à 37 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, ils en informent sans retard injustifié les autorités de protection des données.

Lorsque l'autorité de protection des données compétente est établie dans un autre État membre que la Belgique, le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informe l'autorité de protection des données compétente établie en Belgique de la violation potentielle de données à caractère personnel visée à l'alinéa 1er.

§ 8. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés des autorités visées à l'article 44, § 1er, veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour ledit contrôle.

Art. 49. § 1. Na elke inspectie stellen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst een verslag op en bezorgen ze daarvan een kopie aan de geïnspecteerde entiteit.

§ 2. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheid wisselen hun inspectieverslagen uit.

Art. 50. § 1. De entiteit waarop toezicht wordt uitgeoefend, verleent haar volledige medewerking aan de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de entiteit het nodige materiaal ter beschikking van de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, opdat ze de veiligheidsvoorschriften naleven tijdens de inspecties.

§ 2. De kosten van de inspecties zijn niet ten laste van de entiteiten.

In afwijking van het vorige lid kan de Koning, voor elke sector of deelsector, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de nationale cyberbeveiligingsautoriteit en van de eventuele betrokken sectorale overheid, retributies bepalen voor de inspectieprestaties. De Koning bepaalt de berekenings- en betalingsregels.

§ 3. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

HOOFDSTUK 2. — *De administratieve maatregelen en geldboetes*

Afdeling 1. — Procedure

Art. 51. § 1. Wanneer een of meer inbreuken op de eisen van deze wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kunnen de feiten opgetekend worden in een proces-verbaal door de beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit, van de eventuele sectorale inspectiedienst of van de eventuele betrokken sectorale overheid, overeenkomstig artikel 44, § 1.

Mits de nationale cyberbeveiligingsautoriteit akkoord gaat, kan de sectorale overheid administratieve maatregelen en geldboetes als bedoeld in afdeling 2 opleggen aan een entiteit.

De nationale cyberbeveiligingsautoriteit informeert de betrokken sectorale overheid wanneer zij overweegt om administratieve maatregelen en geldboetes als bedoeld in de artikelen 58 en 59 op te leggen aan een entiteit.

Wanneer de autoriteiten bedoeld in het eerste en tweede lid er tijdens hun toezichtsopdracht kennis van krijgen dat een in het eerste of tweede lid bedoelde inbreuk door een essentiële of belangrijke entiteit een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12), van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.

§ 2. Op basis van het in paragraaf 1 bedoelde proces-verbaal en, in voorkomend geval, van de relevante verslagen bedoeld in artikel 49, § 1, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing opstellen dat minstens de referenties van het proces-verbaal dat de inbreuk vaststelt en de feiten beschrijft die aanleiding hebben gegeven tot de procedure, en een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in artikel 58 en/of 59 bevat, alsook de termijn waarbinnen de betrokken entiteit de administratieve maatregelen zou uitvoeren.

De in het eerste lid bedoelde termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de entiteit en de te nemen maatregelen.

§ 3. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 2 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te

Art. 49. § 1er. Après chaque inspection, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents rédigent un rapport et en transmettent une copie à l'entité inspectée.

§ 2. L'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle se communiquent mutuellement leur rapports d'inspection.

Art. 50. § 1er. L'entité supervisée apporte son entière collaboration aux membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

Si nécessaire, l'entité met à disposition des membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Les coûts des inspections ne sont pas mis à charge des entités.

Par dérogation à l'alinéa précédent, le Roi peut déterminer, par secteur ou sous-secteur, par arrêté délibéré en Conseil des ministres et après avis de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle concernée, des rétributions relatives aux prestations d'inspections. Il en fixe les modalités de calcul et de paiement.

§ 3. Le fait pour quiconque d'empêcher ou d'entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté dans un procès-verbal par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétents.

CHAPITRE 2. — *Les mesures et amendes administratives*

Section 1re. — Procédure

Art. 51. § 1er. Lorsqu'un ou plusieurs manquements aux exigences imposées par la présente loi, ses arrêtés d'exécution ou les décisions administratives individuelles y afférentes sont observés, les faits peuvent être constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité, de l'éventuel service d'inspection sectoriel ou de l'éventuelle autorité sectorielle concernée, conformément à l'article 44, § 1er

Moyennant l'accord de l'autorité nationale de cybersécurité, l'autorité sectorielle peut imposer à une entité des mesures et amendes administratives visées à la section 2.

L'autorité nationale de cybersécurité informe l'autorité sectorielle concernée lorsqu'elle a l'intention d'imposer à une entité des mesures et amendes administratives visées aux articles 58 et 59.

Lorsque les autorités visées aux alinéas 1er et 2 prennent connaissance, dans le cadre de leur mission de supervision, du fait qu'un manquement visé à l'alinéa 1er ou 2, commis par une entité essentielle ou importante, peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12), du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de protection des données compétentes.

§ 2. Sur la base du procès-verbal visé au paragraphe 1er et, le cas échéant, des rapports pertinents visés à l'article 49, § 1er, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut rédiger un projet de décision contenant au moins les références du procès-verbal qui constate l'infraction et qui relate les faits à propos desquels la procédure est entamée et une ou plusieurs mesures ou amendes administratives visées à l'article 58 et/ou 59 envisagées ainsi que le délai endéans lequel l'entité concernée exécuterait les mesures administratives.

Le délai visé à l'alinéa 1er est déterminé en tenant compte des conditions de fonctionnement de l'entité et des mesures à mettre en œuvre.

§ 3. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 2 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amendes administratives envisagées et lui fait part de son droit, dans les trente jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être

dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd.

§ 4. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 3, eerste lid, of in het geval bedoeld in paragraaf 3, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het ontwerp van beslissing bedoeld in paragraaf 2, eerste lid, handhaven, wijzigen of ervan afzien, rekening houdend met de entiteitscategorie waartoe de betrokken entiteit behoort, de verweermiddelen van deze laatste en de in artikel 54 bedoelde elementen.

Art. 52. § 1. Indien de op grond van artikel 58, 1° tot 4°, en 6°, genomen handhavingsmaatregelen ondoeltreffend zijn, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een termijn vaststellen waarbinnen een essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan haar eisen te voldoen.

§ 2. Indien een essentiële entiteit geen gevolg geeft aan de maatregel(en) vermeld in de beslissing bedoeld in artikel 51, § 4, stelt de autoriteit die deze beslissing heeft genomen de feiten vast in een proces-verbaal.

§ 3. Op basis van het in paragraaf 2 bedoelde proces-verbaal stelt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing op dat minstens een of meer overwogen administratieve maatregelen of geldboetes bedoeld in de artikelen 59 en/of 60 bevat.

§ 4. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid verstuurt het in paragraaf 3 bedoelde ontwerp van beslissing naar de betrokken entiteit, met een gedetailleerde motivering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In afwijking van het eerste lid wordt het ontwerp van beslissing niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd.

§ 5. Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 4, eerste lid, of in het geval bedoeld in paragraaf 4, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid het in paragraaf 3 bedoelde ontwerp van beslissing handhaven, wijzigen of ervan afzien, rekening houdend met de verweermiddelen van de betrokken entiteit en de in artikel 54 bedoelde elementen.

Art. 53. De processen-verbaal van de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Art. 54. § 1. Bij het nemen van handhavingsmaatregelen in het kader van de in de artikelen 51 en 52 bedoelde procedures eerbiedigt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid de rechten van de verdediging, houdt zij rekening met de omstandigheden van elk afzonderlijk geval en houdt zij ten minste naar behoren rekening met:

1° de in de artikelen 9 en 10 bedoelde categorie waartoe de betrokken entiteit behoort;

2° de ernst van de inbreuk en het belang van de geschonden bepalingen, waarbij onder meer het volgende in ieder geval een ernstige inbreuk vormt:

a) herhaalde inbreuken;

b) het niet melden of niet verhelpen van significante incidenten;

c) het niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteiten;

d) het belemmeren van audits of monitoringsactiviteiten waartoe de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk;

d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1er, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 4. Après que l'entité concernée a pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3, alinéa 1er, ou dans le cas visé au paragraphe 3, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 2, alinéa 1er ou y renonce, en tenant compte de la catégorie d'entité à laquelle appartient l'entité concernée, des moyens de défense de cette dernière et des éléments visés à l'article 54.

Art. 52. § 1er. Lorsque les mesures d'exécution adoptées en vertu de l'article 58, 1° à 4°, et 6°, sont inefficaces, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut fixer un délai dans lequel une entité essentielle est invitée à prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire à ses exigences.

§ 2. Lorsqu'une entité essentielle ne se conforme pas à la ou aux mesures contenues dans la décision visée à l'article 51, § 4, l'autorité qui a pris cette décision constate les faits dans un procès-verbal.

§ 3. Sur la base du procès-verbal visé au paragraphe 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente rédige un projet de décision contenant au moins une ou plusieurs mesures ou amendes administratives visées aux articles 59 et/ou 60 envisagées.

§ 4. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente envoie le projet de décision visé au paragraphe 3 à l'entité concernée en exposant, en détail, les motifs relatifs aux mesures et/ou amendes administratives envisagées et lui fait part de son droit, dans les trente jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.

Par exception à l'alinéa 1er, le projet de décision n'est pas envoyé au préalable à l'entité concernée dans des cas exceptionnels, dûment motivés, où cela entraverait une intervention immédiate pour prévenir un incident ou y répondre.

§ 5. Après que l'entité concernée ait pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 4, alinéa 1er, ou dans le cas visé au paragraphe 4, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente maintient ou modifie le projet de décision visé au paragraphe 3 ou y renonce en tenant compte des moyens de défense de l'entité concernée et des éléments visés à l'article 54.

