

Avant-projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.	Voorontwerp van wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
Titre 1^{er}. - Définitions et dispositions générales	Titel 1. - Definities en algemene bepalingen
Chapitre 1^{er}. Objet et champ d'application	Hoofdstuk 1. Onderwerp en toepassingsgebied
Section 1^{re}. Objet	Afdeling 1. Onderwerp
Article 1^{er}. La présente loi règle une matière visée à l'article 74 de la Constitution.	Artikel 1. Deze wet regelt een materie als bedoeld in artikel 74 van de Grondwet.
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 ».	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.
Section 2. Champ d'application	Afdeling 2. Toepassingsgebied
Art. 3. § 1^{er}. 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 :	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° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou	1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of
2° une entreprise qui dépasse les plafonds prévus au § 1 ^{er} du même article de cette annexe.	2° een onderneming die de plafonds overschrijdt zoals vastgesteld in lid 1 van hetzelfde artikel van deze bijlage.
L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.	Artikel 3, § 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.
§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit	§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van

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.	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.
Sur base de l'alinéa 1 ^{er} , 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 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.	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 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.
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.	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. 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 :	§ 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° les services sont fournis par :	1° de diensten worden verleend door:
a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;	b) aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten;
a) des prestataires de services de confiance;	b) verleners van vertrouwensdiensten;
b) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;	c) registers voor topleveldomeinnamen en domeinnaamsysteem-dienstverleners;
2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;	2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;
3° l'entité est une entité de l'administration	3° de entiteit is een overheidsinstantie:

publique :	
a) au niveau fédéral;	a) op federaal niveau;
b) au niveau fédéré, identifiée conformément à l'article 11, § 2.	b) op het niveau van de deelgebieden, die overeenkomstig artikel 11, § 2, geïdentificeerd is.
§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme [exploitant d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques / entité critique au sens de la loi CER] .	§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd als [exploitant van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren / kritieke entiteit als bedoeld in de CER-wet] .
§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.	§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.
§ 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.	§ 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^{er}. 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.	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. Par exception au paragraphe 1 ^{er} , la présente loi s'applique :	§ 2. In afwijking van paragraaf 1 is deze wet van toepassing op:
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;	1° aanbieders van openbare elektronische-communicatienetwerken of aanbieders van openbare elektronische-communicatiediensten, wanneer zij deze diensten in België verlenen;
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	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,

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.	onlinezoekmachines of platforms voor socialenetwerkdiensten, wanneer zij hun hoofdvesting in België hebben, overeenkomstig paragraaf 4 en 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.	§ 3. Indien een entiteit als 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. 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.	§ 4. Voor de toepassing van deze wet hebben de in paragraaf 2, 2°, bedoelde entiteiten hun hoofdvesting in België wanneer zij er hoofdzakelijk de beslissingen nemen rond maatregelen voor het beheer van cyberbeveiligingsrisico's.
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.	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 hoofdvesting in België te hebben wanneer zij er hun cyberbeveiligingsactiviteiten uitvoeren.
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.	Indien de plaats waar deze activiteiten plaatsvinden niet kan worden bepaald, worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvesting in België te hebben wanneer hun vestiging met het grootste aantal werknemers zich daar bevindt.
§ 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.	§ 5. Voor de toepassing van deze wet worden de in paragraaf 2, 2°, bedoelde entiteiten geacht hun hoofdvesting 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. 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.	§ 6. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in paragraaf 2, 2°, doet geen afbreuk aan juridische stappen die tegen de entiteit zelf kunnen worden ingesteld.
Art. 5. § 1 ^{er} . 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	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

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.	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. 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.	§ 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. 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.	§ 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 voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.
§ 4. La présente loi ne s'applique pas :	§ 4. Deze wet is niet van toepassing op:
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;	1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;
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;	2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;
3° au Ministère de la Défense visé à l'article 1 ^{er} de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités ;	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° aux services de police visés à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;	4° de politiediensten bedoeld in artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le Ministère public inclus;	5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;
6° le 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°;	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° aux réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;	7° netwerk- en informatiesystemen van diplomatieke en consulaire missies in landen buiten de Europese Unie;
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.	8° de inrichtingen van klasse I als bedoeld in 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.
Par dérogation à l'alinéa 1 ^{er} , 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.	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 de elektriciteit.
§ 5. Les dispositions du titre 3, du titre 4 et du titre 5 ne s'appliquent pas :	§ 5. De bepalingen van titel 3, 4 en 5 zijn niet van toepassing op:
1° à la Direction générale Centre de Crise du Service public fédéral Intérieur, [créée par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise /la loi NCCN];	1° de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht [bij het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering /bij de NCCN-wet];
2° à l'Autorité nationale de cybersécurité visé à l'article 16.	2° de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16.
§ 6. Les paragraphes 4 et 5 ne s'applique pas lorsqu'une de ces entités agit en tant que prestataire de services de confiance.	§ 6. De paragrafen 4 en 5 zijn niet van toepassing wanneer een van deze instanties optreedt als aanbieder van vertrouwensdiensten.
Art. 6. § 1^{er}. 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	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

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.	incidenten melden en indien deze eisen ten minste gelijkwaardig zijn aan de in deze wet vastgestelde verplichtingen, zijn de relevante bepalingen van deze wet niet van toepassing op deze entiteiten.
Lorsqu'un instrument juridique sectoriel de l'Union européenne visé à l'alinéa 1 ^{er} 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.	Indien een in het eerste lid bedoeld sectorspecifiek rechtsinstrument van de Europese Unie niet op alle entiteiten in een specifieke sector betrekking heeft die tot het toepassingsgebied van deze wet behoren, zijn de relevante bepalingen van deze wet van toepassing op de entiteiten waarop dit sectorspecifieke rechtsinstrument van de Europese Unie geen betrekking heeft.
§ 2. Les exigences visées au paragraphe 1 ^{er} , alinéa 1 ^{er} , sont considérées comme ayant un effet équivalent aux obligations de la présente loi lorsque :	§ 2. De in paragraaf 1, eerste lid, bedoelde eisen worden geacht gelijkwaardig te zijn aan de verplichtingen van deze wet wanneer:
1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 30; ou	1° de maatregelen voor het beheer van cyberbeveiligingsrisico's ten minste gelijkwaardig zijn aan de maatregelen bedoeld in artikel 30; of
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 importants sont au moins équivalentes aux obligations prévues aux articles 34 à 37.	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. Les dispositions du titre 3, du titre 4 et du titre 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.	§ 3. De bepalingen van titel 3, 4 en 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 effectenbewaarinstantie verricht door de Nationale Bank van België.
§ 4. Les dispositions du titre 3, chapitre 1 ^{er} , du titre 4 et du titre 5 ne s'appliquent pas :	§ 4. De bepalingen van titel 3, hoofdstuk 1, van titel 4 en van titel 5 zijn niet van toepassing:

1° à la Banque nationale de Belgique, exception faite de son activité de dépositaire central de titres à laquelle s'applique le paragraphe 3;	1° op de Nationale Bank van België, met uitzondering van haar activiteit van centrale effectenbewaarinstantie waarop paragraaf 3 van toepassing is;
2° aux établissements financiers soumis à la supervision de la Banque nationale de Belgique en vertu des articles 8 et 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique qui ne relèvent pas du paragraphe 3.	2° op financiële instellingen die onderworpen zijn aan het toezicht van de Nationale Bank van België krachtens artikel 8 en 12bis 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. Le Roi peut, par arrêté délibéré en Conseil des Ministres :	Art. 7. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad,:
1° préciser les instruments juridiques sectoriels équivalents visés à l'article 6, § 1 ^{er} , alinéa 1 ^{er} ;	1° de gelijkwaardige sectorspecifieke rechtsinstrumenten als bedoeld in artikel 6, § 1, eerste lid, nader bepalen;
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 importants, 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.	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.
Chapitre 2. Définitions	Hoofdstuk 2. Definities
Art. 8. Pour l'application de la présente loi, il faut entendre par :	Art. 8. Voor de toepassing van deze wet moet worden verstaan onder:
1° « réseau et système d'information » :	1° "netwerk- en informatiesysteem":
a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;	a) een elektronische-communicatienetwerk als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
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	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) 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;	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° « 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;	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° « 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) no 526/2013 (règlement sur la cybersécurité), ci-après le « règlement sur la cybersécurité »;	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° « 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;	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 » : 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;	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° « 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;	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° « 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;	7° “grootschalig cyberbeveiligingsincident”: een incident dat leidt tot een verstoringniveau 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° « 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;	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° « risque » : le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise;	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 het incident zich voordoet;
10° « cybermenace » : une cybermenace au sens de l'article 2, 8), du règlement sur la cybersécurité;	10° “cyberdreiging”: een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;
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;	11° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerken en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;
12° « produit TIC » : un produit TIC au sens de l'article 2, 12), du règlement sur la cybersécurité;	12° “ICT-product”: een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;
13° « service TIC » : un service TIC au sens de l'article 2, 13), du règlement sur la cybersécurité;	13° “ICT-dienst”: een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;
14° « processus TIC » : un processus TIC au sens de l'article 2, 14), du règlement sur la cybersécurité;	14° “ICT-proces”: een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;
15° « vulnérabilité » : une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;	15° “kwetsbaarheid”: een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;
16° « norme » : une norme au sens de l'article 2, 1), du règlement (UE) n°1025/2012 du Parlement	16° “norm”: een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het

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 »;	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° « 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;	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° « 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;	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° « fournisseur de services DNS » : une entité qui fournit :	19° “DNS-dienstverlener”: een entiteit die de volgende diensten verleent:
a) des services de résolution de noms de domaine récurrents accessibles au public destinés aux utilisateurs finaux de l’internet; ou	a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers; of
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;	b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers;
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	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

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;	topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamserver, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamserver, 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° « 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;	21° "entiteit die domeinnaamregistratiediensten aanbiedt": een registrar of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;
22° « service numérique » : un service au sens de l'article 1 ^{er} , § 1 ^{er} , 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;	22° "digitale dienst": een dienst als bedoeld in artikel 1, lid 1, 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° « 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 »;	23° "vertrouwensdienst": een vertrouwensdienst als bedoeld in 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° « prestataire de service de confiance » : un prestataire de services de confiance au sens de l'article 3, 19., du règlement eIDAS ;	24° "verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten als bedoeld in artikel 3, 19., van de eIDAS-verordening;
25° « service de confiance qualifié » : un service de confiance qualifié au sens de l'article 3, 17., du règlement eIDAS ;	25° "gekwaliceerde vertrouwensdienst": een gekwalificeerde vertrouwensdienst als bedoeld in artikel 3, 17., van de eIDAS-verordening;
26° « prestataire de services de confiance qualifiés » : un prestataire de services de confiance qualifié au sens de l'article 3, 20., du règlement eIDAS;	26° "gekwaliceerde verlener van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten als bedoeld in artikel 3, 20., van de eIDAS-verordening;
27° « place de marché en ligne » : une place de marché en ligne au sens de l'article I.8, 41°, du Code	27° "onlinemarktplaats": een onlinemarktplaats als bedoeld in artikel I.8, 41°, van het Wetboek

de droit économique;	van economisch recht;
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;	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° « 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;	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° « 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;	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 netwerkkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuur voor energiedistributie en omgevingscontrole;
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;	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° « 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;	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° « 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	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,

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;	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° « entité de l'administration publique » : une autorité administrative visée à l'article 14, § 1 ^{er} , alinéa 1 ^{er} , des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants :	34° "overheidsinstantie": een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:
1° elle n'a pas de caractère industriel ou commercial;	1° zij is niet van industriële of commerciële aard;
2° 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	2° zij oefent niet hoofdzakelijk een activiteit opgesomd in de kolom soort entiteit van een van de andere sector of deelsector van een van de bijlagen;
3° elle n'exerce pas à titre principal ses activités dans le domaine de la sécurité nationale, de la défense ou de la sécurité publique;	3° zij oefent niet hoofdzakelijk activiteiten uit op het gebied van nationale veiligheid, defensie of openbare veiligheid;
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;	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° « 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;	36° "elektronische-communicatiedienst": een elektronische-communicatiedienst als bedoeld in artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
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;	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° « 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;	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° « 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;	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;
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;	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° « recommandation n° 2003/361/CE » : la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;	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° « loi du 13 juin 2005 » : la loi du 13 juin 2005 relative aux communications électroniques;	42° “wet van 13 juni 2005”: de wet van 13 juni 2005 betreffende de elektronische communicatie;
[43° « loi CER » : la loi [CER]; 43° « loi du 1 ^{er} juillet 2011 » : la loi du 1 ^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques;]	[43° “CER-wet”: de wet [CER]; 43° “wet van 1 juli 2011”: de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur;]
[44° « loi NPU » : la loi [NPU];]	[44° “NPU-wet”: de wet [NPU];]
[45° « loi NCCN » : la loi [NCCN]; 45° « arrêté royal NCCN » : l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise]	[45° “NCCN-wet”: de wet [NCCN]; 45° “NCCN-koninklijk besluit”: het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering]
46° « autorité nationale de cybersécurité » : l’autorité visée à l’article 16;	46° “nationale cyberbeveiligingsautoriteit”: de autoriteit bedoeld in artikel 16;
47° « CSIRT national » : le centre national de réponse aux incidents de sécurité informatique;	47° “nationaal CSIRT”: het nationale computer security incident response team;
48° « ENISA » : l’Agence de l’Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;	48° “Enisa”: het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;
49° « NCCN » : le Centre de crise national organisé par [la loi NCCN/l’arrêté royal NCCN];	49° “NCCN”: het Nationaal Crisiscentrum georganiseerd door [de NCCN-wet/het NCCN-koninklijk besluit];
50° « 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	50° “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

caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);	met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
51° « Autorité de protection des données » : autorité de contrôle au sens de l'article 4, 21°, du règlement (UE) 2016/679;	51° “Gegevensbeschermingsautoriteit”: toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;
52° « 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° “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”;
53° la 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° beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”): het beleid vastgelegd in een document als bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen die een essentiële of belangrijke entiteit heeft genomen;
54° « organisme d'évaluation de la conformité » : l'organisme visé à l'article 2, point 13, du règlement (CE) n° 765/2008;	54° “conformiteitsbeoordelingsinstantie”: de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;
55° « autorité sectorielle » : l'autorité visée à l'article 15, § 2;	55° “sectorale overheid”: de overheid bedoeld in artikel 15, § 2;
56° « réseau des CSIRT » : le réseau des CSIRT nationaux institué par l'article 15 de la directive NIS2;	56° “CSIRT-netwerk”: het netwerk van nationale CSIRT's opgericht bij artikel 15 van de NIS2-richtlijn;
57° « groupe de coopération » : le groupe de coopération institué par l'article 14 de la directive NIS2;	57° “samenwerkingsgroep”: de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;
58° « 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 :	58° “significant incident”: elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van bijlage I en II van de wet en dat:
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	1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van bijlage I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of

2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.	2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.
59° « crise cyber » : tout incident de cybersécurité qui, par sa nature ou ses conséquences :	59° “cybercrisis”: elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:
1° menace les intérêts vitaux du pays ou les besoins essentiels de la population;	1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;
2° requiert des décisions urgentes;	2° een dringende besluitvorming vereist;
3° demande une action coordonnée de plusieurs départements et organisations;	3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt;
60° « 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.	60° “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.
Chapitre 3. Catégories d'entités	Hoofdstuk 3. Categorieën van entiteiten
Art. 9. Sont des entités essentielles :	Art. 9. Zijn essentiële entiteiten:
1° les entités d'un type visé à l'annexe I qui excèdent les plafonds applicables aux moyennes entreprises prévus à l'article 2, § 1 ^{er} , de l'annexe de la recommandation n° 2003/361/CE;	1° de entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden die zijn vastgesteld in artikel 2, lid 1, van de bijlage bij Aanbeveling nr. 2003/361/EG;
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;	2° de gekwalificeerde verleners van vertrouwensdiensten en de registers voor topleveldomeinnamen, alsook de DNS-dienstverleners, ongeacht hun omvang;
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;	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° les entités de l'administration publique qui relèvent de l'État fédéral;	4° de overheidsinstanties die tot de Federale Staat behoren;
5° les entités visées à l'article 3, § 4;	5° de entiteiten bedoeld in artikel 3, § 4;
6° toute autre entité d'un type visé à l'annexe I ou II	6° alle andere entiteiten van een in bijlage I of II

qui est identifiée comme entité essentielle conformément à l'article 11.	bedoelde soort die worden geïdentificeerd als essentiële entiteiten overeenkomstig artikel 11.
Art. 10. Sont des entités importantes :	Art. 10. Zijn belangrijke entiteiten:
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;	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° les entités identifiées comme entités importantes conformément à l'article 11.	2° de entiteiten die worden geïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.
Chapitre 4. Identification	Hoofdstuk 4. Identificatie
Art. 11. § 1 ^{er} . 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 :	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° 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;	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 bijlage I en II van de wet;
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;	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° 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;	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° 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.	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. En ce qui concerne les 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.	§ 2. Wat de deelgebieden betreft, 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. Dans le cadre de l'identification visée au paragraphe 1 ^{er} 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.	§ 3. In het kader van de identificatie bedoeld in paragraaf 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.
Lorsqu'aucun avis n'est rendu dans le délai visé à l'alinéa 1 ^{er} , l'avis est réputé être favorable.	Indien binnen de in het eerste lid bedoelde termijn geen advies is uitgebracht, wordt het advies geacht gunstig te zijn.
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.	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.
§ 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 1 ^{er} à 3.	§ 3. De nationale cyberbeveiligingsautoriteit évalueert en actualiseert, in voorkomend geval, minstens om de twee jaar de identificatie van essentiële en belangrijke entiteiten volgens de modaliteiten bedoeld in paragraaf 1 tot 3.
L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités essentielles au NCCN et à l'éventuelle autorité sectorielle concernée.	De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van essentiële entiteiten naar het NCCN en naar de eventuele betrokken sectorale overheid.
L'autorité nationale de cybersécurité adresse les identifications et actualisations des entités importantes à l'éventuelle autorité sectorielle concernée.	De nationale cyberbeveiligingsautoriteit stuurt de identificaties en actualiseringen van belangrijke entiteiten naar de eventuele betrokken sectorale autoriteit.
§ 5. Dans les cas visés au paragraphe 1 ^{er} , 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.	§ 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.
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	Art. 12. In het kader van de identificatie bedoeld in artikel 11 bezorgt de betrokken entiteit op verzoek van de nationale

la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle.	cyberbeveiligingsautoriteit of de sectorale overheid alle informatie die nuttig is voor haar eventuele identificatie.
Chapitre 5. Enregistrement des entités	Hoofdstuk 5. Registratie van de entiteiten
Art. 13. §1 ^{er} . 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 :	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° leur dénomination ainsi que leur numéro d'enregistrement auprès de la Banque-carrefour des entreprises (BCE) ou un enregistrement équivalent dans l'Union européenne;	1° hun naam, alsook hun registratienummer bij de Kruispuntbank van Ondernemingen (KBO) of een gelijkwaardige registratie in de Europese Unie;
2° leur adresse et leurs coordonnées actualisées, y compris leur adresse de courrier électronique, leurs plages d'IP et leur numéro de téléphone;	2° hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereiken en hun telefoonnummer;
3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et	3° indien van toepassing, de relevante sector en deelsector als bedoeld in bijlage I of II, en
4° le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente loi.	4° indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen.
Le Roi peut compléter cette liste d'informations.	De Koning kan deze lijst met informatie aanvullen.
§ 2. Par dérogation au paragraphe 1 ^{er} , alinéa 1 ^{er} , 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 auprès de cette autorité sectorielle ces informations.	§ 2. In afwijking van paragraaf 1, eerste lid, vervoldigt 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.
L'entité visée au paragraphe 1 ^{er} , alinéa 1 ^{er} , communique les informations dans les cinq mois suivant l'entrée en vigueur de la loi, selon les modalités pratiques fixées par l'autorité précitée.	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. Les entités visées au paragraphe 1 ^{er} , alinéa 1 ^{er} , communiquent sans tarder toute modification des	§ 3. De in paragraaf 1, eerste lid, bedoelde entiteiten bezorgen onmiddellijk elke wijziging in

informations qu'elles ont communiquées conformément au paragraphe 1 ^{er} , alinéa 1 ^{er} , et paragraphe 2, alinéa 1 ^{er} , et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.	de bijzonderheden 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. L'autorité sectorielle concernée communique les informations collectées en vertu des paragraphes 2 et 3 à l'autorité nationale de cybersécurité.	§ 4. De betrokken sectorale overheid bezorgt de krachtens paragraaf 2 en 3 verzamelde informatie aan de nationale cyberbeveiligingsautoriteit.
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.	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 ^{er} . 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, § 1 ^{er} , alinéa 1 ^{er} , au moins les informations suivantes :	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 datacentra, 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° leur nom;	1° hun naam;
2° leur secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant;	2° hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;
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;	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° 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;	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° les États membres dans lesquels ils fournissent leurs services relevant du champ d'application de la présente loi ; et	5° de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren; en
6° leurs plages d'IP.	6° hun IP-bereiken.
§ 2. Les entités visées au paragraphe 1 ^{er} notifient à l'autorité nationale de cybersécurité toute modification des informations qu'elles ont communiquées en vertu du paragraphe 1 ^{er} sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.	§ 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. Par dérogation au paragraphe 1 ^{er} , 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 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.	§ 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 van de eIDAS-verordening bedoelde toezichthoudende orgaan, door dat orgaan doorgestuurd naar de nationale cyberbeveiligingsautoriteit, volgens de door de Koning vastgestelde modaliteiten.
Titre 2. Autorités compétentes et coopération au niveau national	Titel 2. Bevoegde autoriteiten en samenwerking op nationaal niveau
Chapitre 1^{er}. Autorités compétentes	Hoofdstuk 1. Bevoegde autoriteiten
Section 1^{re}. Désignation des autorités compétentes	Afdeling 1. Aanwijzing van de bevoegde autoriteiten
Art. 15. § 1^{er}. Le Roi désigne l'autorité nationale de cybersécurité.	Art. 15. § 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.
§ 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.	§ 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 als bedoeld in artikel 33.
Dans le cadre de la désignation visée à l'alinéa 1 ^{er} , le Roi tient compte de l'identité des autorités sectorielles désignées dans le cadre de la loi [CER/du 1 ^{er} juillet 2011].	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 CER-wet/wet van 1 juli 2011 aangewezen sectorale overheden].

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.	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.
Par dérogation à l'alinéa 1 ^{er} , la loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régies par la loi.	In afwijking van het eerste lid wijst de wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.
Section 2. L'autorité nationale de cybersécurité	Afdeling 2. De nationale cyberbeveiligingsautoriteit
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 et incidents de cybersécurité conformément à l'article 18.	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 cyberbeveiligingscrises en -incidenten overeenkomstig artikel 18.
A 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.	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.
Sous-section 1^{re}. Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité	Onderafdeling 1. Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging
Art. 17. Les tâches de l'autorité nationale de cybersécurité sont les suivantes :	Art. 17. De nationale cyberbeveiligingsautoriteit heeft de volgende taken:
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;	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° superviser, coordonner et veiller à la mise en œuvre de la stratégie nationale en matière de cybersécurité visée à l'article 28;	2° het opvolgen en coördineren van en toezien op de uitvoering van de nationale cyberbeveiligingsstrategie bedoeld in artikel 28;

3° identifier des entités essentielles et importantes conformément à l'article 11;	3° het identificeren van de essentiële en belangrijke entiteiten overeenkomstig artikel 11;
4° superviser la mise en œuvre de la loi par les entités essentielles et importantes conformément au titre 4;	4° het toezien op de uitvoering van de wet door de essentiële en belangrijke entiteiten overeenkomstig titel 4;
5° assurer la coordination entre les autorités publiques et le secteur privé ou le monde scientifique;	5° het zorgen voor coördinatie tussen de overheden en de particuliere sector of de wetenschappelijke wereld;
6° formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;	6° het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader op het vlak van cyberbeveiliging;
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;	7° het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor de cyberbeveiliging van de verschillende soorten informatiesystemen;
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;	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° 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 et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes belges;	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 Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde Belgische autoriteiten;
10° coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;	10° het coördineren van de evaluatie en certificering van de beveiliging van informatie- en communicatiesystemen;
11° informer et sensibiliser les utilisateurs des systèmes d'information et de communication;	11° het informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen;
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;	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° faciliter et encourager l'organisation de formations en matière de cybersécurité pour les membres du personnel des entités essentielles ou importantes;	13° het faciliteren en aanmoedigen van de organisatie van opleidingen rond cyberbeveiliging voor personeelsleden van essentiële of belangrijke entiteiten;
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.	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.
Sous-section 2. Tâches relatives au rôle de gestion des crises cyber	Onderafdeling 2. Taken met betrekking tot het cybercrisisbeheer
Art. 18. Sans préjudice des dispositions [de la loi NPU], de [la loi NCCN/l'arrêté royal NCCN] et de leurs arrêtés d'exécution les tâches de l'autorité nationale de cybersécurité relatives au rôle de gestion des crises cyber sont les suivantes :	Art. 18. Onverminderd de bepalingen van [de NPU-wet], [de NCCN-wet/het NCCN-koninklijk besluit] en de uitvoeringsbesluiten ervan vervult de nationale cyberbeveiligingsautoriteit de volgende taken met betrekking tot het cybercrisisbeheer:
1° en collaboration avec le NCCN, recenser les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise cyber;	1° in samenwerking met het NCCN, het vaststellen van de capaciteiten, middelen en procedures die in geval van een cybercrisis kunnen worden ingezet;
2° [par dérogation à l'article 24, 1°, de la loi NCCN], superviser, en collaboration avec le NCCN, la rédaction, l'actualisation et l'opérationnalisation du plan national de réaction aux crises et incidents de cybersécurité majeurs visé à l'article 29;	2° [in afwijking van artikel 24, 1°, van de NCCN-wet], het opvolgen van de opmaak, actualisering en operationalisering van het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons bedoeld in artikel 29, in samenwerking met het NCCN;
3° assurer le rôle de coordinateur dans la gestion des crises et incidents de cybersécurité, le cas échéant conformément au plan visé au 2°, pour autant que ces crises et incidents ne constituent pas des crises nationales [au sens de la loi NPU].	3° het vervullen van de rol van coördinator bij het beheer van cyberbeveiligingscrises en -incidenten, in voorkomend geval overeenkomstig het in 2° bedoelde plan, voor zover deze crises en incidenten geen nationale crises zijn [als bedoeld in de NPU-wet].
Sous-section 3. Tâches et obligations relatives au rôle de CSIRT national	Onderafdeling 3. Taken en voorschriften met betrekking tot de rol van nationaal CSIRT
Art. 19. § 1^{er}. Les tâches du CSIRT national, sont les suivantes :	Art. 19. § 1. Het nationale CSIRT heeft de volgende taken:
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	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

surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information;	belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen;
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;	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° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant;	3° het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;
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;	4° het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;
5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif du réseau et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;	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° 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;	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° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 22;	7° indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 22 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;
8° contribuer au déploiement d'outils sécurisés de partage d'informations;	8° het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie;
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	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

des entités;	heeft voor de werking van de diensten van de entiteiten;
10° détecter, observer et analyser des problèmes de sécurité informatique;	10° het opsporen, observeren en analyseren van computerbeveiligingsproblemen;
11° établir des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente loi;	11° het tot stand brengen van samenwerkingsrelaties met relevante belanghebbenden in de particuliere sector, teneinde de doelstellingen van deze wet te verwezenlijken;
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:	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) les procédures de gestion des incidents;	a) procedures voor de incidentenbehandeling;
b) la gestion de crise; et	b) crisisbeheer; en
c) la divulgation coordonnée des vulnérabilités en vertu de l'article 22;	c) de gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 22;
13° coopérer et, le cas échéant, échanger des informations pertinentes conformément à l'article 27 avec les communautés visées au même article;	13° het samenwerken en in voorkomend geval uitwisselen van relevante informatie overeenkomstig artikel 27 met de in datzelfde artikel bedoelde gemeenschappen;
14° participer aux évaluations par les pairs organisées conformément à l'article 19 de la directive NIS2.	14° het deelnemen aan de overeenkomstig artikel 19 van de NIS2-richtlijn georganiseerde collegiale toetsingen.
Après avis du CSIRT national, le Roi peut, par arrêté délibéré en Conseil des Ministres, lui confier des tâches supplémentaires.	Na advies van het nationale CSIRT kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, dit CSIRT bijkomende taken toevertrouwen.
§ 2. Lorsqu'il exécute les tâches visées au paragraphe 1 ^{er} , le CSIRT national peut donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.	§ 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. Les obligations du CSIRT national sont les suivantes :	Art. 20. De voorschriften voor het nationale CSIRT omvatten het volgende:
1° disposer d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente lui permettant d'échanger des informations avec les	1° beschikken over een passende, veilige en weerbare communicatie- en informatie-infrastructuur waardoor informatie kan worden

entités essentielles et importantes et les autres parties prenantes;	uitgewisseld met essentiële en belangrijke entiteiten en andere relevante belanghebbenden;
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;	2° een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met het nationale CSIRT kan worden opgenomen en contact met anderen kan worden opgenomen; de communicatiekanalen duidelijk specificeren en meedelen aan de gebruikersgroep en de samenwerkingspartners;
3° disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés;	3° beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden;
4° être doté d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;	4° uitgerust zijn met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op doeltreffende en efficiënte overdrachten;
5° garantir la confidentialité et la fiabilité de ses opérations;	5° de vertrouwelijkheid en betrouwbaarheid van zijn activiteiten waarborgen;
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;	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° être doté de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de ses services.	7° uitgerust zijn met redundante systemen en reservewerkruimten om de continuïteit van zijn diensten te waarborgen.
Art. 21. § 1^{er}. 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.	Art. 21. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in artikel 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. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 19, § 1 ^{er} , 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. 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 elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni

2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.	2005 verkrijgen van een operator als bedoeld in artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.
Les finalités poursuivies par les tâches précitées sont :	De doeleinden van voornoemde taken zijn:
1° sans préjudice des compétences des personnes exerçant la police judiciaire [, notamment des procureurs du Roi, du procureur fédéral ou des procureurs généraux, ni des compétences des juges d'instruction], 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;	1° onverminderd de bevoegdheden van de personen die de gerechtelijke politie uitoefenen [, met name de procureurs des Konings, de federale procureur of de procureurs-generaal,] het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;
2° la prévention de menaces graves contre la sécurité publique;	2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;
3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information;	3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen.
Le CSIRT national peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci.	Het nationale CSIRT kan bepalen binnen welke termijn de operator op zijn verzoek moet reageren, naargelang de dringendheid hiervan.
§ 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.	§ 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. 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.	§ 4. Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegevens als bedoeld in 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.
En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 1 ^{er} et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 1 ^{er} pour permettre un contrôle ultérieur.	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.
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 1 ^{er} , le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.	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 verwijdt het de ontvangen metagegevens.
§ 5. Le directeur général du CSIRT national désigne expressément les personnes habilitées à traiter les données de communications électroniques visées au présent article.	§ 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. 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.	§ 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. Sans préjudice des articles 28quiquies, § 1 ^{er} , et 57, § 1 ^{er} , 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.	§ 7. Onverminderd de artikelen 28quiquies, § 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. 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.	§ 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.
Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.	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^{er}. Dans son rôle de coordinateur aux fins de la divulgation coordonnée des vulnérabilités, le	Art. 22. § 1. In zijn rol van coördinator met het oog op een gecoördineerde bekendmaking van

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.	kwetsbaarheden treedt het nationale CSIRT op als een betrouwbare tussenpersoon en vergemakkelijkt, 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.
Dans ce cadre, les tâches du CSIRT national consistent notamment à :	In dat kader omvatten de taken van het nationale CSIRT met name:
1° identifier et contacter les entités concernées;	1° het identificeren van en contact opnemen met de betrokken entiteiten;
2° apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et	2° het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden; en
3° négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.	3° het onderhandelen over tijdschema's voor de bekendmaking, en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.
§ 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.	§ 2. Iedere natuurlijke of rechtspersoon kan, zelfs desgevraagd anoniem, aan het nationale CSIRT het bestaan van een mogelijke kwetsbaarheid melden.
Le signalement est effectué par écrit, selon la procédure détaillée sur le site internet du CSIRT national.	De melding gebeurt schriftelijk, volgens de procedure die op de website van het nationale CSIRT beschreven is.
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.	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 particuliere 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. 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.	§ 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.

Le CSIRT national préserve l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement.	Het nationale CSIRT waarborgt de volledigheid, integriteit, duurzame opslag en geheimhouding van de informatie die via de melding wordt overgemaakt.
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.	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. Tout en respectant les conditions énumérées à l'article 21, § 1 ^{er} 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.	§ 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. 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.	§ 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. Le directeur général du CSIRT national veille, par l'adoption de procédures internes, au respect des conditions visées au présent article.	§ 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^{er}. Dans le cadre de la procédure visée à l'article 22, les auteurs de signalement ne commettent pas d'infraction aux articles 314bis, 458, 550bis, 550ter du Code pénal et de l'article 145 de la loi du 13 juin 2005 à condition:	Art. 23. § 1. In het kader van de procedure bedoeld in artikel 22 plegen melders geen inbreuk op de artikelen 314bis, 458, 550bis en 550ter van het Strafwetboek en op artikel 145 van de wet van 13 juni 2005, op voorwaarde dat:
1° qu'ils aient agi sans intention frauduleuse, ni dessein de nuire;	1° zij zonder bedrieglijk opzet of het oogmerk om te schaden hebben gehandeld;
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 24 heures de la découverte d'une potentielle vulnérabilité, à l'organisation responsable du système et au CSIRT national;	2° zij onverwijld en uiterlijk binnen 24 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° qu'ils aient adressé une notification complète, sans délai et au plus tard dans les 72 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 prévue à l'article 22, § 2;	3° zij onverwijld en uiterlijk binnen 72 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° 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;	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° qu'ils n'aient pas publiquement divulgué les informations relatives à la vulnérabilité découverte et aux systèmes vulnérables, sans l'accord du CSIRT national.	5° zij de informatie over de ontdekte kwetsbaarheid en de kwetsbare systemen niet openbaar hebben gemaakt zonder de toestemming van het nationale CSIRT.
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.	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 modaliteiten en de te hanteren methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden.
§ 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 professionnelle et n'encourent aucune responsabilité d'aucune sorte concernant la transmission d'informations nécessaires pour signaler une potentielle vulnérabilité au CSIRT national.	§ 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. 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 1 ^{er} continue d'être régie par le droit applicable.	§ 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.
Section 3. Les éventuelles autorités sectorielles	Afdeling 3. De eventuele sectorale overheden
Art. 24. Sans préjudice des autres dispositions, l'autorité sectorielle peut :	Art. 24. Onverminderd de andere bepalingen kan de sectorale overheid:

1° organiser des exercices sectoriels, les coordonner ou y participer, pour ce qui concerne les mesures visées aux articles 30 et 33;	1° sectorale oefeningen organiseren, coördineren of eraan deelnemen, voor wat betreft de maatregelen bedoeld in artikelen 30 en 33;
2° analyser et gérer les conséquences d'un incident pour le secteur;	2° de gevolgen van een incident voor de sector analyseren en beheren;
3° participer aux travaux du groupe de coopération pour ce qui concerne les sujets qui touchent à ses compétences;	3° deelnemen aan de werkzaamheden van de samenwerkingsgroep voor de onderwerpen die betrekking hebben op haar bevoegdheden;
4° sensibiliser les entités relevant de son secteur.	4° de entiteiten die onder haar sector vallen sensibiliseren.
Chapitre 2. Coopération au niveau national	Hoofdstuk 2. Samenwerking op nationaal niveau
Art. 25. § 1^{er}. Les autorités visées au chapitre 1 ^{er} du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.	Art. 25. § 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.
§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1 ^{er} 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) n° 300/2008 et n° 2018/1139], les organes de contrôle au titre 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, la Banque nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi CER, 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.	§ 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 CER-wet 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. Les entités essentielles et importantes et les autorités visées au chapitre 1 ^{er} du présent titre	§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel

collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.	werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.
§ 4. Les autorités visées au chapitre 1 ^{er} du présent titre et les autorités compétentes dans le cadre de la loi [CER/du 1 ^{er} juillet 2011] coopèrent et échangent régulièrement des informations sur le recensement des [entités/infrastructures] critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les entités recensées [en tant qu'entités critiques] en vertu de la loi [CER/du 1 ^{er} juillet 2011] et sur les mesures prises pour faire face à ces risques, menaces et incidents.	§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten werken samen en wisselen regelmatig informatie uit inzake het als kritiek aanmerken van [entiteiten/infrastructuren], over risico's, cyberdreigingen en incidenten, alsook over niet-cyber risico's, -dreigingen en -incidenten die gevolgen hebben voor entiteiten die uit hoofde van de [CER-wet/wet van 1 juli 2011] [als kritieke entiteiten] zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.
§ 5. Les autorités visées au chapitre 1 ^{er} du présent titre et les autorités compétentes en vertu 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, 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 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.	§ 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. 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.	§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform opdat 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.
Chapitre 3. Confidentialité et échanges d'information	Hoofdstuk 3. Vertrouwelijkheid en informatie-uitwisseling
Art. 26. § 1^{er}. Le présent article ne porte pas préjudice à l'application 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, de la loi du 15 avril	Art. 26. § 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde

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.	dienst, 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. 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.	§ 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.
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.	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.
Ces personnes obtiennent l'accord des autorités visées à l'article 5, § 4, lorsque ces autorités sont concernées par le secret.	Deze personen verkrijgen de akkoord van de autoriteiten bedoeld in artikel 5, § 4, wanneer deze autoriteiten bij het geheim betrokken zijn.
§ 3. Les autorités visées au chapitre 1 ^{er} 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.	§ 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. Les informations fournies aux autorités visées au chapitre 1 ^{er} 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.	§ 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.
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	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

la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.	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^{er}. A 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:	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° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;	1° beoogt incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;
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° 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 particuliere entiteiten te bevorderen.
§ 2. L'échange d'informations visé au paragraphe 1 ^{er} 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.	§ 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. 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	§ 3. De nationale cyberbeveiligingsautoriteit faciliteert de vaststelling van de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied

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 1 ^{er} .	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. 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.	§ 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.
Chapitre 4. Stratégie nationale en matière de cybersécurité	Hoofdstuk 4. Nationale cyberbeveiligingsstrategie
Art. 28. § 1^{er}. Les Ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les 5 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 contrôle des données à caractère personnel.	Art. 28. § 1. De in Raad vergaderde Ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de 5 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 toezichhoudende autoriteiten persoonsgegevens.
Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.	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. La stratégie nationale en matière de cybersécurité comprend, entre autres :	§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:
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;	1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;
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;	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° 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 1 ^{er} 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;	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° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;	4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;
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;	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 particuliere sector;
6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;	6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;
7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1 ^{er} du présent titre et les autorités compétentes en vertu de la loi [CER /du 1 ^{er} 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;	7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de [CER-wet/wet van 10 juli 2011] bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberbepaalde dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;
8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;	8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;
9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;	9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;
10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.	10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.
§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont	§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale

adoptées et portent sur les éléments suivants :	cyberbeveiligingsstrategie:
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;	1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;
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;	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° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;	3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 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;	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° 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;	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° 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;	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° 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;	7° voor het ondersteunen van academische en onderzoeksinstituten bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;
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	8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillige

cybersécurité entre les entités;	delen van cyberbeveiligingsinformatie tussen entiteiten;
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;	9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiène 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° la promotion d'une cyberprotection active.	10° voor het bevorderen van actieve cyberbescherming.
Chapitre 5. Le plan national de réaction aux crises et incidents de cybersécurité majeurs	Hoofdstuk 5. Het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons
Art. 29. § 1^{er}. Le Roi établit, par arrêté délibéré en Conseil des ministres, un plan national de réaction aux crises et incidents de cybersécurité. Ce plan constitue un plan national [au sens de l'article 21 de la loi NPU].	Art. 29. § 1. De Koning stelt, bij besluit vastgesteld na overleg in de Ministerraad, een nationaal plan voor cyberbeveiligingsincidenten en crisisrespons op. Dit plan is een nationaal plan [als bedoeld in artikel 21 van de NPU-wet].
§ 2. Sans préjudice des éléments devant être contenus dans les plans nationaux [conformément à la loi NPU], le plan national de réaction aux crises et incidents de cybersécurité contient au moins les éléments suivants :	§ 2. Onverminderd de elementen die moeten worden opgenomen in de nationale plannen [overeenkomstig de NPU-wet], bevat het nationale plan voor cyberbeveiligingsincidenten en crisisrespons ten minste:
1° les objectifs des mesures et activités nationales de préparation;	1° de doelstellingen van de nationale paraatheidsmaatregelen en -activiteiten;
2° les tâches et responsabilités des autorités de gestion des crises cyber;	2° de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;
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;	3° de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;
4° les mesures de préparation nationales, y compris des exercices et des activités de formation;	4° de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;
5° les parties prenantes et les infrastructures des secteurs public et privé concernées;	5° de relevante publieke en particuliere belanghebbenden en betrokken infrastructuur;
6° les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le	6° de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van België aan het

soutien effectifs de la Belgique à la gestion coordonnée des crises et incidents de cybersécurité majeurs au niveau de l'Union européenne.	gecoördineerde beheer van grootschalige cyberbeveiligingscrises en -incidenten op het niveau van de Europese Unie en de ondersteuning daarvan te waarborgen.
Titre 3. – Mesures de gestion des risques en matière de cybersécurité et obligations d'information	Titel 3. – Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen
Chapitre 1. Mesures de gestion des risques en matière de cybersécurité	Hoofdstuk 1. Maatregelen voor het beheer van cyberbeveiligingsrisico's
Art. 30. § 1 ^{er} Les entités essentielles et importantes prennent les mesures 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.	Art. 30. § 1. De essentiële en belangrijke entiteiten nemen passende en evenredige maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun werkzaamheden 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. Les mesures visées au paragraphe 1 ^{er} 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.	§ 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. Les mesures visées au paragraphe 1 ^{er} 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:	§ 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° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;	1° beleid inzake risicoanalyse en beveiliging van informatiesystemen;
2° la gestion des incidents;	2° incidentenbehandeling;
3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la	3° bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;

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;	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° 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;	5° beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;	6° beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;	7° basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;	8° beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;	9° beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
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;	10° wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;
11° une politique de divulgation coordonnée des vulnérabilités.	11° een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.
§ 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.	§ 4. Wanneer essentiële en belangrijke entiteiten nagaan welke maatregelen als 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.
Ces mesures doivent être appropriées au regard des résultats des évaluations coordonnées au niveau de l'Union européenne des risques pour la sécurité des	Deze maatregelen moeten passend zijn in het licht van de resultaten van de op het niveau van de Europese Unie gecoördineerde

chaînes d'approvisionnement critiques.	beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.
§ 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.	§ 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. Lorsqu'une entité essentielle ou importante constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 3, elle prend, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.	§ 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 ^{er} . 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.	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.
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.	Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.
§ 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.	§ 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. 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, § 1 ^{er} .	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. 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	Art. 33. Na raadpleging van de nationale cyberbeveiligingsautoriteit en van de eventuele betrokken sectorale overheid en deelgebieden kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, passende en evenredige

des risques en matière de cybersécurité appropriées et proportionnées.	bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's opleggen.
Chapitre 2. Notification d'incidents	Hoofdstuk 2. Melding van incidenten
Section 1^{re}. Notification obligatoire	Afdeling 1. Verplichte melding
Art. 34. § 1^{er}. 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.	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.
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.	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 bijlage I en II.
Le CSIRT national communique immédiatement les notifications visées à l'alinéa 1 ^{er} aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.	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. 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.	§ 2. Indien van toepassing delen de betrokken entiteiten de ontvangers van hun diensten die mogelijk wordt getroffen 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. Après consultation de l'autorité nationale de cybersécurité, des autorités sectorielles, le 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.	§ 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. Le cas échéant, la notification se fait conformément aux actes d'exécution de la Commission européenne, dont celui du [xxx portant	§ 4. In voorkomend geval gebeurt de melding overeenkomstig de uitvoeringshandelingen van de Europese Commissie, waaronder die van [xxx tot

modalités d'application de la Directive (UE) 2022/2255 du Parlement européen et du Conseil précisant les éléments à prendre en considération par certaines entités pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif].	vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2022/2255 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door bepaalde entiteiten in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft].
§ 5. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.	§ 5. Een melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.
Art 35. § 1^{er}. Aux fins de la notification visée à l'article 34, § 1 ^{er} , alinéa 1 ^{er} , les entités concernées soumettent CSIRT national :	Art. 35. § 1. Voor de in artikel 34, § 1, eerste lid, bedoelde melding bezorgen de betrokken entiteiten het nationale CSIRT:
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;	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° sans retard injustifié et en tout état de cause dans les 72 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;	2° onverwijld en in elk geval binnen 72 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;
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;	3° op verzoek van het nationale CSIRT of van de eventuele betrokken sectorale overheid, een tussentijds verslag over relevante updates van de situatie;
4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au 2°, comprenant les éléments suivants:	4° uiterlijk één maand na de indiening van de in 2° bedoelde incidentmelding, een eindverslag waarin het volgende is opgenomen:
a) une description détaillée de l'incident, y compris de sa gravité et de son impact;	a) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;
b) le type de menace ou la cause profonde qui a	b) het soort bedreiging of de grondoorzaak die

probablement déclenché l'incident;	waarschijnlijk tot het incident heeft geleid;
c) les mesures d'atténuation appliquées et en cours;	c) toegepaste en lopende risicobeperkende maatregelen;
d) le cas échéant, l'impact transfrontière de l'incident;	d) in voorkomend geval, de grensoverschrijdende gevolgen van het 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.	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. Par dérogation au paragraphe 1 ^{er} , 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.	§ 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. Le CSIRT national communique, immédiatement, les notifications visées aux paragraphes 1 ^{er} et 2 aux éventuelles autorités sectorielles compétentes. Les notifications des entités essentielles sont également transmises au NCCN.	§ 3. Het nationale CSIRT bezorgt de in 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 ^{er} 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, § 1 ^{er} , 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.	Art. 36. § 1. Het nationale CSIRT verstrekt onverwijld en zo mogelijk binnen vierentwintig uur na ontvangst van de in artikel 35, § 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. 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.	§ 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 rechtshandavingsinstanties.
Art. 37. § 1 ^{er} . Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard	Art. 37. § 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale

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.	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. 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.	§ 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. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1 ^{er} , alinéa 1 ^{er} , aux points de contact uniques des autres États membres touchés.	§ 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. 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, § 1 ^{er} , alinéa 1 ^{er} , et à l'article 38, § 1 ^{er} .	§ 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. Le CSIRT national fournit aux autorités compétentes en vertu de la loi [CER /du 1 ^{er} juillet 2011] des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément l'article 34, § 1 ^{er} , alinéa 1 ^{er} , et à l'article 38, § 1 ^{er} , par les entités identifiées [comme des entités critiques] en vertu de la loi [CER /du 1 ^{er} juillet 2011].	§ 5. Het nationale CSIRT verstrekt de uit hoofde van de [CER-wet/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 entiteiten die uit hoofde van de [CER-wet/wet van 1 juli 2011] [als kritieke entiteiten] zijn aangemerkt.
Section 2. Notification volontaire	Afdeling 2. Vrijwillige melding
Art. 38. § 1^{er}. Outre les obligations de notification prévues à l'article 34, peuvent être notifiés à titre volontaire au CSIRT national par :	Art. 38. § 1. Naast de in artikel 34 bedoelde meldingsverplichtingen kunnen vrijwillig aan het nationale CSIRT worden gemeld door:

1° les entités essentielles et importantes, les incidents, les cybermenaces et les incidents évités;	1° essentiële en belangrijke entiteiten: incidenten, cyberdreigingen en bijna-incidenten;
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° andere dan in 1° bedoelde entiteiten, ongeacht of zij tot het toepassingsgebied van deze wet behoren: significante incidenten, cyberdreigingen en bijna-incidenten.
§ 2. Les notifications volontaires visées au paragraphe 1 ^{er} sont traitées de la même manière que les notifications obligatoires visées à la section 1 ^{re} du présent chapitre.	§ 2. De in paragraaf 1 bedoelde vrijwillige meldingen worden op dezelfde wijze verwerkt als de verplichte meldingen bedoeld in afdeling 1 van dit hoofdstuk.
Les notifications obligatoires peuvent néanmoins être traitées de manière prioritaire par rapport aux notifications volontaires.	Er kan evenwel voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.
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 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.	Onverminderd het voorkomen, opsporen, onderzoeken en vervolgen van misdrijven, mag een vrijwillige melding er niet toe leiden dat de meldende entiteit bijkomende verplichtingen worden opgelegd waaraan zij niet zou zijn onderworpen indien zij de melding niet had ingediend.
Titre 4. – Supervision et sanctions	Titel 4. - Toezicht en sancties
Chapitre 1^{er}. Supervision	Hoofdstuk 1. Toezicht
Section 1^{re}. Évaluation périodique de la conformité	Afdeling 1. Regelmatige conformiteitsbeoordeling
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 :	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° 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 ;	1° ofwel opteren zij voor een in artikel 40 bedoelde regelmatige conformiteitsbeoordeling, op basis van een van de door de Koning bepaalde referentiekaders;
2° Soit en se soumettant à une inspection par l'autorité nationale de cybersécurité, sur base des modalités déterminées par le Roi.	2° ofwel onderwerpen zij zich aan een inspectie door de nationale cyberbeveiligingsautoriteit, op basis van de door de Koning bepaalde nadere regels.

Par dérogation à l'alinéa 1 ^{er} , et à la demande de l'autorité sectorielle concernée, les inspections visées à l'alinéa 1 ^{er} , 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.	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 betrokken inspectiedienst mits akkoord van de nationale cyberbeveiligingsautoriteit.
Lorsque le Roi détermine plusieurs cadres de référence, les entités essentielles choisissent le cadre de référence auquel ils se soumettent.	Indien de Koning meerdere referentiekaders bepaalt, kiezen essentiële entiteiten aan welk referentiekader zij zich onderwerpen.
Art. 40. § 1 ^{er} . L'évaluation périodique de la conformité visée à l'article 39, alinéa 1 ^{er} , 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.	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.
Pour le contrôle des entités [critiques au sens de la loi [CER] identifiées dans le cadre de la loi du 1^{er} 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.	Voor het toezicht op [kritieke entiteiten als bedoeld in de [CER]-wet die in het kader van de wet van 1 juli 2011 zijn geïdentificeerd] en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.
§ 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 1 ^{er} par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.	§ 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. Les entités importantes peuvent, de manière volontaire, se soumettre à une évaluation périodique de la conformité visée à l'article 39, alinéa 1 ^{er} , 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. 41. Belangrijke entiteiten kunnen zich vrijwillig onderwerpen aan een regelmatige conformiteitsbeoordeling, als 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. Les entités essentielles et importantes qui se soumettent à une évaluation périodique de la conformité visée à l'article 39, alinéa 1 ^{er} , 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. 42. Essentiële en belangrijke entiteiten die zich aan een regelmatige conformiteitsbeoordeling, als 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. 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.	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.
Section 2. Dispositions générales relatives au service d'inspection	Afdeling 2. Algemene bepalingen betreffende de inspectiedienst
Art. 44. § 1^{er}. 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.	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.
Par dérogation à l'alinéa 1 ^{er} , 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.	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.
L'autorité sectorielle ou le service d'inspection sectoriel compétent, 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.	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. 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 compétent mentionnent la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies.	§ 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.
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.	De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst kunnen een beroep doen op

	experten.
§ 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.	§ 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. Lorsqu'ils traitent des incidents donnant lieu à des violations de données à caractère personnel, 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.	§ 4. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens, 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^{er}. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent informent les autorités compétentes en vertu de la loi [CER /du 1 ^{er} juillet 2011] lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité définie comme critique en vertu de la loi [CER /du 1 ^{er} juillet 2011] respecte la présente loi. S'il y a lieu, les autorités compétentes en vertu de la loi [CER /du 1 ^{er} 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 compétent d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité qui est définie comme entité critique en vertu de la loi [CER /du 1 ^{er} juillet 2011].	Art. 45. § 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de [CER-wet/wet van 1 juli 2011] bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een entiteit die op grond van de [CER-wet/wet van 1 juli 2011] als kritieke entiteit wordt aangemerkt, voldoet aan deze wet. In voorkomend geval kunnen de uit hoofde van de [CER-wet/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 entiteit die is aangemerkt als kritieke entiteit uit hoofde van de [CER-wet/wet van 1 juli 2011].
§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent 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) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de	§ 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)

l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent 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.	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^{er}. 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 compétent, en concertation avec l'autorité nationale de cybersécurité, peuvent solliciter la coopération et l'assistance des autorités de contrôle compétentes d'autres États membres.	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.
Dans le cadre de la sollicitation visée à l'alinéa 1 ^{er} :	In het kader van het verzoek bedoeld in het eerste lid:
1° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent peuvent demander aux autorités de contrôle compétentes d'autres États membres de prendre des mesures de supervision ou d'exécution;	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° le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent 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.	2° kunnen de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst de bevoegde toezichthoudende autoriteiten van andere lidstaten gemotiveerd om wederzijdse bijstand verzoeken, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.
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.	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. 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 compétent 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.	§ 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 indien deze hierom verzoeken en de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden.
Dans le cadre de la demande visée à l'alinéa 1 ^{er} :	In het kader van het verzoek bedoeld in het eerste lid:
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 compétent et les communique aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres ;	1° centraliseert de nationale cyberbeveiligingsautoriteit de informatie en raadplegingen met betrekking tot de toezichts- en handhavingsmaatregelen die zichzelf 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° ladite demande peut porter sur des mesures de supervision ou d'exécution;	2° dit verzoek kan betrekking hebben op toezichts- of handhavingsmaatregelen;
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.	3° dit verzoek kan, indien het gemotiveerd wordt, betrekking hebben op wederzijdse bijstand, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.
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.	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.
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	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

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 et l'ENISA.	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 Commissie en 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 compétent peuvent mener à bien des actions communes de supervision entre elles et/ou avec les autorités de contrôle compétentes d'autres États membres.	§ 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. Le présent article n'est pas applicable aux missions diplomatiques et consulaires.	§ 4. Dit artikel is niet van toepassing op diplomatieke en consulaire missies.
Art. 47. § 1^{er}. 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 sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.	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. 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.	§ 2. De leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst en de experts die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Zij leggen de eed af bij de leidend ambtenaar van hun dienst.
Les autorités visées à l'article 44, § 1 ^{er} , prennent les mesures nécessaires afin d'assurer l'indépendance des membres de leur personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de leurs tâches.	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.
La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel des autorités visées à l'article 44, § 1 ^{er} , a, directement ou indirectement, un intérêt financier,	Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een personeelslid van de autoriteiten bedoeld in artikel 44, § 1, rechtstreeks of onrechtstreeks financiële,

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.	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. Les membres du personnel des autorités visées à l'article 44, § 1 ^{er} , ne reçoivent ni ne cherchent pas, dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne tierce.	§ 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.
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.	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.
Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.	De Koning kan ook andere situaties benoemen als belangenconflicten.
Section 3. La supervision des entités par le service d'inspection	Afdeling 3. Het door de inspectiedienst uitgeoefende toezicht op de entiteiten
Art. 48. § 1 ^{er} . 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 compétent 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:	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 toezichtsoopdracht 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° 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 de tout autre audit de sécurité effectué par un auditeur qualifié et les éléments de preuve sous-jacents correspondants;	1° toegang vragen tot alle documenten of informatie die nodig zijn voor de uitoefening van hun toezichtsoopdracht en hiervan een kopie verkrijgen, met name de bewijzen van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van conformiteitsbeoordelingen of andere beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen;
2° procéder, sur place ou à distance, à tout examen, contrôle et audition, y compris des contrôles aléatoires effectués par des professionnels formés;	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° 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;	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 risicogereleerde informatie;
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 1 ^{er} et de la mise en œuvre de la présente loi;	4° alle inlichtingen 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° réaliser un audit ad hoc, notamment lorsqu'il est justifié en raison d'un incident significatif ou d'une violation de la présente loi;	5° een ad-hoc audit uitvoeren, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of een inbreuk op deze wet;
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;	6° beveiligingsscan uitvoeren op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;
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. A cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;	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° le cas échéant, demander l'assistance des services de la police fédérale ou locale dans le cadre de l'usage de la force;	8° in voorkomend geval, de bijstand vragen van de federale of lokale politiediensten in het kader van het gebruik van geweld;
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;	9° inlichtingen 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 voortspuitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, voor de uitvoering van de bepalingen van deze wet;

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.	10° zondervoorafgaande 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. Dans le cadre de l'inspection des entités importantes, les compétences de contrôle visées au paragraphe 1 ^{er} s'effectuent de manière ex post, sur base d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente loi.	§ 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 zou naleven.
§ 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 compétent adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes :	§ 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° l'identification des espaces habités auxquels ils souhaitent avoir accès;	1° de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben;
2° les infractions éventuelles qui font l'objet du contrôle;	2° de eventuele inbreuken die het voorwerp zijn van het toezicht;
3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire.	3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.
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 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 compétent 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.	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 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.
Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une	Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen

heures par au moins deux membres du service d'inspection agissant conjointement.	vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.
§ 4. Au début de toute audition, il est communiqué à la personne interrogée :	§ 4. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:
1° que ses déclarations peuvent être utilisées comme preuve en justice;	1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;
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;	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° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.	3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.
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.	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.
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.	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.
A 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.	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.
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 qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.	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. 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 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	§ 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

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.	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.
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 compétent peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.	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. 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 compétent peut solliciter l'intervention d'un juge d'instruction.	§ 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. Lorsque le service d'inspection de l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétent 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.	§ 7. Wanneer de inspectiedienst van de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid of sectorale inspectiedienst er bij toezicht of 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 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 Gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.
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 compétent informe l'autorité de protection des données compétente établie en Belgique de la violation potentielle de données à caractère personnel visée à l'alinéa 1 ^{er} .	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. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés des autorités visées à l'article 44, § 1 ^{er} , veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour ledit contrôle.	§ 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.
Art. 49. § 1^{er}. 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 compétent rédigent un rapport et en transmettent une copie à l'entité inspectée.	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. L'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle se communiquent mutuellement leur rapport d'inspection.	§ 2. De nationale cyberbeveiligingsautoriteit en de eventuele sectorale overheid wisselen hun inspectieverslagen uit.
Art. 50. § 1^{er}. 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 compétent dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.	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.
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 compétent le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.	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, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.
§ 2. Les coûts des inspections ne sont pas mis à charge des entités.	§ 2. De kosten van de inspecties zijn niet ten laste van de entiteiten.
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.	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. 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 compétent, 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 compétent.	§ 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.
Chapitre 2. Les mesures et amendes administratives	Hoofdstuk 2. De administratieve maatregelen en geldboetes
Section 1^{re}. Procédure	Afdeling 1. Procedure
Art. 51. § 1 ^{er} . 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, § 1 ^{er}	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.
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.	Mits de nationale cyberbeveiligingsautoriteit akkoord gaat, kan de sectorale overheid administratieve maatregelen en geldboetes, als bedoeld in afdeling 2, opleggen aan een entiteit.
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.	De nationale cyberbeveiligingsautoriteit informeert de betrokken sectorale overheid wanneer zij overweegt om administratieve maatregelen en geldboetes, als bedoeld in artikel 58 en 59, op te leggen aan een entiteit.
Lorsque les autorités visées aux alinéas 1 ^{er} et 2 prennent connaissance, dans le cadre de leur mission de supervision, du fait qu'un manquement visé à l'alinéa 1 ^{er} 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, 12), du règlement (UE) 2016/679,	Wanneer de autoriteiten bedoeld in het eerste en tweede lid er tijdens hun toezichtsovereenkomst 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, 12), van Verordening (EU) 2016/679 kan

devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de protection des données compétentes.	inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde gegevensbeschermingsautoriteiten daarvan onverwijld in kennis.
§ 2. Sur la base du procès-verbal visé au paragraphe 1 ^{er} et, le cas échéant, des rapports pertinents visés à l'article 49, § 1 ^{er} , 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.	§ 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.
Le délai visé à l'alinéa 1 ^{er} est déterminé en tenant compte des conditions de fonctionnement de l'entité et des mesures à mettre en œuvre.	De in het eerste lid bedoelde termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de entiteit en de te nemen maatregelen.
§ 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 quinze 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.	§ 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 vijftien 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.
Par exception à l'alinéa 1 ^{er} , 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.	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 incidenten te voorkomen of erop te reageren anders zou worden belemmerd.
§ 4. Après que l'entité concernée a pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3, alinéa 1 ^{er} , ou dans le cas visé au paragraphe 3, alinéa 2, l'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle	§ 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

compétente maintient ou modifie le projet de décision visé au paragraphe 2, alinéa 1 ^{er} 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.	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 ^{er} . 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.	Art. 52. § 1. Indien een essentiële entiteit geen gevolg geeft aan een of meer maatregelen vermeld in de beslissing bedoeld in artikel 51, § 4, stelt de autoriteit die deze beslissing heeft genomen de feiten vast in een proces-verbaal.
§ 2. Sur la base du procès-verbal visé au paragraphe 1 ^{er} , 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.	§ 2. Op basis van het in paragraaf 1 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 als bedoeld in artikel 59 en/of 60 bevat.
§ 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 amende administratives envisagées et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant l'envoi du projet de décision précité.	§ 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 vijftien 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.
Par exception à l'alinéa 1 ^{er} , 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.	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 incidenten te voorkomen of erop te reageren anders zou worden belemmerd.
§ 4. Après que l'entité concernée ait pu faire valoir ses moyens de défense, à la fin du délai visé au paragraphe 3, alinéa 1 ^{er} , 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 ou y renonce en	§ 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 in paragraaf 2

tenant compte des moyens de défense de l'entité concernée et des éléments visés à l'article 54.	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. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.	Art. 53. De processen-verbaal van de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.
Art. 54. § 1 ^{er} . 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 :	Art. 54. § 1. Bij het nemen van de handhavingsmaatregelen in het kader van de in artikel 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 la catégorie visée aux articles 9 et 10 à laquelle l'entité concernée appartient;	1° de in artikel 9 en 10 bedoelde categorie waartoe de betrokken entiteit behoort;
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:	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) les violations répétées;	a) herhaalde inbreuken;
b) le fait de ne pas notifier des incidents significatifs ou de ne pas y remédier;	b) het niet melden of niet verhelpen van significante incidenten;
c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes;	c) het niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteiten;
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 compétent à la suite de la constatation d'une violation;	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;
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;	e) het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's of de in titel 3 bedoelde melding van incidenten;
3° de la durée de la violation;	3° de duur van de inbreuk;

4° de toute violation antérieure pertinente commise par l'entité concernée;	4° eventuele relevante eerdere inbreuken door de betrokken entiteit;
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;	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° du fait que l'auteur de la violation a agi délibérément ou par négligence;	6° opzet of nalatigheid van de pleger van de inbreuk;
7° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;	7° door de entiteit genomen maatregelen om de materiële of immateriële schade te voorkomen of te beperken;
8° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;	8° de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;
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 compétent des personnes physiques ou morales tenues pour responsables.	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. 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.	§ 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 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^{er}. Les décisions visées aux articles 51 et 52 sont notifiées par envoi recommandé au contrevenant.	Art. 55. § 1. De in artikel 51 en 52 bedoelde beslissingen worden bij aangetekende zending ter kennis gebracht van de overtreder.
§ 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 1 ^{er} .	§ 2. De 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.
Ce délai peut être augmenté en fonction du montant de l'amende administrative.	Deze termijn kan verlengd worden in functie van het bedrag van de geldboete.
Le délai visé à l'alinéa 1 ^{er} est réputé commencer au	De in het eerste lid bedoelde termijn wordt geacht

plus tard six jours après l'envoi recommandé visé au paragraphe 1 ^{er} .	in te gaan uiterlijk zes dagen na de in paragraaf 1 bedoelde aangetekende zending.
§ 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.	§ 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. 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.	§ 4. De nationale cyberbeveiligingsautoriteit en, desgevalend, de eventuele sectorale overheid wisselen hun in artikel 51 of 52 bedoelde beslissing uit.
Art. 56. § 1 ^{er} . 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.	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.
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.	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. 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.	§ 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. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.	§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.
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.	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.
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,	De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de

alinéa 2, et à l'article 55 de ce Code.	verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.
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.	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.
§ 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.	§ 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.
Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.	De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.
§ 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.	§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.
Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.	Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.
Art. 57. L'autorité nationale de cybersécurité ou l'éventuelle autorité sectorielle compétente ne peut imposer de mesures administratives ni d'amendes administratives à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis.	Art. 57. De nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid kan geen administratieve maatregelen of administratieve geldboetes opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.
Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.	De betaling volgens de administratieve procedure doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.
Section 2. Mesures et amendes administratives	Afdeling 2. Administratieve maatregelen en geldboetes
Art. 58. Les mesures administratives suivantes peuvent être imposées aux entités sur la base de l'article 51 :	Art. 58. De volgende administratieve maatregelen kunnen aan entiteiten worden opgelegd op basis van artikel 51:
1° émettre des avertissements concernant les	1° waarschuwingen geven over inbreuken door de

violations de la présente loi par les entités concernées;	betrokken entiteiten op deze wet;
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;	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° ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer;	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° 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;	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° 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;	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° ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d’un audit de sécurité dans un délai raisonnable;	6° de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;
7° ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique;	7° de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;
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.	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.
Lorsque l’entité concernée est une entité essentielle,	Wanneer de betrokken entiteit een essentiële

les instructions contraignantes visées à l'alinéa 1 ^{er} , 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.	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. Les amendes administratives suivantes peuvent être imposées aux entités sur la base de l'article 51 ou 52:	Art. 59. De volgende administratieve geldboetes kunnen aan entiteiten worden opgelegd op basis van artikel 51 of 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 11, § 5;	1° eenieder die niet voldoet aan de in artikel 11, § 5, bedoelde rapportageverplichtingen wordt bestraft met een geldboete van 500 tot 125 000 euro;
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;	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° Est puni d'une amende de 500 à 200 000 euros quiconque ne se conforme pas aux obligations de contrôle visées au présent titre;	3° eenieder die niet voldoet aan de in deze titel bedoelde toezichtverplichtingen wordt bestraft met een geldboete van 500 tot 200 000 euro;
4° est punie d'une amende de 500 à 7 000 000 euros ou 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus 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;	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 met een geldboete van 500 tot 7 000 000 euro of van 1,4% 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° est punie d'une amende de 500 à 10 000 000 euros ou 2% 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.	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% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, afhankelijk van welk bedrag het hoogst is.
L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois	De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen

ans.	een termijn van drie jaar.
Le concours de plusieurs manquements peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.	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. A défaut de prendre les mesures nécessaires dans le délai imposé par le service d'inspection, les mesures administratives suivantes peuvent être imposées aux entités essentielles sur la base de l'article 52 :	Art. 60. Indien de nodige maatregelen niet binnen de door de inspectiedienst gestelde termijn worden genomen, kunnen aan essentiële entiteiten op grond van artikel 52 de volgende administratieve maatregelen worden opgelegd:
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;	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° 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.	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.
Les suspensions ou interdictions temporaires visées à l'alinéa 1 ^{er} 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.	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. 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.	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.
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	Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.

nommés.	
Titre 5. – Dispositions spécifiques au secteur de l’administration publique	Titel 5. - Specifieke bepalingen voor de overheidssector
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. 62. De administratieve maatregelen en geldboetes bedoeld in artikel 59 en 60 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidssector.
Art. 63. § 1 ^{er} . 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.	Art. 63. § 1. De Koning wordt gemachtigd een autoriteit aan te wijzen als conformiteitsbeoordelingsinstantie voor alle of een deel van de overheidsinstanties.
§ 2. L’autorité visée au paragraphe 1 ^{er} 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 1 ^{er} , 1 ^o .	§ 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 ^o , bedoelde regelmatige conformiteitsbeoordeling uit te voeren.
L’agrément visée à l’alinéa 1 ^{er} porte sur un ou plusieurs des cadres de référence visés à l’article 39.	De in het eerste lid bedoelde erkenning heeft betrekking op een of meer van de in artikel 39 bedoelde referentiekaders.
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. 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. L’article 47 est applicable au service d’inspection visé à l’alinéa 1 ^{er} .	Art. 65. Artikel 47 is van toepassing op de inspectiedienst bedoeld in het eerste lid.
Titre 6. - Traitement des données à caractère personnel	Titel 6. - Verwerking van persoonsgegevens
Chapitre 1^{er}. Principes relatifs au traitement	Hoofdstuk 1. Beginselen betreffende de verwerking
Art. 66. Les définitions du règlement (UE) 2016/679 sont d’application pour le présent titre.	Art. 66. De definities van Verordening (EU) 2016/679 zijn van toepassing op deze titel.
Art. 67. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes :	Art. 67. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:
1 ^o l’amélioration de la cybersécurité à travers la	1 ^o de verbetering van de cyberbeveiliging dankzij

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;	een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;
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;	2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren en sensibiliseren van 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° la gestion des crises et incidents de cybersécurité;	3° het beheer van cyberbeveiligingscrises en -incidenten;
4° l'exécution des tâches du CSIRT national visées aux articles suivants :	4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikelen:
a) 19, § 1 ^{er} ;	a) 19, § 1;
b) 21, § 2, al. 2, 1° à 3°;	b) 21, § 2, tweede lid, 1° tot 3°;
c) 22, § 2 à § 6;	c) 22, § 2 tot § 6;
d) 37, § 1 ^{er} à § 3, et § 5;	d) 37, § 1 tot § 3, en § 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 CER, ainsi que les autorités visées à l'article 25, § 2 dans le cadre de l'exécution de la présente loi et la loi CER;	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 CER-wet, alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en de CER-wet;
6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1 ^{er} ;	6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;
7° le partage d'informations entre les autorités visées à l'article 25, § 5;	7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;
8° la continuité des services prestés par les entités importantes ou essentielles;	8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;
9° la notification d'incidents et d'incidents évités;	9° het melden van incidenten en bijna-incidenten;

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.	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. Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes :	Art. 68. De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:
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°;	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° 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;	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° 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 et incidents de cybersécurité;	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 cyberbeveiligingscrises en -incidenten;
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;	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-communicatiemetagegegevens 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° 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 CER;	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 CER-wet;

6° pour la finalité visée à l'article 67, 6° : les données d'identification des personnes concernées par la coopération;	6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;
7° pour la finalité visée à l'article 67, 7° : les données d'identification des personnes concernées par le partage d'informations;	7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;
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;	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° 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;	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° 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.	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.
Art. 69. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitement sont les suivantes :	Art. 69.. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:
1° les personnes participant directement aux missions confiées à l'autorité nationale de cybersécurité en vertu du titre 2;	1° de personen die rechtstreeks deelnemen aan de opdrachten die krachtens titel 2 zijn toevertrouwd aan de nationale cyberbeveiligingsautoriteit;
2° les personnes visées par les obligations qui incombent aux entités essentielles et importantes en vertu du titre 3;	2° de personen bedoeld in het kader van de verplichtingen voor essentiële en belangrijke entiteiten die voortvloeien uit titel 3;
3° les personnes impliquées dans un incident;	3° de personen die betrokken zijn bij een incident;
4° les personnes directement impliquées dans les exercices de supervision, de contrôle, et de sanction, visés au titre 4.	4° de personen die rechtstreeks betrokken zijn bij het toezicht, de controle en de sancties bedoeld in titel 4.
Art. 70. Les entités suivantes sont responsables des traitements qu'elles effectuent pour la réalisation des finalités visées à l'article 67 :	Art. 70. De volgende entiteiten zijn verantwoordelijk voor de verwerkingen die zij uitvoeren voor de verwezenlijking van de doeleinden bedoeld in artikel 67:
1° l'autorité nationale de cybersécurité;	1° de nationale cyberbeveiligingsautoriteit;

2° le NCCN;	2° het NCCN;
3° l'éventuelle autorité sectorielle;	3° de eventuele sectorale overheid;
4° l'éventuel service d'inspection sectoriel;	4° de eventuele sectorale inspectiedienst;
5° les entités essentielles et importantes;	5° de essentiële en belangrijke entiteiten;
6° les entités fournissant des services d'enregistrement de noms de domaine;	6° de entiteiten die domeinnaamregistratiediensten verlenen;
7° les autorités visées à l'article 23, § 1 ^{er} , 6°.	7° de autoriteiten bedoeld in artikel 23, § 1, 6°.
Chapitre 2. Durée de conservation	Hoofdstuk 2. Bewaartermijn
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 10 ans maximum après le premier traitement effectué.	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.
Chapitre 3. Limitation des droits des personnes concernées	Hoofdstuk 3. Beperking van de rechten van de betrokkenen
Art. 72. § 1^{er}. En application de l'article 23.1, a), b), c), d), e), 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.	Art. 72. § 1. Met toepassing van artikel 23.1, a), b), c), d), e), 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 grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefte doel.
§ 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.	§ 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. L'exemption vaut pour les catégories de données à caractère personnel visées à l'article 68,	§ 3. De vrijstelling geldt voor de categorieën van persoonsgegevens bedoeld in artikel 68, 10°. Deze

10°. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.	vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.
§ 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.	§ 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.
La durée des actes préparatoires, visés à l'alinéa 1 ^{er} , 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.	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. 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 bénéficier de l'exemption.	§ 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 ^{er} . 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 des dites données qui soit nécessaire dans le cadre défini ci-avant.	Art. 73. § 1. De betrokken verwerkingsverantwoordelijke verleent de betrokkene toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze kennisgeving 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.
§ 2. La mesure de refus ou de limitation des droits consacrés par les articles visés à l'article 72, § 2, doit être levée :	§ 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° 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;	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 artikel 34 en 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;	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° 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° 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. 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.	§ 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. 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.	§ 4. In alle toepassingsgevallen van paragraaf 2 en 3 informeert de functionaris voor gegevensbescherming de betrokkene of betrokkenen schriftelijk dat de maatregel betreffende de weigering of beperking is opgeheven.
Chapitre 4. Limitations aux obligations de notification des violations de données à caractère personnel	Hoofdstuk 4. Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens
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.	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.
Titre 7. - Dispositions finales	Titel 7. - Slotbepalingen

Chapitre 1^{er}. Disposition transitoire	Hoofdstuk 1. Overgangsbepaling
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.	Art. 75. De Koning stelt de termijnen vast waarbinnen essentiële entiteiten hun eerste regelmatige conformiteitsbeoordelingen als bedoeld in artikel 39 uitvoeren.
Chapitre 2. Dispositions modificatives	Hoofdstuk 2. Wijzigingsbepalingen
Section 1^{re}. 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	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 voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle
Art. 76. A l'article 1 ^{er} 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 19 décembre 2021, 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 [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ; ».	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 voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, het laatst gewijzigd bij de wet van 19 december 2021, 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 [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;”.
Art. 77. Dans la section 1 ^{re} du chapitre III de la même loi, l'article 15ter, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit :	Art. 77. In afdeling 1 van hoofdstuk III van dezelfde wet wordt artikel 15ter, ingevoegd bij de wet van 7 april 2019, vervangen als volgt:
« Art. 15ter. 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.	“Art. 15ter. 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 de elektriciteit.
Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence. »	De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.”

Section 2. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique	Afdeling 2. Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België
Art. 78. A 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 juillet 2022, le 28° est remplacé par ce qui suit :	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, het laatst gewijzigd bij de wet van 20 juli 2022, wordt punt 28° vervangen als volgt:
« "la loi NIS2" : la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique; »	""de NIS2-wet" : de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;"
Art. 79. A l'article 36/14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées :	Art. 79. In artikel 36/14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:
1° au paragraphe 1 ^{er} , 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, 47°, de la loi NIS2 »;	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, 47°, van de NIS2-wet";
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, 47°, de la loi NIS2 et au CSIRT national visé à l'article 8, 47°, de la même loi »;	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, 47°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 47°, van dezelfde wet";
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 ».	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. L'article 36/47 de la même loi, inséré par la loi du 7 avril 2019, est remplacé par ce qui suit :	Art. 80. Artikel 36/47 van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt vervangen als volgt:
« Art. 36/47. Pour l'application de la loi NIS2, la	" Art. 36/47. Voor de toepassing van de NIS2-wet

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.	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 infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
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 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. »	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 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.”
Section 3. Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	Afdeling 3. Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
Art. 81. A l'article 75, § 1 ^{er} , 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 [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ».	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, het laatst 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 [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.
Section 4. Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	Afdeling 4. Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecomunicatiesector
Art. 82. A l'article 1 ^{er} /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 :	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 telecomunicatiesector, vervangen door de wet van 21 december 2021, wordt punt 1° vervangen als volgt:
« 1° la Directive européenne (UE) 2022/2555 du	“1° Richtlijn (EU) 2022/2555 van het Europees

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; ».	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. A l'article 14 de la même loi, modifié en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées :	Art. 83. In artikel 14 van dezelfde wet, het laatst gewijzigd bij de wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:
1° au paragraphe 1 ^{er} , 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 [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique »;	1° in paragraaf 1 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 [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”;
2° au même paragraphe, le 3°, alinéa 1 ^{er} , h), est remplacé par ce qui suit :	2° in dezelfde paragraaf wordt punt 3°, eerste lid, h), vervangen als volgt:
« h) la loi du [xx xxxx xxxx] 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 pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance; »;	“h) de wet van [xx xxxx xxxx] 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 voor de sector digitaal infrastructuur, met uitzondering van de verleners van vertrouwensdiensten;”;
3° au même paragraphe, le 3°, alinéa 2, est remplacé par ce qui suit :	3° in dezelfde paragraaf wordt punt 3°, tweede lid, vervangen als volgt:
« Pour l'application de la loi du [xx xxxx xxxx] 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 et service d'inspection sectoriel pour le secteur des infrastructures numériques, à l'exception des prestataires de services de confiance. »	“Voor de toepassing van de wet van [xx xxxx xxxx] 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 en sectorale inspectiedienst voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten.”
Section 5. Modifications de la loi du 13 juin 2005 relative aux communications électroniques	Afdeling 5. Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie
Art. 84. A l'article 1 ^{er} de la loi du 13 juin 2005 relative aux communications électroniques, modifiée en dernier lieu par la loi du 30 août 2023, les	Art. 84. In artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, het laatst gewijzigd bij de wet van 30 augustus 2023,

modifications suivantes sont apportées :	worden de volgende wijzigingen aangebracht:
1° à l’alinéa 2, à la fin du 6°, le point est remplacé par un point-virgule;	1° in het tweede lid, aan het einde van punt 6°, wordt het punt vervangen door een puntkomma;
2° le même alinéa est complété par un 7°, rédigé comme suit :	2° hetzelfde lid wordt aangevuld met de bepaling onder 7°, luidende:
« 7° 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) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. »	“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. A l’article 2 de la même loi, les modifications suivantes sont apportées :	Art. 85. In artikel 2 van dezelfde wet worden de volgende wijzigingen aangebracht:
1° le 48/1° est remplacé par ce qui suit :	1° de bepaling onder 48/1° wordt vervangt als volgt:
« 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;	“48/1° “registervoor 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 naamsservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamsservers, 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° le 48/3° est inséré, rédigé comme suit :	2° de bepaling onder 48/3° is ingevoegd, luidende:
« 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; »	“48/3° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrar of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;”
3° les 62/2° et 62/3° sont remplacés par ce qui suit :	3° de bepalingen onder 62/2° en 62/3° worden vervangt als volgt:

« 62/2° « réseau et système d'information » :	“62/2° “netwerk- en informatiesysteem”:
a) un réseau de communications électroniques au sens du 3°;	a) een elektronische-communicatienetwerk als bedoeld in 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	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) 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;	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;
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;	62/3° “beveiliging van netwerk- en informatiesystemen”: het vermogen van netwerken 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° les 62/4° à 62/8° sont insérés, rédigés comme suit :	4° de bepalingen onder 62/4° tot 62/8° worden ingevoegd, luidende:
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;	62/4° “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° « cybersécurité » : la cybersécurité au sens de 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	62/5° “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

communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité);	informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);
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;	62/6° “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° « cybermenace » : une cybermenace au sens de l’article 2, point 8), du règlement (UE) 2019/881;	62/7° “cyberdreiging”: een cyberdreiging als bedoeld in artikel 2, 8), van de cyberbeveiligingsverordening;
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;	62/8° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerken en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;”
5° l’article est complété par un 94°, rédigé comme suit :	5° het artikel wordt aangevuld met de bepaling onder 94°, luidende:
« 94° « opérateur d’infrastructure numérique » : une entité qui relève du secteur infrastructure numérique, à l’exception des prestataires de services de confiance, comme prévu dans la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique. »	“94° “aanbieder van digitale infrastructuur”: een entiteit die behoort tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, zoals bedoeld in de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.”
Art. 86. Dans l’article 6, 4°, de la même loi, les mots « réseaux et services » sont remplacés par les mots « réseaux et systèmes d’information ».	Art. 86. In artikel 6, 4°, van dezelfde wet, worden de woorden “netwerk en diensten” vervangen door de woorden “netwerk- en informatiesystemen”.
Art. 87. Dans la même loi, les articles 107/2 à 107/4 sont remplacés par ce qui suit:	Art. 87. In dezelfde wet worden de artikelen 107/2 tot 107/4 vervangen als volgt:
« Art. 107/2. § 1 ^{er} . Sans préjudice des dispositions de la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, les opérateurs d’infrastructure numérique analysent les risques pour la sécurité de leurs réseaux et systèmes d’information. L’Institut peut	“ Art. 107/2. § 1. Onverminderd de bepalingen van de wet van [xx xxxx xxxx] 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

fixer des modalités de cette analyse de risque.	informatiesystemen. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.
§ 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 "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 "loi du 30 juillet 2018", les opérateurs veillent pour le moins à:	§ 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 "AVG" genoemd, en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna "wet van 30 juli 2018" genoemd, zorgen operatoren ervoor dat in ieder geval:
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;	1° wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens die ze verwerken;
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	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° assurer la mise en oeuvre d'une politique de sécurité relative au traitement des données à caractère personnel.	3° een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.
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.	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. 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.	§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en de internettoegangsdiens ten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.
Le Roi, sur proposition de l'Institut ou d'initiative, sur avis de celui-ci, peut préciser ces mesures.	Op voorstel van het Instituut of op eigen initiatief, en na advies van het Instituut, kan de Koning deze maatregelen preciseren.