Art. 53. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Art. 54. § 1er. Lorsqu'elle prend toute mesure d'exécution dans le cadre des procédures visées aux articles 51 et 52, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente respecte les droits de la défense, tient compte des circonstances propres à chaque cas et, au minimum, tient dûment compte:

1° de la catégorie visée aux articles 9 et 10 à laquelle l'entité concernée appartient;

2° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves:

a) les violations répétées;

b) le fait de ne pas notifier des incidents significatifs ou de ne pas y remédier;

c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes;

d) le fait d'entraver des audits ou des activités de contrôle ordonnées par le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents à la suite de la constatation d'une violation;

e) het verstrekken van valse of heel onnauwkeurige informatie met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's of de in titel 3 bedoelde melding van incidenten;

3° de duur van de inbreuk;

4° eventuele relevante eerdere inbreuken door de betrokken entiteit;

5° elke veroorzaakte materiële of immateriële schade, met inbegrip van elke financiële of economische schade, gevolgen voor andere diensten en het aantal getroffen gebruikers;

6° opzet of nalatigheid van de pleger van de inbreuk;

7° door de entiteit genomen maatregelen om de materiële of immateriële schade te voorkomen of te beperken;

8° de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

9° de mate waarin de aansprakelijk gestelde natuurlijke of rechtspersonen meewerken met de inspectiedienst van de nationale cyberbeveiligingsautoriteit of met de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

§ 2. Indien de gegevensbeschermingsautoriteiten een administratieve geldboete opleggen op grond van artikel 58, lid 2, punt *i)*, van Verordening (EU) 2016/679, legt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid geen administratieve geldboete op voor een inbreuk die voortvloeit uit dezelfde gedraging als die waarvoor een administratieve geldboete uit hoofde van artikel 58, lid 2, punt *i)*, van die verordening is opgelegd.

Art. 55. § 1. De in de artikelen 51 en 52 bedoelde beslissingen worden bij aangetekende zending ter kennis gebracht van de overtreder.

§ 2. De administratieve geldboetes die worden opgelegd door een in artikel 51 of 52 bedoelde beslissing, moeten worden betaald binnen de zestig dagen na ontvangst van de in paragraaf 1 bedoelde aangetekende zending.

Deze termijn kan verlengd worden in functie van het bedrag van de administratieve geldboete.

De in het eerste lid bedoelde termijn wordt geacht in te gaan uiterlijk zes dagen na de in paragraaf 1 bedoelde aangetekende zending.

§ 3. Wanneer een in artikel 51 of 52 bedoelde beslissing een andere administratieve maatregel dan een administratieve geldboete oplegt, vermeldt deze beslissing de termijn waarbinnen de maatregel moet worden uitgevoerd.

§ 4. De nationale cyberbeveiligingsautoriteit en, desgevallend, de eventuele sectorale overheid wisselen hun in artikel 51 of 52 bedoelde beslissing uit.

Art. 56. § 1. Als de betrokken entiteit de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door een wettelijke vertegenwoordiger van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen achtenveertig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het moet worden ingediend door middel van een dagvaarding van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging hiervan, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques en matière de cybersécurité ou aux notifications d'incidents prévues au titre 3;

3° de la durée de la violation;

4° de toute violation antérieure pertinente commise par l'entité concernée;

5° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés;

6° du fait que l'auteur de la violation a agi délibérément ou par négligence;

7° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;

8° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;

9° du degré de coopération avec le service d'inspection de l'autorité nationale de cybersécurité ou avec l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents des personnes physiques ou morales tenues pour responsables.

§ 2. Lorsque les autorités de protection des données imposent une amende administrative en vertu de l'article 58, paragraphe 2, point *i)*, du règlement (UE) 2016/679, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente n'impose pas d'amende administrative pour une violation découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point *i)*, dudit règlement.

Art. 55. § 1er. Les décisions visées aux articles 51 et 52 sont notifiées par envoi recommandé au contrevenant.

§ 2. Les amendes administratives imposées par une décision visée à l'article 51 ou 52 doivent être acquittées dans les soixante jours qui suivent la réception de l'envoi recommandé visé au paragraphe 1er.

Ce délai peut être augmenté en fonction du montant de l'amende administrative.

Le délai visé à l'alinéa 1er est réputé commencer au plus tard six jours après l'envoi recommandé visé au paragraphe 1er.

§ 3. Lorsqu'une décision visée à l'article 51 ou 52 impose une mesure administrative autre qu'une amende administrative, cette décision précise le délai endéans lequel la mesure doit être exécutée.

§ 4. L'autorité nationale de cybersécurité et, le cas échéant, l'éventuelle autorité sectorielle se communiquent mutuellement leur décision visée à l'article 51 ou 52.

Art. 56. § 1er. Lorsque l'entité concernée reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut décerner une contrainte.

La contrainte est décernée par un représentant légal de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les quarante-huit heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation de l'autorité nationale de cybersécurité ou de l'éventuelle autorité sectorielle compétente signifiée par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et à l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de celle-ci, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 57. De feiten zijn drie jaar na het plegen verjaard. De verjaring wordt alleen gestuit door onderzoekshandelingen of door de vervolging een inspectiedienst. Deze handelingen doen een nieuwe periode van gelijke duur lopen, zelfs ten aanzien van personen die niet betrokken zijn.

De administratieve maatregelen of geldboetes verjaren vijf jaar na de datum waarop ze ten uitvoer moeten worden gelegd. De verjaringstermijn wordt geschorst in geval van beroep tegen de administratieve beslissing.

Afdeling 2. — Administratieve maatregelen en geldboetes

Art. 58. De volgende administratieve maatregelen kunnen aan entiteiten worden opgelegd op basis van artikel 51:

1° waarschuwingen geven over inbreuken door de betrokken entiteiten op deze wet;

2° bindende aanwijzingen vaststellen of een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze wet te verhelpen;

3° de betrokken entiteiten gelasten een einde te maken aan gedragingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;

4° de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met titel 3 of te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel;

5° de betrokken entiteiten gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;

6° de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

7° de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;

8° wanneer de betrokken entiteit een essentiële entiteit is, een controlefunctionaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor het beheer van cyberbeveiligingsrisico's en inzake het melden van incidenten bedoeld in titel 3.

Wanneer de betrokken entiteit een essentiële entiteit is, omvatten de bindende aanwijzingen bedoeld in het eerste lid, 2°, ook de maatregelen die nodig zijn om een incident te voorkomen of te verhelpen, alsmede uiterste termijnen voor de uitvoering van dergelijke maatregelen en voor verslaggeving over de uitvoering ervan.

Art. 59. De volgende administratieve geldboetes kunnen aan entiteiten worden opgelegd op basis van artikel 51 of 52:

1° eenieder die niet voldoet aan de in artikel 12 bedoelde rapportageverplichtingen wordt bestraft met een geldboete van 500 tot 125.000 euro;

2° een entiteit die een persoon die optreedt voor haar rekening nadelige gevolgen berokkent ingevolge de uitvoering, te goeder trouw en in het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet, wordt bestraft met een geldboete van 500 tot 200.000 euro;

3° onverminderd artikel 48, § 4, eerste lid, 3°, eenieder die niet voldoet aan de in deze titel bedoelde toezichtverplichtingen wordt bestraft met een geldboete van 500 tot 200.000 euro;

4° een belangrijke entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen bedoeld in titel 3, wordt bestraft

§ 4. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 57. Les faits sont prescrits trois ans après leur commission. La prescription n'est interrompue que par des actes d'enquête ou de poursuite par un service d'inspection. Ces actes font courir un nouveau délai d'égale durée, même à l'égard des personnes qui n'y sont pas impliquées.

Les mesures administratives ou les amendes administratives sont prescrites cinq ans à compter de la date à laquelle elles doivent être exécutées. Le délai de prescription est suspendu en cas d'un recours contre la décision administrative.

Section 2. — Mesures et amendes administratives

Art. 58. Les mesures administratives suivantes peuvent être imposées aux entités sur la base de l'article 51:

1° émettre des avertissements concernant les violations de la présente loi par les entités concernées;

2° adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la présente loi;

3° ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer;

4° ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec le titre 3 ou de respecter les obligations en matière de notification d'incidents énoncées au même titre, de manière spécifique et dans un délai déterminé;

5° ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

6° ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

7° ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique;

8° lorsque l'entité concernée est une entité essentielle, désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des mesures de gestion des risques en matière de cybersécurité et de notification d'incidents visées au titre 3.

Lorsque l'entité concernée est une entité essentielle, les instructions contraignantes visées à l'alinéa 1er, 2°, concernent également les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre.

Art. 59. Les amendes administratives suivantes peuvent être imposées aux entités sur la base de l'article 51 ou 52:

1° est puni d'une amende de 500 à 125.000 euros quiconque ne se conforme pas aux obligations d'information visées à l'article 12;

2° est punie d'une amende de 500 à 200.000 euros l'entité qui fait subir des conséquences négatives à une personne agissant pour son compte en raison de l'exécution, de bonne foi et dans le cadre de ses fonctions, des obligations découlant de la présente loi;

3° sans préjudice de l'article 48, § 4, alinéa 1er, 3°, est puni d'une amende de 500 à 200.000 euros quiconque ne se conforme pas aux obligations de contrôle visées au présent titre;

4° est punie d'une amende de 500 à 7.000.000 d'euros ou 1,4 pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus

met een geldboete van 500 tot 7.000.000 euro of van 1,4 procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort, afhankelijk van welk bedrag het hoogst is;

5° een essentiële entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen bedoeld in titel 3, wordt bestraft met een geldboete van 500 tot 10.000.000 euro of van 2 procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, afhankelijk van welk bedrag het hoogst is.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 60. Indien de gevraagde maatregelen niet binnen de gestelde termijn worden ondernomen, kunnen aan essentiële entiteiten op grond van artikel 52 de volgende administratieve maatregelen worden opgelegd:

1° de nationale cyberbeveiligingsautoriteit verzoeken een certificering of vergunning tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de betrokken entiteit verleende diensten of verrichte activiteiten;

2° een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

De in het eerste lid bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit die deze handhavingsmaatregelen heeft opgelegd.

Art. 61. Elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële of een belangrijke entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, heeft de bevoegdheid om ervoor te zorgen dat deze entiteit deze wet nakomt. Deze personen zijn aansprakelijk voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze wet.

Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde overheidsfunctionarissen.

TITEL 5. — *Specifieke bepalingen voor de overheidssector*

Art. 62. De administratieve maatregelen en geldboetes bedoeld in de artikelen 59 en 60 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidssector.

Art. 63. § 1. De Koning wordt gemachtigd een autoriteit aan te wijzen als conformiteitsbeoordelingsinstantie voor alle of een deel van de overheidsinstanties.

§ 2. De in paragraaf 1 bedoelde autoriteit wordt erkend door de nationale cyberbeveiligingsautoriteit, volgens de door de Koning bepaalde modaliteiten, om de in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling uit te voeren.

De in het eerste lid bedoelde erkenning heeft betrekking op een of meer van de in artikel 39 bedoelde referentiekaders.

Art. 64. De inspectiedienst van de nationale cyberbeveiligingsautoriteit of, in voorkomend geval, de sectorale inspectiedienst die door de Koning is aangewezen voor de overheidssector, is bij de uitvoering van zijn toezichthoudende taken operationeel onafhankelijk van de overheidsinstanties waarop hij toezicht houdt.

Art. 65. Artikel 47 is van toepassing op de inspectiedienst bedoeld in artikel 64.

TITEL 6. — *Verwerking van persoonsgegevens*

HOOFDSTUK 1. — *Beginselen betreffende de verwerking*

Art. 66. De definities van Verordening (EU) 2016/679 zijn van toepassing op deze titel.

Art. 67. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:

1° de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;

élevé étant retenu, l'entité importante qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents visées au titre 3;

5° est punie d'une amende de 500 à 10.000.000 d'euros ou 2 pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu, l'entité essentielle qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents visées au titre 3.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

Le concours de plusieurs manquements peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 60. Si les mesures demandées ne sont pas prises dans le délai imparti, les mesures administratives suivantes peuvent être imposées aux entités essentielles sur la base de l'article 52:

1° demander à l'autorité nationale de cybersécurité de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité concernée;

2° interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité concernée d'exercer des responsabilités dirigeantes dans cette entité.

Les suspensions ou interdictions temporaires visées à l'alinéa 1er sont uniquement appliquées jusqu'à ce que l'entité concernée ait pris les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution.

Art. 61. Toute personne physique responsable d'une entité essentielle ou importante ou agissant en qualité de représentant légal d'une entité essentielle ou importante sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle a le pouvoir de veiller au respect, par l'entité, de la présente loi. Ces personnes sont responsables des manquements à leur devoir de veiller au respect de la présente loi.

Cet article est sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

TITRE 5. — *Dispositions spécifiques au secteur de l'administration publique*

Art. 62. Les mesures et amendes administratives visées aux articles 59 et 60 ne s'appliquent pas aux entités faisant partie du secteur de l'administration publique.

Art. 63. § 1er. Le Roi est habilité à désigner une autorité comme organisme d'évaluation de la conformité de tout ou partie des entités de l'administration publique.

§ 2. L'autorité visée au paragraphe 1er est agréée par l'autorité nationale de cybersécurité, selon les modalités fixées par le Roi, afin d'effectuer l'évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°.

L'agréation visée à l'alinéa 1er porte sur un ou plusieurs des cadres de référence visés à l'article 39.

Art. 64. Le service d'inspection de l'autorité nationale de cybersécurité ou, le cas échéant, le service d'inspection sectoriel désigné par le Roi pour le secteur de l'administration publique exerce ses tâches de supervision en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées.

Art. 65. L'article 47 est applicable au service d'inspection visé à l'article 64.

TITRE 6. — *Traitement des données à caractère personnel*

CHAPITRE 1er. — *Principes relatifs au traitement*

Art. 66. Les définitions du règlement (UE) 2016/679 sont d'application pour le présent titre.

Art. 67. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:

1° l'amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;

2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren en sensibiliseren van de gebruikers van informatie- en communicatiesystemen, het toekennen van subsidies, de internationale samenwerking tussen de nationale cyberbeveiligingsautoriteit, de bevoegde autoriteiten van andere lidstaten, internationale fora voor cyberbeveiliging, Enisa en de Europese Commissie;

3° het beheer van cybercrises en cyberbeveiligingsincidenten;

4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikelen:

a) 19, § 1;

b) 21, § 2, tweede lid, 1° tot 3°;

c) 22, § § 2 tot 6;

d) 37, § § 1 tot 3 en § 5;

5° de samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de wet van 1 juli 2011, alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en de wet van 1 juli 2011;

6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;

7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;

8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;

9° het melden van incidenten en bijna-incidenten;

10° de controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes.

Art. 68. De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:

1° voor het doeleinde bedoeld in artikel 67, 1°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen bedoeld in artikel 67, 1°;

2° voor het doeleinde bedoeld in artikel 67, 2°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit;

3° voor het doeleinde bedoeld in artikel 67, 3°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij cybercrises en cyberbeveiligingsincidenten;

4° voor het doeleinde bedoeld in artikel 67, 4°: de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, en elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van voornoemde wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT;

5° voor het doeleinde bedoeld in artikel 67, 5°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking in het kader van de wet van 1 juli 2011;

6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;

7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;

8° voor het doeleinde bedoeld in artikel 67, 8°: de identificatiegegevens van de personen die betrokken zijn bij het waarborgen van de continuïteit van de dienstverlening;

9° voor het doeleinde bedoeld in artikel 67, 9°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de melding;

10° voor het doeleinde bedoeld in artikel 67, 10°: de persoonsgegevens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controles, dit toezicht of deze sancties.

2° l'exécution des tâches de l'autorité nationale de cybersécurité, notamment l'identification des entités, l'information et la sensibilisation des utilisateurs des systèmes d'information et de communication, l'octroi de subventions, la coopération internationale entre l'autorité nationale de cybersécurité, des autorités compétentes des autres États membres, des forums internationaux de cybersécurité, l'ENISA et la Commission européenne;

3° la gestion des crises cyber et incidents de cybersécurité;

4° l'exécution des tâches du CSIRT national visées aux articles suivants:

a) 19, § 1er;

b) 21, § 2, alinéa 2, 1° à 3°;

c) 22, § § 2 à 6;

d) 37, § § 1er à 3 et § 5;

5° la coopération, notamment l'échange d'informations entre l'autorité nationale de cybersécurité, les éventuelles autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de la loi du 1er juillet 2011, ainsi que les autorités visées à l'article 25, § 2, dans le cadre de l'exécution de la présente loi et la loi du 1er juillet 2011;

6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1er;

7° le partage d'informations entre les autorités visées à l'article 25, § 5;

8° la continuité des services prestés par les entités importantes ou essentielles;

9° la notification d'incidents et d'incidents évités;

10° le contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives.

Art. 68. Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes:

1° pour la finalité visée à l'article 67, 1°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les missions d'amélioration de la cybersécurité, de renforcement des politiques de prévention et de sécurité, de prévention des incidents de sécurité et de défense contre les cybermenaces visées à l'article 67, 1°;

2° pour la finalité visée à l'article 67, 2°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exécution des tâches de l'autorité nationale de cybersécurité;

3° pour la finalité visée à l'article 67, 3°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les crises cyber et incidents de cybersécurité;

4° pour la finalité visée à l'article 67, 4°: les données d'identification, de connexion, de localisation, de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 et des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005, des personnes concernées par l'exécution des tâches du CSIRT;

5° pour la finalité visée à l'article 67, 5°: les données d'identification des personnes concernées par la coopération dans le cadre de la loi du 1er juillet 2011;

6° pour la finalité visée à l'article 67, 6°: les données d'identification des personnes concernées par la coopération;

7° pour la finalité visée à l'article 67, 7°: les données d'identification des personnes concernées par le partage d'informations;

8° pour la finalité visée à l'article 67, 8°: les données d'identification des personnes concernées par l'assurance d'une continuité des services;

9° pour la finalité visée à l'article 67, 9°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exercice de notification;

10° pour la finalité visée à l'article 67, 10°: les données à caractère personnel nécessaires et pertinentes à l'exercice des missions de contrôle, de supervision et de sanction, des personnes concernées par ces contrôles, cette supervision ou ces sanctions.

Art. 69. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:

1° de personen die rechtstreeks deelnemen aan de opdrachten die krachtens titel 2 zijn toevertrouwd aan de nationale cyberbeveiligingsautoriteit;

2° de personen bedoeld in het kader van de verplichtingen voor essentiële en belangrijke entiteiten krachtens titel 3;

3° de personen die betrokken zijn bij een incident;

4° de personen die rechtstreeks betrokken zijn bij het toezicht, de controle en de sancties bedoeld in titel 4.

Art. 70. De volgende entiteiten zijn verantwoordelijk voor de verwerkingen die zij uitvoeren voor de verwezenlijking van de doeleinden bedoeld in artikel 67:

1° de nationale cyberbeveiligingsautoriteit;

2° het NCCN;

3° de eventuele sectorale overheid;

4° de eventuele sectorale inspectiedienst;

5° de essentiële en belangrijke entiteiten;

6° de entiteiten die domeinnaamregistratiediensten verlenen;

7° de autoriteiten bedoeld in artikel 23, § 1, 6°.

HOOFDSTUK 2. — *Bewaartermijn*

Art. 71. De verwerkingsverantwoordelijke bewaart de persoonsgegevens die verwerkt worden in het kader van de in deze wet bedoelde verwerkingen om de doeleinden bedoeld in artikel 67 te realiseren, onverminderd eventuele beroepsprocedures, gedurende vijf jaar na afloop van de laatste verwerking en maximaal gedurende tien jaar na de eerste verwerking.

HOOFDSTUK 3. — *Beperking van de rechten van de betrokkenen*

Art. 72. § 1. Met toepassing van artikel 23.1, punten *a)* tot *e)* en *h)*, van Verordening (EU) 2016/679 worden sommige verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de fundamentele rechten en vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 16, 18 en 19 van voornoemde verordening zijn niet van toepassing op verwerkingen van persoonsgegevens die worden verricht door een autoriteit bedoeld in artikel 15 voor het doeleinde bedoeld in artikel 67, 10°, voor zover de uitoefening van de in deze artikelen vastgelegde rechten nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan.

§ 3. De vrijstelling geldt voor de categorieën van persoonsgegevens bedoeld in artikel 68, 10°. Deze vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 4. De vrijstelling geldt enkel voor de periode tijdens dewelke de betrokkene onderworpen is aan een controle, toezicht of de voorbereidende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit artikel bedoelde afwijking nadelig zou zijn voor de controle, het toezicht of de voorbereidende werkzaamheden ervan. In ieder geval geldt ze slechts maximaal één jaar na aanvang van een controle, toezicht of de voorbereidende werkzaamheden ervan.

De duur van de voorbereidende werkzaamheden bedoeld in het eerste lid, tijdens dewelke de in paragraaf 2 bedoelde artikelen niet van toepassing zijn, is beperkt tot maximaal één jaar na ontvangst van een verzoek betreffende de toepassing van een van de in deze artikelen vastgelegde rechten.

§ 5. De verwerkingsverantwoordelijke die niet voldoet aan alle bepalingen van deze titel en met name van artikel 73, kan geen gebruik maken van de vrijstelling.

Art. 73. § 1. De betrokken verwerkingsverantwoordelijke verleent de betrokkene toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze mededeling de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt. Hierbij moet het voor de betrokkene onmogelijk zijn om na te gaan of hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde gegevens die in het bovenvermelde kader noodzakelijk is, stopzetten.