§ 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.	§ 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. 107/3. § 1 ^{er} . En cas de cybermenace particulière et importante, l'opérateur 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.	Art. 107/3. § 1. In geval van een specifieke en 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.
L'Institut peut préciser les cas dans lesquels une information doit être notifiée ainsi que les modalités de cette communication.	Het Instituut kan de gevallen preciseren waarin informatie moet worden verstrekt alsook de nadere regels voor die kennisgeving.
§ 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.	§ 2. In geval van inbreuk in verband met persoonsgegevens verwittigt de operator van elektronische-communicatiediensten onverwijld de Gegevensbeschermingsautoriteit, die onverwijld het Instituut verwittigt.
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.	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.
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.	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.
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.	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.
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.	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 gezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.
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.	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.
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.	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. 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.	§ 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.
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	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

sa procédure de transmission.	kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt.
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.	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. 107/4. § 1^{er}. Le présent article s'applique sans préjudice des dispositions de la loi du [xx xxxx xxxx] 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.	Art. 107/4. § 1. Dit artikel is van toepassing onverminderd de bepalingen van de wet van [xx xxxx xxxx] 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. 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 [xx xxx xxxx] précitée à un opérateur 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.	§ 2. Het Instituut kan een aanbieder van digitale infrastructuur bindende instructies geven in het kader van artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de bovengenoemd wet van [xx xxx xxxx], 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.
§ 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 [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut peut soumettre l'opérateur d'infrastructure numérique à :	§ 3. In het kader van het toezicht op de artikelen 107/2 en 107/3 en van artikelen 30 en 33 van de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, kan het Instituut de aanbieder van digitale infrastructuur onderwerpen aan:
a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;	a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles, die worden uitgevoerd door daartoe opgeleide professionals;
b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou par l'Institut;	b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Instituut of door een

	onafhankelijke instantie;
c) des audits ad hoc;	c) ad-hocaudits;
d) 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'opérateur d'infrastructure digitale ;	d) beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;
e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'opérateur d'infrastructure digitale concerné;	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) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'Institut pour l'accomplissement de ses tâches de supervision;	f) verzoeken van alle gegevens, documenten en informatie die het Instituut nodig acht voor de uitoefening van haar toezichthoudende taken;
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.	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.
Les audits de sécurité ciblés visés au premier alinéa, point 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.	De in het eerste lid, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door het Instituut of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.
Lorsque l'audit de sécurité visé à l'alinéa 1er, point b) est effectué par un organisme indépendant, l'opérateur 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 à l'opérateur d'infrastructure numérique. A 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 de l'opérateur d'infrastructure numérique, sauf lorsque l'Institut en décide autrement dans des cas dûment motivés.	Wanneer de in het eerste lid, punt 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 onafhankelijke 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 gemotiveerde gevallen waarin het Instituut anders besluit.

Lorsqu'il exerce ses pouvoirs en vertu du paragraphe 1, point e), f) ou g), l'Institut précise la finalité de la demande et les informations exigées.	Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, punt e), f) of g), vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.
L'Institut peut fixer les modalités de la fourniture par l'opérateur d'infrastructure numérique des informations concernant l'analyse de risque.	Het Instituut kan bepalen op welke wijze de aanbieder van digitale infrastructuur informatie over de risicoanalyse moet verstrekken.
A la demande de l'Institut, un opérateur d'infrastructure numérique participe à un exercice relatif à la sécurité des réseaux et systèmes d'information ou organise un tel exercice.	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.
A la demande de l'Institut et dans le cadre de la gestion des incidents de sécurité, un opérateur d'infrastructure numérique communique à l'Institut un point de contact disponible en permanence.	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. A 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 [xx xxxx xxxx] 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, l'opérateur d'infrastructure numérique lui donne accès à tout élément de son réseau.	§ 4. Op verzoek van het Instituut en om een onderzoek in te stellen naar een geval van niet-conformiteit met artikelen 30 en 33 van de wet van [xx xxxx xxxx] 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. 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.	§ 5. Onverminderd de bevoegdheden van de nationale cyberbeveiligingsautoriteit coördineert het Instituut de initiatieven rond de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.
Il supervise la détection, l'observation et l'analyse des problèmes de sécurité, et peut fournir aux utilisateurs des informations en la matière.	Het ziet toe op het opsporen, observeren en analyseren van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.
§ 6. Le non-respect par un opérateur d'infrastructure numérique du présent article ou d'une décision de l'Institut prise sur base du présent article peut faire l'objet des mesures ou amendes administratives visées dans le chapitre 2 de la loi NIS 2.»	§ 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 hoofdstuk 2 van de NIS2-wet bedoelde administratieve maatregelen of geldboetes worden opgelegd.”

Art. 88. A l'article 126/3, § 3, l), de la même loi, 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 [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ».	Art. 88. In artikel 126/3, § 3, l), 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 [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.
Art. 89. A l'article 164/1 de la même loi, les modifications suivantes sont apportées :	Art. 89. In artikel 164/1 van dezelfde wet worden de volgende wijzigingen aangebracht:
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 »;	1° de woorden “Internetdomeinnaamregistreerbureau van het topniveaudomein” worden vervangen door de woorden “register voor topleveldomeinnamen van het topleveldomein”;
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 ».	2° in de bepaling onder 4° wordt het woord “domeinnaamregistreerbureau” vervangen door de woorden “register voor topleveldomeinnamen”;
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 »;	3° in de bepaling onder 4° wordt het woord “Internetdomeinnaamregistreerbureau” vervagen door de woorden “register voor topleveldomeinnamen”;
4° au 5°, dans le texte en néerlandais, le mot “topniveaudomein” est remplacé par le mot “topleveldomein”.	4° in de bepaling onder 5°, in de Nederlandse tekst, wordt het woord “topniveaudomein” vervangen door het woord “topleveldomein”.
Art. 90. A l'article 164/2 de la même loi, les modifications suivantes sont apportées :	Art. 90. In artikel 164/2 van dezelfde wet worden de volgende wijzigingen aangebracht:
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 »;	1° de woorden “Internetdomeinnaamregistreerbureau” worden vervangen door de woorden “register voor topleveldomeinnamen”;
2° dans le texte en néerlandais, le mot « topniveaudomein » est à chaque fois remplacé par le mot « topleveldomein ».	2° in de Nederlandse tekst wordt het woord “topniveaudomein” vervangen door het woord “topleveldomein”.
Art. 91. Dans le titre VI, chapitre 3, de la même loi, il est inséré un article 164/3, rédigé comme suit :	Art. 91. In titel VI, hoofdstuk 3, van dezelfde wet, wordt een artikel 164/3 ingevoegd, luidende:

« Art. 164/3. § 1 ^{er} . Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent les données d'enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d'une base de données spécialisée avec la diligence requise par le droit de l'Union en matière de protection des données pour ce qui concerne les données à caractère personnel.	“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 gegevensbescherming voor wat betreft gegevens die persoonsgegevens zijn.
§ 2. La base de données visée au paragraphe 1 ^{er} contient 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:	§ 2. De database bedoeld in paragraaf 1 bevat 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° le nom de domaine;	1° de domeinnaam;
2° la date d'enregistrement;	2° de registratiedatum;
3° le nom du titulaire, l'adresse de courrier électronique et le numéro de téléphone permettant de le contacter;	3° de naam, het e-mailadres en het telefoonnummer van de registrant;
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.	4° het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de registrant.
§ 3. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1 ^{er} contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.	§ 3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, beschikken over beleidslijnen en procedures, waaronder verificatieprocedures, om ervoor te zorgen dat de in paragraaf 1 bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden openbaar gemaakt.
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 de l'alinéa 1 ^{er} .	Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven, met het oog op de naleving van het eerste lid.
§ 4. 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	§ 4. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, maken de domeinnaamregistratiegegevens die geen

l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.	persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.
§ 5. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine donnent accès aux données spécifiques d'enregistrement de noms de domaine sur demande légitime et dûment motivée des demandeurs d'accès légitimes. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine répondent sans retard injustifié et en tout état de cause dans un délai de 72 heures après réception de toute demande d'accès. Les politiques et procédures de divulgation de ces données sont rendues publiques.	§ 5. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, verschaffen, op rechtmatig en naar behoren gemotiveerd verzoek van legitieme toegangsvragende partijen, toegang tot specifieke gegevens over de registratie van domeinnamen. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, beantwoorden verzoeken om toegang onverwijld en in elk geval binnen 72 uur na ontvangst van het verzoek. Het beleid en de procedures met betrekking tot de bekendmaking van deze gegevens worden openbaar gemaakt.
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, dans au moins une des langues nationales.	De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, stellen de verzoeker in staat om gemakkelijk, in ten minste één van de nationale talen, zijn verzoek in te dienen.
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 des alinéas 1 ^{er} et 2.	Het Instituut kan een register voor topleveldomeinnamen of een entiteit die domeinnaamregistratiediensten verleent bindende instructies geven, met het oog op de naleving van het eerste lid en het tweede lid.
Après avis de l'Institut, le Roi peut préciser qui est considéré comme demandeur d'accès légitime et à quelles données spécifiques d'enregistrement de noms de domaine il convient de donner accès.	De Koning kan, na advies van het Instituut, preciseren wie als legitieme toegangsvragende partij wordt beschouwd en tot welke specifieke gegevens over de registratie van domeinnamen toegang moet worden gegeven.
§ 6. Le respect des obligations visées au présent article n'entraîne pas de répétition inutile de la collecte des données d'enregistrement de noms de domaine. A 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.	§ 6. De naleving van de in dit artikel vastgestelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal moeten worden verzameld. Daartoe werken registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, met elkaar samen.
Après avis de l'Institut, le Roi peut préciser les modalités de cette coopération.	De Koning kan, na advies van het Instituut, de modaliteiten van deze samenwerking preciseren.
Section 6. Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de	Afdeling 6. Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en

la Directive 2014/65/UE	houdende omzetting van Richtlijn 2014/65/EU
Art. 92. A 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 supprimés.	Art. 92. In artikel 71 van de wet van 21 november 2017 over de infrastructuur 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 toezichtopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen" geschrapt.
Art. 93. L'article 79, § 4, de la même loi, inséré par la loi du 7 avril 2019, est abrogé.	Art. 93. Artikel 79, § 4, van dezelfde wet, ingevoegd bij de wet van 7 april 2019, wordt opgeheven.
Chapitre 3. Disposition abrogatoire	Hoofdstuk 3. Opheffingsbepaling
Art. 94. 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.	Art. 94. 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.
Chapitre 4. Entrée en vigueur	Hoofdstuk 4. Inwerkingtreding
Art. 95. La présente loi entre en vigueur le 18 octobre 2024.	Art. 95. Deze wet treedt in werking op 18 oktober 2024.

Le Premier Ministre,

De Eerste Minister,



Alexander De Croo

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, 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
		- Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		- Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		- 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
		- 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
		- 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
	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
	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
		- Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		- Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la

		directive 2009/73/CE
		- Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
		- Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		- Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/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 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, 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) no 1315/2013 du Parlement européen et du Conseil, 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) no 549/2004 du Parlement européen et du Conseil
	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
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, 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) no 725/2004 du Parlement européen et du Conseil, 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, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) no 725/2004, 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
	d) Transports routiers	Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission 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
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) no 575/2013 du Parlement européen et du Conseil
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
		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) no 648/2012 du Parlement européen et du Conseil
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
		Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil
		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
		Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21
		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
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, 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, 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 (interentreprises)		Fournisseurs de services gérés
		Fournisseurs de services de sécurité gérés
10. Administration publique		Entités de l'administration publique fédérale
		Entités de l'administration publique des entités fédérées, identifiés conformément à l'article 11, § 2 de la loi.
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
Bijlage I - Zeer kritieke sectoren - NL		
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, 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
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35, van Richtlijn (EU) 2019/944
		- Producenten zoals gedefinieerd in artikel 2, punt 38, van Richtlijn (EU) 2019/944
		- 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 die aggregatie verrichten of vraagresponsof energieopslagdiensten verstrekken zoals gedefinieerd in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944
		- 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
	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
	d) Aardgas	- Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad
		- Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG
		- Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG
		- Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG
		- LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG

		- Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG
	e) Waterstof	- Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas - 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 die voor commerciële doeleinden worden gebruikt
		- Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad, 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 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 aanbieden
	b) Spoor	- Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad
		- Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, 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 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, inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; 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
	d) Weg	<ul style="list-style-type: none"> - Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie 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
3. Bankwezen		<ul style="list-style-type: none"> - Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad
4. Infrastructuur voor de financiële markt		<ul style="list-style-type: none"> - Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad - Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad
5. Gezondheidszorg		<ul style="list-style-type: none"> - Zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad - EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad 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 - Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 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
6. Drinkwater		<ul style="list-style-type: none"> - 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, 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 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
8. Digitale infrastructuur		- Aanbieders van internetknooppunten
		- DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		- Register voor topleveldomeinnamen
		- Aanbieders van cloudcomputingdiensten
		- Aanbieders van datacenterdiensten
		- 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		- Federale overheidsinstanties
		- Gefedereerde overheidsinstanties die worden geïdentificeerd overeenkomstig artikel 11, §2.
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 elektronische communicatienetwerken

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, 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, 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) no 1907/2006 du Parlement européen et du Conseil 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) no 178/2002 du Parlement européen et du Conseil qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles
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 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, 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 dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de transport	- Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30

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
Bijlage II - Andere kritieke sectoren		
Sector	Deel-sector	Soort entiteit
1. Post- en koeriersdiensten		- Aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1 bis, van Richtlijn 97/67/EG, 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, met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is
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 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 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 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 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 sectie C, afdeling 26, van NACE Rev. 2
	c) Vervaardiging van elektrische	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C,

	apparatuur	afdeling 27, van NACE Rev. 2
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	e) Vervaardiging van motorvoertuigen, aanhangers en opleggers	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	f) Vervaardiging van andere transportmiddelen	- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2
6. Digitale aanbieders		- Aanbieders van onlinemarktplaatsen
		- Aanbieders van onlinezoekmachines
		- Aanbieders van platforms voor socialenetwerkdiensten
7. Onderzoek		- Onderzoeksorganisaties

Le Premier Ministre,

De Eerste Minister,



Alexander De Croo

EXPOSÉ DES MOTIFS	MEMORIE VAN TOELICHTING
Mesdames, Messieurs,	Dames en Heren,
EXPOSÉ GÉNÉRAL	ALGEMENE TOELICHTING
Ce projet de loi vise à transposer 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, dénommée ci-après la « directive NIS2 ».	Dit wetsontwerp voorziet in de omzetting van 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, hierna "NIS2-richtlijn" genoemd.
La directive NIS2 remplace la directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après la « directive NIS1 », laquelle a été transposée en Belgique par 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 (ci-après, la « loi NIS1 »).	De NIS2-richtlijn vervangt Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna "NIS1-richtlijn" genoemd, die in België werd omgezet door 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 (hierna "NIS1-wet" genoemd).
La directive NIS2 fixe, d'une part, des obligations en ce qui concerne les politiques nationales en matière de cybersécurité et, d'autre part, impose pour certaines entités des exigences en matière de gestion des risques de cybersécurité et de notification des incidents.	De NIS2-richtlijn stelt enerzijds verplichtingen vast wat betreft het nationaal cyberbeveiligingsbeleid, en legt anderzijds bepaalde entiteiten eisen op met betrekking tot het beheer van cyberbeveiligingsrisico's en de melding van incidenten.
En ce qui concerne les politiques nationales, il s'agit notamment de la stratégie nationale en matière de cybersécurité, des cadres nationaux de gestion des crises cyber, des tâches des autorités compétentes et de la coopération nationale.	Wat het nationaal beleid betreft, gaat het met name om de nationale cyberbeveiligingsstrategie, nationale kaders voor cybercrisisbeheer, de taken van de bevoegde autoriteiten en de nationale samenwerking.
Au sens de la directive, la cybersécurité est définie comme « les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces ».	In de zin van de richtlijn wordt cyberbeveiliging gedefinieerd als "de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen".
Les réseaux et systèmes d'information sont devenus des caractéristiques essentielles de	Netwerk- en informatiesystemen hebben zich ontwikkeld tot centrale kenmerken van ons

notre vie quotidienne en raison de la transformation numérique rapide et de l'interconnexion de la société.	dagelijks leven door de snelle digitale transformatie en de onderlinge verbondenheid van de samenleving.
Cette évolution a conduit à une expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices.	Die ontwikkeling heeft geleid tot een uitbreiding van het cyberdreigingslandschap, wat nieuwe uitdagingen met zich meebrengt, die een aangepaste, gecoördineerde en innovatieve respons vereisen.
La cybersécurité constitue ainsi une matière propre, avec des règles générales communes et cohérentes applicables à tous les réseaux et systèmes d'information, indépendamment du domaine d'activités dans lesquels ceux-ci sont utilisés. En effet, il existe des menaces communes (indisponibilité, modification, vol ou perte des données, non-respect de la confidentialité ou de l'authenticité, etc.) à tous les réseaux et systèmes d'information. Il existe ainsi des normes techniques internationales en matière de sécurité de l'information générales et transversales à tous les secteurs (par exemple, les normes de la famille ISO/IEC 27000, les Center for Internet Security (CIS) Controls ou encore le National Institute of Standards and Technology (NIST) Cybersecurity framework).	Cyberbeveiliging is dus een specifieke aangelegenheid, met gemeenschappelijke en coherente algemene regels die van toepassing zijn op alle netwerk- en informatiesystemen, ongeacht het werkkterrein waarop deze worden gebruikt. Er zijn immers dreigingen (onbeschikbaarheid, wijziging, diefstal of verlies van gegevens, niet-naleving van de vertrouwelijkheid of authenticiteit, enz.) die alle netwerk- en informatiesystemen gemeen hebben. Daarom bestaan er algemene, sectoroverschrijdende internationale technische normen voor informatiebeveiliging (bijvoorbeeld, de ISO/IEC 27000 normenreeks, de Center for Internet Security (CIS) Controls of het National Institute of Standards and Technology (NIST) Cybersecurity framework).
Le nombre, l'ampleur, la sophistication, la fréquence et l'impact des cyberincidents ne cessent de croître et représentent une menace considérable pour le bon fonctionnement de certaines activités sociétales ou économiques critiques ou encore des services publics.	Het aantal, de omvang, de complexiteit, de frequentie en de impact van cyberincidenten nemen toe en vormen een grote bedreiging voor de goede werking van sommige kritieke maatschappelijke of economische activiteiten of van openbare diensten.
Dans le prolongement de la directive NIS1, les entités concernées par la directive NIS2 ne sont pas toutes les organisations établies en Belgique mais bien celles fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques en Belgique, spécifiées dans les annexes de la directive « secteurs hautement critiques » (annexe 1) ou « autres secteurs critiques » (annexe 2).	In het verlengde van de NIS1-richtlijn omvatten de entiteiten die onder de NIS2-richtlijn vallen niet alle in België gevestigde organisaties, maar wel degene die diensten verlenen die essentieel zijn voor de instandhouding van kritieke maatschappelijke of economische activiteiten in België, zoals gespecificeerd in de bijlagen bij de richtlijn "zeer kritieke sectoren" (bijlage 1) of "andere kritieke sectoren" (bijlage 2).
Là où la directive NIS1 prévoyait une procédure nationale d'identification des opérateurs de services essentiels, la directive NIS2 utilise désormais l'activité exercée au sein de l'une de	Terwijl de NIS1-richtlijn voorzag in een nationale procedure voor de identificatie van aanbieders van essentiële diensten, gebruikt de NIS2-richtlijn de activiteit die wordt uitgevoerd

ses annexes et la taille de l'entité comme critères pour déterminer si celle-ci entre ou non dans le champ d'application.	binnen een van de bijlagen ervan en de omvang van de entiteit als criteria om te bepalen of deze al dan niet onder het toepassingsgebied valt.
L'objectif demeure néanmoins toujours de protéger les entités fournissant un service essentiel au maintien d'activités sociétales ou économiques critiques dans des domaines tels que l'énergie, le transport, la santé, l'eau potable les infrastructures numériques, l'espace, les fournisseurs de services de technologie de l'information et de la communication ou encore l'administration publique. Indépendamment de la taille de l'organisation, la directive prévoit d'ailleurs que les Etats membres doivent inclure également au niveau national certaines entités en raison du caractère critique du service essentiel fourni, du risque systémique important ou encore de l'impact important sur la sécurité publique.	Niettemin is het doel nog steeds om entiteiten te beschermen die een dienst verlenen die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten op gebieden zoals energie, vervoer, gezondheid, drinkwater, digitale infrastructuur, ruimtevaart, aanbieders van ICT-diensten of het overheidsbestuur. Ongeacht de omvang van de organisatie verplicht de richtlijn lidstaten ook om bepaalde entiteiten op nationaal niveau op te nemen vanwege de kritieke aard van de verleende essentiële dienst, het aanzienlijke systeemrisico of de aanzienlijke gevolgen voor de openbare veiligheid.
En ce qui concerne les mesures de gestion des risques en matière de cybersécurité, les entités concernées devront notamment assurer la prise de mesures adaptées aux risques encourus, en tenant 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, au regard des éventuelles conséquences sociétales et économiques.	Wat betreft de maatregelen voor het beheer van cyberbeveiligingsrisico's moeten de betrokken entiteiten er met name voor zorgen dat maatregelen worden genomen die zijn afgestemd op de risico's, waarbij rekening wordt 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, in het licht van de mogelijke maatschappelijke en economische gevolgen.
La directive prévoit la notification aux autorités compétentes des incidents significatifs afin d'atténuer leur propagation potentielle, de permettre aux entités de chercher de l'aide, de gérer au mieux les situations de crises et de partager les informations techniques pertinentes avec les autres entités.	De richtlijn voorziet in de melding van significante incidenten aan de bevoegde autoriteiten om de potentiële verspreiding ervan te beperken, entiteiten in staat te stellen bijstand te vragen, crisissituaties zo goed mogelijk te beheren en relevante technische informatie met andere entiteiten te delen.
Comme exposé ci-avant, des obligations de la directive NIS2 ne s'appliquent qu'à un nombre limité d'entités faisant partie de secteurs critiques et fournissant des services d'intérêt général pour la population et les entreprises, ou critiques pour le potentiel économique du pays.	Zoals hierboven uiteengezet, zijn de verplichtingen van de NIS2-richtlijn alleen van toepassing op een beperkt aantal entiteiten die deel uitmaken van kritieke sectoren en diensten van algemeen belang verlenen voor de bevolking en de ondernemingen, of kritiek zijn voor het economisch potentieel van ons land.
Le contenu de la directive ne règle pas la	De inhoud van de richtlijn regelt de

matière de la cybersécurité dans un domaine spécifique mais impose la prise de mesures minimales destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union pour certaines entités fournissant des services essentiels.	aangelegenheid cyberbeveiliging niet op een specifiek gebied, maar legt minimummaatregelen op voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie voor bepaalde entiteiten die essentiële diensten leveren.
Un cyberincident est, en effet, susceptible de provoquer des perturbations opérationnelles graves de ces services essentiels et d'affecter des personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables. Un incident, peut, par exemple, avoir pour conséquence de rendre inopérante la distribution d'électricité ou de rendre indisponibles des services de transport. En ce qu'ils affectent des acteurs essentiels de secteurs clés, en ce compris les pouvoirs publics, ces incidents constituent des menaces graves pour la sécurité publique. Les obligations de la directive relèvent dès lors en droit belge du domaine de la sécurité publique.	Een cyberincident kan immers een ernstige operationele verstoring van deze essentiële diensten veroorzaken en natuurlijke personen of rechtspersonen treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Een incident kan er bijvoorbeeld toe leiden dat de elektriciteitsdistributie buiten werking wordt gesteld of vervoersdiensten niet meer beschikbaar zijn. Aangezien deze incidenten essentiële spelers in sleutelsectoren, waaronder overheden, treffen, vormen ze een ernstige bedreiging voor de openbare veiligheid. Bijgevolg vallen de verplichtingen van de richtlijn in Belgisch recht onder de openbare veiligheid.
Comme la directive NIS1, la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral (voir notamment les avis du Conseil d'Etat n°63.296/4 du 2 mai 2018 sur l'avant-projet devenu la loi NIS1 et n°48 989/VR du 9 décembre 2010 relatif à un avant-projet de loi devenue la loi du 1 ^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques).	Net als de NIS1-richtlijn leidt de omzetting van deze richtlijn hoofdzakelijk tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort (zie met name de adviezen van de Raad van State nr. 63.296/4 van 2 mei 2018 over het voorontwerp dat de NIS1-wet is geworden en nr. 48 989/VR van 9 december 2010 over een voorontwerp van wet dat de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur is geworden).
La circonstance que le fondement juridique de la directive en droit européen repose sur des considérations relatives au bon fonctionnement du marché intérieur ne détermine pas la matière au sens du niveau national qui est réglée par le contenu de celle-ci. Or, c'est en fonction de cette matière uniquement qu'il convient de s'interroger sur le niveau de pouvoir compétent, en droit interne, pour légiférer dans cette matière et, partant, pour transposer la directive. La mise en œuvre de mesures communes	Het feit dat de rechtsgrond van de richtlijn in Europees recht is gebaseerd op overwegingen die verband houden met de goede werking van de interne markt, bepaalt niet welke aangelegenheid in de zin van het nationaal recht door de inhoud van deze richtlijn wordt geregeld. Het is echter enkel in functie van deze aangelegenheid dat men zich moet afvragen welk beleidsniveau in nationaal recht bevoegd is om ter zake wetgeving vast te stellen en dus om de richtlijn om te zetten. De uitvoering van minimale gemeenschappelijke cyberbeveiligingsmaatregelen op nationaal

minimales de cybersécurité au niveau national pour certaines entités critiques constitue avant tout des mesures de protection de la population et des entreprises du pays. La continuité des échanges économiques au sein du marché intérieur n'est qu'une conséquence indirecte de ces mesures de protection. (...)	niveau voor bepaalde kritieke entiteiten is in de eerste plaats een middel om de bevolking en ondernemingen van ons land te beschermen. De continuïteit van het economisch verkeer in de interne markt is slechts een onrechtstreeks gevolg van deze beschermingsmaatregelen. (...)
Il faut en conclure que la transposition de la directive NIS2, qui vise à définir des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné en matière de cybersécurité, relève de la compétence générale de la sécurité publique de l'Etat fédéral.	Hieruit moet worden besloten dat de omzetting van de NIS2-richtlijn, die tot doel heeft minimumvoorschriften vast te stellen voor de werking van een gecoördineerd regelgevingskader op het gebied van cyberbeveiliging, onder de algemene bevoegdheid inzake openbare veiligheid van de Federale Staat valt.
L'exercice de la compétence fédérale dans le projet de loi reste, en tout état de cause, proportionné et n'a pas pour conséquence de rendre impossible ou exagérément difficile l'exercice normal des compétences régionales ou communautaires dans les domaines d'activités de certaines entités essentielles ou importantes concernées. D'ailleurs, il est prévu dans le projet de loi de consulter, de manière facultative et en manière telle que leur éventuelle abstention de collaborer n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale, les entités fédérées lorsque certaines entités seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires.	De uitoefening van de federale bevoegdheid in het wetsontwerp blijft in elk geval in verhouding en heeft niet tot gevolg dat het voor de gewesten of gemeenschappen onmogelijk of bovenmatig moeilijk zou zijn om hun bevoegdheden op de werkterreinen van sommige betrokken essentiële of belangrijke entiteiten gewoon uit te oefenen. Bovendien bepaalt het wetsontwerp dat de deelgebieden worden geraadpleegd wanneer sommige entiteiten voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsregels. Deze raadpleging is facultatief en gebeurt op een zodanige wijze dat, indien de deelgebieden verzuimen om mee te werken, dit niet verhindert dat de federale overheid de voorgenomen maatregelen kan nemen.
La directive NIS2 doit être transposée en droit belge pour le 17 octobre 2024 au plus tard et être applicable le 18 octobre 2024.	De NIS2-richtlijn moet uiterlijk op 17 oktober 2024 omgezet zijn in Belgisch recht en moet van toepassing zijn op 18 oktober 2024.
COMMENTAIRES DES ARTICLES	ARTIKELSGEWIJZE TOELICHTING
TITRE 1^{er}	TITEL 1
<i>Définitions et dispositions générales</i>	<i>Definities en algemene bepalingen</i>
CHAPITRE 1^{er}	HOOFDSTUK 1
Objet et champ d'application	Onderwerp en toepassingsgebied

Section 1^{ère}	Afdeling 1
<i>Objet</i>	<i>Onderwerp</i>
Article 1 ^{er}	Artikel 2
Cet article précise le fondement constitutionnel du présent projet de loi.	Dit artikel bevat de grondwettelijke grondslag van dit wetsontwerp.
Article 2	Artikel 2
Cet article précise la directive transposée par la loi, à savoir la directive NIS2.	Dit artikel vermeldt de richtlijn die door de wet wordt omgezet, namelijk de NIS2-richtlijn.
Article 3	Artikel 3
Cet article définit le champ d'application personnel du présent projet de loi.	Dit artikel bepaalt het personele toepassingsgebied van dit wetsontwerp.
Le paragraphe 1 ^{er} établit le principe selon lequel les entités reprises aux annexes qui constituent des entreprises moyennes au sens de la recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (ci-après, la « recommandation UE 2003/361 ») ou qui dépassent le plafond établi à l'article 2 de l'annexe de ladite recommandation rentrent dans le champ d'application du présent projet de loi.	Paragraaf 1 stelt het beginsel vast volgens hetwelk de in de bijlagen opgenomen entiteiten die middelgrote ondernemingen zijn als bedoeld in de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (hierna "EU-aanbeveling 2003/361") of die het in artikel 2 van de bijlage bij deze aanbeveling vastgestelde plafond overschrijden, onder het toepassingsgebied van dit wetsontwerp vallen.
Le paragraphe 2 permet à l'autorité nationale de cybersécurité de prendre en compte le degré d'indépendance d'une organisation, vis-à-vis d'éventuelles entreprises partenaires ou d'entreprises liées au sens de l'annexe de la recommandation 2003/361/CE.	Op grond van paragraaf 2 kan de nationale cyberbeveiligingsautoriteit rekening houden met de mate van onafhankelijkheid van een organisatie ten opzichte van eventuele partnerondernemingen of verbonden ondernemingen als bedoeld in de bijlage bij Aanbeveling 2003/361/EG.
En effet, le considérant 16 de la directive précise que « afin d'éviter que des entités ayant des entreprises partenaires ou des entreprises liées ne soient considérées comme des entités essentielles ou importantes lorsque cela serait disproportionné, les États membres sont en mesure de tenir compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées lorsqu'ils appliquent l'article 6, paragraphe 2, de l'annexe de la recommandation	Overweging 16 van de richtlijn stelt immers het volgende: "Om te voorkomen dat entiteiten met partnerondernemingen of verbonden ondernemingen als essentiële of belangrijke entiteiten worden beschouwd wanneer dit onevenredig zou zijn, kunnen de lidstaten bij de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling 2003/361/EG rekening houden met de mate van onafhankelijkheid welke die entiteiten ten opzichte van hun partnerondernemingen of verbonden

2003/361/CE. En particulier, les États membres sont en mesure de tenir compte du fait qu'une entité est indépendante de son partenaire ou d'entreprises liées en ce qui concerne le réseau et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit. Sur cette base, s'il y a lieu, les États membres peuvent considérer qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation 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 ».	ondernemingen genieten. Meer bepaald kunnen de lidstaten rekening houden met het feit dat een entiteit onafhankelijk is van haar partnerondernemingen of verbonden ondernemingen wat de netwerk- en informatiesystemen betreft waarvan die entiteit gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die de entiteit verleent. Op basis daarvan kunnen de lidstaten een dergelijke entiteit in voorkomend geval beschouwen als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 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."
L'article 3 de l'annexe de la Recommandation UE 2003/361 définit les entreprises liées comme les entreprises qui entretiennent entre elles l'une des relations suivantes :	In artikel 3 van de bijlage bij Aanbeveling EU 2003/361 worden verbonden ondernemingen gedefinieerd als ondernemingen die met elkaar een van de volgende banden onderhouden:
a) une entreprise a la majorité des droits de vote des actionnaires ou associés d'une autre entreprise;	a) een onderneming heeft de meerderheid van de stemrechten van de aandeelhouders of vennoten van een andere onderneming;
b) une entreprise a le droit de nommer ou de révoquer la majorité des membres de l'organe d'administration, de direction ou de surveillance d'une autre entreprise;	b) een onderneming heeft het recht de meerderheid van de leden van het bestuurs-, leidinggevend of toezichhoudend orgaan van een andere onderneming te benoemen of te ontslaan;
c) une entreprise a le droit d'exercer une influence dominante sur une autre entreprise en vertu d'un contrat conclu avec celle-ci ou en vertu d'une clause des statuts de celle-ci;	c) een onderneming heeft het recht een overheersende invloed op een andere onderneming uit te oefenen op grond van een met deze onderneming gesloten overeenkomst of een bepaling in de statuten van laatstgenoemde onderneming;
d) une entreprise actionnaire ou associée d'une autre entreprise contrôle seule, en vertu d'un accord conclu avec d'autres actionnaires ou associés de cette autre entreprise, la majorité	d) een onderneming die aandeelhouder of vennoot is van een andere onderneming, heeft op grond van een met andere aandeelhouders of vennoten van die andere onderneming

des droits de vote des actionnaires ou associés de celle-ci.	gesloten overeenkomst als enige zeggenschap over de meerderheid van de stemrechten van de aandeelhouders of vennoten van laatstgenoemde onderneming.
Sauf certaines exceptions, l'article 3 de l'annexe de la Recommandation UE 2003/361 qualifie d'« entreprises partenaires » toutes les entreprises qui ne sont pas qualifiées comme entreprises liées et qui entre lesquelles existe la relation suivante: une entreprise (entreprise en amont) détient, seule ou conjointement avec une ou plusieurs entreprises liées, 25 % ou plus du capital ou des droits de vote d'une autre entreprise (entreprise en aval).	Behoudens bepaalde uitzonderingen kwalificeert artikel 3 van de bijlage bij Aanbeveling EU 2003/361 als "partnerondernemingen" alle ondernemingen die niet als verbonden ondernemingen worden aangemerkt en waartussen de volgende band bestaat: een onderneming (van een hoger niveau) heeft, alleen of samen met een of meer verbonden ondernemingen, 25 % of meer van het kapitaal of de stemrechten van een andere onderneming (van een lager niveau).
Le mécanisme envisagé permettrait ainsi de qualifier une entité d'importante (plutôt qu'essentielle) ou de l'exclure du champ d'application lorsque l'entreprise petite ou moyenne fait partie d'un groupe d'entreprises (liées ou partenaires) mais utilise des réseaux ou des systèmes d'information indépendants de ces autres entreprises pour fournir ses services dans l'Union européenne et que l'application des règles du calcul de la taille de l'entreprise (consolidation des chiffres d'affaires et des membres du personnel entre entreprises) s'avère disproportionnée.	Het bedoelde mechanisme zou het aldus mogelijk maken een entiteit als belangrijk (in plaats van essentieel) aan te merken of van het toepassingsgebied uit te sluiten, indien de kleine of middelgrote onderneming deel uitmaakt van een groep van ondernemingen (verbonden ondernemingen of partnerondernemingen), maar gebruik maakt van netwerk- of informatiesystemen die onafhankelijk zijn van deze andere ondernemingen om haar diensten in de Europese Unie te verlenen en de toepassing van de regels voor de berekening van de grootte van de onderneming (consolidatie van de omzet en personeelsleden tussen ondernemingen) onevenredig blijkt.
Au besoin, il est prévu que le Roi peut déterminer les critères précis sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.	Indien nodig is voorzien dat de Koning de precieze criteria kan bepalen op basis waarvan de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen en verbonden ondernemingen wordt beoordeeld.
Les paragraphes 3 à 5 de cette disposition établissent les exceptions au principe établi au paragraphe 1 ^{er} au travers desquelles la loi s'applique à certains types d'entités, quelle que soit leur taille.	De paragrafen 3 tot 5 van deze bepaling stellen de uitzonderingen vast op het in paragraaf 1 bepaalde beginsel waardoor de wet van toepassing is op bepaalde soorten entiteiten, ongeacht hun omvang.
Le dernier paragraphe donne la compétence au Roi d'ajouter des secteurs ou sous-secteurs aux annexes I et II du présent projet de loi. De cette manière, lorsqu'il apparaît, dans le futur, qu'un	De laatste paragraaf geeft de Koning de bevoegdheid om sectoren of deelsectoren toe te voegen aan bijlage I en II van dit wetsontwerp. Op die manier kunnen de bijlagen

secteur ne se trouvant pas encore dans le champ d'application du présent projet de loi devrait y être intégré, en raison de son importance pour des activités sociétales et/ou économiques critiques, les annexes pourront être étendues.	worden uitgebreid wanneer in de toekomst blijkt dat een sector die nog niet onder het toepassingsgebied van dit wetsontwerp valt, daarin moet worden opgenomen wegens zijn belang voor kritieke maatschappelijke en/of economische activiteiten.
Article 4	Artikel 4
Cette disposition définit le champ d'application territorial du présent projet de loi.	Deze bepaling omschrijft het territoriale toepassingsgebied van dit wetsontwerp.
Le paragraphe 1 ^{er} établit le principe selon lequel la loi s'applique aux entités qui sont établies en Belgique et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.	Paragraaf 1 legt het beginsel vast dat de wet van toepassing is op entiteiten die in België zijn gevestigd en die hun diensten verlenen of hun activiteiten verrichten in de Europese Unie.
Conformément au considérant 114 de la directive NIS2, « le critère d'établissement aux fins de la présente directive suppose l'exercice effectif d'une activité au moyen d'une installation stable ».	Overeenkomstig overweging 114 van de NIS2-richtlijn houdt "het vestigingscriterium voor de toepassing van deze richtlijn [...] de daadwerkelijke uitoefening van de activiteit in door middel van stabiele regelingen".
Le paragraphe 2 prévoit des exceptions par rapport à certains types d'entités, pour lesquels la loi s'applique soit lorsqu'ils fournissent leurs services en Belgique, soit lorsqu'ils ont leur établissement principal en Belgique (notion d'établissement principal à ne pas confondre avec la notion d'établissement reprise au paragraphe 1 ^{er}).	Paragraaf 2 voorziet in uitzonderingen bij bepaalde soorten entiteiten, waarvoor de wet van toepassing is wanneer zij hun diensten in België verlenen of wanneer zij hun hoofdvestiging in België hebben (het begrip "hoofdvestiging" mag niet worden verward met het begrip "vestiging" in paragraaf 1).
Le paragraphe 3 prévoit qu'une entité qui n'est pas établie dans l'Union européenne mais y fournit des services désigne un représentant dans l'Union.	Paragraaf 3 bepaalt dat een entiteit die niet in de Europese Unie is gevestigd maar er diensten verleent, een vertegenwoordiger in de Unie aanwijst.
Les paragraphes 4 et 5 prévoient un système en cascade permettant de déterminer si une entité a son établissement principal en Belgique ou non.	De paragrafen 4 en 5 voorzien in een cascadesysteem om te bepalen of een entiteit haar hoofdvestiging al dan niet in België heeft.
Article 5	Artikel 5
Cet article précise certaines exceptions et exclusions au champ d'application du présent projet de loi.	Dit artikel bepaalt een aantal uitzonderingen en uitsluitingen van het toepassingsgebied van dit wetsontwerp.
La disposition précise que la loi ne porte pas préjudice à l'application du RGPD, aux lois et	De bepaling verduidelijkt dat de wet geen afbreuk doet aan de toepassing van de AVG,

<p>règlements qui le complètent ou le précisent ainsi qu'à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.</p>	<p>aan de wetten en reglementen die deze aanvullen of verduidelijken of aan de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.</p>
<p>Il est aussi rappelé que les dispositions du présent projet de loi ne portent pas préjudice à l'application de certaines autres dispositions légales, dont celles relatives au traitement des informations classifiées au sens 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 ainsi que les 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. Par ailleurs, la présente loi ne porte pas préjudice à la loi du 5 août 1992 sur la fonction de police.</p>	<p>Tevens wordt erop gewezen dat de bepalingen van dit wetsontwerp geen afbreuk doen aan de toepassing van een aantal andere wettelijke bepalingen, waaronder die betreffende de verwerking van geclassificeerde informatie als bedoeld in de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, en de regels die van toepassing zijn op nucleaire documenten als bedoeld in de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle. Bovendien doet deze wet geen afbreuk aan de wet van 5 augustus 1992 op het politieambt.</p>
<p>Par exemple, si certaines informations qui doivent être échangées en application du projet de loi sont classifiées en tout ou en partie en vertu de la loi du 11 décembre 1998 précitée, cette dernière et ses actes d'exécution demeurent entièrement applicables.</p>	<p>Indien bijvoorbeeld bepaalde informatie die overeenkomstig het wetsontwerp moet worden uitgewisseld, volledig of gedeeltelijk geclassificeerd is krachtens voornoemde wet van 11 december 1998, blijven de laatstgenoemde wet en de uitvoeringsbesluiten ervan volledig van toepassing.</p>
<p>Par ailleurs, les systèmes de communication et d'information approuvés pour utiliser des informations classifiées sous forme électronique dans le cadre de la loi précitée ne sont pas soumis aux dispositions du présent projet de loi, notamment en matière de mesures de gestion des risques en matière de cybersécurité. Cela a pour conséquence que certaines entités seront soumises au projet de loi et devront appliquer les dispositions de la présente loi à leurs réseaux et systèmes d'information, à l'exclusion des systèmes de communication et d'information approuvés dans le cadre de la loi précitée du 11 décembre 1998. Cette exception au champ d'application ne permet pas à une entité d'être</p>	<p>Bovendien zijn communicatie- en informatiesystemen die in het kader van voornoemde wet zijn goedgekeurd om geclassificeerde informatie in elektronische vorm te gebruiken, niet onderworpen aan de bepalingen van dit wetsontwerp, met name wat betreft de maatregelen voor het beheer van cyberbeveiligingsrisico's. Bijgevolg zullen bepaalde entiteiten onderworpen zijn aan het wetsontwerp en zullen zij de bepalingen van deze wet moeten toepassen op hun netwerk- en informatiesystemen, met uitzondering van de communicatie- en informatiesystemen die in het kader van voornoemde wet van 11 december 1998 goedgekeurd zijn. Deze uitzondering op het toepassingsgebied laat niet</p>

complètement exclue du champ d'application. Elle permet, du point de vue du champ d'application matériel, d'exclure ces systèmes approuvés des obligations en matière d'analyses des risques, de mesures de sécurité à adopter, de notifications, etc.	toe dat een entiteit hiervan volledig wordt uitgesloten. Wat het materiële toepassingsgebied betreft, laat ze toe dat deze goedgekeurde systemen worden uitgesloten van de verplichtingen met betrekking tot risicoanalyses, te nemen beveiligingsmaatregelen, meldingen, enz.
Le paragraphe 4 précise que les dispositions du présent projet de loi ne s'appliquent pas à certaines administrations publiques ou entités limitativement énumérées car elles exercent des activités principalement dans les domaines de la sécurité nationale, de la sécurité publique, de la justice ou de la défense. L'article 2, § 7 et 8 de la directive exclut effectivement de son champ d'application les entités de l'administration publique ou des entités spécifiques qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense, ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière, pour autant qu'ils ne constituent pas des prestataires de services de confiance (l'article 2, § 9, de la directive).	Paragraaf 4 verduidelijkt dat de bepalingen van dit wetsontwerp niet van toepassing zijn op bepaalde limitatief opgesomde overheidsinstanties of entiteiten omdat deze hoofdzakelijk activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, justitie of defensie. Artikel 2, lid 7 en 8, van de richtlijn sluit overheidsinstanties of specifieke entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, inderdaad uit van het toepassingsgebied, voor zover zij geen aanbieders van vertrouwensdiensten zijn (artikel 2, lid 9, van de richtlijn).
En son article 2, § 6, la directive rappelle également qu'elle est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public.	Tevens wijst artikel 2, lid 6, van de richtlijn erop dat de richtlijn de verantwoordelijkheid van de lidstaten om de nationale veiligheid te beschermen en hun bevoegdheid om andere essentiële staatsfuncties te beschermen, waaronder het verdedigen van de territoriale integriteit van de staat en het handhaven van de openbare orde, onverlet laat.
Dans le même contexte, il est prévu d'exclure les 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. Ceux-ci sont soumis à des exigences nationales et internationales spécifiques, sous le contrôle de l'Agence fédérale de contrôle nucléaire. A l'instar de la loi NIS actuelle, il est néanmoins prévu que les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de	In dezelfde context wordt voorzien in een uitsluiting van inrichtingen van klasse I als bedoeld in 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. Deze zijn onderworpen aan specifieke nationale en internationale eisen, onder toezicht van het Federaal Agentschap voor Nucleaire Controle. Net als in de huidige NIS-wet wordt niettemin bepaald dat de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de

L'électricité demeurent eux soumis à la présente loi.	transmissie van de elektriciteit, onderworpen blijven aan deze wet.
Le paragraphe exclut aussi les réseaux et systèmes d'information des missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne, dès lors que les règles de la directive ne s'appliquent pas à ceux-ci, comme le mentionne le considérant 8 de la directive.	In de paragraaf worden tevens de netwerk- en informatiesystemen van Belgische diplomatieke en consulaire missies in landen buiten de Europese Unie uitgesloten, aangezien de regels van de richtlijn hierop niet van toepassing zijn, zoals vermeld in overweging 8 van de richtlijn.
L'exclusion des mesures de gestion des risques en matière de cybersécurité, de notification des incidents et de supervision du présent projet de loi ne signifie pas que les administrations et entités concernées ne doivent pas mettre en œuvre des mesures de cybersécurité. Compte tenu de leur caractère critique, ces administrations doivent au contraire atteindre un niveau équivalent, voire supérieur aux exigences minimales imposées aux entités essentielles.	Het feit dat de betrokken overheidsinstanties en entiteiten worden uitgesloten van de maatregelen van dit wetsontwerp voor het beheer van cyberbeveiligingsrisico's, de melding van incidenten en het toezicht, betekent niet dat zij geen cyberbeveiligingsmaatregelen moeten nemen. Gelet op hun kritieke aard moeten deze overheidsinstanties integendeel een gelijkwaardig of zelfs hoger niveau bereiken dan het basisniveau dat aan essentiële entiteiten wordt opgelegd.
Comme cela est déjà le cas actuellement, les cyberincidents significatifs (pour autant qu'ils ne concernent pas des réseaux et systèmes d'information approuvés pour traiter des informations classifiées) sont notifiés au Centre pour la Cybersécurité Belgique (ci-après, CCB), dans le respect des exigences liées à la sécurité nationale et du plan national d'urgence cyber, selon des modalités particulières.	Zoals momenteel al het geval is, worden significante cyberincidenten (voor zover ze geen betrekking hebben op netwerk- en informatiesystemen die zijn goedgekeurd om geclassificeerde informatie te verwerken) gemeld aan het Centrum voor Cybersecurity België (hierna CCB), met inachtneming van de eisen in verband met de nationale veiligheid en het nationaal cybernoodplan, volgens bijzondere modaliteiten.
En outre, les activités les plus sensibles des administrations précitées sont réalisées au moyen des réseaux et systèmes approuvés pour traiter des informations classifiées.	Bovendien worden de meest gevoelige activiteiten van voornoemde overheidsinstanties uitgevoerd door middel van netwerken en systemen die zijn goedgekeurd voor de verwerking van geclassificeerde informatie.
Selon le paragraphe 5 les titres 3 à 5 du présent projet de loi ne sont pas applicables au NCCN et au CCB. Il demeure nécessaire de rendre applicables à ces administrations publiques certaines parties du présent projet de loi, à savoir les titres 1 ^{er} « Définitions et dispositions générales », 2 « Autorités compétentes et coopération au niveau national », 6	Volgend paragraaf 5 zijn titels 3 tot 5 niet van toepassing op het NCCN en het CCB. Het is echter nog steeds noodzakelijk om bepaalde delen van dit wetsontwerp toepasselijk te maken op deze overheidsinstanties, namelijk titel 1 "Definities en algemene bepalingen", titel 2 "Bevoegde autoriteiten en samenwerking op nationaal niveau", titel 6 "Verwerking van

« Traitement des données à caractère personnel » et 7 « Dispositions finales ». Ces dispositions s'avèrent, en effet, nécessaires pour permettre l'échange d'informations, notamment sur les notifications d'incidents, et la coopération (en ce compris le traitement de données à caractère personnel).	persoonsgegevens" en titel 7 "Slotbepalingen". Deze bepalingen zijn immers nodig om de uitwisseling van informatie, met name over meldingen van incidenten, en de samenwerking (met inbegrip van de verwerking van persoonsgegevens) mogelijk te maken.
Les autorités relevant des pouvoirs judiciaires et législatifs ne sont pas mentionnées dans cette disposition car elles ne sont pas incluses dans la notion d'entité de l'administration publique.	Autoriteiten van de rechterlijke en wetgevende macht worden in deze bepaling niet vermeld, omdat zij niet onder het begrip "overheidsinstantie" vallen.
Article 6	Artikel 6
Cet article, qui transpose l'article 4 de la directive NIS2, prévoit un mécanisme permettant de déroger à certaines dispositions de la loi lorsque des instruments juridiques sectoriels de l'Union européenne prévoient des mesures de gestion des risques en matière de cybersécurité et/ou des mesures en matière de notification d'incidents significatifs et que ces mesures ont un effet au moins équivalent à celui des obligations du présent projet de loi. Le paragraphe 2 de cet article précise ce qu'il faut entendre par effet équivalent.	Dit artikel, dat voorziet in de omzetting van artikel 4 van de NIS2-richtlijn, stelt een mechanisme vast om af te wijken van sommige bepalingen van de wet indien sectorspecifieke rechtsinstrumenten van de Europese Unie voorzien in maatregelen voor het beheer van cyberbeveiligingsrisico's en/of maatregelen voor de melding van significante incidenten en deze maatregelen ten minste gelijkwaardig zijn aan de verplichtingen van dit wetsontwerp. Paragraaf 2 van dit artikel verduidelijkt wat onder "gelijkwaardig" wordt verstaan.
Sur base de cette disposition, certaines articles du présent projet de loi, pour lesquels il existe un équivalent au travers d'un instrument juridique sectoriel de l'Union européenne, ne sont pas applicables aux entités concernées.	Op basis van deze bepaling zijn sommige artikelen van dit wetsontwerp, waarvoor een equivalent bestaat via een sectorspecifiek rechtsinstrument van de Europese Unie, niet van toepassing op de betrokken entiteiten.
Le paragraphe 3 porte sur un tel acte juridique sectoriel de l'Union européenne, à savoir le 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, ci-après le règlement DORA, et sur les dérogations au présent projet de loi qui en découlent.	Paragraaf 3 heeft betrekking op een dergelijk sectorspecifiek rechtsinstrument van de Europese Unie, namelijk 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) nr. 2016/1011, hierna de DORA-verordening, en op de daaruit voortvloeiende afwijkingen van dit wetsontwerp.
Ce paragraphe prévoit que les entités relevant des secteurs bancaires et des infrastructures des marchés financiers qui tombent dans le	Deze paragraaf bepaalt dat entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt die

champ d'application du règlement DORA ne sont pas soumises aux dispositions relatives à la gestion des risques de cybersécurité, à la notification d'incidents, à la supervision et à l'exécution.	onder het toepassingsgebied van de DORA-verordening vallen, niet onderworpen zijn aan de bepalingen met betrekking tot het beheer van cyberbeveiligingsrisico's, de melding van incidenten, het toezicht en de handhaving.
Le paragraphe 4 met également en œuvre la dérogation visée au paragraphe 1 ^{er} dans le secteur bancaire. Selon ce paragraphe, les dispositions du projet de loi relatives aux mesures de gestion des risques en matière de cybersécurité, à la supervision et à l'exécution ne s'appliquent pas aux entités listées. Il est important de noter que les dispositions en matière de notification d'incidents sont, elles, toujours applicables.	Paragraaf 4 implementeert de in de eerste paragraaf bedoelde afwijking ook in het bankwezen. Volgens deze paragraaf zijn de bepalingen van het wetsontwerp betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's, het toezicht en de handhaving niet van toepassing op de opgelijste entiteiten. Het is belangrijk op te merken dat de bepalingen over de melding van incidenten wel van toepassing zijn.
La dérogation du paragraphe 4 s'applique d'abord à la Banque nationale de Belgique, ci-après, la « BNB ». En effet, la BNB, en tant que banque centrale, fait partie du système européen de banques centrales (le « SEBC »), constitué de l'ensemble des banques centrales européennes. Le SEBC impose toute une série d'orientations et d'instructions en matière de sécurité informatique applicables à toutes les banques centrales.	De afwijking van paragraaf 4 is in de eerste plaats van toepassing op de Nationale Bank van België, hierna de "NBB". Als centrale bank maakt de NBB immers deel uit van het Europees Stelsel van Centrale Banken (het "ESCB"), dat bestaat uit alle Europese centrale banken. Het ESCB legt alle centrale banken een hele reeks richtsnoeren en instructies inzake IT-beveiliging op.
Article 7	Artikel 7
Sur base de l'article 6, la dérogation au champ d'application s'applique <i>de jure</i> , sans nécessairement d'intervention du Roi. Cette habilitation dévolue au Roi permet d'expliciter, de manière non exhaustive, des instruments juridiques sectoriels de l'Union européenne (présents ou futurs) comme équivalents, en vue d'améliorer la prévisibilité et la sécurité juridique. Cette disposition donne également compétence au Roi d'établir les règles spécifiques en matière d'échange d'informations et de notification d'incidents entre les autorités compétentes, dans le cadre de la dérogation visée aux paragraphes 3 et 4 de l'article 6. Cette dernière attribution de compétence permet d'assurer un échange d'informations adéquats lors d'incidents de cybersécurité.	Op basis van artikel 6 is de afwijking van het toepassingsgebied <i>de jure</i> van toepassing, zonder dat de tussenkomst van de Koning vereist is. Deze machtiging aan de Koning maakt het mogelijk om (huidige of toekomstige) sectorspecifieke rechtsinstrumenten van de Europese Unie op niet-exhaustieve wijze uitdrukkelijk als gelijkwaardig aan te duiden, met het oog op een betere voorspelbaarheid en rechtszekerheid. Deze bepaling geeft de Koning ook de bevoegdheid om specifieke regels vast te stellen met betrekking tot de uitwisseling van informatie en de melding van incidenten tussen de bevoegde autoriteiten, in het kader van de afwijking bedoeld in paragraaf 3 en 4 van artikel 6. Deze laatste bevoegdheidstoekenning zorgt voor een adequate informatie-uitwisseling bij cyberbeveiligingsincidenten.
CHAPITRE 2	HOOFDSTUK 2

Définitions	Definities
Article 8	Artikel 8
Cet article reprend pour l'essentiel les définitions telles qu'établies par la directive NIS2 ainsi que certains éléments spécifiques au cadre législatif belge.	Dit artikel bevat in hoofdzaak de definities zoals die zijn vastgesteld door de NIS2-richtlijn, alsook sommige aspecten die specifiek betrekking hebben op het Belgische wetgevende kader.
La notion de réseau et système d'information, défini à l'article 6, 1°, de la directive NIS2 est complétée à l'article 8, 1°, b) pour préciser, entre autres choses, que sont bien inclus dans cette définition les réseaux interconnectés de manière permanente ou temporaire et les composants numériques, électroniques ou mécaniques d'un dispositif permettant notamment l'automatisation de processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel.	Het begrip "netwerk- en informatiesysteem", gedefinieerd in artikel 6, 1°, van de NIS2-richtlijn, wordt aangevuld in artikel 8, 1°, b), om onder andere te verduidelijken dat deze definitie ook slaat op netwerken die permanent of tijdelijk met elkaar verbonden zijn en op de digitale, elektronische of mechanische componenten van een apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken.
Il s'agit de confirmer explicitement l'application de la directive notamment aux systèmes d'acquisition et de contrôle de données industriels (en anglais "Supervisory Control And Data Acquisition", en abrégé "SCADA"), ainsi que les dispositifs interconnectés de manière permanente ou temporaire.	Doel is uitdrukkelijk te bevestigen dat de richtlijn met name van toepassing is op SCADA-systemen ("Supervisory Control And Data Acquisition") en op apparaten die permanent of tijdelijk met elkaar verbonden zijn.
Pour la définition d'une entité de l'administration publique, l'article 6, 35) de la directive précise que la notion doit être reconnue comme telle conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales. Ainsi, il a été choisi de faire référence à des notions existantes en droit belge qui couvrent les entités concernées afin de ne pas multiplier l'application de notions différentes.	Voor de definitie van een overheidsinstantie verduidelijkt artikel 6, 35), van de richtlijn dat het begrip overeenkomstig het nationale recht als zodanig erkend moet zijn, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom werd ervoor gekozen te verwijzen naar bestaande begrippen in het Belgisch recht die de betrokken entiteiten omvatten, zodat er niet te veel verschillende begrippen zouden worden toegepast.
En l'occurrence, la définition reprend la notion d'autorité administrative visée à l'article 14, § 1 ^{er} , alinéa 1 ^{er} , des lois coordonnées du 12 janvier 1973 sur le Conseil d'État, à laquelle sont rajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs repris dans les annexes du présent projet de loi et de	In dit geval bevat de definitie het begrip "administratieve overheid" als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, waaraan de criteria worden toegevoegd om niet van industriële of commerciële aard te zijn, niet hoofdzakelijk een activiteit uit te oefenen die tot een van de andere sectoren of deelsectoren opgenomen in

ne pas exercer à titre principal ses activités dans le domaine de la sécurité nationale ou de la sécurité publique.	de bijlagen bij dit wetsontwerp behoort, en niet hoofdzakelijk activiteiten uit te oefenen op het gebied van nationale of openbare veiligheid.
Ce choix s'explique de par le fait que la plupart des critères repris dans la définition de la directive se retrouvent dans les critères qui délimitent la notion d'autorité administrative au sens des lois coordonnées sur le Conseil d'Etat.	Deze keuze wordt verklaard door het feit dat de meeste criteria in de definitie van de richtlijn terug te vinden zijn in de criteria die het begrip "administratieve overheid" als bedoeld in de gecoördineerde wetten op de Raad van State afbakenen.
S'agissant du caractère industriel ou commercial, l'appréciation de ce caractère doit se faire sur base d'indices objectifs au cas par cas. A cet égard, il est intéressant de relever que la notion de « besoins d'intérêt général ayant un caractère autre qu'industriel et commercial » est issue du droit dérivé européen, et plus particulièrement des directives européennes sur la passation des marchés publics. Il s'ensuit que les entités qui sont qualifiées de pouvoirs adjudicateurs au sens de l'article 2, 1°, c) de la loi du 17 juin 2016 relative aux marchés publics remplissent la condition de la satisfaction d'un besoin d'intérêt général ayant un caractère autre qu'industriel et commercial. Sur cette condition, il est donc pertinent de se référer à la liste non limitative des « pouvoirs adjudicateurs » au sens de la loi précitée, dressée dans l'arrêté royal du 18 avril 2017 relatif à la passation des marchés publics dans les secteurs classés.	De industriële of commerciële aard moet geval per geval worden beoordeeld op basis van objectieve aanwijzingen. In dit verband is het interessant op te merken dat het begrip "behoeften van algemeen belang die niet van industriële of commerciële aard zijn" afkomstig is uit het Europese afgeleide recht, en meer bepaald uit de Europese richtlijnen betreffende de plaatsing van overheidsopdrachten. Hieruit volgt dat entiteiten die worden beschouwd als aanbestedende overheden in de zin van artikel 2, 1°, c), van de wet van 17 juni 2016 inzake overheidsopdrachten, voldoen aan de voorwaarde dat zij voorzien in een behoefte van algemeen belang die niet van industriële of commerciële aard is. Wat deze voorwaarde betreft, is het dus relevant om te verwijzen naar de niet-limitatieve lijst van "aangebestedende overheden" als bedoeld in voornoemde wet, die is opgenomen in het koninklijk besluit van 18 april 2017 plaatsing overheidsopdrachten in de klassieke sectoren.
S'agissant de la condition de ne pas exercer 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, celle-ci permet de ne pas créer de différence de traitement entre les entités publiques et privées actives dans un même secteur ou sous-secteur, notamment en ce qui concerne les sanctions administratives éventuellement applicables.	De voorwaarde om niet hoofdzakelijk een activiteit opgesomd in de kolom soort entiteit van een van de andere sector of deelsector van een van de bijlagen, zorgt ervoor dat publieke en private entiteiten die in dezelfde sector of deelsector actief zijn, niet verschillend behandeld worden, met name wat eventueel toepasselijke administratieve sancties betreft.
S'agissant de la condition de ne pas exercer à titre principal des activités dans le domaine de la sécurité nationale ou de la sécurité publique, il s'agit d'un rappel de l'exclusion prévue par l'article 2, § 7, de la directive.	De voorwaarde om niet hoofdzakelijk activiteiten uit te oefenen op het gebied van nationale of openbare veiligheid verwijst naar de uitsluiting in artikel 2, lid 7, van de richtlijn.

Cet article définit également diverses notions reprises de la directive afin d'en clarifier le contenu (voir les définitions aux 42°, 48°, 49°, 51° et 57° à 59°).	In dit artikel worden ook verschillende begrippen omschreven die afkomstig zijn uit de richtlijn, om de inhoud ervan te verduidelijken (zie de definities in de punten 42°, 48°, 49°, 51° en 57° tot 59°).
Par ailleurs, des notions spécifiques à la loi sont définies, aux 43° à 47°, 50° et 52° au 56°, notamment l'autorité nationale de cybersécurité, désignée par le Roi, qui joue un rôle central dans la mise en œuvre de la loi (voir ci-dessous, les articles 17 et suivants) ou l'autorité sectorielle, jouant le cas échéant un rôle spécifique dans le secteur auquel elle se rapporte.	Daarnaast worden in de punten 43° tot 47°, 50° en 52° tot 56° begrippen gedefinieerd die specifiek zijn voor de wet, met name de nationale cyberbeveiligingsautoriteit, aangewezen door de Koning, die een centrale rol speelt bij de uitvoering van dit wetsontwerp (zie artikel 17 en volgende hierna) of de sectorale overheid, die in voorkomend geval een specifieke rol speelt in de sector waarop zij betrekking heeft.
CHAPITRE 3	HOOFDSTUK 3
Catégories d'entités	Categorieën van entiteiten
Article 9	Artikel 9
Cette disposition énumère les types d'entités qualifiées d'essentiels.	Deze bepaling somt de soorten entiteiten op die als essentieel worden beschouwd.
La distinction précédemment établie par la directive NIS1 entre les « opérateurs de services essentiels » (OSE) et de « fournisseurs de service numérique » (FSN) disparaît et laisse place à une distinction entre entités « essentielles » et « importantes ». Désormais, cette distinction se fait en principe automatiquement sur la base de la taille de l'entité et du type d'entité concernée figurant dans l'une des deux annexes du projet de loi. Cette distinction joue un rôle important dans les régimes de supervision et d'exécution applicables à ces deux catégories d'entités, afin de garantir un juste équilibre entre les exigences et les obligations basées sur les risques, d'une part, et la charge administrative qui découle du contrôle de la conformité, d'autre part.	Het onderscheid dat voorheen in de NIS1-richtlijn werd gemaakt tussen "aanbieders van essentiële diensten" (AED's) en "digitaal dienstverleners" (DDV's) verdwijnt en wordt vervangen door een onderscheid tussen "essentiële" en "belangrijke" entiteiten. Voortaan wordt dit onderscheid in principe automatisch gemaakt op basis van de omvang van de betrokken entiteit en het soort betrokken entiteit dat in een van de twee bijlagen bij het wetsontwerp is opgenomen. Dit onderscheid speelt een belangrijke rol bij de toezichts- en handhavingsregelingen voor deze twee categorieën entiteiten, om te zorgen voor een billijk evenwicht tussen risicogebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.
Cet article reprend le contenu de la directive NIS2 et qualifie d'essentiels les entités d'un type visé à l'annexe I qui dépassent les plafonds des entreprises moyennes ; certains types d'entités actifs en matière de services de confiance ou de services de noms de domaines ;	Dit artikel bevat de inhoud van de NIS2-richtlijn en beschouwt de volgende entiteiten als essentiële entiteiten: entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden; bepaalde soorten entiteiten die actief zijn op

les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent au moins des moyennes entreprises ; les entités critiques au sens de la [loi CER] ; les entités publiques fédérales ; toute autre entité identifiée comme entité essentielle conformément à l'article 12 du présent projet de loi (voir <i>infra</i>).	het gebied van vertrouwensdiensten of domeinnaamdiensten; aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen; kritieke entiteiten als bedoeld in de [CER-wet]; federale overheidsinstanties; alle andere entiteiten die overeenkomstig artikel 12 van dit wetsontwerp worden geïdentificeerd als essentiële entiteiten (zie <i>infra</i>).
Article 10	Artikel 10
Cette disposition énumère les types d'entités qualifiées d'importantes, à savoir les entités visées aux annexes I et II qui ne sont pas qualifiées d'essentielles sur base de l'article précédent ou qui sont identifiées comme importantes conformément à l'article 12 du présent projet de loi (voir <i>infra</i>).	Deze bepaling somt de soorten entiteiten op die als "belangrijk" worden beschouwd, namelijk de entiteiten bedoeld in bijlage I en II die niet als essentiële entiteiten worden beschouwd op basis van het vorige artikel of die overeenkomstig artikel 12 van dit wetsontwerp als belangrijke entiteiten worden geïdentificeerd (zie <i>infra</i>).
CHAPITRE 4	HOOFDSTUK 4
Identification	Identificatie
Article 11	Artikel 11
Cet article permet à l'autorité nationale de cybersécurité d'identifier, en plus des entités déjà qualifiées d'essentielles ou importantes sur base des dispositions précédentes, des entités comme essentielles ou importantes, après avoir consulté l'autorité sectorielle concernée et potentiellement sur base de sa proposition (pour autant qu'une telle autorité ait été désignée pour le secteur concerné). Le paragraphe 1 ^{er} , qui transpose l'article 2, § 2, b) à e), de la directive NIS2, précise les critères sur base desquels une identification peut être effectuée. Cette procédure peut être mise en œuvre quelle que soit la taille de l'entité.	Op grond van dit artikel kan de nationale cyberbeveiligingsautoriteit, naast de entiteiten die al op basis van de voorgaande bepalingen als essentiële of belangrijke entiteiten worden aangemerkt, entiteiten als essentieel of belangrijk identificeren, na raadpleging van de betrokken sectorale overheid en mogelijk op basis van het voorstel van die laatste (voor zover een dergelijke overheid is aangewezen voor de betrokken sector). Paragraaf 1, die voorziet in de omzetting van artikel 2, § 2, b) tot e), van de NIS2-richtlijn, stelt de criteria vast op basis waarvan een identificatie kan worden uitgevoerd. Deze procedure kan worden uitgevoerd ongeacht de omvang van de entiteit.
Le paragraphe 2 précise que l'autorité nationale de cybersécurité procède également à l'identification des administrations publiques relevant des entités fédérées qui, à la suite	Paragraaf 2 bepaalt dat de nationale cyberbeveiligingsautoriteit ook de overheidsinstanties van de deelgebieden identificeert die, na een risicobeoordeling,

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. En pratique, cette identification sera réalisée sur base de consultations étroites avec chaque entité fédérée. Cette dernière pourra ainsi proposer une liste des administrations publiques fournissant des services critiques et relevant de son niveau de pouvoir.	diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten. In de praktijk zal deze identificatie gebeuren op basis van nauw overleg met elk deelgebied, dat een lijst kan voorstellen van overheidsinstanties die kritieke diensten verlenen en onder zijn bevoegdheid vallen.
Le paragraphe 3 indique que l'autorité nationale de cybersécurité consulte les éventuelles autorités sectorielles, les entités fédérées et l'entité concernée dans le cadre de la procédure d'identification. Concrètement, l'autorité nationale de cybersécurité associe dès le départ les autorités sectorielles concernées (éventuellement à l'origine de la proposition d'identification), les entités fédérées et le Centre de crise national. Une procédure formelle d'avis de l'autorité sectorielle est mise en place. Pour des motifs liés à la sécurité public et à la procédure administrative en cours, il est mentionné explicitement que cet avis n'est pas publié. En cas d'avis défavorable de l'autorité sectorielle et si l'autorité nationale de cybersécurité souhaite maintenir son projet de décision, il est alors requis que le dossier soit soumis pour accord préalable au Comité stratégique du renseignement et de la sécurité.	Paragraaf 3 bepaalt dat de nationale cyberbeveiligingsautoriteit de eventuele sectorale overheden, de deelgebieden en de betrokken entiteit raadpleegt in het kader van de identificatieprocedure. Concreet betreft de nationale cyberbeveiligingsautoriteit van bij het begin de betrokken sectorale overheden (die mogelijk het identificatievoorstel hebben geformuleerd), de deelgebieden en het Nationaal Crisiscentrum. Er wordt een formele procedure ingevoerd om het advies van de sectorale overheid in te winnen. Om redenen van openbare veiligheid en de lopende administratieve procedure wordt uitdrukkelijk vermeld dat dit advies niet wordt gepubliceerd. In geval van een ongunstig advies van de sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, moet het dossier vooraf ter goedkeuring worden voorgelegd aan het Strategisch Comité voor Inlichtingen en Veiligheid.
Conformément à l'article 3, § 4, de la directive NIS2, l'actualisation des identifications s'effectue tous les deux ans, le cas échéant après consultation des autorités sectorielles. Il est également prévu que les identifications et actualisations sont adressées aux autorités sectorielles concernées (pour autant qu'une telle autorité ait été désignée) ainsi qu'au Centre de crise national.	Overeenkomstig artikel 3, § 4, van de NIS2-richtlijn worden de identificaties om de twee jaar geactualiseerd, in voorkomend geval na raadpleging van de sectorale overheden. Tevens is bepaald dat de identificaties en actualisering en naar de betrokken sectorale overheden (voor zover een dergelijke overheid is aangewezen) en naar het Nationaal Crisiscentrum worden gestuurd.
La communication aux autorités sectorielles (pour autant qu'elles existent) s'explique du fait que ces autorités peuvent être compétentes pour superviser la mise en œuvre de mesures spécifiques sectorielles.	De kennisgeving aan de sectorale overheden (voor zover deze bestaan) wordt verklaard door het feit dat deze overheden bevoegd kunnen zijn om toezicht te houden op de uitvoering van sectorspecifieke maatregelen.

La communication au Centre national de crise et aux éventuelles autorités sectorielles permet également d'assurer une cohérence entre l'identification des entités essentielles et des entités critiques visées par la directive UE 2022/2557 du 14 décembre 2022 sur la résilience des entités critiques (directive CER).	De kennisgeving aan het Nationaal Crisiscentrum en aan de eventuele sectorale overheden laat ook toe te zorgen voor coherentie tussen de identificatie van de essentiële entiteiten en van de kritieke entiteiten bedoeld in EU-richtlijn 2022/2557 van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten (CER-richtlijn).
La communication au Centre de crise nationale des identifications et actualisations visées au présent article est également prévue au vu de l'importance que revêt ces identifications dans le cadre de la gestion de crises. En effet, les incidents touchant les entités identifiées comme essentielles sont bien plus susceptibles de constituer des incidents nationaux, voire des crises nationales au sens de la loi [relative à la gestion de crise], que les incidents touchant les entités identifiées comme importantes. Pour cette raison, il est important que le Centre de crise nationale, chargée de la coordination en matière de crise nationale, soit informé de l'identification et de l'actualisation d'entités essentielles.	De kennisgeving aan het Nationaal Crisiscentrum van de in dit artikel bedoelde identificaties en actualisering is ook voorzien omdat deze identificaties van belang zijn in het kader van het crisisbeheer. Incidenten die van invloed zijn op entiteiten die als essentiële entiteiten zijn geïdentificeerd, zijn immers veel vaker nationale incidenten of zelfs nationale crises als bedoeld in de wet [betreffende het crisisbeheer] dan incidenten die gevolgen hebben voor entiteiten die als belangrijke entiteiten zijn geïdentificeerd. Daarom is het belangrijk dat het Nationaal Crisiscentrum, dat belast is met de coördinatie bij nationale crises, op de hoogte wordt gebracht van de identificatie en actualisering van essentiële entiteiten.
Le paragraphe 5 prévoit la possibilité pour le Roi, par arrêté délibéré en Conseil des ministres, de désigner individuellement comme entité essentielle ou importante une entité qui ne fait pas partie des secteurs visés en annexe de la loi. En effet, une entité ou un sous-traitant particulier d'une entité NIS pourrait fournir un service critique justifiant d'être soumis aux dispositions de la loi alors que par ailleurs ses activités ne relèvent pas de l'un des secteurs repris dans les annexes de la loi. L'application de cet article est limité à des cas particuliers et implique au préalable de la décision du Comité stratégique du renseignement et de la sécurité, une concertation entre l'entité concernée, l'autorité nationale de cybersécurité, les entités fédérées et l'éventuelle autorité sectorielle.	Op grond van paragraaf 5 kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een entiteit die niet tot de in de bijlage bij de wet bedoelde sectoren behoort, individueel aanwijzen als een essentiële of belangrijke entiteit. Een entiteit of een bepaalde onderaannemer van een NIS-entiteit kan immers een kritieke dienst verlenen die rechtvaardigt dat zij of hij onderworpen is aan de bepalingen van de wet, ook al behoren haar of zijn activiteiten niet tot een van de sectoren opgenomen in de bijlagen bij de wet. De toepassing van dit artikel is beperkt tot bijzondere gevallen en houdt in dat, vóór de beslissing van het Strategisch Comité voor Inlichtingen en Veiligheid, overleg wordt gepleegd tussen de betrokken entiteit, de nationale cyberbeveiligingsautoriteit, de deelgebieden en de eventuele sectorale overheid.
Article 12	Artikel 12

national, les États membres peuvent décider des mécanismes appropriés permettant d'identifier les entités relevant du champ d'application » (considérant 18 et article 3, § 4, alinéa 4, de la directive NIS2). En pratique, une plateforme, accessible par internet, sera mise à disposition des entités afin qu'elles puissent y indiquer les informations nécessaires.	<i>registers bestaan op nationaal niveau, kunnen de lidstaten besluiten over passende mechanismen voor de identificatie van binnen het toepassingsgebied van deze richtlijn vallende entiteiten" (overweging 18 en artikel 3, lid 4, vierde alinea, van de NIS2-richtlijn). In de praktijk zal via internet een platform ter beschikking van de entiteiten worden gesteld, zodat zij hier de nodige informatie kunnen invoeren.</i>
Afin d'assurer la mise en œuvre du principe de simplification administrative (« only once »), il est prévu qu'une entité qui a déjà communiqué à une éventuelle autorité sectorielle concernée certaines des informations, en vertu d'une obligation légale, puisse simplement compléter les informations requises auprès de cette autorité sectorielle.	Om ervoor te zorgen dat het beginsel van administratieve vereenvoudiging ("only once") wordt toegepast, is voorzien dat een entiteit die al een deel van de informatie aan een eventuele betrokken sectorale overheid heeft meegedeeld krachtens een wettelijke verplichting, de vereiste informatie gewoon kan aanvullen bij deze sectorale overheid.
Ensuite, l'autorité sectorielle concernée communique les informations collectées à l'autorité nationale de cybersécurité.	Vervolgens bezorgt de betrokken sectorale overheid de ingezamelde informatie aan de nationale cyberbeveiligingsautoriteit.
En complément de ces informations, l'autorité sectorielle transmettra sur base des éléments en sa possession une analyse de la qualification de l'entité comme essentielle ou importante.	Naast deze informatie bezorgt de sectorale overheid, op basis van de elementen waarover zij beschikt, een analyse volgens dewelke de entiteit als essentieel of belangrijk wordt aangemerkt.
En cas de modification des informations devant être communiquées, il appartient à l'entité concernée de notifier ces modifications à l'autorité nationale de cybersécurité ou à l'autorité sectorielle concernée.	Indien de te verstrekken informatie wijzigt, dient de betrokken entiteit deze wijzigingen aan de nationale cyberbeveiligingsautoriteit of aan de betrokken sectorale overheid te melden.
Le paragraphe 4 prévoit que 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.	Paragraaf 4 bepaalt dat de nationale cyberbeveiligingsautoriteit de nodige maatregelen neemt om ervoor te zorgen dat de sectorale overheden de verstrekte gegevens kunnen raadplegen voor de sectoren die hen aangaan.
Article 14	Artikel 14

Cet article transpose l'article 27, § 2, § 3 et § 5, de la directive NIS2. Il organise l'enregistrement pour 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 et détermine les informations qui doivent être renseignées par ces entités.	Dit artikel voorziet in de omzetting van artikel 27, lid 2, 3 en 5, van de NIS2-richtlijn. Het regelt de registratie voor DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten, en bepaalt welke informatie door deze entiteiten moet worden verstrekt.
Cet enregistrement devra être effectué dans les deux mois suivant l'entrée en vigueur de la loi. Ce délai est nécessaire afin de respecter l'obligation prévue à l'article 27, § 2, de la directive NIS2.	Deze registratie dient te gebeuren binnen twee maanden na de inwerkingtreding van de wet. Deze termijn is nodig om te voldoen aan de verplichting waarvan sprake in artikel 27, § 2, van de NIS2-richtlijn.
Cet article prévoit que les modalités de communication des informations sont celles prévues à l'article précédent. En effet, la directive NIS2 permet, en son article 27, § 5, que le même mécanisme peut être utilisé pour la communication d'informations par les entités visées à cet article et les entités visées à l'article 14 du projet de loi.	Dit artikel bepaalt dat de modaliteiten voor het verstrekken van informatie dezelfde zijn als in het vorige artikel. Op basis van artikel 27, lid 5, van de NIS2-richtlijn kunnen de in dit artikel bedoelde entiteiten en de in artikel 14 van het wetsontwerp bedoelde entiteiten immers hetzelfde mechanisme gebruiken voor het verstrekken van informatie.
D'une manière similaire à l'article précédent, le paragraphe 2 impose aux entités concernées de notifier toute modification des informations devant être communiquées à l'autorité nationale de cybersécurité.	Op vergelijkbare wijze als in het vorige artikel verplicht paragraaf 2 de betrokken entiteiten om de nationale cyberbeveiligingsautoriteit in kennis te stellen van alle wijzigingen in de in te dienen informatie.
Une exception est prévue au paragraphe 3 en ce qui concerne les prestataires de services de confiance qualifiés afin de garantir le respect du principe de collecte unique des données.	Paragraaf 3 voorziet in een uitzondering voor gekwalificeerde verleners van vertrouwensdiensten om de naleving van het principe van de unieke gegevensinzameling te waarborgen.