Art. 69. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitement sont les suivantes:

1° les personnes participant directement aux missions confiées à l'autorité nationale de cybersécurité en vertu du titre 2;

2° les personnes visées par les obligations qui incombent aux entités essentielles et importantes en vertu du titre 3;

3° les personnes impliquées dans un incident;

4° les personnes directement impliquées dans les exercices de supervision, de contrôle et de sanction, visés au titre 4.

Art. 70. Les entités suivantes sont responsables des traitements qu'elles effectuent pour la réalisation des finalités visées à l'article 67:

1° l'autorité nationale de cybersécurité;

2° le NCCN;

3° l'éventuelle autorité sectorielle;

4° l'éventuel service d'inspection sectoriel;

5° les entités essentielles et importantes;

6° les entités fournissant des services d'enregistrement de noms de domaine;

7° les autorités visées à l'article 23, § 1er, 6°.

CHAPITRE 2. — *Durée de conservation*

Art. 71. Les données à caractère personnel traitées dans le cadre des traitements visés par la présente loi en vue de réaliser les finalités prévues à l'article 67, sont conservées, sans préjudice de recours éventuels, par le responsable du traitement cinq ans après la fin du dernier traitement effectué et dix ans maximum après le premier traitement effectué.

CHAPITRE 3. — *Limitation des droits des personnes concernées*

Art. 72. § 1er. En application de l'article 23.1, points *a)* à *e)* et *h)*, du règlement (UE) 2016/679, certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent chapitre. Ces limitations ou exclusions ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 16, 18 et 19 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel effectués par une autorité visée à l'article 15 pour la finalité visée à l'article 67, 10°, dans la mesure où l'exercice des droits consacrés par ces articles nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à celui-ci.

§ 3. L'exemption vaut pour les catégories de données à caractère personnel visées à l'article 68, 10°. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 4. L'exemption ne s'applique que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci, dans la mesure où l'exercice des droits faisant l'objet de la dérogation visée au présent article nuirait aux besoins du contrôle, de la supervision ou des actes préparatoires à ceux-ci et, en tous les cas, ne s'applique que jusqu'à un an après le début d'un contrôle, d'une supervision ou d'actes préparatoires à ceux-ci.

La durée des actes préparatoires, visés à l'alinéa 1er, pendant laquelle les articles visés au paragraphe 2 ne sont pas applicables, ne peut excéder un an à partir de la réception d'une demande relative à l'application d'un des droits consacrés par ces articles.

§ 5. Le responsable du traitement qui ne se conforme pas à toutes les dispositions du présent titre et en particulier de l'article 73, ne peut pas bénéficier de l'exemption.

Art. 73. § 1er. Le responsable du traitement concerné donne accès à la personne concernée à des informations limitées concernant le traitement de ses données à caractère personnel, pour autant que cette communication ne compromette pas la réalisation des objectifs de la présente loi et de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données à caractère personnel, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 2. De maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, moet worden opgeheven:

1° voor maatregelen die gerechtvaardigd zijn door de verplichtingen inzake het melden van incidenten, bij het afsluiten van de verwerking van een incident door de autoriteiten bedoeld in de artikelen 34 en 38;

2° voor maatregelen die gerechtvaardigd zijn door de verplichtingen krachtens titel 4, bij het afsluiten van de controle, het toezicht of de voorbereidende werkzaamheden ervan door de inspectiedienst, alsook in de periode tijdens dewelke de eventuele sectorale overheid de stukken verwerkt die afkomstig zijn van de inspectiedienst met het oog op vervolging;

3° uiterlijk één jaar na ontvangst van het verzoek dat is ingediend overeenkomstig de artikelen bedoeld in artikel 72, § 2, behalve indien een controle of toezicht loopt.

§ 3. De betrokken verwerkingsverantwoordelijke heft de maatregel betreffende de weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, ook op zodra deze maatregel niet meer nodig is voor het nakomen van een van de doeleinden bedoeld in artikel 67.

§ 4. In alle toepassingsgevallen van de paragrafen 2 en 3 informeert de functionaris voor gegevensbescherming de betrokkene of betrokkenen schriftelijk dat de maatregel betreffende de weigering of beperking is opgeheven.

HOOFDSTUK 4. — *Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens*

Art. 74. De betrokken verwerkingsverantwoordelijke is vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een of meer welbepaalde betrokkenen, in de zin van artikel 34 van Verordening EU 2016/679, mits toestemming van de nationale cyberbeveiligingsautoriteit, voor zover deze individuele kennisgeving de verwezenlijking van de doeleinden bedoeld in artikel 72, § 2, in het gedrang zou brengen.

TITEL 7. — *Slotbepalingen*

HOOFDSTUK 1. — *Overgangsbepaling*

Art. 75. De Koning stelt de termijnen vast waarbinnen essentiële entiteiten hun eerste regelmatige conformiteitsbeoordelingen bedoeld in artikel 39 uitvoeren.

HOOFDSTUK 2. — *Wijzigingsbepalingen*

Afdeling 1. — Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 76. In artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, laatstelijk gewijzigd bij de wet van 7 februari 2024, worden de woorden ″- ″de wet van 7 april 2019″: 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;″ vervangen door de woorden ″- de NIS2-wet: de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;″.

Art. 77. In hoofdstuk III, afdeling 1, van dezelfde wet wordt artikel 15*ter*, ingevoegd bij de wet van 7 april 2019, vervangen als volgt:

″Art. 15*ter*. Het Agentschap wordt aangewezen als sectorale inspectiedienst, in de zin van de NIS2-wet, voor de sector energie, wat betreft de bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's die van toepassing zijn op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.″

Afdeling 2. — Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 78. In artikel 36/1 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, laatstelijk gewijzigd bij de wet van 20 december 2023, wordt de bepaling onder 28° vervangen als volgt:

″28° ″de NIS2-wet″: de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;″.

§ 2. La mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, doit être levée:

1° pour les mesures justifiées par les obligations en matière de notification d'incidents, lors de la clôture du traitement d'un incident par les autorités visées aux articles 34 et 38;

2° pour les mesures justifiées par les obligations en vertu du titre 4, lors de la clôture du contrôle, de la supervision ou des actes préparatoires à ceux-ci effectués par le service d'inspection, ainsi que pendant la période durant laquelle l'éventuelle autorité sectorielle traite les pièces provenant du service d'inspection en vue d'exercer des poursuites;

3° au plus tard un an à partir de la réception de la demande introduite en application des articles visés à l'article 72, § 2, sauf si un contrôle ou une supervision sont en cours.

§ 3. Le responsable du traitement concerné lève également la mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, dès qu'une telle mesure n'est plus nécessaire au respect d'une des finalités visées à l'article 67.

§ 4. Dans tous les cas d'application des paragraphes 2 et 3, le délégué à la protection des données informe par écrit la ou les personnes concernées de la levée de la mesure de refus ou de limitation.

CHAPITRE 4. — *Limitations aux obligations de notification des violations de données à caractère personnel*

Art. 74. Le responsable du traitement concerné est dispensé de communiquer une violation de données à caractère personnel à une ou des personnes concernées bien déterminées, au sens de l'article 34 du règlement (UE) 2016/679, moyennant l'autorisation de l'autorité nationale de cybersécurité, pour autant que et dans la mesure où une telle notification individuelle risque de compromettre la réalisation des finalités visées à l'article 72, § 2.

TITRE 7. — *Dispositions finales*

CHAPITRE 1er. — *Disposition transitoire*

Art. 75. Le Roi fixe les délais endéans lesquels les entités essentielles effectuent leurs premières évaluations périodiques de la conformité visées à l'article 39.

CHAPITRE 2. — *Dispositions modificatives*

Section 1re. — Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 76. Dans l'article 1er de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, modifié en dernier lieu par la loi du 7 février 2024, les mots ″- ″la loi du 7 avril 2019″: 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;″ sont remplacés par les mots ″- la loi NIS2: la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;″.

Art. 77. Dans le chapitre III, section 1re, de la même loi, l'article 15*ter*, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

″Art. 15*ter*. L'Agence est désignée comme service d'inspection sectoriel, au sens de la loi NIS2, pour le secteur de l'énergie, en ce qui concerne les mesures supplémentaires de gestion des risques en matière de cybersécurité applicables aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence.″

Section 2. — Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 78. Dans l'article 36/1 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, modifié en dernier lieu par la loi du 20 décembre 2023, le 28° est remplacé par ce qui suit:

″28° ″la loi NIS2″: la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;″.

Art. 79. In artikel 36/14 van dezelfde wet, laatstelijk gewijzigd bij de wet van 20 december 2023, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, 20°, worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019" vervangen door de woorden "aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet";

2° in dezelfde paragraaf, 20° /1, worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, 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 - NIS-wet" vervangen door de woorden "aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 46°, van dezelfde wet";

3° in dezelfde paragraaf, 24°, worden de woorden "aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019" vervangen door de woorden "aan de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet".

Art. 80. Artikel 36/47 van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt vervangen als volgt:

"Art. 36/47. Voor de toepassing van de NIS2-wet wordt de Bank aangewezen als sectorale overheid en sectorale inspectiedienst voor de entiteiten van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

Wanneer zij dit nuttig acht, deelt de Bank zo snel mogelijk met de ECB relevante informatie over incidentmeldingen die zij ontvangt krachtens de NIS2-Wet of Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011."

Afdeling 3. — Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 81. In artikel 75, § 1, 15°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, laatstelijk gewijzigd bij de wet van 20 juli 2020, worden de woorden "artikel 7 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" vervangen door de woorden "artikel 15 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Afdeling 4. — Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 82. In artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, vervangen bij de wet van 21 december 2021, wordt de bepaling onder 1° vervangen als volgt:

"1° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148;".

Art. 83. In artikel 14 van dezelfde wet, laatstelijk gewijzigd bij de wet van 17 december 2023, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

2° in dezelfde paragraaf, eerste lid, 3°, wordt de bepaling onder *h)*, vervangen als volgt:

"h) de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid en de sectorale inspectiedienst voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet;";

Art. 79. À l'article 36/14 de la même loi, modifié en dernier lieu par la loi du 20 décembre 2023, les modifications suivantes sont apportées:

1° au paragraphe 1er, 20°, les mots "à l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019" sont remplacés par les mots "à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2";

2° au même paragraphe, 20° /1, les mots "à l'autorité visée à l'article 7, § 1er, 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 - loi NIS" sont remplacés par les mots "à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et au CSIRT national visé à l'article 8, 46°, de la même loi";

3° au même paragraphe, 24°, les mots "aux autorités visées à l'article 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019" sont remplacés par les mots "aux autorités visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2".