TITRE 2	TITEL 2
<i>Autorités compétentes et coopération au niveau national</i>	<i>Bevoegde autoriteiten en samenwerking op nationaal niveau</i>
CHAPITRE 1 ^{ER}	HOOFDSTUK 1
Autorités compétentes	Bevoegde autoriteiten
Section 1^{re}	Afdeling 1
<i>Désignation des autorités compétentes</i>	<i>Aanwijzing van de bevoegde autoriteiten</i>
Article 15	Artikel 15
Cet article désigne les autorités compétentes dans le cadre du présent projet de loi, le cas échéant au travers d'une désignation par le Roi.	In dit artikel worden de autoriteiten aangewezen die in het kader van dit wetsontwerp bevoegd zijn, in voorkomend geval door middel van een aanwijzing door de Koning.
L'autorité envisagée pour remplir le rôle d'autorité nationale de cybersécurité est le Centre pour la Cybersécurité Belgique. Il n'est pas directement cité dans la loi car, comme a déjà pu le préciser la section de législation du Conseil d'Etat, notamment dans l'avis 63.296/4, désigner directement des services du pouvoir exécutif créés par le Roi et qui dépendent de Lui serait une immixtion du pouvoir législatif dans l'organisation interne du pouvoir exécutif.	De autoriteit die de rol van nationale cyberbeveiligingsautoriteit moet vervullen, is het Centrum voor Cybersecurity België. Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en op Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.
C'est en principe au Roi qu'il revient de désigner l'administration chargée d'exécuter les missions de l'autorité nationale de cybersécurité.	In principe is het aan de Koning om te bepalen welke administratie verantwoordelijk is voor het uitvoeren van de opdrachten van de nationale cyberbeveiligingsautoriteit.
Le rôle et les tâches de l'autorité nationale de cybersécurité sont décrits aux articles suivants (voir <i>infra</i>).	De rol en de taken van de nationale cyberbeveiligingsautoriteit worden beschreven in de volgende artikelen (zie <i>infra</i>).
Le paragraphe 2 laisse au Roi la possibilité de nommer des autorités sectorielles et/ou des services d'inspection sectoriels, après avis de l'autorité nationale de cybersécurité, pour autant que les autorités envisagées ne soient pas créées par la loi, auquel cas il revient à la loi	Paragraaf 2 biedt de Koning de mogelijkheid om sectorale overheden en/of sectorale inspectiediensten aan te wijzen, na advies van de nationale cyberbeveiligingsautoriteit, voor zover de beoogde autoriteiten niet bij wet zijn opgericht, in welk geval het aan de wet is om ze

de les désigner. Le cas échéant, selon les secteurs, le Roi peut créer des autorités composées de représentants de l'Etat fédéral et des entités fédérées, conformément à l'article 92ter de la loi du 8 aout 1980.	aan te wijzen. In voorkomend geval kan de Koning, naargelang de sector, autoriteiten oprichten die bestaan uit vertegenwoordigers van de Federale Staat en de deelgebieden, overeenkomstig artikel 92ter van de wet van 8 augustus 1980.
La disposition prévoit que le Roi, dans le cadre de la désignation des autorités sectorielles et/ou des services d'inspections sectoriels, tient compte des autorités sectorielles désignées conformément à la loi [CER]. La directive NIS2 insiste à plusieurs reprises sur le fait que les autorités compétentes dans le cadre de la directive NIS2 et de la directive CER devraient coopérer de manière étroite.	De bepaling voorziet dat de Koning, in het kader van de aanwijzing van sectorale overheden en/of sectorale inspectiediensten, rekening houdt met de sectorale overheden die overeenkomstig de [CER]-wet zijn aangewezen. In de NIS2-richtlijn wordt herhaaldelijk benadrukt dat de autoriteiten die in het kader van de NIS2-richtlijn en de CER-richtlijn bevoegd zijn, nauw moeten samenwerken.
Section 2	Afdeling 2
<i>L'autorité nationale de cybersécurité</i>	<i>De nationale cyberbeveiligingsautoriteit</i>
Article 16	Artikel 16
Cet article décrit le rôle de l'autorité nationale de cybersécurité.	In dit artikel wordt de rol van de nationale cyberbeveiligingsautoriteit beschreven.
L'objectif est de créer une autorité centralisant les compétences en matière de cybersécurité, avec un rôle particulièrement important dans la mise en œuvre du présent projet de loi. Au sens de la directive NIS2, l'autorité nationale de cybersécurité est :	Doel is om een autoriteit op te richten die de bevoegdheden op het gebied van cyberbeveiliging centraliseert, met een bijzonder belangrijke rol bij de uitvoering van dit wetsontwerp. In de zin van de NIS2-richtlijn is de nationale cyberbeveiligingsautoriteit:
1° l'autorité compétente, chargée de la cybersécurité, des tâches de supervision et de contrôler la mise en œuvre de la directive en Belgique (article 8, § 1 et 2, de la directive NIS2), à l'exception de la mise en œuvre de l'article 34 du présent projet de loi qui revient, le cas échéant, aux autorités sectorielles et/ou aux services d'inspection sectoriels ;	1° de bevoegde autoriteit, verantwoordelijk voor cyberbeveiliging, toezichthoudende taken en het monitoren van de tenuitvoerlegging van de richtlijn in België (artikel 8, lid 1 en 2, van de NIS2-richtlijn), met uitzondering van de uitvoering van artikel 34 van dit wetsontwerp, waarmee, in voorkomend geval, de sectorale overheden en/of sectorale inspectiediensten belast zijn;
2° le point de contact unique, exerçant une fonction de liaison visant à assurer la coopération transfrontière des autorités belges avec les autorités compétentes des autres États membres et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes en Belgique (article 8, § 4 de la	2° het centrale contactpunt, dat een verbindingsfunctie vervult om te zorgen voor grensoverschrijdende samenwerking van de Belgische autoriteiten met de relevante autoriteiten van andere lidstaten en in voorkomend geval met de Commissie en Enisa, alsook om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde

directive NIS2) ;	autoriteiten in België (artikel 8, lid 4, van de NIS2-richtlijn);
3° le CSIRT national, c'est-à-dire le centre national de réponse aux incidents de sécurité informatique, chargé de la gestion des incidents ;	3° het nationale CSIRT, d.w.z. het nationale computer security incident response team, dat verantwoordelijk is voor de behandeling van incidenten;
4° sans préjudice des dispositions nationales existantes en matière de gestion de crise, et plus précisément des compétences du Centre de crise national et du Ministre de l'Intérieur, l'autorité chargée de la gestion des incidents et crises de cybersécurité majeurs ;	4° onverminderd de bestaande nationale bepalingen inzake crisisbeheer, en meer bepaald de bevoegdheden van het Nationaal Crisiscentrum en van de minister van Binnenlandse Zaken, de autoriteit die verantwoordelijk is voor de behandeling van grootschalige cyberincidenten en -crises;
5° représentant de la Belgique dans le cadre de la coopération internationale organisée par la directive NIS2. L'autorité nationale de cybersécurité est notamment représentante de la Belgique au sein du groupe de coopération (article 14 de la directive NIS2), au sein de EU-CyCLONE (article 16, § 2, de la directive NIS2) et au sein du réseau des CSIRT (article 15 de la directive NIS2).	5° de vertegenwoordiger van België in het kader van de internationale samenwerking georganiseerd door de NIS2-richtlijn. De nationale cyberbeveiligingsautoriteit vertegenwoordigt België met name in de samenwerkingsgroep (artikel 14 van de NIS2-richtlijn), in EU-CyCLONE (artikel 16, lid 2, van de NIS2-richtlijn) en in het CSIRT-netwerk (artikel 15 van de NIS2-richtlijn).
<i>Sous-section 1^{re}</i>	<i>Onderafdeling 1</i>
<i>Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité</i>	<i>Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging</i>
Article 17	Artikel 17
Cet article énumère les tâches de l'autorité nationale de cybersécurité en sa qualité d'autorité compétente, chargée de veiller à la mise en œuvre du présent projet de loi.	In dit artikel worden de taken opgesomd van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van bevoegde autoriteit die verantwoordelijk is voor de uitvoering van dit wetsontwerp.
Cette disposition reprend, en plus des tâches découlant de la directive NIS2, les tâches existantes dévolues au Centre pour la Cybersécurité Belgique telles que la gestion, par une approche intégrée et centralisée, des différents projets relatifs à la cybersécurité ; la coordination entre les autorités publiques et le secteur privé ou le monde scientifique ; la formulation de propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité ; l'élaboration, la diffusion et la mise en œuvre des standards, directives et	Naast de taken die voortvloeien uit de NIS2-richtlijn, bevat deze bepaling de bestaande taken van het Centrum voor Cybersecurity België, zoals het beheer, vanuit een geïntegreerde en gecentraliseerde aanpak, van de verschillende projecten op het vlak van cyberbeveiliging; de coördinatie tussen overheden en de private sector of de wetenschappelijke wereld; het formuleren van voorstellen tot aanpassing van het wettelijk en regelgevend kader inzake cyberbeveiliging; het opstellen, verspreiden en uitvoeren van

normes de sécurité pour les différents types de systèmes d'information ; la coordination de la représentation belge aux forums internationaux sur la cybersécurité, du suivi des obligations internationales et de la présentation du point de vue national en la matière.	beveiligingsstandaarden, -richtlijnen en -normen voor de verschillende soorten informatiesystemen; 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.
Afin d'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, l'autorité nationale de cybersécurité développera une connaissance spécifique aux différentes entités actives dans les secteurs visés par la loi.	Om de coördinatie te verzekeren tussen de bevoegde autoriteiten in het kader van de toepassing van deze wet, alsook tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberveiligheid in België, zal de nationale autoriteit voor cyberveiligheid specifieke kennis ontwikkelen van de verschillende entiteiten die actief zijn in de sectoren die onder de wet vallen.
Parmi ses tâches, l'autorité nationale de cybersécurité a également la possibilité d'accorder des subventions pour autant que cela soit possible au travers des crédits budgétaires de l'année en cours et que les conditions d'octroi aient été fixées au préalable par le Roi. Ces subventions, pour autant que des crédits y soient alloués, doivent notamment pouvoir aider les petites et moyennes entreprises à mettre en œuvre les obligations qui découlent du présent projet de loi.	Een van de taken van de nationale cyberbeveiligingsautoriteit bestaat er tevens in subsidies toe te kennen, voor zover dit mogelijk is via de begrotingskredieten van het lopende jaar en de toekenningsvoorwaarden vooraf zijn vastgesteld door de Koning. Deze subsidies, voor zover er kredieten aan zijn toegekend, moeten met name kleine en middelgrote ondernemingen helpen om de verplichtingen die voortvloeien uit dit wetsontwerp uit te voeren.
<i>Sous-section 2</i>	<i>Onderafdeling 2</i>
<i>Tâches relatives au rôle de gestion des crises cyber</i>	<i>Taken met betrekking tot het cybercrisisbeheer</i>
Article 18	Artikel 18
Cet article transpose l'article 9, § 1 ^{er} et § 2, de la directive NIS2. Il établit les tâches dévolues à l'autorité nationale de cybersécurité en sa qualité d'autorité compétente en matière de gestion de crises et incidents cyber. A noter que la notion de crise doit s'entendre ici au sens commun [et non dans le sens de la loi du xx sur la gestion de crise et la planification d'urgence]. Plusieurs tâches en matière de gestion de crises et incidents cyber sont effectués en collaboration avec le Centre de crise national car cette autorité joue un rôle centrale dans la coordination dans le cadre de la gestion de	Dit artikel voorziet in de omzetting van artikel 9, lid 1 en 2, van de NIS2-richtlijn. Het bepaalt de taken van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van autoriteit die verantwoordelijk is voor het beheer van cybercrises en -incidenten. Opgemerkt wordt dat het begrip "crisis" hier moet worden verstaan in de algemene betekenis [en niet als bedoeld in de wet van xx betreffende het crisisbeheer en de noodplanning]. Verschillende taken met betrekking tot het beheer van cybercrises en -incidenten worden uitgevoerd in

crises.	samenwerking met het Nationaal Crisiscentrum, aangezien deze autoriteit een centrale rol speelt bij de coördinatie in het kader van het crisisbeheer.
Par ailleurs, l'article dispose que lorsque une crise ou un incident cyber constitue une crise nationale [au sens de la loi du xx sur la planification d'urgence], la coordination de la crise nationale est assurée par le Ministre de l'Intérieur.	Het artikel bepaalt tevens dat wanneer een cybercrisis of -incident een nationale crisis is [als bedoeld in de wet van xx betreffende de noodplanning], de coördinatie van de nationale crisis wordt verzekerd door de minister van Binnenlandse Zaken.
<i>Sous-section 3</i>	<i>Onderafdeling 3</i>
<i>Tâches et obligations relatives au rôle de CSIRT national</i>	<i>Taken en voorschriften met betrekking tot de rol van nationaal CSIRT</i>
Article 19	Article 19
Cet article énumère les tâches de l'autorité nationale de cybersécurité en sa qualité de CSIRT national. Il transpose l'article 11, § 3 à 5, de la directive NIS2 et reprend les tâches déjà dévolues au CISRT national sur base de la loi NIS1.	In dit artikel worden de taken opgesomd van de nationale cyberbeveiligingsautoriteit in haar hoedanigheid van nationaal CSIRT. Het voorziet in de omzetting van artikel 11, lid 3 tot 5, van de NIS2-richtlijn en bevat de taken die al op basis van de NIS1-wet aan het nationale CISRT zijn toegewezen.
Conformément au paragraphe 2, transposant l'article 11, § 3, alinéa 3, de la directive NIS2, le CSIRT national peut prioriser certaines de ses tâches par rapport à d'autres, sur base d'une approche basée sur les risques.	Overeenkomstig paragraaf 2, dat voorziet in de omzetting van artikel 11, lid 3, derde alinea, van de NIS2-richtlijn, kan het nationale CSIRT, op grond van een risicogebaseerde benadering, aan sommige van zijn taken prioriteit geven boven andere.
Comme cela lui est déjà permis dans le cadre de la loi NIS1, le CSIRT national peut 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. L'objectif poursuivi est d'avertir le responsable du système vulnérable afin que celui-ci puisse se protéger avant la survenance d'un incident.	Zoals reeds toegestaan in het kader van de NIS1-wet, kan het nationale CSIRT overgaan tot het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen, wanneer een dergelijk scannen wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren. Het scannen mag geen negatieve gevolgen hebben voor de werking van de diensten van de entiteiten. Het is de bedoeling om de verantwoordelijke van het kwetsbare systeem te verwittigen zodat hij zich kan beschermen voordat er een incident plaatsvindt.
La réalisation d'un scan non intrusif de réseaux	Bij het niet-intrusief scannen van openbaar

et systèmes d'information accessibles au public consiste concrètement à rechercher les ports ouverts sur un serveur de réseau ou un système informatique dans le but de détecter des vulnérabilités ou défauts de configuration, lesquels pourraient être utilisés par des personnes malveillantes. En effet, la détection de vulnérabilités nécessite une certaine forme d'interaction avec les ports du systèmes informatiques concernés. Il n'est toutefois pas recueilli plus d'informations sur le système d'information que nécessaire pour déterminer l'existence d'une vulnérabilité et alerter le responsable du système affecté.	toegankelijke netwerk- en informatiesystemen wordt concreet gezocht naar open poorten op een netwerkserver of in een informaticasysteem om kwetsbaarheden of configuratiefouten op te sporen die door kwaadwillende personen kunnen worden gebruikt. Het opsporen van kwetsbaarheden vereist immers een zekere vorm van interactie met de poorten van de betrokken informatiesystemen. Er wordt evenwel niet meer informatie over het informatiesysteem verzameld dan nodig is om het bestaan van een kwetsbaarheid vast te stellen en de verantwoordelijke van het getroffen systeem te waarschuwen.
Les réseaux et systèmes d'information accessibles au public sont ceux qui sont connectés à internet et auxquels un utilisateur peut avoir accès à distance. L'absence d'effet négatif sur le fonctionnement des services des entités concernés implique que le recueil de ces informations est réalisé sans causer de dommages aux réseaux et systèmes d'informations concernés.	Openbaar toegankelijke netwerk- en informatiesystemen zijn verbonden met het internet en toegankelijk op afstand voor gebruikers. Het verzamelen van deze informatie mag geen negatieve gevolgen hebben voor de werking van de diensten van de betrokken entiteiten, en dus geen schade aan de betrokken netwerk- en informatiesystemen veroorzaken.
Enfin, l'utilisation de cette méthode de recherche de vulnérabilités par le CSIRT national depuis plusieurs années a permis de protéger nombreuses organisations en Belgique et n'a pas causé de problème technique aux organisations concernées.	Tot slot heeft deze methode die het nationale CSIRT al een aantal jaren gebruikt voor het scannen op kwetsbaarheden, veel organisaties in België beschermd en geen technische problemen veroorzaakt voor de betrokken organisaties.
Article 20	Artikel 20
Cet article transpose l'article 11, § 1 ^{er} , de la directive NIS2 et reprend les obligations auxquelles doit satisfaire le CSIRT national.	Dit artikel voorziet in de omzetting van artikel 11, lid 1, van de NIS2-richtlijn en bevat de voorschriften waaraan het nationale CSIRT moet voldoen.
Comme le prévoit le considérant 41 de la directive NIS2, « les CSIRT devraient se conformer aux exigences établies dans la présente directive afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union ».	Zoals bepaald in overweging 41 van de NIS2-richtlijn moeten "de CSIRT's [...] voldoen aan de in deze richtlijn vastgestelde eisen om te garanderen dat zij over doeltreffende en compatibele capaciteiten beschikken om incidenten en risico's aan te pakken en om een efficiënte samenwerking op het niveau van de Unie te waarborgen".
Article 21	Artikel 21

Cette disposition reprend le contenu de l'article 62 de la loi NIS1.	Deze bepaling bevat de inhoud van artikel 62 van de NIS1-wet.
<p>L'article précise que le CSIRT national prendra toutes les mesures adéquates, proportionnelles et prudentes afin de réaliser ses missions légales.</p> <p>Cette disposition permet, si nécessaire, au CSIRT national de déroger à certaines dispositions du Code pénal pour l'exécution de ses missions légales, par application de l'article 70 du Code pénal. Cela étant, les compétences du CSIRT national ne portent pas préjudice aux compétences des procureurs, des juges d'instruction, des officiers de police judiciaire ou de toute autre personne exerçant la police judiciaire. Par ailleurs, les compétences du CSIRT national ne peuvent violer le secret de l'information ni le secret de l'instruction.</p>	<p>Het artikel verduidelijkt dat het nationale CSIRT alle passende, evenredige en behoedzame maatregelen zal nemen om zijn wettelijke opdrachten te verwezenlijken. Deze bepaling laat het nationale CSIRT indien nodig toe om af te wijken van sommige bepalingen van het Strafwetboek voor de uitvoering van zijn wettelijke opdrachten, met toepassing van artikel 70 van het Strafwetboek. De bevoegdheden van het nationale CSIRT doen echter geen afbreuk aan de bevoegdheden van de procureurs, onderzoeksrechters, officieren van gerechtelijke politie of andere personen die de gerechtelijke politie uitoefenen. Voorts mogen de bevoegdheden van het nationale CSIRT het geheim van het opsporingsonderzoek en gerechtelijk onderzoek niet schenden.</p>
<p>De plus, la disposition permet au CSIRT national, dans le respect des conditions imposées et poursuivant certains objectifs précis, de demander des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, alinéa 1^{er}, 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 du 13 juin 2005 relative aux communications électroniques auprès des opérateurs de communications électroniques, lorsque cela s'avère strictement nécessaire à la réalisation de certaines de ses tâches (la diffusion d'informations sur les risques et incidents en matière de sécurité des réseaux et systèmes d'information, l'intervention en cas d'incident, l'analyse dynamique des risques et incidents, ainsi que la détection, l'observation et l'analyse des problèmes de sécurité informatique).</p>	<p>Bovendien laat de bepaling het nationale CSIRT toe om, met inachtneming van de opgelegde voorwaarden en met het oog op bepaalde specifieke doelstellingen, gegevens op te vragen betreffende de gebruiker of abonnee 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 elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 betreffende de elektronische communicatie bij elektronische-communicatieoperatoren, indien dat strikt noodzakelijk is voor de uitvoering van sommige van zijn taken (verspreiding van informatie over risico's en incidenten in verband met de beveiliging van netwerk- en informatiesystemen, reageren op incidenten, zorgen voor een dynamische risico- en incidentanalyse, alsook het opsporen, observeren en analyseren van computerbeveiligingsproblemen).</p>
<p>Cette habilitation découle de la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, afin de mener à bien ses missions dans le cadre de la prévention</p>	<p>Deze machtiging vloeit voort uit de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, om zijn opdrachten uit te voeren in het kader van het voorkomen en opsporen</p>

et de la détection des infractions en matière de cybercriminalité, de la prévention de menaces contre la sécurité publique liées à la cybersécurité ainsi que de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques.	van misdrijven inzake cybercriminaliteit, het voorkomen van bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging en het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten.
Il s'agit pour le CSIRT national de protéger les entités essentielles et importantes au sens du présent projet de loi, dont font partie, au moins partiellement, les autorités publiques.	Doel van het nationale CSIRT is het beschermen van de essentiële en belangrijke entiteiten als bedoeld in dit wetsontwerp, waartoe, ten minste gedeeltelijk, de overheidsinstanties behoren.
En ce qu'ils affectent des acteurs essentiels de secteurs clés, en ce compris les pouvoirs publics, ces incidents constituent des menaces graves pour la sécurité publique.	Aangezien deze incidenten essentiële spelers in sleutelsectoren, waaronder overheden, treffen, vormen ze een ernstige bedreiging voor de openbare veiligheid.
Le CSIRT national joue également un rôle de prévention, de recherche et de détection en matière d'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. Il doit être en mesure, le cas échéant, d'obtenir des différents opérateurs, des données de communications électroniques afin d'accomplir ses missions légales. Les finalités poursuivies par ces différentes tâches sont énumérées au paragraphe 2, alinéa 2. Il s'agit notamment de la prévention de menaces graves contre la sécurité publique, de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information, de la prévention et, le cas échéant, la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques. La détection et la recherche des infractions seront effectuées par les services de police, avec le soutien éventuel du CERT en tant qu'expert.	Het nationale CSIRT speelt ook een rol bij het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten. Het moet in voorkomend geval elektronische-communicatiegegevens kunnen verkrijgen van de verschillende operatoren om zijn wettelijke opdrachten uit te voeren. De doeleinden die met deze verschillende taken worden nagestreefd, worden opgesomd in paragraaf 2, tweede lid. Het gaat met name om het voorkomen van ernstige bedreigingen voor de openbare veiligheid, het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen, en het voorkomen en desgevallend opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd. Het opsporen en onderzoeken van misdrijven zal door de politieke diensten gebeuren, al dan niet met steun als expert door het CERT.
Article 22	Artikel 22
Cet article transpose l'article 12 de la directive NIS2 et reprend les éléments déjà existants à l'article 62/1 de la loi NIS1, tel qu'inséré par la loi du 28 novembre 2022 relative à la protection des personnes qui signalent des violations au	Dit artikel voorziet in de omzetting van artikel 12 van de NIS2-richtlijn en bevat de al bestaande elementen van artikel 62/1 van de NIS1-wet, zoals ingevoegd bij de wet van 28 november 2022 betreffende de bescherming

droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.	van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector.
La disposition prévoit que le CSIRT national est coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Il fait office d'intermédiaire de confiance et de facilitateur 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.	De bepaling voorziet dat het nationale CSIRT de coördinator is met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. Het treedt op als een betrouwbare tussenpersoon en vergemakkelijkt 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.
L'importance croissante des réseaux et systèmes d'information au sein de nos sociétés augmente considérablement le risque d'être confronté à des incidents liés à la sécurité de ceux-ci. Ces incidents peuvent, par exemple, avoir pour conséquence d'affecter la disponibilité d'un service fourni, l'intégrité, l'authenticité, ou la confidentialité de données.	Het toenemende belang van netwerk- en informatiesystemen in onze samenleving leidt tot een veel hoger risico op incidenten in verband met de beveiliging van deze systemen. Deze incidenten kunnen bijvoorbeeld gevolgen hebben voor de beschikbaarheid van een verleende dienst of voor de integriteit, authenticiteit of vertrouwelijkheid van gegevens.
Parmi les causes de ces incidents, l'existence de vulnérabilités constitue un risque majeur. Une « vulnérabilité » est définie à l'article 8, 15° comme : une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace. Celui-ci est toutefois inhérent au processus de développement, d'utilisation et de mise à jour de ces systèmes. Ces vulnérabilités peuvent être détectées tant par des personnes bien intentionnées que par des personnes mal intentionnées. Les "hackers éthiques" souhaitent eux contribuer à l'amélioration de la sécurité des technologies de l'information en identifiant les vulnérabilités existantes et en aidant à les résoudre.	Wat de oorzaken van deze incidenten betreft, vormt het bestaan van kwetsbaarheden een groot risico. Een "kwetsbaarheid" wordt in artikel 8, 15°, gedefinieerd als een zwakte, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit. Dit risico is echter inherent aan het ontwikkelings-, gebruiks- en updateproces van deze systemen. Zowel mensen met goede bedoelingen als mensen met slechte bedoelingen kunnen deze kwetsbaarheden opsporen. "Ethische hackers" willen bijdragen aan een betere beveiliging van informatietechnologieën door bestaande kwetsbaarheden op te sporen en ze te helpen oplossen.
Compte tenu de l'ampleur et de la technicité de ce problème, le rôle sociétal de ces "hackers éthiques" est important.	Rekening houdend met de omvang en techniciteit van dit probleem is de maatschappelijke rol van deze "ethische hackers" belangrijk.
Or, un hacker éthique peut, dans certaines circonstances, remplir le rôle "lanceur d'alerte numérique" pour les vulnérabilités en matière	In bepaalde omstandigheden kunnen ethische hackers echter de rol van "digitale klokkenluider" vervullen voor kwetsbaarheden

de technologies de l'information et de la communication. À ce titre, il mérite de se voir reconnaître, moyennant le respect de certaines conditions, une protection légale, indépendamment de l'existence d'une politique de divulgation coordonnée des vulnérabilités ou des mesures adoptées par le responsable du système informatique.	inzake informatie- en communicatietechnologie. Hierbij moeten zij onder bepaalde voorwaarden wettelijke bescherming genieten, ongeacht het bestaan van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden of de maatregelen genomen door de verantwoordelijke van het informaticasysteem.
Le paragraphe 2 autorise le signalement, le cas échéant anonyme, de l'existence d'une potentielle vulnérabilité. La procédure pour ce faire doit être décrite par le CSIRT national et mis à disposition en ligne.	Krachtens paragraaf 2 mag, in voorkomend geval anoniem, het bestaan van een mogelijke kwetsbaarheid worden gemeld. De procedure hiervoor moet door het nationale CSIRT worden beschreven en online beschikbaar worden gesteld.
Le troisième paragraphe dispose que le CSIRT national est tenu de préserver l'exhaustivité, l'intégrité, le stockage durable et la confidentialité des informations transmises au travers du signalement, ainsi que de l'identité de la personne à l'origine de la transmission, (lorsque le signalement n'est pas anonyme). L'auteur du signalement ne doit dès lors pas craindre, par exemple, que le CSIRT national transmette son identité à d'autres autorités publiques, quand il a demandé à rester anonyme et a respecté les conditions visées à l'article suivant.	De derde paragraaf bepaalt dat het nationale CSIRT de volledigheid, integriteit, duurzame opslag en geheimhouding moet waarborgen van de via de melding overgemaakte informatie, alsook van de identiteit van de persoon die de informatie heeft overgemaakt (wanneer de melding niet anoniem is). Melders hoeven dus bijvoorbeeld niet te vrezen dat het nationale CSIRT hun identiteit aan andere overheidsinstanties zou doorgeven, wanneer zij gevraagd hebben anoniem te blijven en de in het volgende artikel bedoelde voorwaarden hebben nageleefd.
De plus, l'accès à ces informations doit demeurer limité aux personnes habilitées par le directeur général du CSIRT national. Cette alinéa ne fait pas préjudice à l'exécution des missions légales du CSIRT national énumérées à l'article 20 et qui impliquerait le partage des informations techniques issues du signalement avec d'autres autorités publiques.	Bovendien moet de toegang tot deze informatie beperkt blijven tot de personen die daartoe door de directeur-generaal van het nationale CSIRT gemachtigd zijn. Dit lid doet geen afbreuk aan de uitvoering van de in artikel 20 opgesomde wettelijke opdrachten van het nationale CSIRT, waarbij technische informatie uit de melding met andere overheidsinstanties zou worden gedeeld.
Le quatrième paragraphe autorise, dans le respect des conditions énumérées à l'article 22, § 1 ^{er} et § 4, le CSIRT national à utiliser éventuellement des méthodes d'observation, d'étude et de test des mesures de sécurité d'un système d'information ou d'un réseau afin de déterminer l'existence d'une vulnérabilité potentielle et de vérifier les méthodes utilisées par l'auteur d'un signalement. Il peut s'agir notamment de méthodes d'ingénierie inversée (en anglais, reverse engineering).	Krachtens de vierde paragraaf mag het nationale CSIRT, met inachtneming van de voorwaarden opgesomd in artikel 22, § 1 en § 4, eventueel gebruikmaken van methoden voor het observeren, onderzoeken en testen van de beveiligingsmaatregelen van een netwerk- of informatiesysteem, om te bepalen of er sprake is van een mogelijke kwetsbaarheid en de door de melder gebruikte methoden na te gaan. Hierbij kunnen met name reverse engineering-methoden worden aangewend.

Le cinquième paragraphe dispose que le CSIRT national doit coopérer avec les CSIRT des autres États membres lorsqu’une vulnérabilité signalée (que ce soit au travers d’une divulgation coordonnée ou d’un signalement) est susceptible d’avoir un impact significatif sur des entités dans plusieurs États membres.	De vijfde paragraaf bepaalt dat het nationale CSIRT moet samenwerken met de CSIRT's van andere lidstaten wanneer een gemelde kwetsbaarheid (via een gecoördineerde bekendmaking of een melding) significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat.
Enfin, le sixième paragraphe prévoit que le directeur général du CSIRT national doit veiller au respect des conditions précitées par l’adoption de procédures internes.	Tot slot wijst de zesde paragraaf erop dat de directeur-generaal van het nationale CSIRT moet zorgen voor de naleving van bovengenoemde voorwaarden en hiervoor interne procedures uitwerkt.
Article 23	Artikel 23
La disposition a pour objectif de créer, dans certaines conditions strictes, un cadre protecteur (“safe harbour”) pour les hackers éthiques ou “lanceurs d’alerte numériques”, auteurs d’un signalement auprès du CSIRT national.	De bepaling is bedoeld om onder bepaalde strikte voorwaarden een beschermend kader (“safe harbour”) uit te werken voor ethische hackers of “digitale klokkenluiders”, die een melding naar het nationale CSIRT sturen.
Afin de bénéficier de cette protection, il faut que les lanceurs d’alerte numériques respectent la procédure prévue par l’article 22 et les conditions énoncées par le présent article.	Om deze bescherming te genieten, moeten digitale klokkenluiders de procedure van artikel 22 en de voorwaarden van dit artikel naleven.
Premièrement, le hacker éthique ne peut utiliser ses recherches pour des motifs frauduleux ou dans l’intention de nuire. Par exemple, celui-ci ne peut tenter de monnayer les informations découvertes auprès de l’organisation responsable (en l’absence d’un programme de récompense prédéfini) ou de tiers. De même, le hacker éthique ne peut utiliser à son profit la vulnérabilité découverte.	Ten eerste mogen ethische hackers hun onderzoek niet gebruiken met bedrieglijk opzet of het oogmerk om te schaden. Ze mogen de verantwoordelijke organisatie (bij gebrek aan een vooraf bepaald beloningsprogramma) of derden bijvoorbeeld niet trachten te laten betalen voor de ontdekte informatie. Ethische hackers mogen de ontdekte kwetsbaarheid evenmin in hun voordeel gebruiken.
Deuxièmement, le hacker éthique (personne physique ou morale) doit avoir informé l’organisation concernée sans délai et au plus tard dans les 24 heures de la découverte d’une potentielle vulnérabilité.	Ten tweede moeten ethische hackers (natuurlijke of rechtspersonen) de betrokken organisatie onverwijld en uiterlijk binnen 24 uur na de ontdekking van een mogelijke kwetsbaarheid hiervan op de hoogte hebben gebracht.
Troisièmement, le hacker éthique doit adresser à l’organisation et au CSIRT national une notification complète sans délai et au plus tard dans les 72 heures suivant la découverte d’une	Ten derde moeten ethische hackers de organisatie en het nationale CSIRT onverwijld en uiterlijk binnen 72 uur na de ontdekking van een mogelijke kwetsbaarheid een volledige

potentielle vulnérabilité.	kennisgeving sturen.
La ou les personne(s) physique(s) ou morale(s) effectuant le signalement doivent avoir participé partiellement ou complètement aux recherches relatives à la vulnérabilité découverte. En effet, l'auteur du signalement doit pouvoir, le cas échéant, être tenu responsable des méthodes de recherches utilisées: il doit donc y avoir contribué au moins partiellement. Lorsque plusieurs chercheurs ont participé aux recherches, le signalement peut être effectué au nom de plusieurs personnes qui en assument alors collectivement la responsabilité. Par facilité, plusieurs découvertes peuvent être également communiquées dans un seul signalement.	De natuurlijke persoon (personen) of rechtspersoon (rechtspersonen) die de melding doet (doen), moet(en) hebben deelgenomen aan het volledige onderzoek rond de ontdekte kwetsbaarheid of aan een deel ervan. In voorkomend geval moet de melder immers aansprakelijk kunnen worden gesteld voor de gebruikte onderzoeksmethoden: hij moet hier dus ten minste gedeeltelijk aan hebben bijgedragen. Indien meerdere onderzoekers aan het onderzoek hebben deelgenomen, kan de melding gebeuren op naam van verschillende personen, die dan samen de verantwoordelijkheid op zich nemen. Gemakshalve kunnen verschillende ontdekkingen ook in één melding worden meegedeeld.
Quatrièmement, le hacker éthique doit s'engager dans ses actions et ses méthodes de recherches à respecter les principes de nécessité et de proportionnalité. Son attitude doit rester nécessaire et proportionnée au regard de l'objectif poursuivi de vérifier l'existence d'une vulnérabilité en vue d'améliorer la sécurité du système, du processus ou du contrôle concerné. Les techniques utilisées doivent être strictement nécessaires et proportionnées à la démonstration d'une faille de sécurité.	Ten vierde moeten ethische hackers zich ertoe verbinden de beginselen van noodzakelijkheid en evenredigheid in acht te nemen bij hun acties en onderzoeksmethoden. Hun gedrag moet noodzakelijk zijn om na te gaan of er sprake is van een kwetsbaarheid teneinde de beveiliging van het systeem, het proces of de controle in kwestie te verbeteren, en evenredig zijn met dit doel. De gebruikte technieken moeten strikt noodzakelijk en evenredig zijn om een beveiligingsprobleem aan te tonen.
Si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin. De même, il n'est pas justifié de perturber la disponibilité des services fournis par l'équipement concerné.	Indien het beveiligingsprobleem op kleine schaal is aangetoond, moet niet verder worden gegaan. Het is evenmin verantwoord om de beschikbaarheid van de door de betrokken apparatuur verleende diensten te verstoren.
De même, toutes les données collectées par le hacker éthique devraient être supprimées dans un délai raisonnable après le signalement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps ou si une procédure judiciaire est en cours, le hacker éthique doit veiller à ce que ces données sont conservées en toute sécurité durant cette période.	Ook moeten alle door ethische hackers verzamelde gegevens binnen een redelijke termijn na de melding worden verwijderd. Indien het noodzakelijk is om deze gegevens nog enige tijd te bewaren of indien er een gerechtelijke procedure loopt, moeten ethische hackers ervoor zorgen dat deze gegevens in deze periode veilig worden bewaard.
Afin d'aider les hackers éthiques dans cette évaluation, le CSIRT national fournira sur son	Om ethische hackers bij deze evaluatie te helpen, zal het nationale CSIRT op zijn website

site internet une liste indicative des techniques pouvant être considérées comme nécessaires et proportionnées.	een indicatieve lijst van technieken publiceren die als noodzakelijk en evenredig kunnen worden beschouwd.
<p>Dans un tel cadre, peuvent être considérées notamment comme des actions nécessaires pour vérifier l'existence d'une vulnérabilité et pour la rapporter :</p> <ul style="list-style-type: none"> - l'accès ou la tentative d'accès non autorisée à un système informatique (art. 550 bis, § 1 et 4, du Code pénal); - le dépassement ou la tentative de dépassement d'une autorisation d'accès à un système informatique (550 bis, § 2 et 4, du Code pénal); - la reprise ou la copie de données informatiques (art. 550 bis, § 3 du Code pénal); - l'élaboration ou la détention de hacking tools (art. 550 bis, § 5 du Code pénal); - la détention, la révélation, l'usage ou la divulgation d'information issues d'un accès non autorisé – par exemple des informations disponibles sur internet (550 bis § 7 du Code pénal); - l'introduction ou la modification de données dans un système informatique (550 ter du Code pénal); - l'interception ou la tentative d'interception de communications (l'article 145 de la loi du 13 juin 2005 relative aux communications électroniques); - la violation d'une obligation de secret professionnel (art. 458 du Code pénal) ou d'une obligation contractuelle de confidentialité. 	<p>In dat kader kunnen met name de volgende acties als noodzakelijk worden beschouwd om het bestaan van een kwetsbaarheid na te gaan en te melden:</p> <ul style="list-style-type: none"> - - het ongeoorloofd binnendringen in een informaticasysteem of de poging daartoe (art. 550 bis, § 1 en 4, van het Strafwetboek); - - het overschrijden van een toegangsbevoegdheid tot een informaticasysteem of de poging daartoe (art. 550 bis, § 2 en 4, van het Strafwetboek); - - het overnemen of kopiëren van informaticagegevens (art. 550 bis, § 3 van het Strafwetboek); - - het ontwikkelen of bezitten van hacking tools (art. 550 bis, § 5, van het Strafwetboek); - - het bijhouden, onthullen, gebruiken of verspreiden van informatie die door ongeoorloofde binnendringing is verkregen - bijvoorbeeld informatie die beschikbaar is op het internet (art. 550 bis, § 7, van het Strafwetboek); - - het invoeren of wijzigen van gegevens in een informaticasysteem (art. 550 ter van het Strafwetboek); - - het onderscheppen van communicatie of de poging daartoe (artikel 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie); - - de schending van een beroepsgeheim (artikel 458 van het Strafwetboek) of van een contractuele geheimhoudingsplicht.
Cinquièmement, il est exigé que le hacker éthique n'ait pas publiquement divulgué les informations relatives à la vulnérabilité découverte, sans l'accord du CSIRT national.	Ten vijfde mogen ethische hackers geen informatie over de ontdekte kwetsbaarheid openbaar hebben gemaakt zonder de toestemming van het nationale CSIRT.
En effet, la divulgation publique d'une vulnérabilité alors que celle-ci existe toujours auprès de nombreux utilisateurs, constitue un risque important de sécurité en matière de technologies de l'information. En effet, des tiers malveillants pourraient développer et répandre	Het openbaar maken van een kwetsbaarheid, terwijl die nog altijd bij tal van gebruikers bestaat, vormt immers een groot beveiligingsrisico inzake informatietechnologie. Derden met slechte bedoelingen zouden immers

des outils spécifiques pour exploiter cette vulnérabilité. Il n'est donc pas souhaitable qu'une faille de sécurité soit divulguée au public, avant qu'elle n'ait été corrigée par l'organisation responsable, en lui accordant le temps nécessaire à la résolution du problème, ou avant que l'organisation responsable n'ait pu en informer préalablement ses clients ou utilisateurs.	specifieke tools kunnen ontwikkelen en verspreiden om misbruik te maken van deze kwetsbaarheid. Het is dus niet wenselijk om een beveiligingsprobleem openbaar te maken voordat het door de verantwoordelijke organisatie wordt verholpen, die daarvoor de nodige tijd moet krijgen, of voordat de verantwoordelijke organisatie haar klanten of gebruikers hierover heeft kunnen informeren.
La divulgation complète est également susceptible de retarder le déploiement efficace d'une solution à la vulnérabilité en imposant à l'organisation responsable de réagir en situation de crise. De même, la révélation publique de failles de sécurité peut porter atteinte à la réputation de l'organisation responsable et entamer la confiance des utilisateurs dans les technologies concernées.	De volledige bekendmaking kan ook de doeltreffende toepassing van een oplossing voor de kwetsbaarheid vertragen door de verantwoordelijke organisatie te verplichten om in een crisissituatie te reageren. Ook kan het openbaar maken van beveiligingsproblemen de reputatie van de verantwoordelijke organisatie schaden en het vertrouwen van gebruikers in de betrokken technologieën ondermijnen.
Par voie de conséquence, la divulgation publique d'informations sur une vulnérabilité doit être réalisée avec beaucoup de précaution et de manière coordonnée au moins avec le CCB.	Daarom moet het openbaar maken van informatie over een kwetsbaarheid heel omzichtig en minstens in overleg met het CCB gebeuren.
Sixièmement, il est prévu une condition supplémentaire pour les réseaux et systèmes d'information des organisations visées à l'article 5, § 4 et § 5, et des organes judiciaires ainsi que pour les informations traitées par eux ou pour leur compte. Dans ce cas, il est nécessaire que le chercheur ait conclu, avant la commission de ces actes, un accord écrit avec le service compétent sur les modalités et la méthodologie à utiliser dans le cadre de la recherche de potentielles vulnérabilités. Les informations et les systèmes de certaines entités sont tels qu'ils sont non seulement particulièrement sensibles, mais qu'ils peuvent également avoir un impact considérable sur la sécurité publique et le secret des enquêtes criminelles et de renseignement. Le(s) service(s) concerné(s) peut (peuvent) alors imposer des modalités particulières obligatoires par le biais d'une « politique » annexée à l'accord. Par exemple, il est possible pour ces entités d'imposer des délais particuliers de notification et des conditions de publication ou d'identification préalable.	Ten zesde is een bijkomende voorwaarde toegevoegd voor de netwerk- en informatiesystemen van de in artikel 5, § 4 en § 5, bedoelde organisaties en van de rechterlijke instanties, alsook voor de informatie die door hen of namens hen wordt verwerkt. In dat geval moet de onderzoeker vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde dienst over de modaliteiten en de te hanteren methodologie in het kader van het onderzoek naar mogelijke kwetsbaarheden. De informatie en systemen van bepaalde entiteiten zijn van die aard dat ze niet alleen bijzonder gevoelig zijn maar tevens een enorme impact kunnen hebben op de openbare veiligheid en het geheim van strafrechtelijke en inlichtingenonderzoeken. De betrokken dienst(en) kan (kunnen) dan specifieke regels opleggen via een bij de overeenkomst gevoegde "policy". Deze entiteiten kunnen bijvoorbeeld specifieke meldingstermijnen opleggen, alsook voorwaarden inzake bekendmaking en voorafgaande identificatie.

Moyennant le respect de ces différentes conditions et indépendamment de l'existence ou non d'une politique de divulgation coordonnée des vulnérabilités, le lanceur d'alerte n'est alors pas considéré comme ayant commis une infraction aux articles 314bis, 458, 550bis, 550ter du Code pénal ni à l'article 145 de la loi du 13 juin 2005.	Indien deze verschillende voorwaarden zijn vervuld en ongeacht het eventuele bestaan van een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, wordt de klokkenluider dan niet geacht een inbreuk te hebben gepleegd op de artikelen 314bis, 458, 550bis, 550ter van het Strafwetboek noch op artikel 145 van de wet van 13 juni 2005.
Les actions doivent être limitées strictement aux faits nécessaires pour permettre la recherche et le signalement d'une vulnérabilité d'un réseau et système d'information.	De acties moeten strikt beperkt blijven tot feiten die noodzakelijk zijn om een kwetsbaarheid in een netwerk- en informatiesysteem te kunnen opsporen en melden.
<p>Le troisième paragraphe rappelle que, toute autre responsabilité, en ce compris pénale, 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 premier, continue d'être régie par le droit applicable. Cela signifie que l'auteur du signalement pourra être poursuivi pénalement, civilement ou disciplinairement pour tous les actes accomplis qui n'étaient pas nécessaires pour vérifier l'existence d'une vulnérabilité. De même, l'auteur d'un signalement ne bénéficie pas de la protection légale prévue au paragraphe premier lorsqu'il agit avec une intention frauduleuse ou par dessein de nuire.</p> <p>Enfin, il faut tenir compte du fait que cette protection légale est limitée à l'application du droit belge et est sans préjudice du statut juridique spécifique des organisations internationales et européennes ou des missions diplomatiques établies sur le territoire national.</p>	<p>De derde paragraaf wijst erop dat het toepasselijke recht blijft gelden voor elke andere aansprakelijkheid, met inbegrip van de strafrechtelijke aansprakelijkheid, 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 de eerste paragraaf. Dit betekent dat melders strafrechtelijk, burgerrechtelijk of tuchtrechtelijk kunnen worden vervolgd voor alle handelingen die niet noodzakelijk waren om na te gaan of er sprake was van een kwetsbaarheid. Ook komen melders niet in aanmerking voor de in de eerste paragraaf bedoelde wettelijke bescherming indien ze handelen met bedrieglijk opzet of met het oogmerk om te schaden.</p> <p>Tot slot moet rekening worden gehouden met het feit dat deze wettelijke bescherming beperkt is tot de toepassing van het Belgisch recht en geen afbreuk doet aan het specifiek juridisch statuut van internationale en Europese organisaties of van diplomatieke missies die op het nationale grondgebied gevestigd zijn.</p>
Section 2	Afdeling 2
<i>Les éventuelles autorités sectorielles</i>	<i>De eventuele sectorale overheden</i>
Article 24	Artikel 24
Cet article octroie des compétences aux éventuelles autorités sectorielles, en plus des	Dit artikel verleent bevoegdheden aan de eventuele sectorale overheden, naast de taken

tâches et compétences visées aux différents articles du présent projet de loi.	en bevoegdheden waarvan sprake in de verschillende artikelen van dit wetsontwerp.
L'analyse et la gestion des conséquences d'un incident pour un secteur ne se confond pas avec les compétences relatives à la gestion d'incidents prévue par le présent projet de loi. Il s'agit pour l'éventuelle autorité sectorielle de gérer les conséquences hors cyber qu'un incident peut avoir pour un secteur en particulier.	De analyse en het beheer van de gevolgen van een incident voor een sector mag niet verward worden met de bevoegdheden inzake het beheer van incidenten waarin dit wetsontwerp voorziet. De eventuele sectorale overheid dient de niet-cybergevolgen te beheren die een incident voor een bepaalde sector kan hebben.
CHAPITRE 2	HOOFDSTUK 2
Coopération au niveau national	Samenwerking op nationaal niveau
Article 25	Artikel 25
Cet article porte sur la coopération au niveau national.	Dit artikel is gewijd aan de samenwerking op nationaal niveau.
Le paragraphe 1 ^{er} dispose que les autorités compétentes dans le cadre du présent projet de loi, à savoir l'autorité nationale de cybersécurité et, le cas échéant, les autorités sectorielles, coopèrent entre elles dans le cadre de l'exécution du présent projet de loi.	Paragraaf 1 bepaalt dat de uit hoofde van dit wetsontwerp bevoegde autoriteiten, namelijk de nationale cyberbeveiligingsautoriteit en, in voorkomend geval, de sectorale overheden, samenwerken in het kader van de uitvoering van dit wetsontwerp.
Le paragraphe 2 permet également la coopération, en ce compris l'échange d'informations, entre les autorités précitées et le Centre de crise nationale, les services administratifs de l'État, les autorités administratives, les autorités judiciaires, les services de renseignement et de sécurité, les services de police et les autorités de contrôle des données à caractère personnel. Sont comprises dans les autorités précitées, les autorités visées à l'article 13, § 4, de la directive NIS2.	Paragraaf 2 maakt samenwerking ook mogelijk, met inbegrip van informatie-uitwisseling, tussen voornoemde autoriteiten en het Nationaal Crisiscentrum, de administratieve diensten van de Staat, de administratieve overheden, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten, de politiediensten en de toezichthoudende autoriteiten persoonsgegevens. Ook de in artikel 13, lid 4, van de NIS2-richtlijn bedoelde autoriteiten behoren tot voornoemde autoriteiten.
L'article dispose également que les entités essentielles et importantes doivent collaborer avec les autorités visées au paragraphe 1 ^{er} . La collaboration se caractérise par l'échange d'informations concernant la sécurité de leurs systèmes et réseaux d'informations.	Het artikel bepaalt ook dat essentiële en belangrijke entiteiten moeten samenwerken met de in paragraaf 1 bedoelde autoriteiten. De samenwerking wordt gekenmerkt door de uitwisseling van informatie over de beveiliging van hun netwerk- en informatiesystemen.
Le paragraphe 4 transpose l'article 13, § 5, <i>initio</i> , de la directive NIS2, selon lequel les autorités compétentes en vertu des directives	Paragraaf 4 voorziet in de omzetting van artikel 13, lid 5, <i>initio</i> , van de NIS2-richtlijn, volgens hetwelke de autoriteiten die bevoegd zijn uit

NIS2 et (UE) 2022/2557 (directive CER) coopèrent et échangent régulièrement des informations en matière de recensement des entités critiques, de risques, de cybermenaces et d'incidents ainsi qu'en matière de risques, menaces et incidents non cyber qui touchent les entités critiques au sens de la loi CER, qui sont pour rappel <i>de facto</i> des entités essentielles au sens du présent projet de loi.	hoofde van de NIS2-richtlijn en van Richtlijn (EU) 2022/2557 (de CER-richtlijn) samenwerken en regelmatig informatie uitwisselen inzake het als kritiek aanmerken van entiteiten, over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor kritieke entiteiten als bedoeld in de CER-wet, die <i>de facto</i> immers essentiële entiteiten zijn als bedoeld in dit wetsontwerp.
Le paragraphe 5 transpose l'article 13, § 5, <i>in fine</i> , de la directive NIS2, selon lequel les autorités compétentes en vertu du présent projet de loi, du règlement (UE) n° 910/2014, la Banque nationale de Belgique, la FSMA et l'Institut belge des services postaux et des télécommunications échangent régulièrement des informations pertinentes.	De paragraaf 5 voorziet in de omzetting van artikel 13, lid 5, <i>in fine</i> , van de NIS2-richtlijn, volgens hetwelke de autoriteiten die bevoegd zijn uit hoofde van dit wetsontwerp en Verordening (UE) nr. 910/2014, de Nationale Bank van België, de FSMA en het Belgisch Instituut voor postdiensten en telecommunicatie regelmatig relevante informatie uitwisselen.
Le dernier paragraphe impose la création d'une plateforme au sein de laquelle les autorités compétentes dans le cadre du présent projet de loi pourront échanger de l'information et se coordonner afin d'exécuter les obligations du présent projet de loi.	Volgens de laatste paragraaf wordt een platform opgericht dat de in het kader van dit wetsontwerp bevoegde autoriteiten toelaat informatie uit te wisselen en hun optreden op elkaar af te stemmen om de verplichtingen van dit wetsontwerp uit te voeren.
Au travers de cette plateforme, il sera possible d'établir des rapports d'évaluation de l'exécution de la loi, d'organiser et de coordonner les inspections, d'échanger sur les pratiques de supervision, d'offrir des formations, voire d'assurer plus de coordination entre les autorités publiques et le secteur privé ou le monde scientifique (via la consultation de parties prenantes notamment).	Dit platform biedt de mogelijkheid om beoordelingsverslagen op te stellen over de uitvoering van de wet, inspecties te organiseren en te coördineren, toezichtspraktijken uit te wisselen, opleidingen aan te bieden en zelfs om te zorgen voor een betere coördinatie tussen de overheden en de particuliere sector of de wetenschappelijke wereld (met name via de raadpleging van stakeholders).
CHAPITRE 3	HOOFDSTUK 3
Confidentialité et échanges d'information	Vertrouwelijkheid en informatie-uitwisseling
Article 26	Artikel 26
Cet article porte sur la confidentialité et l'échange d'informations. Cela étant, cette disposition ne porte pas préjudice aux règles applicables de par la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de	Dit artikel behandelt de vertrouwelijkheid en de informatie-uitwisseling. Deze bepaling doet evenwel geen afbreuk aan de regels die van toepassing zijn krachtens de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten,

sécurité et au service public réglementé, 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, la loi du 11 avril 1994 relative à la publicité de l'administration ou de par d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.	veiligheidsadviezen en de publiek gereuleerde dienst, de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspuitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of krachtens andere wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de nationale openbare veiligheid waarborgen.
L'article impose, en son paragraphe 2, un secret professionnel, au sens de l'article 458 du Code pénal, à toute personne appelée à prêter son concours professionnel à l'évaluation de la conformité ou à la supervision dans le cadre de la présente loi.	Paragraaf 2 van het artikel bepaalt dat eenieder die beroepshalve zijn medewerking dient te verlenen aan de conformiteitsbeoordeling of het toezicht in het kader van dit wetsontwerp, onderworpen is aan het beroepsgeheim bedoeld in artikel 458 van het Strafwetboek.
Selon cette disposition, les autorités compétentes dans le cadre du présent projet de loi, les entités essentielles et importantes et leurs sous-traitants limitent l'accès aux informations relatives à l'exécution du présent projet de 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 le présent projet de loi. De plus, les membres du personnel des entités essentielles et importantes sont soumis au secret professionnel.	Volgens deze bepaling beperken de uit hoofde van dit wetsontwerp bevoegde autoriteiten, de essentiële en belangrijke entiteiten en hun onderaannemers de toegang tot de informatie betreffende de uitvoering van dit wetsontwerp 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 dit wetsontwerp. Bovendien zijn de personeelsleden van de essentiële en belangrijke entiteiten onderworpen aan het beroepsgeheim.
L'article prévoit en son paragraphe 4 que l'échange d'information avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, est possible pour autant que cela soit nécessaire à l'application du présent projet de loi et que cet échange d'informations respecte les dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique.	Volgens paragraaf 4 van het artikel is mogelijk om informatie uit te wisselen met autoriteiten van de Europese Unie, buitenlandse of nationale autoriteiten, voor zover dit noodzakelijk is voor de toepassing van dit wetsontwerp en deze informatie-uitwisseling voldoet aan de wettelijke bepalingen die de vertrouwelijkheid van informatie met betrekking tot de wezenlijke belangen van de openbare veiligheid waarborgen.
Article 27	Artikel 27
Cet article transpose l'article 29 de la directive NIS2. Il prévoit que, lorsque des entités échangent des informations au sein de communautés, notamment relatives aux cybermenaces, aux incidents évités ou encore aux vulnérabilités, cet échange d'informations	Dit artikel voorziet in de omzetting van artikel 29 van de NIS2-richtlijn. Het bepaalt dat, wanneer entiteiten informatie uitwisselen binnen gemeenschappen, met name betreffende cyberdreigingen, bijna-incidenten of kwetsbaarheden, deze informatie-

se fait au travers d'accords de partage d'informations en matière de cybersécurité.	uitwisseling gebeurt door middel van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging.
L'autorité nationale de cybersécurité a pour tâche de faciliter la mise en place de tels accords et reçoit des informations des entités soumises au champ d'application du projet de loi lorsque ces entités concluent de tels accords ou lorsqu'elles s'en retirent.	De nationale cyberbeveiligingsautoriteit heeft tot taak de vaststelling van deze regelingen te faciliteren en ontvangt informatie van de entiteiten die onderworpen zijn aan het toepassingsgebied van het wetsontwerp wanneer deze entiteiten dergelijke regelingen aangaan of zij er zich uit terugtrekken.
CHAPITRE 4	HOOFDSTUK 4
Stratégie nationale en matière de cybersécurité	Nationale cyberbeveiligingsstrategie
Article 28	Artikel 28
Cet article porte sur la stratégie nationale en matière de cybersécurité, les autorités impliquées dans sa conception, ses mises à jours et son contenu.	Dit artikel gaat nader in op de nationale cyberbeveiligingsstrategie en de autoriteiten die betrokken zijn bij het ontwerp, de bijwerkingen en de inhoud ervan.
La stratégie consiste en un cadre cohérent « <i>prévoyant des objectifs stratégiques et des priorités dans le domaine de la cybersécurité et de la gouvernance pour les atteindre</i> » (directive NIS2, considérant 48).	De strategie bestaat uit een samenhangend kader " <i>met strategische doelstellingen en prioriteiten op het gebied van cyberbeveiliging en de governance om deze te verwezenlijken</i> " (NIS2-richtlijn, overweging 48).
Cette stratégie comprend, entre autres, les objectifs et les priorités de la stratégie, un cadre de gouvernance visant à atteindre ces objectifs et priorités, une liste des différents acteurs et autorités concernés, un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité, etc.	Deze strategie omvat onder meer doelstellingen en prioriteiten van de strategie, een governancekader om deze doelstellingen en prioriteiten te verwezenlijken, een lijst van de verschillende betrokken belanghebbenden en autoriteiten, een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren, enz.
Dans le cadre de cette stratégie, la Belgique devra adopter des politiques, entre autres, dans le domaine de la chaîne d'approvisionnement, de la gestion des vulnérabilités et de la divulgation coordonnée des vulnérabilités, des marchés publics, du partage d'informations, etc.	In het kader van deze strategie moet België beleidsmaatregelen nemen, onder meer op het gebied van de toeleveringsketen, het beheer van kwetsbaarheden en de gecoördineerde bekendmaking van kwetsbaarheden, overheidsopdrachten, het delen van informatie, enz.
Le premier paragraphe dispose que cette stratégie est adoptée par le Conseil des Ministres et est mise à jour au moins tous les 5	Paragraaf 1 bepaalt dat deze strategie wordt aangenomen bij de Ministerraad en minstens om de 5 jaar wordt bijgewerkt, na advies van de

ans, après avis du Conseil national de sécurité, des autorités compétentes dans le cadre du présent projet de loi, du Centre de crise national et des autorités de protection des données.	Nationale Veiligheidsraad, de uit hoofde van dit wetsontwerp bevoegde autoriteiten, het Nationaal Crisiscentrum en de gegevensbeschermingsautoriteiten.
Les deuxième et troisième paragraphes déterminent les éléments devant être contenus dans la stratégie.	De paragrafen 2 en 3 bepalen welke elementen de strategie moet bevatten.
CHAPITRE 5	HOOFDSTUK 5
Le plan national de réaction aux crises et incidents de cybersécurité majeurs	Het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons
Article 29	Artikel 29
Cet article transpose l'article 9, § 4, de la directive NIS2 en assurant la cohérence avec l'application du cadre national de gestion de crise.	Dit artikel voorziet in de omzetting van artikel 9, lid 4, van de NIS2-richtlijn en zorgt voor samenhang met de toepassing van het nationale crisisbeheerkader.
Il dispose que le Roi adopte, par arrêté royal, un plan national de réaction aux crises et incidents de cybersécurité et précise que ce plan constitue un plan national au sens de l'article 21 de la loi du [xx sur la gestion de crise et la planification d'urgence].	Het bepaalt dat de Koning, bij koninklijk besluit, een nationaal plan voor cyberbeveiligingsincidenten en crisisrespons goedkeurt en verduidelijkt dat dit plan een nationaal plan is als bedoeld in artikel 21 van de wet van [xx betreffende het crisisbeheer en de noodplanning].
Il énumère également les éléments devant se trouver dans ce plan selon l'article 9, § 4, de la directive NIS2 tout en précisant que cela ne préjudicie l'application de la loi du [xx sur la gestion de crise et la planification d'urgence]. De cette manière, le projet de loi ajoute les exigences de la directive NIS2 relatives au contenu du plan national de gestion de crise cyber aux exigences déterminées par le cadre général de gestion de crise, qui demeure applicable.	Het somt ook de elementen op die dit plan ten minste moet bevatten overeenkomstig artikel 9, lid 4, van de NIS2-richtlijn en verduidelijkt dat dit geen afbreuk doet aan de toepassing van de wet van [xx betreffende het crisisbeheer en de noodplanning]. Op die manier voegt het wetsontwerp de voorschriften van de NIS2-richtlijn betreffende de inhoud van het nationaal plan voor cybercrisisbeheer toe aan de voorschriften die bepaald worden door het algemene crisisbeheerkader, dat van toepassing blijft.
TITRE 3	TITEL 3
<i>Mesures de gestion des risques en matière de cybersécurité et obligations d'information</i>	<i>Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen</i>
CHAPITRE 1 ^{ER}	HOOFDSTUK 1

Mesures de gestion des risques en matière de cybersécurité	Maatregelen voor het beheer van cyberbeveiligingsrisico's
Article 30	Artikel 30
Cet article transpose l'article 21 de la directive NIS2 et contient les principales exigences légales des entités soumises à la loi en matière de mesures de cybersécurité.	Dit artikel voorziet in de omzetting van artikel 21 van de NIS2-richtlijn en bevat de belangrijkste wettelijke voorschriften inzake cyberbeveiligingsmaatregelen voor de entiteiten die onderworpen zijn aan de wet.
Les entités essentielles et importantes ont l'obligation de prendre les mesures appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent et pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services ainsi que sur d'autres services. Comme le précise le considérant 77 de la directive NIS2, « dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d'information. Il convient de promouvoir et de faire progresser une culture de la gestion des risques impliquant une analyse des risques et l'application de mesures de gestion des risques en matière de cybersécurité adaptées aux risques encourus ».	Essentiële en belangrijke entiteiten zijn verplicht passende en evenredige maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de ontvangers van hun diensten en voor andere diensten te beperken. Overweging 77 van de NIS2-richtlijn verduidelijkt in dit verband dat "de verantwoordelijkheid voor het waarborgen van de beveiliging van netwerk- en informatiesystemen [...] voor een groot deel bij de essentiële en belangrijke entiteiten [ligt]. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst".
Les mesures devant être adoptées par les entités essentielles et importantes doivent être appropriées et proportionnées. Sur ce point, la directive NIS2 précise que « pour éviter que la charge financière et administrative imposée aux entités essentielles et importantes ne soit disproportionnée, il convient que les mesures de gestion des risques en matière de cybersécurité soient proportionnées aux risques auxquels le réseau et le système d'information concernés sont exposés, en prenant en compte l'état de l'art de ces mesures ainsi que, s'il y a lieu, des normes européennes ou internationales pertinentes, et du coût de mise en œuvre de ces mesures » (considérant 81).	Essentiële en belangrijke entiteiten moeten maatregelen nemen die passend en evenredig zijn. Op dit punt bevat de NIS2-richtlijn de volgende toelichting: "Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de maatregelen voor het beheer van cyberbeveiligingsrisico's in verhouding staan tot de risico's voor het betrokken netwerk- en informatiesysteem, rekening houdend met de stand van de techniek van dergelijke maatregelen en, in voorkomend geval, de relevante Europese en internationale normen, alsook met de kosten voor de uitvoering ervan." (overweging 81).
De plus, « les mesures de gestion des risques en matière de cybersécurité devraient être proportionnées au degré d'exposition de l'entité essentielle ou importante aux risques et à	Bovendien moeten "maatregelen voor het beheer van cyberbeveiligingsrisico's [...] in verhouding staan tot de mate waarin de essentiële of belangrijke entiteit aan risico's is

<p><i>l'impact sociétal et économique potentiel d'un incident. Lors de la mise en place de mesures de gestion des risques en matière de cybersécurité adaptées aux entités essentielles et importantes, il convient de tenir dûment compte des différents niveaux d'exposition aux risques des entités essentielles et importantes, telles que la criticité de l'entité, les risques, y compris les risques sociétaux, auxquels elle est exposée, la taille de l'entité et la probabilité de survenance d'incidents et leur gravité, y compris leur impact sociétal et économique »</i> (considérant 82, directive NIS2). Ces considérations, fondamentales dans l'évaluation des mesures à adopter, reprises dans l'article 21, § 1^{er}, de la directive NIS2, sont transposées au sein du présent article.</p>	<p><i>blootgesteld en de maatschappelijke en economische gevolgen die een incident zou hebben. Bij het vaststellen van maatregelen voor het beheer van cyberbeveiligingsrisico's die zijn aangepast aan essentiële en belangrijke entiteiten, moet terdege rekening worden gehouden met de uiteenlopende mate waarin essentiële en belangrijke entiteiten aan risico's zijn blootgesteld, overeenkomstig het kritieke karakter van de entiteit, de risico's, met inbegrip van maatschappelijke risico's, waaraan de entiteit 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"</i> (overweging 82, NIS2-richtlijn). Deze overwegingen zijn fundamenteel bij de beoordeling van de te nemen maatregelen. Ze zijn opgenomen in artikel 21, lid 1, van de NIS2-richtlijn en worden omgezet in dit artikel.</p>
<p>Le paragraphe 3 de la présente disposition contient deux obligations à charge des entités essentielles et importantes : fonder l'adoption des mesures précitées sur une approche tout risque et comprendre au moins les mesures visées à ce paragraphe. L'approche tout risque et les mesures énumérées aux points 1° à 10° transposent directement l'article 21, § 2, de la directive NIS2.</p>	<p>Paragraaf 3 van deze bepaling bevat twee verplichtingen voor essentiële en belangrijke entiteiten: voornoemde maatregelen moeten gebaseerd zijn op een benadering die alle gevaren omvat en ten minste betrekking hebben op de in deze paragraaf bedoelde maatregelen. De benadering die alle gevaren omvat en de maatregelen opgesomd in de punten 1° tot 10° voorzien rechtstreeks in de omzetting van artikel 21, lid 2, van de NIS2-richtlijn.</p>
<p>Une précision est apportée au 11° du paragraphe 3, à savoir l'exigence d'adopter une politique de divulgation coordonnée des vulnérabilités. Cet élément découle de l'article 21, § 2, sous e), de la directive qui prévoit le traitement et la divulgation des vulnérabilités, ainsi que de la politique nationale en la matière promue par le CCB.</p>	<p>Er wordt een verduidelijking aangebracht in punt 11° van paragraaf 3, betreffende de vereiste om een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden in te voeren. Dit element vloeit voort uit artikel 21, lid 2, onder e), van de richtlijn dat voorziet in de respons op en de bekendmaking van kwetsbaarheden, alsook uit het nationale beleid ter zake dat het CCB voorstaat.</p>
<p>Etant donné l'importance des risques liés à des vulnérabilités, la volonté est d'insérer clairement l'adoption d'une telle politique de divulgation coordonnée des vulnérabilités dans les mesures obligatoires de mesures de gestion des risques en matière de cybersécurité.</p>	<p>Gezien het belang van de risico's van kwetsbaarheden, is het de bedoeling om de invoering van een dergelijk beleid voor de gecoördineerde bekendmaking van kwetsbaarheden duidelijk op te nemen bij de verplichte maatregelen voor het beheer van cyberbeveiligingsrisico's.</p>

Le paragraphe 4 dispose que, dans le cadre de l'adoption des mesures précitées, les entités essentielles et importantes 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.	Paragraaf 4 bepaalt dat, in het kader van de invoering van voornoemde maatregelen, essentiële en belangrijke entiteiten rekening houden 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.
Selon la directive, « <i>il est tout particulièrement important de répondre aux risques découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs [...] vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et où des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers</i> » (considérant 85).	Volgens de richtlijn is “het aanpakken van risico's die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, [...] bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geweest van cyberaanvallen en waarbij kwaadwillende daders de beveiliging van de netwerk- en informatiesystemen van een entiteit in gevaar hebben kunnen brengen door gebruik te maken van kwetsbaarheden die van invloed zijn op producten en diensten van derden” (overweging 85).
Le cas échéant, des évaluations coordonnées des risques pour la sécurité de certaines chaînes d'approvisionnement pourront être effectuées par le groupe de coopération, en coopération avec la Commission européenne et l'ENISA, conformément à l'article 22, § 1 ^{er} , de la directive NIS2. Les mesures adoptées par les entités essentielles et importantes devront être appropriées au regard de ces évaluations.	In voorkomend geval kan de samenwerkingsgroep, in samenwerking met de Europese Commissie en Enisa, gecoördineerde beveiligingsrisicobeoordelingen van bepaalde toeleveringsketens uitvoeren, overeenkomstig artikel 22, lid 1, van de NIS2-richtlijn. De door essentiële en belangrijke entiteiten genomen maatregelen moeten passend zijn in het licht van deze beoordelingen.
Le paragraphe 5 précise explicitement que les entités essentielles et importantes sont tenues de réaliser une analyse des risques pour déterminer leurs mesures de cybersécurité, comme cela découle des différentes exigences de l'article 21, paragraphes 1 ^{er} et 2. A cette fin, des recommandations seront fournies par l'autorité nationale de cybersécurité sur la manière de réaliser cette analyse de risques.	Paragraaf 5 bepaalt uitdrukkelijk dat essentiële en belangrijke entiteiten een risicoanalyse moeten uitvoeren om hun cyberbeveiligingsmaatregelen te bepalen, zoals volgt uit de verschillende voorschriften van artikel 21, leden 1 en 2. De nationale cyberbeveiligingsautoriteit zal daartoe aanbevelingen verstrekken over de uitvoeringswijze van deze risicoanalyse.
Le même paragraphe souligne également que les mesures de gestion des risques adoptées par les entités essentielles et importantes doivent être documentées au moins dans une politique de sécurité des systèmes et réseaux d'information (« P.S.I. »).	Dezelfde paragraaf wijst er ook op dat de risicobeheersmaatregelen die essentiële en belangrijke entiteiten nemen, minstens in een beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”) moeten worden gedocumenteerd.
Il s'agit du maintien d'une obligation qui existait	Deze verplichting voor aanbieders van

déjà dans le cadre de la loi NIS1, à charge des opérateurs de services essentiels et qui se trouve de manière implicite dans la directive NIS2 au travers des mesures devant être adoptées par les entités (article 21, § 2, de la directive NIS2).	essentiële diensten die al bestond in het kader van NIS1-wet, wordt behouden. Ze is impliciet opgenomen in de NIS2-richtlijn via de maatregelen die entiteiten moeten nemen (artikel 21, lid 2, van de NIS2-richtlijn).
Enfin en son dernier paragraphe, la présente disposition prévoit que toute entité essentielle ou importante qui constate qu'elle ne se conforme pas aux mesures précitées, doit prendre, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées, conformément à l'article 21, § 4, de la directive NIS2.	Tot slot vermeldt de laatste paragraaf van deze bepaling dat elke essentiële en belangrijke entiteit die vaststelt dat zij niet voldoet aan voornoemde maatregelen, onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen moet nemen, overeenkomstig artikel 21, lid 4, van de NIS2-richtlijn.
Article 31	Artikel 31
Cet article transpose l'article 20 de la directive NIS2, selon lequel les organes de direction des entités essentielles et importantes doivent approuver les mesures évoquées au commentaire de l'article 30, superviser leur mise en œuvre et sont responsables en cas de violations des obligations visées à l'article 30 du présent projet de loi.	Dit artikel voorziet in de omzetting van artikel 20 van de NIS2-richtlijn, volgens hetwelke de bestuursorganen van essentiële en belangrijke entiteiten de in de commentaar bij artikel 30 vermelde maatregelen moeten goedkeuren, toezien op de uitvoering ervan en aansprakelijk zijn voor inbreuken op de in artikel 30 van dit wetsontwerp bedoelde verplichtingen.
A cette fin, les membres des organes de direction précités doivent suivre une formation permettant de démontrer qu'ils ont acquis des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis.	Daartoe moeten de leden van voornoemde bestuursorganen een opleiding volgen zodat ze kunnen aantonen over voldoende vaardigheden te beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de verleende diensten te kunnen beoordelen.
La directive NIS2 précise, en son article 20, § 1 ^{er} , alinéa 2, que cette disposition ne porte pas préjudice au droit national en ce qui concerne les règles de responsabilité applicables aux institutions publiques et les règles de responsabilité des agents de la fonction publique et des responsables élus ou nommés.	Artikel 20, lid 1, tweede alinea, van de NIS2-richtlijn verduidelijkt dat deze bepaling geen afbreuk doet aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen.
Cette disposition est transposée dans le projet de loi au paragraphe 1 ^{er} , alinéa 2, de l'article faisant l'objet du présent commentaire. En droit belge, cela signifie que le présent projet de loi ne déroge aux règles existantes en matière de responsabilité précitées, notamment la loi du 10 février 2003 relative à la responsabilité des	Deze bepaling wordt in het wetsontwerp omgezet via paragraaf 1, tweede lid, van het artikel waarop deze commentaar betrekking heeft. Naar Belgisch recht betekent dit dat dit wetsontwerp niet afwijkt van de bestaande aansprakelijkheidsregels waarnaar hierboven wordt verwezen, met name de wet van 10

et pour les membres du personnel au service des personnes publiques.	februari 2003 betreffende de aansprakelijkheid van en voor personeelsleden in dienst van openbare rechtspersonen.
Article 32	Artikel 32
Indépendamment des tâches éventuellement confiées à des sous-traitants, cet article rappelle que les entités essentielles et importantes demeurent responsables de l'analyse des risques à effectuer, du choix des mesures ainsi que de leur mise en œuvre dans le cadre du présent projet de loi. Cette disposition ne fait pas préjudice à l'article 31, § 1 ^{er} , alinéa 1 ^{er} , du présent projet de loi, évoqué <i>supra</i> .	Ongeacht de taken die eventueel aan onderaannemers worden toevertrouwd, herinnert dit artikel eraan dat essentiële en belangrijke entiteiten verantwoordelijk blijven voor de uit te voeren risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen in het kader van dit wetsontwerp. Deze bepaling doet geen afbreuk aan artikel 31, § 1, eerste lid, van dit wetsontwerp, waarnaar hierboven wordt verwezen.
Cela transparaît de la directive NIS2. L'article 21, § 1 ^{er} , dispose que ce sont les entités qui prennent les mesures techniques, opérationnelles et organisationnelles. Le considérant 77 explique que, « <i>dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d'information</i> », le considérant 83 indique que « <i>les entités essentielles et importantes devraient garantir la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités. Il s'agit principalement de réseaux et de systèmes d'information privés qui sont gérés par les services informatiques des entités essentielles ou importantes ou dont la gestion de la sécurité a été sous-traitée. Les mesures de gestion des risques en matière de cybersécurité et les obligations d'information prévues par la présente directive devraient s'appliquer aux entités essentielles et importantes, indépendamment du fait que ces entités effectuent la maintenance de leurs réseaux et systèmes d'information en interne ou qu'elles l'externalisent</i> » et le considérant 89 que « <i>les entités essentielles et importantes devraient adopter une vaste gamme de pratiques de cyberhygiène de base, [...]</i> ».	Dat blijkt uit de NIS2-richtlijn. Artikel 21, lid 1, bepaalt dat de entiteiten technische, operationele en organisatorische maatregelen moeten nemen. Volgens overweging 77 ligt “ <i>de verantwoordelijkheid voor het waarborgen van de beveiliging van netwerk- en informatiesystemen [...] voor een groot deel bij de essentiële en belangrijke entiteiten</i> ”. Overweging 83 wijst erop dat “ <i>essentiële en belangrijke entiteiten [...] de beveiliging van de netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, [moeten] waarborgen. Die systemen zijn voornamelijk particuliere netwerk- en informatiesystemen die door de interne IT-medewerkers van essentiële en belangrijke entiteiten worden beheerd of waarvan de beveiliging is uitbesteed. De maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen die in deze richtlijn zijn vastgesteld, moeten van toepassing zijn op de relevante essentiële en belangrijke entiteiten, ongeacht of deze entiteiten het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden</i> ” en overweging 89 voegt hieraan toe dat essentiële en belangrijke entiteiten “ <i>een breed scala aan basispraktijken op het gebied van cyberhygiëne [moeten] toepassen, [...]</i> ”.
L'objectif du présent article est d'explicitier cette responsabilité incombant aux entités essentielles et importantes, nonobstant l'application de l'article 31, § 1 ^{er} , alinéa 1 ^{er} .	Dit artikel heeft tot doel om deze verantwoordelijkheid van essentiële en belangrijke entiteiten toe te lichten, onverminderd de toepassing van artikel 31, § 1,

	eerste lid.
Article 33	Article 33
Cet article donne compétence au Roi, par arrêté délibéré en Conseil des Ministres, d'imposer des mesures supplémentaires de gestion des risques en matière de cybersécurité spécifiques à un ou plusieurs (sous-)secteurs.	Dit artikel verleent de Koning de bevoegdheid, bij besluit vastgesteld na overleg in de Ministerraad, om bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's op te leggen die specifiek zijn voor een of meer (deel)sectoren.
Ces mesures supplémentaires peuvent être adoptées après consultation de l'autorité nationale de cybersécurité et, le cas échéant, des autorités sectorielles concernées (pour autant qu'une autorité sectorielle ait été désignée pour le ou les (sous-)secteurs concernés) et des entités fédérées concernées.	Deze bijkomende maatregelen kunnen worden genomen na raadpleging van de nationale cyberbeveiligingsautoriteit en, in voorkomend geval, van de betrokken sectorale overheden (voor zover een sectorale overheid is aangewezen voor een of meer betrokken (deel)sectoren) en betrokken deelgebieden.
Certains (sous-)secteurs pourraient, selon leurs spécificités, nécessiter des mesures supplémentaires. Celles-ci peuvent être de deux types soit des mesures additionnelles c'est à dire des mesures autres que celles déjà prévues par l'ISO IEC 27001 ou le Cyberfundamentals soit des mesures spécifiques c'est à dire des mesures qui explicitent comment comprendre la norme ISO IEC 27001 ou le Cyberfundamentals pour le secteur concerné.	Voor sommige (deel)sectoren kunnen, naargelang hun specifieke kenmerken, aanvullende maatregelen vereisen. Deze kunnen van twee typen zijn: ofwel aanvullende maatregelen, d.w.z. maatregelen die afwijken van de maatregelen waarin ISO IEC 27001 of de Cyberfundamentals al voorzien, ofwel specifieke maatregelen, d.w.z. maatregelen die uitleggen hoe ISO IEC 27001 of de Cyberfundamentals voor de betreffende sector moeten worden.
Cette disposition permet d'adopter, à posteriori de telles mesures lorsque cela s'avère nécessaire.	Deze bepaling maakt het mogelijk om deze maatregelen, indien nodig, achteraf te nemen.
CHAPITRE 2	HOOFDSTUK 2
Notification d'incidents	Melding van incidenten
Section 1^{re}	Afdeling 1
<i>Notification obligatoire</i>	<i>Verplichte melding</i>
Article 34	Artikel 34
Cet article reprend les dispositions en matière de notifications obligatoires d'incidents de la directive NIS2, plus précisément le contenu de l'article 23, §§ 1 ^{er} à 3.	Dit artikel bevat de bepalingen inzake de verplichte melding van incidenten van de NIS2-richtlijn, meer bepaald de inhoud van artikel 23, leden 1 tot 3.
Tout d'abord, il est important de noter que le	In de eerste plaats is het belangrijk te