Art. 80. L'article 36/47 de la même loi, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit:

"Art. 36/47. Pour l'application de la loi NIS2, la Banque est désignée comme autorité sectorielle et service d'inspection sectoriel pour les entités du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE.

Si elle le juge utile, la Banque partage le plus vite possible avec la BCE les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi NIS2 ou du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.".

Section 3. — Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 81. Dans l'article 75, § 1er, 15°, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, modifié en dernier lieu par la loi du 20 juillet 2020, les mots "l'article 7 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" sont remplacés par les mots "l'article 15 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

Section 4. — Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 82. À l'article 1er/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, remplacé par la loi du 21 décembre 2021, le 1° est remplacé par ce qui suit:

"1° la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148;".

Art. 83. À l'article 14 de la même loi, modifié en dernier lieu par la loi du 17 décembre 2023, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 1er, les mots "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" sont remplacés par les mots "loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique";

2° au même paragraphe, alinéa 1er, 3°, le *h)*, est remplacé par ce qui suit:

"h) la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle et au service d'inspection sectoriel pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de la même loi;";

3° in dezelfde paragraaf wordt het tweede lid vervangen als volgt:

"Voor de toepassing van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid in de zin van artikel 8, 54°, van dezelfde wet en als sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet, en voor de sector post- en koeriersdiensten."

Afdeling 5. — Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 84. Artikel 1, tweede lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 21 december 2021,wordt aangevuld met een bepaling onder 7°, luidende:

"7° Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148."

Art. 85. In artikel 2 van dezelfde wet, laatstelijk gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° de bepaling onder 48/1° wordt vervangen als volgt:

"48/1° "register voor topleveldomeinnamen": een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;";

2° de bepaling onder 48/3° wordt ingevoegd, luidende:

"48/3° "entiteit die domeinnaamregistratiediensten aanbiedt": een registrator of een agent die namensregistrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;";

3° de bepalingen onder 62/2° en 62/3° worden vervangen als volgt:

"62/2° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk bedoeld in de bepaling onder3°;

b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in de bepalingen onder *a)* en *b)* bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

62/3° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;";

4° de bepalingen onder 62/4° tot 62/8° worden ingevoegd, luidende:

"62/4° "beveiligingsincident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

62/5° "cyberbeveiliging": cyberbeveiliging bedoeld in artikel 2, punt 1), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

3° au même paragraphe, l'alinéa 2 est remplacé par ce qui suit:

"Pour l'application de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle au sens de l'article 8, 54°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1er, alinéa 2, de cette même loi pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi, et pour le secteur des services postaux et d'expédition.".

Section 5. — Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 84. L'article 1er, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques, modifié en dernier lieu par la loi du 21 décembre 2021, est complété par le 7° rédigé comme suit:

"7° la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.".

Art. 85. À l'article 2 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1° le 48/1° est remplacé par ce qui suit:

"48/1° "registre de noms de domaine de premier niveau": une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;";

2° le 48/3° est inséré rédigé comme suit:

"48/3° "entité fournissant des services d'enregistrement de noms de domaine": un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;";

3° les 62/2° et 62/3° sont remplacés par ce qui suit:

"62/2° "réseau et système d'information":

a) un réseau de communications électroniques visé au 3°;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points *a)* et *b)* en vue de leur fonctionnement, utilisation, protection et maintenance;

62/3° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;";

4° les 62/4° à 62/8° sont insérés rédigés comme suit:

"62/4° "incident de sécurité": un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

62/5° "cybersécurité": la cybersécurité visée à l'article 2, point 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité);

62/6° ″incidentenbehandeling″: alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een beveiligingsincident;

62/7° ″cyberdreiging″: een cyberdreiging als bedoeld in artikel 2, punt 8), van Verordening (EU) 2019/881;

62/8° ″significante cyberdreiging″: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële, lichamelijke of immateriële schade;″;

5° het artikel wordt aangevuld met een bepaling onder 94°, luidende:

″94° ″aanbieder van digitale infrastructuur″: een entiteit die behoort tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, in de zin van artikel 8, 24°, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.″.

Art. 86. In artikel 6, 4°, van dezelfde wet, vervangen bij de wet van 21 december 2021, worden de woorden ″netwerken en diensten″ vervangen door de woorden ″netwerk- en informatiesystemen″.

Art. 87. In artikel 105, § 2, 2°, van dezelfde wet, vervangen bij de wet van 17 februari 2022, worden de woorden ″of als aanbieder van essentiële diensten in de zin 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″ opgeheven.

Art. 88. In dezelfde wet wordt artikel 107/2, ingevoegd bij de wet van 21 december 2021, vervangen als volgt:

″Art. 107/2. § 1. Onverminderd de bepalingen van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid analyseren de aanbieders van digitale infrastructuur de risico's voor de beveiliging van hun netwerk- en informatiesystemen. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.

§ 2. Onverminderd Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna te noemen de AVG, en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna te noemen de wet van 30 juli 2018, zorgen de operatoren ervoor dat in ieder geval:

1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens die ze verwerken;

2° opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en

3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door deze operatoren genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald.

§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en de internettoegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

Op voorstel van het Instituut of op eigen initiatief, en na advies van het Instituut, kan de Koning deze maatregelen preciseren.

§ 4. De operatoren bieden hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.″.

Art. 89. In dezelfde wet wordt artikel 107/3, ingevoegd bij de wet van 21 december 2021, vervangen als volgt:

″Art. 107/3. § 1. In geval van een significante cyberdreiging informeert de aanbieder van digitale infrastructuur het Instituut over de dreiging, over mogelijke beschermingsmaatregelen of oplossingen die de gebruikers kunnen toepassen, alsook over de maatregelen die hij heeft genomen of overweegt te nemen.

62/6° ″traitement des incidents″: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

62/7° ″cybermenace″: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

62/8° ″cybermenace importante″: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;″;

5° l'article est complété par le 94°, rédigé comme suit:

″94° ″fournisseur d'infrastructure numérique″: une entité qui relève du secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance, au sens de l'article 8, 24°, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.″.

Art. 86. Dans l'article 6, 4°, de la même loi, remplacé par la loi du 21 décembre 2021, les mots ″réseaux et services″ sont remplacés par les mots ″réseaux et systèmes d'information″.

Art. 87. Dans l'article 105, § 2, 2°, de la même loi, remplacé par la loi du 17 février 2022, les mots ″ou comme opérateur de services essentiels au sens 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″ sont abrogés.

Art. 88. Dans la même loi, l'article 107/2, inséré par la loi du 21 décembre 2021, est remplacé par ce qui suit:

″Art. 107/2. § 1er. Sans préjudice des dispositions de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les fournisseurs d'infrastructure numérique analysent les risques pour la sécurité de leurs réseaux et systèmes d'information. L'Institut peut fixer les modalités de cette analyse des risques.

§ 2. Sans préjudice du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après dénommé le RGPD et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ci-après dénommée la loi du 30 juillet 2018, les opérateurs veillent pour le moins à:

1° garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel qu'ils traitent;

2° protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites; et

3° assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

L'Institut est habilité à vérifier les mesures prises par ces opérateurs ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre.

§ 3. Les opérateurs prennent toutes les mesures nécessaires, y compris préventives, pour assurer la disponibilité la plus complète possible des services de communications vocales et des services d'accès à l'internet en cas de défaillance exceptionnelle des réseaux ou de force majeure.

Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures.

§ 4. Les opérateurs offrent gratuitement à leurs abonnés, compte tenu des possibilités techniques, les services sécurisés adéquats, afin de permettre aux utilisateurs finaux d'éviter toute forme de communication électronique non souhaitée.″.

Art. 89. Dans la même loi, l'article 107/3, inséré par la loi du 21 décembre 2021, est remplacé par ce qui suit:

Art. 107/3. § 1er. En cas de cybermenace importante, le fournisseur d'infrastructure numérique informe l'Institut de la cybermenace, de toute mesure de protection ou correctrice que ses utilisateurs peuvent prendre ainsi que des mesures qu'il a prises ou envisage de prendre.

Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de nadere regels voor die kennisgeving.

§ 2. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de Gegevensbeschermingsautoriteit, die onverwijld het Instituut verwittigt.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoonlijke levenssfeer van een abonnee of een individueel persoon, stelt de operator van elektronische-communicatiediensten onverwijld ook de betrokken abonnee of individuele persoon in kennis van de inbreuk.

De Gegevensbeschermingsautoriteit gaat na of de operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel is dat dit niet het geval is.

De kennisgeving van een inbreuk in verband met persoonsgegevens aan een betrokken abonnee of individuele persoon is niet vereist wanneer de operator van elektronische-communicatiediensten tot voldoening van het Instituut heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator van elektronische-communicatiediensten om de betrokken abonnees en individuele personen in kennis te stellen, indien deze operator de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan het Instituut op verzoek van de Gegevensbeschermingsautoriteit hem, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk in verband met persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

De kennisgeving aan de Gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk in verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde of getroffen maatregelen om die inbreuk te verhelpen.

§ 3. Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van de Gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

Onder voorbehoud van technische uitvoeringsmaatregelen van de Europese Commissie overeenkomstig artikel 4, punt 5, van Richtlijn 2002/58/EG, en na advies van het Instituut, kan de Gegevensbeschermingsautoriteit richtsnoeren aannemen en, waar nodig, instructies uitvaardigen betreffende het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt.

De operatoren van elektronische-communicatiediensten houden een inventaris bij van inbreuken in verband met persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de Gegevensbeschermingsautoriteit en het Instituut kunnen nagaan of de bepalingen van paragraaf 2 werden nageleefd. Deze inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.".

Art. 90. In dezelfde wet wordt artikel 107/4, ingevoegd bij de wet van 21 december 2021, vervangen als volgt:

"Art. 107/4. § 1. Dit artikel is van toepassing, onverminderd de bepalingen van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met name voor wat betreft de toezichtsbevoegdheden verleend aan de sectorale overheid of de sectorale inspectiedienst.

§ 2. Het Instituut kan een aanbieder van digitale infrastructuur bindende instructies geven in het kader van de artikelen 107/2 en 107/3 en van de artikelen 30 en 33 van de bovengenoemde wet van 26 april 2024, onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.

L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.

§ 2. En cas de violation de données à caractère personnel, l'opérateur de services de communications électroniques avertit sans délai l'Autorité de protection des données, qui en avertit sans délai l'Institut.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'opérateur de services de communications électroniques avertit également sans délai l'abonné ou le particulier concerné de la violation.

L'Autorité de protection des données examine si l'opérateur se conforme à cette obligation et informe l'Institut lorsqu'elle estime que cela n'est pas le cas.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si l'opérateur de services de communications électroniques a prouvé, à la satisfaction de l'Institut, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation de l'opérateur de service de communications électroniques d'informer les abonnés et les particuliers concernés, si cet opérateur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'Institut peut, à la demande de l'Autorité de protection des données, après avoir examiné les effets potentiellement négatifs de cette violation, exiger qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel.

La notification faite à l'Autorité de protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par l'opérateur de services de communications électroniques pour y remédier.

§ 3. Sous réserve de mesures d'exécution techniques émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Autorité de protection des données, l'Institut peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles les opérateurs de services de communications électroniques sont tenus de notifier la violation de données à caractère personnel.

Sous réserve de mesures techniques d'application émanant de la Commission européenne conformément à l'article 4, point 5, de la directive 2002/58/CE, et après avis de l'Institut, l'Autorité de protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant le format applicable à cette notification et sa procédure de transmission.

Les opérateurs de services de communications électroniques tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de sorte que l'Autorité de protection des données et l'Institut puissent vérifier le respect des dispositions du paragraphe 2. Cet inventaire comprend uniquement les informations nécessaires à cette fin.".

Art. 90. Dans la même loi, l'article 107/4, inséré par la loi du 21 décembre 2021, est remplacé par ce qui suit:

"Art. 107/4. § 1er. Le présent article s'applique sans préjudice des dispositions de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, notamment en ce qui concerne les pouvoirs de supervision accordés à l'autorité sectorielle ou au service d'inspection sectoriel.

§ 2. L'Institut peut donner des instructions contraignantes dans le cadre des articles 107/2, 107/3 ainsi que des articles 30 et 33 de la loi du 26 avril 2024 précitée à un fournisseur d'infrastructure numérique, y compris les mesures requises pour remédier à un incident de sécurité ou empêcher qu'un tel incident ne se produise lorsqu'une cybermenace importante a été identifiée, ainsi que les dates limites de mise en œuvre de ces instructions.

§ 3. In het kader van het toezicht op de artikelen 107/2 en 107/3 en op de artikelen 30 en 33 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyber- beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, kan het Instituut de aanbieder van digitale infrastructuur onderwerpen aan:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles, die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Instituut of door een onafhankelijke instantie;

c) ad-hocaudits;

d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;

e) verzoeken om informatie die nodig is om de door de betrokken aanbieder van digitale infrastructuur genomen maatregelen voor het beheer van cyberbeveiligingsrisico's;

f) verzoeken van toegang tot alle gegevens, documenten en informatie die het Instituut nodig acht voor de uitoefening van zijn toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in het eerste lid, *b)*, bedoelde gerichte beveiligingsaudits zijn gebaseerd op door het Instituut of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.

Wanneer de in het eerste lid, *b)*, bedoelde beveiligingsaudit wordt uitgevoerd door een onafhankelijke instantie, dan stelt de aanbieder van digitale infrastructuur een of meer instanties ter goedkeuring aan het Instituut voor. Het Instituut geeft zijn akkoord wanneer de onafhankelijke instantie gekwalificeerd is om de audit uit te voeren en onafhankelijk is van de aanbieder van digitale infrastructuur. Bij uitblijven van een akkoord vanwege het Instituut binnen de termijn die het bij het verzoek heeft vastgesteld, wijst het Instituut zelf de onafhankelijk instantie aan. Deze laatste bezorgt aan het Instituut het volledige verslag en de resultaten van deze audit en de kosten van de audit zijn ten laste van de aanbieder van digitale infrastructuur, behalve in naar behoren met redenen omklede gevallen waarin het Instituut anders besluit.

Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, *e)*, f) of *g)*, vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.

Het Instituut kan bepalen op welke wijze de aanbieder van digitale infrastructuur informatie over de risicoanalyse moet verstrekken.

Op verzoek van het Instituut neemt een aanbieder van digitale infrastructuur deel aan een oefening in verband met de beveiliging van de netwerk- en informatiesystemen of organiseert hij een dergelijke oefening.

Op verzoek van het Instituut en in het kader van het beheer van beveiligingsincidenten, deelt een aanbieder van digitale infrastructuur het Instituut een contactpersoon mee die steeds bereikbaar is.

§ 4. Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met de artikelen 30 en 33 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, of met een uitvoeringsmaatregel, alsook naar de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen, geeft de aanbieder van digitale infrastructuur het Instituut toegang tot alle elementen van zijn netwerk.

§ 5. Onverminderd de bevoegdheden van de nationale cyberbeveiligingsautoriteit coördineert het Instituut de initiatieven rond de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

Het ziet toe op het opsporen, observeren en analyseren van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.

§ 6. Indien een aanbieder van digitale infrastructuur dit artikel of een op grond van dit artikel genomen beslissing van het Instituut niet naleeft, kunnen de in titel 4, hoofdstuk 2, van de wet van 26 april 2024

§ 3. Dans le cadre de la supervision des articles 107/2 et 107/3 ainsi que des articles 30 et 33 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut peut soumettre le fournisseur d'infrastructure numérique à:

a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou par l'Institut;

c) des audits ad hoc;

d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération du fournisseur d'infrastructure numérique;

e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par le fournisseur d'infrastructure numérique concerné;

f) des demandes d'accès à des données, à des documents et à toutes informations que l'Institut estime nécessaire pour l'accomplissement de ses tâches de supervision;

g) des demandes de preuves de la mise en oeuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés à l'alinéa 1er, *b)*, sont basés sur des évaluations des risques effectuées par l'Institut ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Lorsque l'audit de sécurité visé à l'alinéa 1er, *b)*, est effectué par un organisme indépendant, le fournisseur d'infrastructure numérique propose à l'Institut un ou plusieurs organismes pour accord. L'Institut donne son accord lorsque l'organisme indépendant est qualifié pour effectuer l'audit et est indépendant par rapport au fournisseur d'infrastructure numérique. À défaut d'accord de l'Institut dans le délai qu'il a fixé lors de la demande, l'Institut désigne lui-même l'organisme indépendant. Ce dernier communique à l'Institut le rapport complet et les résultats de cet audit. Les coûts de l'audit sont à la charge du fournisseur d'infrastructure numérique, sauf lorsque l'Institut en décide autrement dans des cas dûment motivés.

Lorsqu'il exerce ses pouvoirs en vertu du paragraphe 1, *e)*, f) ou *g)*, l'Institut précise la finalité de la demande et les informations exigées.

L'Institut peut fixer les modalités de la fourniture par le fournisseur d'infrastructure numérique des informations concernant l'analyse de risque.

À la demande de l'Institut, un fournisseur d'infrastructure numérique participe à un exercice relatif à la sécurité des réseaux et systèmes d'information ou organise un tel exercice.

À la demande de l'Institut et dans le cadre de la gestion des incidents de sécurité, un fournisseur d'infrastructure numérique communique à l'Institut un point de contact disponible en permanence.

§ 4. À la demande de l'Institut et pour enquêter sur un cas de non-conformité par rapport aux articles 30 et 33 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou à une mesure d'exécution ainsi que sur son effet sur la sécurité des réseaux et systèmes d'information, le fournisseur d'infrastructure numérique lui donne accès à tout élément de son réseau.

§ 5. Sans préjudice des compétences de l'autorité nationale de cybersécurité, l'Institut coordonne les initiatives relatives à la sécurité des réseaux publics de communications électroniques et des services de communications électroniques accessibles au public.

Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.

§ 6. Le non-respect par un fournisseur d'infrastructure numérique du présent article ou d'une décision de l'Institut prise sur base du

tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatregelen of geldboetes worden opgelegd.".

Art. 91. In artikel 126/3, § 3, *l)*, van dezelfde wet, ingevoegd bij de wet van 20 juli 2022, worden de woorden "essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis 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" vervangen door de woorden "diensten van essentiële entiteiten in de zin van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Art. 92. In artikel 164/1 van dezelfde wet, ingevoegd bij de wet van 10 juli 2012, worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau van het topniveaudomein" worden vervangen door de woorden "register voor topleveldomeinnamen van het topleveldomein";

2° in de bepaling onder 4° wordt het woord "domeinnaamregistreerbureau" vervangen door de woorden "register voor topleveldomeinnamen";

3° in de bepaling onder 4° wordt het woord "Internetdomeinnaamregistreerbureau" vervagen door de woorden "register voor topleveldomeinnamen";

4° in de bepaling onder 5° wordt het woord "topniveaudomein" vervangen door het woord "topleveldomein".

Art. 93. In artikel 164/2 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "Internetdomeinnaamregistreerbureau" worden vervangen door de woorden "register voor topleveldomeinnamen";

2° in de Nederlandse tekst wordt het woord "topniveaudomein" vervangen door het woord "topleveldomein".

Art. 94. In titel VI, hoofdstuk III, van dezelfde wet, wordt een artikel 164/3 ingevoegd, luidende:

"Art. 164/3. § 1. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verzamelen met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens en houden deze bij in een speciale database overeenkomstig het Unierecht inzake de bescherming van persoonsgegevens.

§ 2.De domeinregistratiegegevens bedoeld in het eerste lid bevatten de noodzakelijke informatie om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren. Die informatie omvat ten minste:

1° de domeinnaam;

2° de registratiedatum;

3° de naam van de houder van de domeinnaam, zijn e-mailadres en zijn telefoonnummer;

4° het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de houder van de domeinnaam.

De Koning kan, na advies van het Instituut, aanbieders van privacy- of proxy-registratiediensten en wederverkopers gelasten de domeinnaamregistratiegegevens die ze hebben verzameld te delen met de registrators, en de modaliteiten daarvan bepalen.

De naleving van de in dit artikel bedoelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal worden verzameld bij de betrokkene. Daartoe werken de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, met elkaar samen.

De Koning kan, na advies van het Instituut, de modaliteiten van deze samenwerking preciseren.

§ 2. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, beschikken over beleidslijnen en procedures, waaronder verificatieprocedures, om te garanderen dat de in paragraaf 1, eerste lid, bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden openbaar gemaakt.

présent article peut faire l'objet des mesures ou amendes administratives visées dans le titre 4, chapitre 2, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.".