présent projet de loi a opté pour la terminologie « d'incidents significatifs », dans une volonté de continuité avec la terminologie employée dans la loi NIS1, là où la directive NIS2 emploie les termes « incidents importants ». Cela étant, les termes « incidents significatifs » du projet de loi doivent se comprendre comme ayant la même portée que les termes « incidents importants » de la directive.	vermelden dat in de Franse versie van dit wetsontwerp is gekozen voor de term “incidents significatifs” om redenen van coherentie met de terminologie van de NIS1-wet, terwijl de Franse versie van de NIS2-richtlijn de term “incidents importants” gebruikt. De term “incidents significatifs” in het wetsontwerp wordt verondersteld dezelfde draagwijdte te hebben als de term “incidents importants” in de richtlijn.
L'approche de la directive NIS2 en matière de notification d'incidents significatifs, transposée par le présent projet de loi, établit plusieurs étapes « afin de trouver le juste équilibre entre, d'une part, la notification rapide qui aide à atténuer la propagation potentielle des incidents importants et permet aux entités essentielles et importantes de chercher de l'aide et, d'autre part, la notification approfondie qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la cyberrésilience des entreprises individuelles et de secteurs tout entiers » (considérant 101). La description de ces étapes et des obligations y afférentes sont transposées par les articles suivants du projet de loi.	De aanpak van de NIS2-richtlijn inzake melding van significante incidenten, die is omgezet door dit wetsontwerp, voorziet in meerdere fasen “om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van significante incidenten helpt te beperken en essentiële en belangrijke entiteiten in staat stelt om bijstand te vragen, en anderzijds een grondige melding die het mogelijk maakt waardevolle lessen te trekken uit afzonderlijke incidenten en mettertijd de digitale weerbaarheid van afzonderlijke entiteiten en hele sectoren verbetert” (overweging 101). De beschrijving van deze fasen en de eraan verbonden verplichtingen worden omgezet door de volgende artikelen van het wetsontwerp.
Le présent article dispose que les entités essentielles et importantes doivent notifier tout incident significatif sur la fourniture de leurs services fournis dans les (sous-)secteurs repris aux annexes du projet de loi, en ce compris, le cas échéant, les informations qui permettent de déterminer si l'incident en question a un impact transfrontière.	Volgens dit artikel moeten essentiële en belangrijke entiteiten elk significant incident melden dat betrekking heeft op het verlenen van hun diensten in de (deel)sectoren opgenomen in de bijlagen van het wetsontwerp, met inbegrip van, in voorkomend geval, de informatie die nodig is om te bepalen of het betrokken incident grensoverschrijdende gevolgen heeft.
La notification de l'incident significatif se fait au CSIRT national, selon les modalités fixées par un protocole conclu entre le CSIRT national et le NCCN, étant donné la nécessaire collaboration étroite entre ces deux autorités.	Signifiante incidenten worden aan het nationale CSIRT gemeld volgens de modaliteiten bepaald in een protocol gesloten tussen het nationale CSIRT en het NCCN. Het is immers noodzakelijk dat deze beide autoriteiten nauw samenwerken.
Le projet de loi utilise les termes « l'éventuelle » car il n'est pas certain qu'une autorité sectorielle soit désignée pour tous les secteurs repris aux annexes du projet de loi. Pour autant qu'une autorité sectorielle ait été	Het wetsontwerp gebruikt de woorden “de eventuele” omdat het niet zeker is dat een sectorale overheid wordt aangewezen voor alle sectoren opgenomen in de bijlagen van het wetsontwerp. Voor zover een sectorale

désignée et qu'un incident impacte une entité faisant partie du secteur pour lequel l'autorité sectorielle a été désignée, la notification doit se faire également auprès de cette entité.	overheid is aangewezen en een incident gevolgen heeft voor een entiteit die tot de sector behoort waarvoor de sectorale overheid is aangewezen, moet de melding ook aan deze entiteit worden bezorgd.
Les entités essentielles doivent également, le cas échéant, notifier sans retard injustifié aux destinataires de leurs services les incidents significatifs susceptibles de nuire à la fourniture des services précités.	In voorkomend geval moeten essentiële entiteiten ook de ontvangers van hun diensten onverwijld in kennis stellen van significante incidenten die een nadelige invloed kunnen hebben op de verlening van voornoemde diensten.
De plus, en cas de cybermenace importante, les entités essentielles et importantes doivent notifier, encore une fois sans retard injustifié, aux destinataires de leurs services potentiellement affectés par cette cybermenace, la cybermenace elle-même (lorsque cela est approprié) et toutes les mesures ou corrections qui peuvent être appliqués par ces destinataires en réponse à la cybermenace importante.	Verder moeten essentiële en belangrijke entiteiten, in geval van een significante cyberdreiging, nogmaals onverwijld, de ontvangers van hun diensten die mogelijk wordt getroffen door deze cyberdreiging worden getroffen (indien van toepassing) in kennis stellen van de cyberdreiging zelf en hen meedelen welke maatregelen die ontvangers kunnen nemen in reactie op die significante cyberdreiging.
Par incidents significatifs, il faut comprendre les incidents qui « <i>pourraient entraîner des perturbations opérationnelles graves des services ou des pertes financières pour [l'entité concernée], ou nuire à d'autres personnes physiques ou morales en causant un dommage matériel, corporel ou moral considérable. Cette évaluation initiale devrait tenir compte, entre autres, du réseau et des systèmes d'information touchés et notamment de leur importance dans la fourniture des services de l'entité, de la gravité et des caractéristiques techniques de la cybermenace et de toutes les vulnérabilités sous-jacentes qui sont exploitées ainsi que de l'expérience de l'entité en matière d'incidents similaires. Des indicateurs tels que la mesure dans laquelle le fonctionnement du service est affecté, la durée d'un incident ou le nombre de bénéficiaires de services touchés pourraient jouer un rôle important pour déterminer si la perturbation opérationnelle du service est grave</i> » (directive NIS2, considérant 101).	Onder significante incidenten moeten incidenten worden verstaan die <i>“ernstige operationele verstoring van de dienstverlening of financiële verliezen voor [de betrokken entiteit] kunnen veroorzaken of andere natuurlijke of rechtspersonen kunnen treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Bij een dergelijke initiële beoordeling moet rekening worden gehouden met onder meer de getroffen netwerk- en informatiesystemen, en met name het belang daarvan voor de door de entiteit verleende diensten, de ernst en technische kenmerken van een cyberdreiging en eventuele onderliggende kwetsbaarheden die worden uitgebuit, alsook de ervaring van de entiteit met soortgelijke incidenten. Indicatoren zoals de mate waarin de werking van de dienst wordt aangetast, de duur van een incident of het aantal getroffen afnemers van de diensten kunnen van belang zijn om vast te stellen of er sprake is van een ernstige operationele verstoring van de dienst”</i> (NIS2-richtlijn, overweging 101).
Le paragraphe 3 habilite le Roi à établir, par arrêté délibéré en Conseil des ministres, après les consultations nécessaires, des seuils précis	Paragraaf 3 machtigt de Koning om, bij besluit vastgesteld na overleg in de Ministerraad en na de nodige raadplegingen, precieze

de notification en fonction du degré d'impact ou d'urgence de l'incident.	meldingsdrempels te bepalen naargelang de impact of dringendheid van het incident.
La paragraphe 4 indique que la notification doit, le cas échéant, se faire conformément aux actes d'exécution de la Commission européenne pour certaines catégories d'entités (les fournisseurs de services DNS, les registres de noms de domaine de premier niveau, les entités fournissant 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 ou les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux).	Paragraaf 4 wijst erop dat de melding, in voorkomend geval, overeenkomstig de uitvoeringsverordeningen van de Europese Commissie gebeurt voor bepaalde categorieën van entiteiten (DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten of aanbieders van onlinemarktplaatsen, onlinezoekmachines of platforms voor sociale netwerkdiensten).
Enfin, il est indiqué que le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité à l'origine de la notification.	Tot slot wordt vermeld dat een melding niet leidt tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.
Article 35	Artikel 35
Cet article détermine les étapes de la notification obligatoire d'incidents significatifs visée à l'article précédent. Il transpose l'article 23, § 4, de la directive NIS2.	Dit artikel bepaalt de fasen van de verplichte melding van significante incidenten als bedoeld in het vorige artikel. Het voorziet in de omzetting van artikel 23, § 4, van de NIS2-richtlijn.
Comme mentionné <i>supra</i> , la directive prévoit une approche par étapes de la notification obligatoire précitée.	Zoals hierboven vermeld, voorziet de richtlijn in een gefaseerde aanpak van voornoemde verplichte melding.
En cas d'incidents significatifs, les étapes suivantes doivent être respectées par l'entité concernée dans le cadre de la notification :	In geval van significante incidenten moet de betrokken entiteit de volgende fasen doorlopen in het kader van de melding en bezorgt zij:
1° sans retard injustifié et tout au plus dans les 24 heures après avoir pris connaissance de l'incident significatif, l'entité transmet une alerte précoce ;	1° onverwijld en uiterlijk binnen 24 uur nadat zij kennis heeft gekregen van het significante incident, een vroegtijdige waarschuwing;
2° sans retard injustifié et tout au plus dans les 72 heures après avoir pris connaissance de l'incident significatif, l'entité communique une notification d'incident. A noter que les prestataires de services de confiance doivent communiquer la notification d'incident dans les	2° onverwijld en uiterlijk binnen 72 uur nadat zij kennis heeft gekregen van het significante incident, een incidentmelding. Opgemerkt wordt dat verleners van vertrouwensdiensten de incidentmelding binnen 24 uur moeten indienen wanneer het incident gevolgen heeft

24 heures lorsque l'incident a un impact sur la fourniture de leurs services de confiance ;	voor de verlening van hun vertrouwensdiensten;
3° à la demande du CSIRT national ou, le cas échéant, de l'autorité sectorielle concernée (si une telle autorité a été désignée par le Roi), l'entité communique un rapport intermédiaire ;	3° op verzoek van het nationale CSIRT of, indien van toepassing, van de betrokken sectorale overheid (indien deze autoriteit is aangewezen door de Koning), een tussentijds verslag;
4° au plus tard un mois après la notification d'incident visée au 2°, l'entité transmet un rapport final ;	4° uiterlijk één maand na de in 2° bedoelde incidentmelding, een eindverslag;
5° Si le rapport final visé au 4° ne peut être transmis car l'incident est encore en cours, l'entité transmet un rapport d'avancement puis, dans le mois suivant le traitement définitif de l'incident, le rapport final.	5° Indien het in 4° bedoelde eindverslag niet kan worden ingediend omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en, binnen één maand nadat zij het incident definitief heeft afgehandeld, het eindverslag.
L'alerte précoce indique si l'on suspecte que l'incident significatif pourrait avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière. Cette alerte précoce « <i>devrait inclure uniquement les informations nécessaires pour porter l'incident important à la connaissance du CSIRT, ou, le cas échéant, de l'autorité compétente, et permettre à l'entité concernée de demander une assistance, si nécessaire</i> » (considérant 102, directive NIS2). Cette alerte ne doit pas détourner « <i>les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard</i> » (même considérant).	In de vroegtijdige waarschuwing wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben. Deze vroegtijdige waarschuwing " <i>mag enkel de informatie bevatten die noodzakelijk is om het CSIRT of, in voorkomend geval, de bevoegde autoriteit op de hoogte te brengen van het significante incident en de betrokken entiteit in staat te stellen om indien nodig bijstand te vragen</i> " (overweging 102, NIS2-richtlijn). Deze waarschuwing mag " <i>de middelen van de meldende entiteit</i> " niet afleiden van " <i>van activiteiten die verband houden met de behandeling van het incident en die als prioritair moeten worden aangemerkt, teneinde te voorkomen dat de verplichtingen inzake de melding van incidenten middelen onttrekken aan de respons op significante incidenten of de inspanningen van de entiteit op dat gebied anderszins in gevaar brengen</i> " (dezelfde overweging).
La notification d'incident visée 2° (voir <i>supra</i>) a pour objectif de mettre à jour les informations communiquées dans le cadre de l'alerte précoce. Elle fournit également une évaluation initiale de l'incident, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles. Comme pour l'alerte précoce, la notification	De in 2° bedoelde incidentmelding (zie hierboven) heeft tot doel de informatie bij te werken die bij de vroegtijdige waarschuwing is ingediend. Ze bevat ook een initiële beoordeling van het incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting. Net zoals bij de vroegtijdige waarschuwing mag de

d'incident ne doit pas détourner les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents significatifs ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.	incidentmelding de middelen van de meldende entiteit niet afleiden van activiteiten die verband houden met de behandeling van het incident en die als prioritair moeten worden aangemerkt, teneinde te voorkomen dat de verplichtingen inzake de melding van incidenten middelen onttrekken aan de respons op significante incidenten of de inspanningen van de entiteit op dat gebied anderszins in gevaar brengen.
Le rapport intermédiaire contient les mises à jour pertinentes de la situation.	Het tussentijdse verslag bevat relevante updates van de situatie.
Le rapport final doit comprendre une description détaillée de l'incident, y compris de sa gravité et de son impact ; le type de menace ou la cause profonde qui a probablement déclenché l'incident ; les mesures d'atténuation appliquées et en cours ; le cas échéant, l'impact transfrontière de l'incident.	Het eindverslag bevat een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan; het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; de toegepaste en lopende risicobeperkende maatregelen; in voorkomend geval, de grensoverschrijdende gevolgen van het incident.
Le rapport d'avancement contient les informations qui devraient se trouver dans le rapport final et qui sont en la possession de l'entité au moment de la communication du rapport d'avancement.	Het voortgangsverslag bevat de informatie die in het eindverslag zou moeten staan, en waarover de entiteit beschikt op het moment dat het voortgangsverslag wordt ingediend.
Article 36	Artikel 36
Cet article transpose l'article 23, § 5, de la directive NIS2, portant sur une partie des obligations du CSIRT national en matière de notifications obligatoires d'incidents.	Dit artikel voorziet in de omzetting van artikel 23, lid 5, van de NIS2-richtlijn, dat betrekking heeft op een deel van de verplichtingen van het nationale CSIRT inzake de verplichte melding van incidenten.
Dans le cadre d'une notification obligatoire d'un incident significatif, le CSIRT national doit fournir sans retard injustifié et si possible dans les 24 heures suivant la réception de l'alerte précoce, une réponse à l'entité émettrice, en ce 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.	In het kader van de verplichte melding van een significant incident verstrekt het nationale CSIRT onverwijld, en zo mogelijk binnen 24 uur na ontvangst van de 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.
De plus, à la demande de l'entité, le CSIRT national doit fournir un soutien technique	Bovendien moet het nationale CSIRT aanvullende technische ondersteuning verlenen

supplémentaire. Si il existe des suspicions 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.	indien de entiteit daarom verzoekt. Wanneer het vermoeden bestaat dat het incident van criminele aard is, verstrekt het nationale CSIRT ook richtsnoeren voor het melden van het significante incident aan de rechtshandhavinginstanties.
Il est important de noter que, dans le cadre de ses missions, y compris les présentes tâches liées à l'intervention en cas d'incidents significatifs, le CSIRT national peut donner la priorité à certaines tâches plutôt qu'à d'autres, sur la base d'une approche basée sur les risques. Ainsi, si les ressources du CSIRT national sont fortement monopolisées par un incident particulièrement grave, et qu'il n'est pas possible de fournir une réponse à une alerte précoce dans les 24 heures ou de fournir, sans retard, un soutien technique à une entité ayant soumis une notification d'incident sans compromettre son intervention dans le cadre de l'incident particulièrement grave précité, le CSIRT national peut privilégier l'intervention dans le cadre l'incident particulièrement grave pour autant que cela se justifie du point de vue des risques.	Het is belangrijk te vermelden dat het nationale CSIRT, in het kader van zijn opdrachten, met inbegrip van deze taken in verband met de respons op significante incidenten, voorrang kan geven aan bepaalde taken boven andere taken, op grond van een risicogebaseerde benadering. Indien de middelen van het nationale CSIRT bijvoorbeeld sterk in beslag worden genomen door een bijzonder ernstig incident, en het niet mogelijk is om binnen 24 uur te reageren op een vroegtijdige waarschuwing of onverwijld technische ondersteuning te bieden aan een entiteit die een incidentmelding heeft ingediend, zonder zijn respons op voornoemd ernstig incident in het gedrang te brengen, kan het nationale CSIRT voorrang geven aan de respons op het bijzonder ernstige incident voor zover dit gerechtvaardigd is wat de risico's betreft.
Article 37	Artikel 37
Cet article transpose l'article 23, §§ 6 à 10, et porte sur le reste des obligations du CSIRT national et des autorités compétentes dans le cadre du présent projet de loi.	Dit artikel voorziet in de omzetting van artikel 23, leden 6 tot 10 en heeft betrekking op de overige verplichtingen van het nationale CSIRT en van de uit hoofde van dit wetsontwerp bevoegde autoriteiten.
En premier lieu, lorsqu'un incident significatif concerne deux États membres ou plus (ou de manière générale, lorsque c'est approprié), le CSIRT national doit informer sans retard injustifié les autres États membres touchés par l'incident en question. Dans ce cadre, sont partagées des informations similaires à ce qui est communiqué au CSIRT national dans le cadre des alertes précoces, notifications d'incidents et rapports subséquents visés à l'article 35 du projet de loi. 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	In de eerste plaats moet het nationale CSIRT, wanneer een significant incident betrekking heeft op twee of meer lidstaten (of in het algemeen, indien van toepassing), de andere lidstaten die door het betrokken incident zijn getroffen onverwijld in kennis stellen. Daarbij wordt informatie gedeeld die vergelijkbaar is met die welke aan het nationale CSIRT wordt verstrekt in het kader van vroegtijdige waarschuwingen, incidentmeldingen en daaropvolgende verslagen als bedoeld in artikel 35 van het wetsontwerp. Daarbij moet het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte

communiquées.	informatie beschermen.
Ensuite, lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou encore lorsque la divulgation de l'incident significatif est dans l'intérêt public, le CSIRT national a la possibilité d'informer le public de l'incident significatif ou exiger que l'entité informe elle-même le public de cet incident. Pour ce faire, le CSIRT national doit avoir consulté au préalable l'entité concernée, le NCCN, l'autorité concernée (lorsqu'une telle autorité a été désignée) et, si l'entité concernée relève du pouvoir exécutif fédéral, le Ministre compétent.	Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of nog wanneer de bekendmaking van het significante incident in het algemeen belang is, heeft het nationale CSIRT vervolgens de mogelijkheid om het publiek te informeren over het significante incident informeren of van de entiteit te verlangen dat zij het publiek zelf informeert over dat incident. Daartoe moet het nationale CSIRT vooraf de betrokken entiteit, het NCCN, de betrokken autoriteit (wanneer deze autoriteit is aangewezen) en, indien de betrokken entiteit tot de federale uitvoerende macht behoort, de bevoegde minister raadplegen.
Conformément au paragraphe 3, le CSIRT national transmet les notifications obligatoires d'incidents significatifs reçues aux points de contacts des autres États membres touchés par les incidents en question. Cette communication peut également se faire à la demande d'une autorité sectorielle.	Overeenkomstig paragraaf 3 stuurt het nationale CSIRT de ontvangen verplichte meldingen van significante incidenten door naar de contactpunten van de andere lidstaten die getroffen zijn door de betrokken incidenten. Deze kennisgeving kan ook gebeuren op verzoek van een sectorale overheid.
En exécution de la directive NIS2, l'autorité nationale de cybersécurité doit rédiger des rapports 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, § 1 ^{er} , et à l'article 38, § 1 ^{er} , du projet de loi, afin de les communiquer à l'ENISA tous les 3 mois.	In uitvoering van de NIS2-richtlijn moet de nationale cyberbeveiligingsautoriteit samenvattende verslagen opstellen met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, en artikel 38, § 1, van het wetsontwerp zijn gemeld, teneinde deze om de 3 maanden aan Enisa te bezorgen.
Enfin, dans le cadre de la coopération accrue avec les autorités compétentes dans le cadre de la loi CER, le CSIRT national fournit à ces autorités des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1er, et à l'article 38, § 1er, par les entités identifiées comme des entités critiques en vertu de la loi CER.	Tot slot verstrekt het nationale CSIRT de uit hoofde van de CER-wet bevoegde autoriteiten, in het kader van de nauwere samenwerking met deze autoriteiten, informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, en artikel 38, § 1, zijn gemeld door entiteiten die uit hoofde van de CER-wet als kritieke entiteiten zijn aangemerkt.
Section 2	Afdeling 2
<i>Notification volontaire</i>	<i>Vrijwillige melding</i>

Article 38	Artikel 38
Cette article transpose l'article 30 de la directive NIS2 et porte sur la notification volontaire d'incidents.	Dit artikel voorziet in de omzetting van artikel 30 van de NIS2-richtlijn en heeft betrekking op de vrijwillige melding van incidenten.
La disposition fait la différence entre deux possibilités :	De bepaling maakt een onderscheid tussen twee mogelijkheden:
Premièrement, les entités essentielles et importantes peuvent notifier les incidents (non significatifs, qui eux <i>doivent</i> être notifiés), les cybermenaces et les incidents évités.	In de eerste plaats kunnen essentiële en belangrijke entiteiten (niet significante) incidenten (significante incidenten <i>moeten</i> immers worden gemeld), cyberdreigingen en bijna-incidenten melden.
Deuxièmement, les entités autres que les entités essentielles et importantes, même si elles ne relèvent pas du champ d'application du projet de loi, peuvent notifier les incidents significatifs, les cybermenaces et les incidents évités.	Op de tweede plaats kunnen andere entiteiten dan essentiële en belangrijke entiteiten, ook al behoren ze niet tot het toepassingsgebied van het wetsontwerp, significante incidenten, cyberdreigingen en bijna-incidenten melden.
Dans ces deux situations, le CSIRT national doit traiter ces notifications de la même manière que les notifications obligatoires évoquées <i>supra</i> . Cela étant, les notifications obligatoires peuvent être traitées de manière prioritaire par rapport aux notifications volontaires.	In deze beide situaties moet het nationale CSIRT deze meldingen op dezelfde wijze verwerken als bovenvermelde verplichte meldingen. Er kan evenwel voorrang worden gegeven aan de verwerking van verplichte meldingen boven die van vrijwillige meldingen.
D'une manière similaire à ce qui est prévu pour les notifications obligatoires, en principe, un signalement volontaire n'a pas pour effet 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.	Net zoals voor verplichte meldingen geldt in principe dat een vrijwillige melding er niet toe mag leiden dat de meldende entiteit bijkomende verplichtingen worden opgelegd waaraan zij niet zou zijn onderworpen indien zij de melding niet had ingediend.
TITRE 4	TITEL 4
<i>Supervision et sanctions</i>	<i>Toezicht en sancties</i>
CHAPITRE 1 ^{ER}	HOODSTUK 1
Supervision	Toezicht
Section 1^{re}	Afdeling 1
<i>Evaluation périodique de la conformité</i>	<i>Regelmatige conformiteitsbeoordeling</i>
Article 39	Artikel 39

Cet article établit l'obligation pour les entités essentielles de se soumettre à une évaluation périodique de la conformité de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité et habilite le Roi à déterminer les modalités de cette évaluation ainsi que les cadres de références sur base desquels l'évaluation est effectuée. La fréquence de l'évaluation sera déterminée par les cadres de références eux-mêmes.	Dit artikel bepaalt dat essentiële entiteiten verplicht zijn zich te onderwerpen aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's en machtigt de Koning om de modaliteiten van deze beoordeling te bepalen, alsook de referentiekaders op basis waarvan de beoordeling gebeurt. De frequentie van de beoordeling wordt bepaald door de referentiekaders zelf.
L'évaluation régulière de la conformité peut consister soit en une évaluation effectuée par un organisme d'évaluation de la conformité agréé, soit en une inspection régulière effectuée par le service d'inspection de l'autorité nationale de cybersécurité. A la demande des autorités sectorielles, ces inspections peuvent être menées de manière conjointe sous la direction de l'autorité nationale de cybersécurité. A la demande des autorités sectorielles et moyennant l'accord de l'autorité nationale de cybersécurité, cette dernière peut ordonner au service d'inspection sectoriel d'effectuer l'inspection en ce qui concerne son secteur ou ses sous-secteurs.	De regelmatige conformiteitsbeoordeling kan ofwel een beoordeling door een erkende conformiteitsbeoordelingsinstantie zijn, of de vorm aannemen van een regelmatige inspectie door de inspectiedienst van de nationale cyberbeveiligingsautoriteit. Op verzoek van de sectorale overheden kunnen deze inspecties gezamenlijk worden uitgevoerd onder leiding van de nationale cyberveiligheidsautoriteit. Op verzoek van de sectorale overheden en mits akkoord van de nationale cyberbeveiligingsautoriteit kan deze laatste de sectorale inspectiedienst gelasten om de inspectie voor wat betreft haar sector of subsectoren alleen uit te voeren.
Si le Roi a établi des mesures supplémentaires (additionnelles ou spécifiques) pour un ou plusieurs secteurs, ces mesures font l'objet d'une inspection par les services d'inspection des autorités sectorielles concernées. L'autorité nationale de cybersécurité reçoit copie des rapports d'inspection ou participe, à sa demande, aux inspections de manière conjointe, sous la direction de l'autorité sectorielle concernée.	Indien de Koning bijkomende of bijzondere maatregelen (specifieke of aanvullende) voor één of meerdere sectoren heeft vastgelegd, worden deze maatregelen geïnspecteerd door de inspectiediensten van de betrokken sectorale overheden. De nationale autoriteit voor cyberveiligheid ontvangt een kopie van de inspectieverslagen of neemt, op verzoek, deel aan de inspecties gezamenlijk, onder leiding van de betrokken sectorale overheid.
Lorsque plusieurs cadres de références sont déterminés par le Roi, les entités essentielles choisissent librement parmi ces cadres de références, lequel ils appliquent dans le cadre de l'évaluation de la conformité.	Wanneer de Koning meerdere referentiekaders bepaalt, staat het essentiële entiteiten vrij om te kiezen welk referentiekader ze gebruiken in het kader van de conformiteitsbeoordeling.
Un tel mécanisme d'évaluation de la conformité a pour objectif non seulement de s'assurer de la conformité d'une entité à un moment donné, à l'issue d'un cycle d'évaluation périodique de la conformité mais également de permettre un	Doel van een dergelijk conformiteitsbeoordelingsmechanisme is niet alleen om na te gaan of een entiteit op een bepaald ogenblik, na afloop van een regelmatige conformiteitsbeoordelingscyclus,

premier contrôle ainsi que de fournir aux entités un processus d'auto-évaluation des risques encourus, des mesures mises en place et de la maturité de l'entité. L'usage de ces cadres de références est toujours basé sur l'analyse des risques réalisée par l'entité.	aan de conformiteitsregels voldoet, maar ook om een eerste controle mogelijk te maken, alsook om entiteiten een zelfbeoordelingsproces te bieden van de risico's die ze hebben gelopen, de maatregelen die ze hebben genomen en van de maturiteit van de entiteit. Het gebruik van deze referentiekaders wordt altijd gebaseerd op de risicoanalyse die door de entiteit gerealiseerd wordt.
Dans le cadre de cette évaluation périodique de la conformité, l'autorité nationale de cybersécurité fournira des outils permettant aux entités essentielles d'effectuer une analyse des risques encourus. L'autorité développera également un cadre de référence, basé sur des normes et bonnes pratiques internationalement reconnus, qui sera mis à disposition gratuitement.	In het kader van deze regelmatige conformiteitsbeoordeling zal de nationale cyberbeveiligingsautoriteit instrumenten beschikbaar stellen waarmee essentiële entiteiten een risicoanalyse kunnen uitvoeren. De autoriteit zal ook een referentiekader uitwerken op basis van internationaal erkende normen en goede praktijken, dat gratis beschikbaar zal worden gesteld.
Article 40	Article 40
Cet article porte sur l'évaluation périodique de la conformité effectuée par un organisme d'évaluation de la conformité.	Dit artikel heeft betrekking op de regelmatige conformiteitsbeoordeling die wordt uitgevoerd door een conformiteitsbeoordelingsinstantie.
Cet organisme d'évaluation de la conformité doit pouvoir être en mesure d'évaluer adéquatement les entités essentielles sur base des cadres de références déterminés par le Roi. Pour s'en assurer, les organismes d'évaluation de la conformité devront être agréés selon les conditions fixées par le Roi. L'objectif de cette agrégation est de s'assurer que les organismes d'évaluation de la conformité respectent les conditions nécessaires à l'évaluation de la conformité visée à l'article 39, alinéa 1 ^{er} , 1°. L'agrégation permet également d'ajouter des conditions particulières, nécessaires pour la sécurité d'un ou plusieurs secteurs spécifiques.	Deze conformiteitsbeoordelingsinstantie moet essentiële entiteiten adequaat kunnen beoordelen op basis van door de Koning bepaalde referentiekaders. Daartoe moeten conformiteitsbeoordelingsinstanties erkend zijn volgens de door de Koning bepaalde voorwaarden. Deze erkenning heeft tot doel te waarborgen dat deze instanties voldoen aan de voorwaarden die nodig zijn voor de in artikel 39, eerste lid, 1°, bedoelde conformiteitsbeoordeling. De erkenning maakt het ook mogelijk om specifieke voorwaarden toe te voegen die nodig zijn voor de veiligheid van een of meer specifieke sectoren.
Pour pouvoir vérifier que les organismes d'évaluation de la conformité agréés continuent de respecter les conditions de l'agrégation, le service d'inspection de l'autorité nationale de cybersécurité peut faire usage de ses pouvoirs de contrôle.	Om na te gaan of erkende conformiteitsbeoordelingsinstanties nog aan de erkenningsvoorwaarden voldoen, kan de inspectiedienst van de nationale cyberbeveiligingsautoriteit gebruik maken van zijn toezichtsbevoegdheden.
Par ailleurs, lorsque l'évaluation de la conformité concerne des entités critiques ou des entités de l'administration publique,	Wanneer de conformiteitsbeoordeling betrekking heeft op kritieke entiteiten of overheidsinstanties, moeten de

l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui effectueront l'évaluation devront disposer d'une habilitation de sécurité, obtenue conformément à 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.	conformiteitsbeoordelingsinstantie en de natuurlijke personen die de beoordeling uitvoeren bovendien over een veiligheidsmachtiging beschikken, die wordt verkregen overeenkomstig de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst.
Article 41	Artikel 41
Cet article permet aux entités importantes de se soumettre également à une évaluation périodique de la conformité. Une telle évaluation ne leur est pas imposée car, conformément à l'article 33, § 1 ^{er} , de la directive NIS2, ces entités ne sont soumises qu'à un contrôle <i>ex post</i> dans le cadre du présent projet de loi.	Dit artikel wijst erop dat belangrijke entiteiten zich ook kunnen onderwerpen aan een regelmatige conformiteitsbeoordeling. Deze beoordeling is niet verplicht omdat deze entiteiten, overeenkomstig artikel 33, lid 1, van de NIS2-richtlijn, alleen onderworpen zijn aan toezicht achteraf in het kader van dit wetsontwerp.
Article 42	Artikel 42
Selon cet article, toute entité qui se soumet à l'évaluation de la conformité visée aux articles 39, alinéa 1 ^{er} , 1°, et 41 bénéficie d'une présomption de conformité des obligations visées à l'article 30. Cette présomption peut être renversée par le service d'inspection compétent lorsque ce dernier constate des manquements aux obligations créées par le présent projet de loi.	Volgens dit artikel geniet elke entiteit die zich onderwerpt aan de in artikel 39, eerste lid, 1°, en 41 bedoelde conformiteitsbeoordeling het vermoeden dat de in artikel 30 bedoelde verplichtingen worden nageleefd. Dit vermoeden kan worden weerlegd door de bevoegde inspectiedienst wanneer deze laatste inbreuken vaststelt op de door dit wetsontwerp ingevoerde verplichtingen.
Article 43	Artikel 43
Cet article prévoit que l'autorité nationale de cybersécurité doit établir, maintenir à jour et rendre disponible une liste des organismes d'évaluation de la conformité agréés par elle.	Dit artikel bepaalt dat de nationale cyberbeveiligingsautoriteit een lijst van de door haar erkende conformiteitsbeoordelingsinstanties moet opstellen, bijhouden en beschikbaar stellen.
Section 2	Afdeling 2
<i>Dispositions générales relatives au service d'inspection</i>	<i>Algemene bepalingen betreffende de inspectiedienst</i>
Article 44	Artikel 44
Cet article porte sur les autorités pouvant être compétentes en matière de supervision et sur leurs tâches de contrôle.	Dit artikel heeft betrekking op de autoriteiten die kunnen bevoegd zijn voor het toezicht en op hun toezichthoudende taken.

Le service d'inspection de l'autorité nationale de cybersécurité a pour tâche de réaliser 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.	Het is de taak van de inspectiedienst van de nationale cyberbeveiligingsautoriteit om controles uit te voeren om na te gaan of essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.
Il est possible que, dans le cadre du projet de loi, des dispositions (sous-)sectorielles spécifiques en matière de mesures de gestion des risques en matière de cybersécurité aient été adoptées conformément à l'article 33.	Het is mogelijk dat, in het kader van het wetsontwerp, specifieke (deel)sectorale bepalingen inzake maatregelen voor het beheer van cyberbeveiligingsrisico's zijn aangenomen overeenkomstig artikel 33.
En principe, l'autorité sectorielle compétente ou le service d'inspection sectoriel compétent pour un (sous-)secteur pour lequel il existe de telles dispositions (sous-)sectorielles spécifiques doit réaliser des contrôles du respect par les entités essentielles et importantes relevant dudit (sous-)secteur des dispositions (sous-)sectorielles spécifiques précitées. Cela étant, en l'absence d'autorité sectorielle ou de service d'inspection sectoriel compétent, le service d'inspection de l'autorité nationale de cybersécurité réalise les contrôles précités.	In principe moet de bevoegde sectorale overheid of de sectorale inspectiedienst die bevoegd is voor een (deel)sector waarin deze specifieke (deel)sectorale bepalingen gelden, controles uitvoeren om na te gaan of essentiële en belangrijke entiteiten die tot deze (deel)sector behoren, voornoemde specifieke (deel)sectorale bepalingen naleven. Bij gebrek aan een sectorale overheid of bevoegde sectorale inspectiedienst voert de inspectiedienst van de nationale cyberbeveiligingsautoriteit genoemde controles uit.
Dans le cadre du commentaires des articles du présent projet de loi, le service d'inspection de l'autorité nationale de cybersécurité, les autorités sectorielles (dans le cadre de leurs potentielles compétences de contrôle) et/ou les services d'inspection sectoriels sont collectivement appelés les autorités compétentes pour le contrôle.	In het kader van de commentaar bij de artikelen van dit wetsontwerp worden de inspectiedienst van de nationale cyberbeveiligingsautoriteit, de sectorale overheden (in het kader van hun mogelijke toezichtsbevoegdheden) en/of de sectorale inspectiediensten samen de voor het toezicht bevoegde autoriteiten genoemd.
Le présent article dispose que, dans le cadre d'une demande d'informations ou de preuves, les autorités compétentes pour le contrôle doivent mentionner la finalité de la demande, les informations ou preuves précises demandées et le délai dans lequel celles-ci doivent être fournies par l'entité à qui s'adresse la demande.	Dit artikel bepaalt dat, in het kader van een verzoek om informatie of bewijzen, de voor het toezicht bevoegde autoriteiten het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt door de entiteit aan wie het verzoek is gericht, moeten vermelden.
Le cas échéant, les autorités compétentes pour le contrôle peuvent faire appel à des experts dans le cadre de leur tâches de contrôle ou fixer des priorités dans l'exécution de leurs tâches.	In voorkomend geval kunnen de voor het toezicht bevoegde autoriteiten een beroep doen op experten in het kader van hun toezichthoudende taken of prioriteiten bepalen

	bij de uitvoering van hun taken.
Article 45	Artikel 45
Cet article porte sur la coopération et l'échange d'informations entre autorités dans le cadre du projet de loi, lorsque les entités inspectées relèvent par ailleurs du champ d'application de la directive CER ou du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (ci-après le « règlement DORA »), conformément aux articles 32, §§ 9 et 10, et 33, § 6, de la directive NIS2.	Dit artikel is gewijd aan de samenwerking en informatie-uitwisseling tussen autoriteiten in het kader van het wetsontwerp, wanneer de geïnspecteerde entiteiten bovendien tot het toepassingsgebied behoren van de CER-richtlijn of van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector (hierna "DORA-verordening"), overeenkomstig artikel 32, leden 9 en 10, en 33, lid 6, van de NIS2-richtlijn.
Ces trois textes juridiques sont fortement liés, raison pour laquelle « <i>il convient d'assurer la cohérence des approches entre la directive (UE) 2022/2557, [...]. Les autorités compétentes en vertu de la [directive NIS2] et les autorités compétentes en vertu de la directive [CER] devraient, si possible en temps réel, coopérer et échanger des informations à cette fin.</i> » (considérant 30, directive NIS2) et « <i>il est important de conserver une relation forte et de maintenir l'échange d'informations avec le secteur financier dans le cadre de la présente directive. À cet effet, le règlement [DORA] permet aux autorités européennes de surveillance (AES) et aux autorités compétentes en vertu dudit règlement de participer aux activités du groupe de coopération, ainsi que d'échanger des informations et de coopérer avec les points de contact uniques ainsi qu'avec les CSIRT et les autorités compétentes en vertu de la [directive NIS2]</i> » (considérant 28, directive NIS2).	Deze drie juridische teksten zijn nauw met elkaar verweven. Om die reden " <i>moet een coherente aanpak worden gewaarborgd tussen Richtlijn (EU) 2022/2557 [...]. Daartoe moeten de uit hoofde van [de NIS2-richtlijn] deze richtlijn bevoegde autoriteiten en die uit hoofde van [de CER-richtlijn], indien mogelijk in realtime, samenwerken en informatie uitwisselen.</i> " (overweging 30, NIS2-richtlijn) en " <i>is het van belang een sterke relatie en de uitwisseling van informatie met de financiële sector uit hoofde van deze richtlijn in stand te houden. Daartoe biedt [de DORA-verordening] de Europese toezichthoudende autoriteiten (ETA's) en de uit hoofde van die verordening bevoegde autoriteit en de mogelijkheid deel te nemen aan de activiteiten van de samenwerkingsgroep en informatie uit te wisselen en samen te werken met de centrale contactpunten en met de CSIRT's en de uit hoofde van [de NIS2-richtlijn] bevoegde autoriteiten.</i> " (overweging 28, NIS2-richtlijn).
Article 46	Artikel 46
Cet article porte sur l'assistance mutuelle entre autorités des États membres dans le cadre de la supervision et de l'exécution des lois nationales transposant la directive NIS2.	Dit artikel heeft betrekking op de wederzijdse bijstand tussen autoriteiten van lidstaten in het kader van het toezicht op en de uitvoering van de nationale wetten die voorzien in de omzetting van de NIS2-richtlijn.
Selon la directive NIS2, « <i>afin de garantir le respect par les entités des obligations qui leur incombent en vertu de la présente directive, les</i>	Volgens de NIS2-richtlijn moeten lidstaten " <i>om ervoor te zorgen dat entiteiten hun in deze richtlijn vastgelegde verplichtingen nakomen,</i>

<i>États membres devraient coopérer et se prêter mutuellement assistance en ce qui concerne les mesures de supervision et d'exécution, en particulier lorsqu'une entité fournit des services dans plus d'un État membre ou lorsque son réseau et ses systèmes d'information sont situés dans un État membre autre que celui où elle fournit des services » (considérant 134).</i>	<i>(...) met elkaar samenwerken en elkaar bijstaan op het gebied van toezicht- en handhavingsmaatregelen, met name wanneer een entiteit diensten verleent in meer dan één lidstaat of wanneer haar netwerk- en informatiesystemen zich bevinden in een andere lidstaat dan die waar zij diensten verleent.” (overweging 134).</i>
Ainsi, la disposition permet aux autorités compétentes pour le contrôle de solliciter la coopération et l'assistance des autorités d'autres États membres compétentes dans le cadre de leur propre loi de transposition de la directive NIS2. Cette sollicitation peut porter sur des mesures de supervision et d'exécution ou consister en une demande (motivée) d'assistance mutuelle en vue d'assurer la mise en œuvre effective, efficace et cohérente des mesures de supervision ou d'exécution. Une demande d'assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle.	Zo verduidelijkt de bepaling dat de voor het toezicht bevoegde autoriteiten de autoriteiten van andere bevoegde lidstaten om samenwerking en bijstand kunnen verzoeken in het kader van hun eigen omzettingwet van de NIS2-richtlijn. Dit verzoek kan betrekking hebben op toezichts- en handhavingsmaatregelen of op een (met redenen omkleed) verzoek om wederzijdse bijstand zijn met het oog op een effectieve, efficiënte en consistente uitvoering van de toezichts- of handhavingsmaatregelen. Een verzoek om wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen.
Selon la directive toujours, « lorsqu'une autorité compétente fournit une assistance qui lui est demandée, elle devrait prendre des mesures de supervision ou d'exécution conformément au droit national » (considérant 134). Ainsi, « l'État membre qui a reçu une demande d'assistance mutuelle devraient [sic], dans les limites de cette demande, prendre des mesures de supervision et d'exécution appropriées à l'égard de l'entité faisant l'objet de cette demande et qui fournit des services ou possède un réseau et un système d'information sur le territoire dudit État membre » (considérant 135).	Verder wijst de richtlijn op het volgende: “Bij het verlenen van bijstand moet de aangezochte bevoegde autoriteit toezicht- of handhavingsmaatregelen nemen overeenkomstig het nationale recht.” (overweging 134). Zo “moet een lidstaat die een verzoek om wederzijdse bijstand heeft ontvangen, binnen de grenzen van dat verzoek passende toezichts- en handhavingsmaatregelen nemen ten aanzien van de entiteit die het voorwerp van dat verzoek is, en die diensten verleent of over een netwerk- en informatiesysteem op het grondgebied van die lidstaat beschikt” (overweging 135).
Conformément à la directive (les considérants précités et l'article 35), le présent article prévoit en son paragraphe 2 que les autorités compétentes pour le contrôle coopèrent avec 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 concerné sont situés dans le territoire belge. Cette coopération et/ou assistance de la part des	Overeenkomstig de richtlijn (voornoemde overwegingen en artikel 35) bepaalt paragraaf 2 van dit artikel dat de voor het toezicht bevoegde autoriteiten samenwerken met en bijstand verlenen aan de toezichthoudende autoriteiten bevoegd voor cyberbeveiliging van andere lidstaten indien deze hierom verzoeken en de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden. Deze samenwerking en/of bijstand door de Belgische autoriteiten moet in

autorités belges doit se faire de manière proportionnée à leurs ressources et rentrer dans le cadre de leurs compétences.	verhouding staan tot hun middelen en binnen hun bevoegdheden vallen.
Dans le cadre de cette coopération et/ou assistance, les autorités belges compétentes pour le contrôle appliquent les dispositions du présent projet de loi et pas celles des lois de transposition des autres Etats membres.	In het kader van deze samenwerking en/of bijstand passen de voor het toezicht bevoegde Belgische autoriteiten de bepalingen van dit wetsontwerp toe en niet de omzettingswetten van de andere lidstaten.
La demande précitée peut porter sur des mesures de supervision et d'exécution ou consister en une demande (motivée) d'assistance mutuelle en vue d'assurer la mise en œuvre effective, efficace et cohérente des mesures de supervision ou d'exécution. Une demande d'assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle.	Voornoemd verzoek kan betrekking hebben op toezichts- en handhavingsmaatregelen of een (met redenen omkleed) verzoek om wederzijdse bijstand zijn met het oog op een effectieve, efficiënte en consistente uitvoering van de toezichts- of handhavingsmaatregelen. Een verzoek om wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen.
Dans le cadre de cette coopération et/ou assistance de la part des autorités belges, l'autorité nationale de cybersécurité doit, en tant que point de contact unique, rassembler les informations, y compris concernant les consultations, en ce qui concerne les mesures de supervision et d'exécution prises au niveau national et les communiquer aux autorités de contrôle compétentes en matière de cybersécurité d'autres États membres.	In het kader van deze samenwerking en/of bijstand door de Belgische autoriteiten moet de nationale cyberbeveiligingsautoriteit, als centraal contactpunt, informatie verzamelen, met inbegrip van informatie inzake raadplegingen, over de toezichts- en handhavingsmaatregelen die op nationaal niveau zijn genomen en deze aan de autoriteiten van andere lidstaten bezorgen die bevoegd zijn voor het toezicht inzake cyberbeveiliging.
Une demande de coopération ou d'assistance d'un autre État membre ne peut être refusée que s'il est établi que l'autorité concernée par la demande 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 pouvoir refuser la demande, l'autorité faisant l'objet de la demande doit consulter les autres autorités concernées et, le cas échéant, la Commission européenne et l'ENISA si un État membre le demande.	Een verzoek om samenwerking of bijstand van een andere lidstaat mag alleen worden geweigerd indien wordt vastgesteld dat de autoriteit aan wie het verzoek is gericht, 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 het verzoek te kunnen afwijzen, moet de autoriteit aan wie het verzoek is gericht, de andere betrokken autoriteiten raadplegen en, in voorkomend geval, de Europese Commissie en Enisa indien een lidstaat hierom verzoekt.