Art. 91. Dans l'article 126/3, § 3, *l)*, de la même loi, inséré par la loi du 20 juillet 2022, les mots "essentiels des fournisseurs de service essentiels désignés sur la base 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" sont remplacés par les mots "des entités essentielles au sens de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

Art. 92. À l'article 164/1 de la même loi, inséré par la loi du 10 juillet 2012, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet du domaine de premier niveau" sont remplacés par les mots "registre de noms de domaine de premier niveau du domaine de premier niveau";

2° au 4°, les mots "bureau d'enregistrement des noms de domaine" sont remplacés par les mots "registre de noms de domaine de premier niveau".

3° au 4°, les mots "bureau d'enregistrement des noms de domaine Internet" sont remplacés par les mots "registre de noms de domaine de premier niveau";

4° au 5°, dans le texte néerlandais, le mot "topniveaudomein" est remplacé par le mot "topleveldomein".

Art. 93. À l'article 164/2 de la même loi, les modifications suivantes sont apportées:

1° les mots "bureau d'enregistrement de noms de domaine Internet" sont chaque fois remplacés par les mots "registre de noms de domaine de premier niveau";

2° dans le texte en néerlandais, le mot "topniveaudomein" est à chaque fois remplacé par le mot "topleveldomein".

Art. 94. Dans le titre VI, chapitre III, de la même loi, il est inséré un article 164/3, rédigé comme suit:

"Art. 164/3. § 1er. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent, avec toute la diligence requise, les données d'enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d'une base de données spécialisée conformément au droit de l'Union en matière de protection des données à caractère personnel.

§ 2. Les données d'enregistrement de noms de domaine visées à l'alinéa 1er contiennent les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent au moins les éléments suivants:

1° le nom de domaine;

2° la date d'enregistrement;

3° le nom du titulaire de nom de domaine, son adresse de courrier électronique et son numéro de téléphone;

4° l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

Après avis de l'Institut, le Roi peut ordonner aux fournisseurs et aux revendeurs de services d'anonymisation ou d'enregistrement fiduciaire de partager les données d'enregistrement de noms de domaine avec les bureaux d'enregistrement et en définir les modalités.

Le respect des obligations visées au présent article ne doit pas entraîner de répétition inutile de la collecte des données d'enregistrement de noms de domaine auprès de la personne concernée. À cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.

Après avis de l'Institut, le Roi peut préciser les modalités de cette coopération.

§ 2. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine disposent des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1er, alinéa 1er, contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

Wanneer de domeinnaamregistratiegegevens opgesomd in paragraaf 1, tweede lid, van een domeinnaam onjuist, onnauwkeurig of onvolledig zijn, blokkeren de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen onmiddellijk het functioneren van deze domeinnaam tot de houder van de domeinnaam de registratiegegevens corrigeert zodat deze juist, nauwkeurig en volledig worden.

Indien de houder van de domeinnaam nalaat om dit te doen binnen de termijn zoals bepaald door het register voor topleveldomeinnamen of door de entiteit die domeinnaamregistratiediensten verleent, wordt de domeinnaam geannuleerd.

De transfer van een geblokkeerde domeinnaam naar een andere entiteit die domeinnaamregistratiediensten verleent, is verboden.

§ 3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, maken de domeinnaamregistratiegegevens die geen persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.

§ 4. Op een naar behoren met redenen omkleed verzoek, verschaffen de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, kosteloos, aan de legitieme toegangvragende partijen, de gegevens opgesomd in paragraaf 1, tweede lid, onverwijld en in elk geval binnen tweeënzeventig uur na ontvangst van het verzoek, of vierentwintig uur na ontvangst van het verzoek ingeval van hoogdringendheid.

Legitieme toegangvragende partijen omvatten elke natuurlijke of rechtspersoon die een verzoek indient voor het onderzoeken, vaststellen, uitoefenen of verdedigen van strafrechtelijke, burgerrechtelijke of andere bepalingen in het Unierecht of Belgisch recht.

Als legitieme toegangvragende partij worden beschouwd:

1° elke persoon in het kader van inbreuken op intellectuele eigendomsrechten of naburige rechten;

2° het Instituut;

3° het CCB;

4° het nationale CSIRT;

5° de politiediensten;

6° de gerechtelijke overheden;

7° de inlichtingen- en veiligheidsdiensten;

8° de FOD Economie;

9° de FOD Financiën.

De Koning kan, na advies van het Instituut, bijkomende legitieme toegangvragende partijen aan deze lijst toevoegen.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, stellen de verzoeker in staat om gemakkelijk zijn verzoek in te dienen.

Er is sprake van hoogdringendheid indien het gebruik van een domeinnaam kan leiden tot levensbedreigende situaties en/of onherstelbare schade.

Elke weigering van een naar behoren met redenen omkleed verzoek wordt met redenen omkleed.

Het beleid en de procedures met betrekking tot de bekendmaking van deze gegevens worden openbaar gemaakt.

De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, mogen de houder van een domeinnaam niet op de hoogte brengen wanneer een verzoek zoals bedoeld in het eerste lid werd ingediend.

§ 5. Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven met het oog op de naleving van dit artikel.

§ 6. Indien een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent dit artikel, een in uitvoering van dit artikel aangenomen koninklijk besluit of een bindende instructie van het Instituut niet naleeft, kan het Instituut de in hoofdstuk 2 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatregelen of geldboetes opleggen.”.

Si les données d'enregistrement de noms de domaine énumérées au paragraphe 1er, alinéa 2, d'un nom de domaine sont incorrectes, inexactes ou incomplètes, les registres de noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine bloquent immédiatement le fonctionnement de ce nom de domaine jusqu'à ce que le titulaire du nom de domaine corrige les données d'enregistrement pour qu'elles deviennent correctes, exactes et complètes.

Si le titulaire du nom de domaine ne le fait pas dans le délai fixé par le registre des noms de domaine de premier niveau ou par l'entité fournissant des services d'enregistrement de nom de domaine, le nom de domaine est annulé.

Le transfert d'un nom de domaine bloqué à une autre entité fournissant des services d'enregistrement de noms de domaine est interdit.

§ 3. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

§ 4. Sur demande dûment motivée, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine fournissent gratuitement les données énumérées au paragraphe 1er, alinéa 2, aux demandeurs d'accès légitimes, sans retard injustifié et en tout état de cause dans un délai de septante-deux heures après réception de toute demande d'accès, ou vingt-quatre heures après réception de toute demande d'accès en cas d'urgence.

Les demandeurs d'accès légitimes comprennent toute personne physique ou morale qui formule une demande d'examen, de constatation, d'exercice ou de défense de dispositions pénales, civiles ou autres du droit de l'Union ou du droit belge.

Sont considérés comme demandeurs d'accès légitimes:

1° toute personne dans le cadre de violations des droits de propriété intellectuelle ou des droits voisins;

2° l'Institut;

3° le CCB;

4° le CSIRT national;

5° les services de police;

6° les autorités judiciaires;

7° les services de renseignement et de sécurité;

8° le SPF Économie;

9° le SPF Finances.

Après avis de l'Institut, le Roi peut ajouter à cette liste des demandeurs d'accès légitimes supplémentaires.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine, offrent au demandeur la possibilité d'introduire aisément sa demande.

Il est question d'urgence si l'utilisation d'un nom de domaine peut conduire à des situations de danger de mort et/ou à des dommages irréparables.

Tout refus d'une demande dûment motivée est motivé.

Les politiques et procédures de divulgation de ces données sont rendues publiques.

Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine ne peuvent pas informer le titulaire d'un nom de domaine lorsqu'une demande visée à l'alinéa 1er a été formulée.

§ 5. L'Institut peut donner des instructions contraignantes à un registre de noms de domaine de premier niveau ou à une entité fournissant des services d'enregistrement de noms de domaine, en vue du respect du présent article.

§ 6. Si un registre de noms de domaine de premier niveau ou une entité fournissant des services d'enregistrement de noms de domaine ne respecte pas le présent article, un arrêté royal adopté en vertu du présent article ou une instruction contraignante émise par l'Institut, l'Institut peut imposer les mesures ou amendes administratives visées au chapitre 2 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.”.

Afdeling 6. — Wijzigingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU

Art. 95. In artikel 71 van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU, gewijzigd bij de wet van 7 april 2019, worden de woorden "en van titel 2 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. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtsopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen" opgeheven.

Art. 96. Artikel 79, § 4, van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt opgeheven.

HOOFDSTUK 3. — *Opheffingsbepaling*

Art. 97. 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 wordt opgeheven.

HOOFDSTUK 4. — *Inwerkingtreding*

Art. 98. Deze wet treedt in werking op 18 oktober 2024.

Kondigen deze wet af, bevelen dat zij met 's Lands Zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 26 april 2024.

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister Binnenlandse Zaken,
A. VERLINDEN

Met 's Lands zegel gezegeld:

De Minister van Justitie,

P. VAN TIGCHELT

Nota

(1) Kamer van volksvertegenwoordigers (www.dekamer.be) :
Stukken : 55 3862
Integraal verslag : 18 april 2024.

Section 6. — Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE

Art. 95. Dans l'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la directive 2014/65/UE, modifié par la loi du 7 avril 2019, les mots "et du titre 2 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. Pour l'exécution des missions précitées concernant la loi du 7 avril 2019, la FSMA peut néanmoins charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire" sont abrogés.

Art. 96. L'article 79, § 4, de la même loi, inséré par la loi du 7 avril 2019, est abrogé.

CHAPITRE 3. — *Disposition abrogatoire*

Art. 97. 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 est abrogée.

CHAPITRE 4. — *Entrée en vigueur*

Art. 98. La présente loi entre en vigueur le 18 octobre 2024.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du Sceau de l'Etat et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 26 avril 2024.

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

La Ministre de l'Intérieur,
A. VERLINDEN

Scellé du sceau de l'Etat :

Le Ministre de la Justice,

P. VAN TIGCHELT

Note

(1) Chambres des représentants (www.lachambre.be) :
Documents : 55 3862
Compte rendu intégral : 18 avril 2024.

Bijlage I bij de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	- Elektriciteitsbedrijven zoals gedefinieerd in artikel 2, punt 57, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU, die de functie verrichten van "levering" zoals gedefinieerd in artikel 2, punt 12, van die richtlijn
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 29, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Producenten zoals gedefinieerd in artikel 2, punt 38, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
		- Benoemde elektriciteitsmarktbeheerders zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad
		- Marktdeelnemers zoals gedefinieerd in artikel 2, punt 25, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit, die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken zoals gedefinieerd in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944 van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Exploitanten van een laadpunt die verantwoordelijk zijn voor het beheer en de exploitatie van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten
	b) Stadsverwarming en -koeling	- Exploitanten van stadsverwarming of stadskoeling zoals gedefinieerd in artikel 2, punt 19, van Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen
	c) Aardolie	- Exploitanten van oliepijpleidingen
		- Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
		- Centrale entiteiten voor de voorraadvorming zoals gedefinieerd in artikel 2, punt *f)*, van Richtlijn 2009/119/EG van de Raad van 14 september 2009 houdende verplichting voor de lidstaten om minimumvoorraden ruwe aardolie en/of aardolieproducten in opslag te houden
	d) Aardgas	- Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	e) Waterstof	- Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof
2. Vervoer	a) Lucht	- Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002, die voor commerciële doeleinden worden gebruikt

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
		- Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden
		- Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim aanbieden
	b) Spoor	- Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte
		- Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU van 21 november 2012 tot instelling van één Europese spoorwegruimte, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die richtlijn
	c) Water	- Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten als bedrijven in maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen
		- Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens, inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten; alsook entiteiten die werken en uitrusting in havens beheren
		- Exploitanten van verkeersbegeleidingssystemen (VBS) zoals gedefinieerd in artikel 3, punt *o)*, van Richtlijn 2002/59/EG van het Europees Parlement en de Raad van 27 juni 2002 betreffende de invoering van een communautair monitoring en informatiesysteem voor de zeescheepvaart en tot intrekking van Richtlijn 93/75/EEG van de Raad
	d) Weg	- Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is
		- Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
3. Bankwezen		- Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012
4. Infrastructuur voor de financiële markt		- Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU
		- Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters
5. Gezondheidszorg		- Zorgaanbieders zoals gedefinieerd in artikel 3, punt *g),* van Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg
		- EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad van 23 november 2022 inzake ernstige grensoverschrijdende gezondheidsbedreigingen en tot intrekking van Besluit nr. 1082/2013/EU inzake ernstige grensoverschrijdende bedreigingen van de gezondheid
		- Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik
		- Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in bijlage I, sectie C, afdeling 21, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden vervaardigen
		- Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (”de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen”) in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad van 25 januari 2022 betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen
6. Drinkwater		- Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in artikel 2, punt 1, *a),* van Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water, met uitzondering van distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten
7. Afvalwater		- Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater zoals gedefinieerd in artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG van de Raad van 21 mei 1991 inzake de behandeling van stedelijk afvalwater opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater een niet-essentieel onderdeel van hun algemene activiteit is

Bijlage I - Zeer kritieke sectoren		
Sector	Deelsector	Soort entiteit
8. Digitale infrastructuur		- Aanbieders van internetknooppunten
		- DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		- Registers voor topleveldomeinnamen
		- Aanbieders van cloudcomputingdiensten
		- Aanbieders van datacentrumdiensten
		- Aanbieders van netwerken voor de levering van inhoud
		- Verleners van vertrouwensdiensten
		- Aanbieders van openbare elektronische-communicatienetwerken
		- Aanbieders van openbare elektronische-communicatiediensten
9. Beheer van ICT-diensten (business-to-business)		- Aanbieders van beheerde diensten
		- Aanbieders van beheerde beveiligingsdiensten
10. Overheid		- Overheidsinstanties die van de Federale Staat afhangen
		- Overheidsinstanties die van de deelgebieden afhangen, geïdentificeerd overeenkomstig artikel 11, § 2, van de wet
		- De hulpverleningszones in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp opgericht door de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp
11. Ruimtevaart		- Exploitanten van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronischecommunicatienetwerken

Gezien om te worden gevoegd bij de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister van Binnenlandse Zaken,
A. VERLINDEN

Bijlage II bij de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Bijlage II - Andere kritieke sectoren		
Sector	Deelsector	Soort entiteit
1. Post- en koeriersdiensten		- Aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1*bis*, van Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst, met inbegrip van aanbieders van koeriersdiensten
2. Afvalstoffenbeheer		- Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren zoals gedefinieerd in artikel 3, punt 9, van Richtlijn 2008/98/EG van het Europees Parlement en de Raad van 19 november 2008 betreffende afvalstoffen en tot intrekking van een aantal richtlijnen, met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is

Bijlage II - Andere kritieke sectoren		
Sector	Deelsector	Soort entiteit
3. Vervaardiging, productie en distributie van chemische stoffen		- Ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren als bedoeld in artikel 3, punten 9 en 14, van Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad van 18 december 2006 inzake de registratie en beoordeling van en de autorisatie en beperkingen ten aanzien van chemische stoffen (REACH), tot oprichting van een Europees Agentschap voor chemische stoffen, houdende wijziging van Richtlijn 1999/45/EG en houdende intrekking van Verordening (EEG) nr. 793/93 van de Raad en Verordening (EG) nr. 1488/94 van de Commissie alsmede Richtlijn 76/769/EEG van de Raad en de Richtlijnen 91/155/EEG, 93/67/EEG, 93/105/EG en 2000/21/EG van de Commissie en ondernemingen die voorwerpen zoals gedefinieerd in artikel 3, punt 3, van die verordening produceren uit stoffen of mengsels
4. Productie, verwerking en distributie van levensmiddelen		- Levensmiddelenbedrijven zoals gedefinieerd in artikel 3, punt 2, Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad van 28 januari 2002 tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden die zich bezighouden met groothandel en industriële productie en verwerking
5. Vervaardiging	a) Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	- Entiteiten die medische hulpmiddelen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn
	b) Vervaardiging van informaticaproducten en van elektronische en optische producten	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 26, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	c) Vervaardiging van elektrische apparatuur	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 27, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 28, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
	e) Vervaardiging van motorvoertuigen, aanhangers en opleggers	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 29, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden

Bijlage II - Andere kritieke sectoren		
Sector	Deelsector	Soort entiteit
	f) Vervaardiging van andere transportmiddelen	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 30, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden
6. Digitale aanbieders		- Aanbieders van onlinemarktplaatsen
		- Aanbieders van onlinezoekmachines
		- Aanbieders van platforms voor socialenetwerkdiensten
7. Onderzoek		- Onderzoeksorganisaties

Gezien om te worden gevoegd bij de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister van Binnenlandse Zaken,
A. VERLINDEN

Annexe I à la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Annexe I - Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	- Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE, qui remplissent la fonction de "fourniture" au sens de l'article 2, point 12), de ladite directive
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE
		- Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité
		- Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE

Annexe I - Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
		- Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseau de chaleur et de froid	- Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables
	c) Pétrole	- Exploitants d'oléoducs
		- Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		- Entités centrales de stockage au sens de l'article 2, point *f)*, de la directive 2009/119/CE du Conseil du 14 septembre 2009 faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers
	d) Gaz	- Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE
		- Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	- Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	- Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, utilisés à des fins commerciales
		- Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n ° 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports
		- Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen

Annexe I - Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
	b) Transports ferroviaires	- Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen
		- Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	- Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, à l'exclusion des navires exploités à titre individuel par ces sociétés
		- Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports
		- Exploitants de services de trafic maritime (STM) au sens de l'article 3, point *o)*, de la directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil
	d) Transports routiers	- Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		- Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport
3. Secteur bancaire		- Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012
4. Infrastructures des marchés financiers		- Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE
		- Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Santé		- Prestataires de soins de santé au sens de l'article 3, point *g)*, de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers
		- Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision n° 1082/2013/UE

Annexe I - Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
		- Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain
		- Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de l'annexe I, section C, division 21 du Règlement (CE) no 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) no 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
		- Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux
6. Eau potable		- Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) *a)*, de la directive (UE) 2020/2184 du Parlement européen et du Conseil du 16 décembre 2020 relative à la qualité des eaux destinées à la consommation humaine, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		- Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil, du 21 mai 1991, relative au traitement des eaux urbaines résiduaires, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		- Fournisseurs de points d'échange internet
		- Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		- Registres de noms de domaine de premier niveau
		- Fournisseurs de services d'informatique en nuage
		- Fournisseurs de services de centres de données
		- Fournisseurs de réseaux de diffusion de contenu
		- Prestataires de services de confiance
		- Fournisseurs de réseaux de communications électroniques publics
		- Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (inter-entreprises)		- Fournisseurs de services gérés
		- Fournisseurs de services de sécurité gérés
10. Administration publique		- Entités de l'administration publique qui dépendent de l'Etat fédéral
		- Entités de l'administration publique qui dépendent des entités fédérées, identifiés conformément à l'article 11, § 2 de la loi

Annexe I - Secteurs hautement critiques		
Secteur	Sous-secteur	Type d'entité
		- Les zones de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale créé par l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale
11. Espace		- Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

Vu pour être annexé à la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

La Ministre de l'Intérieur,
A. VERLINDEN

Annexe II à la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Annexe II - Autres secteurs critiques		
Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		- Prestataires de services postaux au sens de l'article 2, point 1 *bis*), de la directive 97/67/CE du Parlement Européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service, y compris les prestataires de services d'expédition
2. Gestion des déchets		- Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil du 19 novembre 2008 relative aux déchets et abrogeant certaines directives, à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		- Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) n° 1907/2006 du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH), instituant une agence européenne des produits chimiques, modifiant la directive 1999/45/CE et abrogeant le règlement (CEE) n° 793/93 du Conseil et le règlement (CE) n° 1488/94 de la Commission ainsi que la directive 76/769/CEE du Conseil et les directives 91/155/CEE, 93/67/CEE, 93/105/CE et 2000/21/CE de la Commission et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		- Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) n° 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles

Annexe II - Autres secteurs critiques		
Secteur	Sous-secteur	Type d'entité
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	- Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive
	b) Fabrication de produits informatiques, électroniques et optiques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 26 du Règlement (CE) nº 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) nº 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	c) Fabrication d'équipements électriques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 27 du Règlement (CE) nº 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) nº 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	d) Fabrication de machines et équipements n.c.a.	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 28 du Règlement (CE) nº 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) nº 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	e) Construction de véhicules automobiles, remorques et semi-remorques	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 29 du Règlement (CE) nº 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) nº 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
	f) Fabrication d'autres matériels de transport	- Entreprises exerçant l'une des activités économiques visées à l'annexe I, section C, division 30 du Règlement (CE) nº 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) nº 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques
6. Fournisseurs numériques		- Fournisseurs de places de marché en ligne
		- Fournisseurs de moteurs de recherche en ligne
		- Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		- Organismes de recherche

Vu pour être annexé à la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

La Ministre de l'Intérieur,
A. VERLINDEN