Article 47	Artikel 47
Cet article porte sur les membres des autorités compétentes pour le contrôle qui effectuent les tâches d'inspection.	Dit artikel heeft betrekking op de leden van de voor het toezicht bevoegde autoriteiten die inspectietaken uitvoeren.
Ces membres doivent être dotés d'une carte de légitimation afin de pouvoir prouver leur identité et leur appartenance à l'une des autorités compétentes pour le contrôle. La compétence de fixer le modèle de cette carte de légitimation est dévolue au Roi.	Deze leden beschikken over een legitimatiekaart om hun identiteit te bewijzen en aan te tonen dat zij tot een van de voor het toezicht bevoegde autoriteiten behoren. De Koning is bevoegd om het model van deze legitimatiekaart te bepalen.
Le paragraphe 2 de cette disposition porte sur les conflits d'intérêts. Par principe, les membres des autorités compétentes pour le contrôle qui effectuent les tâches de contrôle ne peuvent avoir d'intérêt dans les entités qu'ils doivent contrôler, susceptible de compromettre leur objectivité, impartialité ou indépendance, quel qu'il soit. Ces personnes doivent prêter serment auprès du fonctionnaire dirigeant de leur service.	Paragraaf 2 van deze bepaling behandelt de belangenconflicten. In principe mogen de leden van de voor het toezicht bevoegde autoriteiten die toezichthoudende taken uitvoeren, geen enkel belang hebben in de entiteiten waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit, onpartijdigheid of onafhankelijkheid in het gedrang zou kunnen komen. Deze personen moeten de eed afleggen de eed bij de leidend ambtenaar van hun dienst.
Les membres des autorités compétentes pour le contrôle qui effectuent les tâches d'inspection ne peuvent pas non plus recevoir d'instructions de personnes tierces dans le cadre de leurs attributions. Par ailleurs, afin d'éviter les situations de conflits d'intérêt, il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt quelconque.	De leden van de voor het toezicht bevoegde autoriteiten die inspectietaken uitvoeren, mogen evenmin instructies van derden krijgen in het kader van hun bevoegdheden. Om belangenconflicten te voorkomen is het hen bovendien verboden aanwezig te zijn bij een beraadslaging of beslissing over dossiers waarin zij enig belang hebben.
La compétence de désigner d'autres situations comme constituant des conflits d'intérêts est dévolue au Roi.	De Koning is bevoegd om andere situaties te benoemen als belangenconflicten.
Les autorités compétentes pour le contrôle doivent prendre les mesures nécessaires pour assurer l'indépendance de leurs membres qui effectuent les tâches de contrôle. Ces mesures doivent permettre de prévenir, d'identifier et, le cas échéant, de résoudre les conflits d'intérêts actuels ou potentiels.	De voor het toezicht bevoegde autoriteiten moeten de nodige maatregelen nemen om de onafhankelijkheid te waarborgen van hun leden die toezichthoudende taken uitvoeren. Deze maatregelen hebben tot doel de huidige of mogelijke belangenconflicten te voorkomen, te identificeren en, in voorkomend geval, op te lossen.
Section 3	Afdeling 3

<i>La supervision des entités par le service d'inspection</i>	<i>Het door de inspectiedienst uitgeoefende toezicht op de entiteiten</i>
Article 48	Article 48
<p>Cet article porte sur les pouvoirs en matière de contrôle des autorités compétentes pour le contrôle et les garde-fous y afférents afin de garantir le respect des droits des personnes inspectées. Ces autorités disposent de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du projet de loi. Étant donné l'étendue des pouvoirs conférés à ces autorités, l'article précise, en son paragraphe 7, que les moyens mis en œuvre par les membres assermentés des autorités compétentes pour le contrôle doivent être appropriés et nécessaires au contrôle du respect du projet de loi. Par ailleurs, il faut souligner que les membres assermentés ne sont pas des officiers de police judiciaire. Ils ne peuvent faire usage de la contrainte à l'encontre des personnes contrôlées et ne peuvent, dès lors, forcer l'accès aux informations, <i>a fortiori</i> aux informations protégées par l'article 458 du Code pénal.</p>	<p>Dit artikel heeft betrekking op de toezichthoudende bevoegdheden van de voor het toezicht bevoegde autoriteiten en de eraan verbonden waarborgen om ervoor te zorgen dat de rechten van de geïnspecteerde personen worden gerespecteerd. Deze autoriteiten beschikken over ruime bevoegdheden om grondige controles uit te voeren op de naleving van het wetsontwerp. Gezien de omvang van de bevoegdheden van deze autoriteiten verduidelijkt paragraaf 7 van dit artikel dat de middelen die de beëdigde leden van de voor het toezicht bevoegde autoriteiten gebruiken, passend en noodzakelijk moeten zijn voor het toezicht op de naleving van het wetsontwerp. Voorts moet worden benadrukt dat beëdigde leden geen officieren van gerechtelijke politie zijn. Zij mogen geen gebruik maken van dwang jegens gecontroleerde personen en kunnen bijgevolg geen toegang afdwingen tot informatie, <i>a fortiori</i> tot de informatie die door artikel 458 van het Strafwetboek beschermd is.</p>
<p>La disposition reprend les pouvoirs listés aux articles 32, § 2, et 33, § 2, de la directive NIS2. De plus, d'autres pouvoirs sont conférés aux autorités compétentes pour le contrôle afin qu'elles puissent mener à bien leurs tâches de contrôle et d'imposition de mesures administratives.</p>	<p>De bepaling bevat de bevoegdheden die zijn opgesomd in de artikelen 32, lid 2, en 33, lid 2, van de NIS2-richtlijn. Bovendien worden andere bevoegdheden toevertrouwd aan de voor het toezicht bevoegde autoriteiten met het oog op de uitvoering van hun toezichthoudende taken en het opleggen van administratieve maatregelen.</p>
<p>Les autorités compétentes pour le contrôle peuvent notamment prendre l'identité des personnes présentes lors d'un contrôle et pénétrer sans avertissement préalable dans tous les locaux utilisés par l'entité contrôlée. En pratique, le nom des personnes pouvant pénétrer sans avertissement préalable peut être fourni à l'avance pour plus de prévisibilité. Lorsqu'il s'agit de locaux habités, ces autorités ne peuvent y pénétrer que moyennant l'autorisation préalable d'un juge d'instruction. Les paragraphes 2 et 3 déterminent la procédure et les éléments à fournir au juge d'instruction. Les autorités compétentes peuvent aussi</p>	<p>De voor het toezicht bevoegde autoriteiten mogen met name de identiteit opnemen van de personen die aanwezig zijn bij een controle en zonder voorafgaande verwittiging alle lokalen betreden die door de gecontroleerde entiteit worden gebruikt. In de praktijk kunnen de namen van de personen die zonder voorafgaande verwittiging mogen binnengaan, vooraf worden verstrekt om de voorspelbaarheid te verbeteren. Indien de lokalen bewoond zijn, mogen deze autoriteiten de lokalen alleen betreden mits vooraf een machtiging is uitgereikt door de onderzoeksrechter. De paragrafen 2 en 3 gaan</p>

demander l'assistance des services de la police fédérale ou locale. A noter qu'il ne s'agit pas pour les services de police locale ou fédérale d'une obligation d'assistance. Lorsque, par exemple, l'état de leur effectif ne leur permet pas d'assister l'autorité compétente pour le contrôle qui aurait introduit une demande, les services de police peuvent évidemment refuser cette demande.	nader in op de procedure en de informatie die aan de onderzoeksrechter moet worden verstrekt. De bevoegde autoriteiten kunnen ook de bijstand vragen van federale of lokale politiediensten. Opgemerkt wordt dat federale of lokale politiediensten niet verplicht zijn om deze bijstand te verlenen. Wanneer hun personeelsbestand bijvoorbeeld niet toelaat om bijstand te verlenen aan de voor het toezicht bevoegde autoriteit die een verzoek heeft ingediend, kunnen de politiediensten dit verzoek uiteraard weigeren.
Il est précisé également les règles à respecter en cas d'audition et celles relatives aux données consultables.	Voorts komen de na te leven regels aan bod in geval van een verhoor en met betrekking tot de gegevens die mogen worden geraadpleegd.
Dans le cadre des contrôles, les autorités compétentes pour le contrôle peuvent consulter tous les supports d'information et les données qu'ils contiennent, se faire produire 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.	In het kader van de controles mogen de voor het toezicht bevoegde autoriteiten alle informatiedragers en de erin opgenomen gegevens raadplegen, zich 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.
Lorsque les autorités compétentes pour le contrôle constatent une violation de données à caractère personnel au sens du règlement européen 2016/679 (RGPD), ils doivent informer l'Autorité de protection des données sans retard injustifié.	Wanneer de voor het toezicht bevoegde autoriteiten een inbreuk in verband met persoonsgegevens zoals gedefinieerd in Europese verordening 2016/679 (AVG) vaststellen, moeten zij de Gegevensbeschermingsautoriteit daarvan onverwijld in kennis stellen.
Pour finir, les contrôles auprès des entités importantes ne peuvent s'organiser que de manière <i>ex post</i> .	Tot slot mogen controles van belangrijke entiteiten alleen achteraf worden georganiseerd.
Article 49	Article 49
Cet article dispose que chaque autorité compétente pour le contrôle rédige un rapport à la fin de chaque contrôle et le communique, d'abord à l'entité inspectée, ensuite aux autres autorités compétentes pour le contrôle.	Dit artikel bepaalt dat elke voor het toezicht bevoegde autoriteit een verslag opstelt na afloop van elke controle en het eerst aan de geïnspecteerde entiteit bezorgt en vervolgens aan de andere voor het toezicht bevoegde autoriteiten.
Article 50	Article 50
Cet article impose à l'entité contrôlée	Dit artikel bepaalt dat de gecontroleerde

d'apporter son entière collaboration aux autorités compétentes pour le contrôle.	entiteit haar volledige medewerking moet verlenen aan de voor het toezicht bevoegde autoriteiten.
Le Roi est habilité à déterminer, par (sous-)secteur, des rétributions, en ce compris les modalités de calcul et de paiement, relatives aux prestations d'inspection. Une telle décision ne peut avoir lieu qu'après avis de l'autorité nationale de cybersécurité, par arrêté délibéré en Conseil des Ministres.	De Koning is gemachtigd om, per (deel)sector, retributies te bepalen, met inbegrip van de berekenings- en betalingsregels, voor de inspectieprestaties. Een dergelijke beslissing kan slechts worden genomen na advies van de nationale cyberbeveiligingsautoriteit, bij besluit vastgesteld na overleg in de Ministerraad.
Pour rappel, n'étant pas des officiers de police judiciaire, les membres des autorités compétente pour le contrôle qui effectuent les tâches de contrôle ne peuvent forcer l'entité à coopérer. Cela étant, ils peuvent consigner dans un procès-verbal le refus de l'entité d'apporter sa collaboration lors du contrôle, voir la communication volontaire d'informations inexacts ou incomplètes ou l'empêchement ou l'entrave volontaire de l'exécution du contrôle par les autorités compétentes pour le contrôle, conformément au paragraphe 3.	Ter herinnering, aangezien zij geen officieren van gerechtelijke politie zijn, mogen de leden van de voor het toezicht bevoegde autoriteiten die toezichthoudende taken uitvoeren, de entiteit niet dwingen om mee te werken. Zij kunnen evenwel optekenen in een proces-verbaal dat de entiteit weigert mee te werken bij een controle, of zelfs opzettelijk foutieve of onvolledige informatie verstrekt of de uitvoering van een controle door de voor het toezicht bevoegde autoriteiten opzettelijk verhindert of belemmert, overeenkomstig paragraaf 3.
CHAPITRE 2	HOODSTUK 2
Les mesures et amendes administratives	De administratieve maatregelen en geldboetes
Section 1^{re}	Afdeling 1
<i>Procédure</i>	<i>Procedure</i>
Dans le cadre de la présente section, il faut préciser qu'en l'absence de dispositions spécifiques, le Conseil d'Etat est compétent pour les recours en annulation des décisions imposant des mesures administratives prises en exécution du présent projet de loi.	In het kader van deze afdeling moet worden verduidelijkt dat, indien geen specifieke bepalingen van toepassing zijn, de Raad van State bevoegd is voor beroepen tot nietigverklaring van beslissingen die administratieve maatregelen opleggen die worden genomen in uitvoering van dit wetsontwerp.
Article 51	Artikel 51
Cet article détermine la procédure à l'issue de laquelle des mesures administratives peuvent être prises par les autorités compétentes pour le contrôle à l'égard d'entités essentielles ou importantes qui ne respecteraient pas le projet de loi.	Dit artikel bepaalt de procedure na afloop waarvan de voor het toezicht bevoegde autoriteiten administratieve maatregelen kunnen nemen ten aanzien van essentiële of belangrijke entiteiten die het wetsontwerp niet zouden naleven.

Dans un premier temps, les manquements doivent être constatés dans un procès-verbal par les membres assermentés des autorités compétentes pour le contrôle. En principe, les manquements aux dispositions du projet de loi relèvent de la compétence de l'autorité nationale de cybersécurité. Cela étant, les manquements aux mesures de gestion des risques en matière de cybersécurité sectorielles ou sous-sectorielles supplémentaires visées à l'article 34 relèvent de l'autorité sectorielle compétente ou du service d'inspection compétent, pour autant qu'une telle autorité ait été désignée.	Eerst moeten de inbreuken worden opgetekend in een proces-verbaal door de beëdigde leden van de voor het toezicht bevoegde autoriteiten. In principe is de nationale cyberbeveiligingsautoriteit bevoegd voor inbreuken op de bepalingen van het wetsontwerp. Inbreuken op bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's, als bedoeld in artikel 34, behoren evenwel tot de bevoegdheid van de bevoegde sectorale overheid of inspectiedienst, voor zover een dergelijke autoriteit is aangewezen.
De plus, l'autorité nationale de cybersécurité peut accepter de déléguer l'imposition de mesures administratives à une autorité sectorielle. Cette procédure permet de garantir le suivi des dossiers en cas de charges de travail importantes.	Daarnaast kan de nationale cyberbeveiligingsautoriteit ermee instemmen om het opleggen van administratieve maatregelen te delegeren aan een sectorale overheid. Deze procedure waarborgt de opvolging van de dossiers in geval van hoge werklast.
Sur la base du procès-verbal évoqué <i>supra</i> et des rapports des autorités compétentes pour le contrôle, l'autorité compétente pour le contrôle rédige un projet de décision contenant une ou plusieurs mesures pouvant être prises en constatation de manquements et/ou une amende. Ces mesures et amendes se trouvent aux articles 58 et 59 qui transposent les articles 32, § 4, 33, § 4 et 34, §§ 3 à 5, de la directive NIS2. Le projet de décision, non définitif, comprend également le délai qui serait laissé à l'entité concernée pour exécuter les mesures. Ce délai doit prendre en considération les conditions de fonctionnement de l'entité et les mesures elles-mêmes.	Op basis van voornoemd proces-verbaal en de verslagen van de voor het toezicht bevoegde autoriteiten, stelt de voor het toezicht bevoegde autoriteit een ontwerp van beslissing op dat een of meer mogelijke maatregelen voor de vaststelling van inbreuken en/of een geldboete bevat. Deze maatregelen en geldboetes komen aan bod in de artikelen 58 en 59 die voorzien in de omzetting van de artikelen 32, lid 4, 33, lid 4 en 34, leden 3 tot 5, van de NIS2-richtlijn. Het ontwerp van beslissing, dat nog niet definitief is, vermeldt ook de termijn waarover de betrokken entiteit beschikt om de maatregelen uit te voeren. Deze termijn moet rekening houden met de werkingsomstandigheden van de entiteit en met de maatregelen zelf.
Ensuite, ce projet de décision est envoyé à l'entité concernée avec d'une part, les motifs relatifs aux mesures et/ou amendes envisagés et, d'autre part, l'information que l'entité a 15 jours, à partir de la réception du projet de décision, pour formuler par écrit ses moyens de défense ou de demander à être entendu. L'information est présumée avoir été portée à la connaissance de l'entité concernée 6 jours	Vervolgens wordt dit ontwerp van beslissing naar de betrokken entiteit gestuurd, samen met de motivering voor de overwogen maatregelen en/of geldboetes en de mededeling dat de entiteit over 15 dagen beschikt, vanaf de ontvangst van het ontwerp van beslissing, om haar verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De betrokken entiteit wordt geacht in kennis te zijn

après l'envoi du projet de décision.	gesteld van de informatie 6 dagen na de verzending van het ontwerp van beslissing.
Le projet de loi prévoit qu'il est possible de déroger à la communication du projet de décision, uniquement dans de très rares cas où cette communication empêcherait une intervention immédiate pour prévenir un incident ou y répondre. L'usage de cette exception doit être dûment motivé.	Het wetsontwerp bepaalt dat het enkel mogelijk is om af te wijken van de verplichting om het ontwerp van beslissing mee te delen in heel zeldzame gevallen waarin een onmiddellijk optreden om incidenten te voorkomen of erop te reageren anders zou worden belemmerd. Het gebruik van deze uitzondering moet naar behoren worden gemotiveerd.
Après que l'entité concernée ait pu faire valoir ses moyens de défenses, par écrit ou en étant directement entendu, à la fin du délai de 15 jours en l'absence de réaction de la part de l'entité ou dans le cas d'exception où la communication du projet de décision ne doit pas être faite, l'autorité compétente pour le contrôle maintient, modifie ou renonce au projet de décision. Pour ce faire, elle doit prendre en compte la catégorie d'entité à laquelle appartient l'entité concernée (essentielle ou importante), les moyens de défense avancés par l'entité et les éléments visés à l'article 54. L'article 54 transpose l'article 32, § 7, de la directive NIS2 et porte sur les éléments qui doivent être pris en considération lors d'une prise de décision (nous renvoyons au commentaire de cet article <i>infra</i> pour plus de détails). Une décision devra toujours être proportionnée, spécifique par rapport aux circonstances des faits. Dans ce cadre, l'amende n'est pas considérée comme la mesure ou la sanction par défaut. Une amende n'est infligée que lorsque cela est proportionné.	Nadat de betrokken entiteit haar verweermiddelen heeft kunnen aanvoeren, schriftelijk of door rechtstreeks te worden gehoord, op het einde van de termijn van 15 dagen bij het uitblijven van een reactie van de entiteit of in het uitzonderlijke geval waarin het ontwerp van beslissing niet moet worden meegedeeld, zal de voor het toezicht bevoegde autoriteit het ontwerp van beslissing handhaven, wijzigen of ervan afzien. Daartoe moet zij rekening houden met de entiteitscategorie waartoe de betrokken (essentiële of belangrijke) entiteit behoort, de door de entiteit aangevoerde verweermiddelen en de in artikel 54 bedoelde elementen. Artikel 54 voorziet in de omzetting van artikel 32, lid 7, van de NIS2-richtlijn en heeft betrekking op de elementen waarmee rekening moet worden gehouden bij het nemen van een beslissing (voor meer informatie verwijzen we naar de commentaar bij dit artikel hieronder). Een beslissing moet altijd evenredig zijn en rekening houden met de specifieke omstandigheden van de feiten. In dit kader wordt de geldboete niet als een standaardmaatregel of -sanctie beschouwd. Een geldboete wordt alleen opgelegd als die evenredig is.
Si maintenue ou modifiée, l'entité doit se conformer à la décision prise par l'autorité, sans préjudice de son droit à faire appel de la décision (voir <i>infra</i>).	De entiteit moet de beslissing van de autoriteit naleven, ongeacht of deze behouden of gewijzigd wordt, onverminderd haar recht om in beroep te gaan tegen de beslissing (zie <i>infra</i>).
Article 52	Artikel 52
Cet article porte sur la procédure à suivre lorsqu'une entité essentielle ne se conforme pas à une décision prise par une autorité compétente pour le contrôle, visée à l'article	Dit artikel beschrijft de te volgen procedure wanneer een essentiële entiteit geen gevolg geeft aan een beslissing van een voor het toezicht bevoegde autoriteit, als bedoeld in het

précédent.	vorige artikel.
Il est renvoyé <i>mutatis mutandis</i> au commentaire de l'article précédent. En effet, la procédure est la même. La seule différence est que les mesures administratives possibles, lorsque l'entité essentielle ne se conforme pas à une décision de l'autorité prise conformément à l'article 51, sont celles visées aux articles 59 et 60, transposant l'article 32, § 6, de la directive NIS2. Les amendes sont toujours possibles.	Er wordt <i>mutatis mutandis</i> verwezen naar de commentaar bij het vorige artikel. De procedure is immers dezelfde. Het enige verschil is dat de mogelijke administratieve maatregelen, wanneer de essentiële entiteit geen gevolg geeft aan een door de autoriteit genomen beslissing overeenkomstig artikel 51, de maatregelen deze bedoeld in artikel 59 en 60 zijn, die voorzien in de omzetting van artikel 32, lid 6, van de NIS2-richtlijn. Geldboetes zijn altijd mogelijk.
Article 53	Artikel 53
Conformément à cet article, les procès-verbaux des membres assermentés de l'autorité compétente pour le contrôle font foi jusqu'à preuve du contraire.	Overeenkomstig dit artikel hebben de processen-verbaal van de beëdigde leden van de voor het toezicht bevoegde autoriteit bewijskracht tot het tegendeel is bewezen.
Article 54	Artikel 54
Cet article énumère les éléments qui doivent être pris en compte par le directeur de l'autorité compétente pour le contrôle avant de prendre une décision au sens des articles 51 et 52.	Dit artikel somt de elementen op waarmee de directeur van de voor het toezicht bevoegde autoriteit rekening moet houden alvorens een beslissing te nemen als bedoeld in artikel 51 en 52.
La disposition transpose l'article 32, § 7, de la directive NIS2. Elle rappelle l'obligation de respecter les droits de la défense et de tenir compte des circonstances propres à chaque cas. Il est important de noter que le respect des droits de la défense est assuré, en plus du présent article, par les articles 51, §§ 3 et 4, et 52, §§ 3 et 4, qui mettent en place le principe <i>audi alteram partem</i> .	De bepaling voorziet in de omzetting van artikel 32, lid 7, van de NIS2-richtlijn. Ze herinnert aan de verplichting om de rechten van de verdediging te eerbiedigen en rekening te houden met de omstandigheden van elk afzonderlijk geval. Het is belangrijk te vermelden dat de eerbiediging van de rechten van de verdediging, behalve door dit artikel, ook gewaarborgd wordt door de artikelen 51, §§ 3 en 4, en 52, §§ 3 en 4, die het principe <i>audi alteram partem</i> vastleggen.
La disposition énumère les circonstances minimum auxquelles il doit être tenu compte. Parmi celles-ci, se trouvent la catégorie à laquelle appartient l'entité, le caractère répété ou non des violations, la durée de la violation, les dommages causés, ...	De bepaling somt de minimale omstandigheden op waarmee rekening moet worden gehouden. Deze omvatten de categorie waartoe de entiteit behoort, het al dan niet herhaaldelijke karakter van inbreuken, de duur van de inbreuk, de veroorzaakte schade, ...
L'article précise par ailleurs que, lorsque l'Autorité de protection des données a imposé une amende pour un ou plusieurs faits, les	Het artikel verduidelijkt bovendien dat, wanneer de Gegevensbeschermingsautoriteit een geldboete heeft opgelegd voor een of meer

autorités compétentes pour le contrôle ne peuvent plus imposer d'amendes pour les mêmes faits. Il s'agit là d'une application du principe <i>non bis in idem</i> .	feiten, de voor het toezicht bevoegde autoriteiten geen geldboete kunnen opleggen voor dezelfde feiten. Het betreft hier een toepassing van het principe <i>non bis in idem</i> .
Article 55	Artikel 55
Cet article porte sur la communication de la décision finale prise par l'autorité compétente pour le contrôle et le délai endéans lequel l'entité doit s'acquitter de l'amende.	Dit artikel gaat nader in op de mededeling van de definitieve beslissing van de voor het toezicht bevoegde autoriteit en de termijn waarbinnen de entiteit de geldboete moet betalen.
Les décisions précitées sont envoyées par envoi recommandé.	Voorname beslissingen worden aangetekend verzonden.
Les amendes administratives doivent être acquittées dans le 60 jours. Ce délai est réputé commencer au plus tard 6 jours après l'envoi par recommandé de la décision.	Administratieve geldboetes moeten binnen de 60 dagen worden betaald. Deze termijn wordt geacht in te gaan uiterlijk 6 dagen nadat de beslissing aangetekend is verzonden.
Pour les autres mesures administratives, la décision précise le délai d'exécution des mesures imposées.	Voor de andere administratieve maatregelen vermeldt de beslissing de uitvoeringstermijn van de opgelegde maatregelen.
Article 56	Artikel 56
Cet article porte sur les conséquences d'un défaut de paiement d'une amende administrative imposée à une entité au travers d'une décision visée à l'article 51 ou 52.	Dit artikel behandelt de gevolgen van het niet betalen van een administratieve geldboete die is opgelegd aan een entiteit bij een in artikel 51 of 52 bedoelde beslissing.
En cas de défaut de paiement, l'autorité compétente pour le paiement peut décerner une contrainte au travers du représentant légal de cette autorité ou d'un membre habilité à cette fin.	In geval van wanbetaling kan de voor de betaling bevoegde overheid een dwangbevel uitvaardigen via een wettelijke vertegenwoordiger van deze autoriteit of een daartoe gemachtigd personeelslid.
Cette contrainte doit être signifiée par exploit d'un huissier de justice et contenir un commandement à l'entité de payer l'amende dans les 48 heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.	Dit dwangbevel moet bij gerechtsdeurwaarderexploot worden betekend en een aan de entiteit gericht bevel bevatten om de geldboete te betalen binnen 48 uur, op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.
L'entité peut former opposition à la contrainte devant le juge des saisies, de manière motivée, au travers d'une citation de l'autorité compétente pour le contrôle dans les 15 jours à	De entiteit kan tegen het dwangbevel verzet aantekenen bij de beslagrechter, mits motivering, door middel van een dagvaarding van de voor het toezicht bevoegde autoriteit

partir de la signification de la contrainte. En ce cas, les dispositions pertinentes du Code judiciaire sont applicables à ce délai.	binnen 15 dagen vanaf de betekening van heet dwangbevel. In elk geval zijn de relevante bepalingen van het Gerechtelijk Wetboek van toepassing op deze termijn.
L'exercice de l'opposition suspend l'exécution de la contrainte le temps qu'il soit statué sur le fond, les saisies déjà effectuées gardant leur caractère conservatoire.	De uitoefening van verzet schorst de tenuitvoerlegging van het dwangbevel tot uitspraak ten gronde is gedaan, waarbij de reeds gelegde beslagen hun bewarend karakter behouden.
Le paragraphe 4 du présent article permet à l'autorité compétente pour le contrôle de pratiquer des saisies conservatoires et d'exécuter la contrainte par les voies d'exécutions de la cinquième partie du Code judiciaire.	Paragraaf 4 van dit artikel staat de voor het toezicht bevoegde autoriteit toe om bewarend beslag te leggen en het dwangbevel uit te voeren met de middelen tot tenuitvoerlegging van het vijfde deel van het Gerechtelijk Wetboek.
Les frais de signification par exploit d'huissier, établis conformément aux règles établies pour ces actes de signification sont à charge de l'entité concernée.	De kosten voor de betekening bij gerechtsdeurwaarderexploot die worden bepaald volgens de regels die gelden voor deze betekeningsakten, zijn ten laste van de betrokken entiteit.
Article 57	Artikel 57
Cet article établit le délai de prescription extinctive des mesures et amendes administratives pouvant être imposées en vertu du projet de loi. Ce délai est de 3 ans, à compter du jour où les faits ont été commis.	Dit artikel bepaalt de bevrijdende verjaringstermijn van de maatregelen en administratieve geldboetes die kunnen worden opgelegd krachtens het wetsontwerp. Deze termijn bedraagt 3 jaar, te rekenen vanaf de dag waarop de feiten zijn gepleegd.
Afin de respecter le principe <i>non bis in idem</i> , le paiement de l'amende administrative imposée pour des faits précis éteint les possibilités de poursuites pénales pour ces mêmes faits.	Teneinde het principe <i>non bis in idem</i> na te leven, doet de betaling van de administratieve geldboete die is opgelegd voor precieze feiten de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor dezelfde feiten.
Section 2	Afdeling 2
<i>Mesures et amendes administratives</i>	<i>Administratieve maatregelen en geldboetes</i>
Article 58	Article 58
Cet article transpose les articles 32, § 4, et 33, § 4, de la directive NIS2. Il reprend les différentes mesures administratives pouvant être prises par les autorités compétentes pour le contrôle en cas de constatation de manquements par les entités essentielles ou importantes.	Dit artikel voorziet in de omzetting van de artikelen 32, lid 4, en 33, lid 4, van de NIS2-richtlijn. Het beschrijft de verschillende administratieve maatregelen die de voor het toezicht bevoegde autoriteiten kunnen nemen indien inbreuken door essentiële of belangrijke

	entiteiten worden vastgesteld.
La disposition spécifie les mesures qui ne s'appliqueraient qu'à une catégorie d'entité. Le corollaire de cette spécification est que chaque mesure pour laquelle rien n'est spécifié peut être prise à l'encontre des entités, qu'elles soient essentielles ou importantes.	De bepaling specificeert welke maatregelen alleen gelden voor een entiteitscategorie. Deze specificering heeft tot gevolg dat elke maatregel waarvoor niets gespecificeerd is kan worden genomen ten aanzien van entiteiten, ongeacht of ze essentieel of belangrijk zijn.
Article 59	Artikel 59
Cet article énumère les amendes administratives qui peuvent être imposées.	Dit artikel somt de administratieve geldboetes op die kunnen worden opgelegd.
La disposition spécifie les amendes qui ne s'appliqueraient qu'à une catégorie d'entité. Le corollaire de cette spécification est que chaque amende pour laquelle rien n'est spécifié peut être infligée aux entités, qu'elles soient essentielles ou importantes.	De bepaling specificeert welke geldboetes alleen gelden voor een entiteitscategorie. Deze specificering heeft tot gevolg dat elke geldboete waarvoor niets gespecificeerd is kan worden opgelegd aan entiteiten, ongeacht of ze essentieel of belangrijk zijn.
L'alinéa 1 ^{er} , 4° et 5°, transpose l'article 34, §§ 4 et 5, de la directive NIS2. Le reste de la disposition reprend le contenu des articles 52, §§ 4, 5 et 6, et 55, § 4, alinéa 2, et § 5, de la loi NIS1.	Het eerste lid, 4° et 5°, voorziet in de omzetting van artikel 34, leden 4 en 5, van de NIS2-richtlijn. Voor het overige bevat de bepaling de inhoud van de artikelen 52, §§ 4, 5 en 6, en 55, § 4, tweede lid, en § 5, van de NIS1-wet.
Article 60	Artikel 60
Cette disposition transpose l'article 32, § 5, de la directive NIS2. Elle reprend les différentes mesures administratives pouvant être prises par les autorités compétentes pour le contrôle dans le cas où les mesures administratives déjà prises à l'encontre d'une entité ne sont pas exécutées par l'entité dans le délai imparti.	Deze bepaling voorziet in de omzetting van artikel 32, lid 5, van de NIS2-richtlijn. Ze bevat de verschillende administratieve maatregelen die de voor het toezicht bevoegde autoriteiten kunnen nemen indien de administratieve maatregelen die al genomen zijn ten aanzien van een entiteit, niet worden uitgevoerd door deze laatste binnen de toegestane termijn.
Ces mesures sont uniquement appliquées jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente pour le contrôle.	Deze maatregelen worden alleen toegepast tot de betrokken entiteit de nodige maatregelen neemt om de tekortkomingen te verhelpen of te voldoen aan de eisen van de voor het toezicht bevoegde autoriteit.
Article 61	Artikel 61
Cette disposition transpose les articles 32, § 6, et 32, § 5, de la directive NIS2. Selon cet article, sans préjudice des dispositions nationales spécifiques en matière de responsabilité des agents de la fonction publique, les personnes	Deze bepaling voorziet in de omzetting van de artikelen 32, lid 6, en 32, lid 5, van de NIS2-richtlijn. Volgens dit artikel moeten de natuurlijke personen die aansprakelijk zijn voor een entiteit of optreden als wettelijke

physiques responsables d'une entité ou agissant en qualité de représentant légal d'une entité doivent avoir le pouvoir de veiller au respect, par l'entité, du présente projet de loi.	vertegenwoordiger van een entiteit, onverminderd de specifieke nationale bepalingen inzake de aansprakelijkheid van ambtenaren, de bevoegdheid hebben om ervoor te zorgen dat de entiteit dit wetsontwerp naleeft.
TITRE 5	TITEL 5
<i>Dispositions spécifiques au secteur de l'administration publique</i>	<i>Specifieke bepalingen voor de overheidssector</i>
Article 62	Artikel 62
Cet article rend inapplicables les amendes et les mesures des articles 60 et 61 aux entités faisant partie du secteur de l'administration publique. Cette dérogation est, en partie, laissée à l'appréciation des États membres par la directive NIS2, au travers de l'article 34, § 7 (en matière d'amendes administratives) et, pour l'autre partie, prévue par la directive NIS2 elle-même, au travers de l'article 32, § 5, alinéa 3.	Dit artikel bepaalt dat de geldboetes en maatregelen bedoeld in artikel 60 en 61 niet van toepassing zijn op entiteiten die deel uitmaken van de overheidssector. De NIS2-richtlijn laat deze afwijking gedeeltelijk over aan het oordeel van de lidstaten, via artikel 34, lid 7 (inzake administratieve geldboetes) en, voor het overige gedeelte, waarin de NIS2-richtlijn zelf voorziet, via artikel 32, lid 5, derde alinea.
Article 63	Artikel 63
Cette disposition habilite le Roi à désigner une ou plusieurs autorités comme organismes d'évaluation de la conformité spécifiques au secteur des entités de l'administration publique. Par autorité, il faut entendre autorité publique.	Deze bepaling machtigt de Koning om een of meer autoriteiten aan te wijzen als specifieke conformiteitsbeoordelingsinstanties voor de overheidssector. In de Franse versie moet onder "autorité" "autorité publique" worden verstaan.
L'évaluation de la conformité se fait selon les conditions fixées par le Roi conformément à l'article 39, alinéa 1 ^{er} , 1° du projet de loi.	De conformiteitsbeoordeling gebeurt volgens de voorwaarden bepaald door de Koning overeenkomstig artikel 39, eerste lid, 1°, van het wetsontwerp.
En tant qu'organisme d'évaluation de la conformité, l'autorité désignée doit être agréée par l'autorité nationale de cybersécurité avant d'effectuer des évaluations de la conformité. La détermination des conditions de l'agrément est laissée au Roi.	De autoriteit die is aangewezen als conformiteitsbeoordelingsinstantie moet door de nationale cyberbeveiligingsautoriteit worden erkend, alvorens conformiteitsbeoordelingen te kunnen uitvoeren. Het bepalen van de erkenningsvoorwaarden wordt overgelaten aan de Koning.
Comme le prévoit le paragraphe 3, lorsqu'une autorité a été désignée comme organisme d'évaluation de la conformité pour des entités de l'administration publique, ces entités doivent effectuer leurs audits auprès de ladite	Zoals bepaald in paragraaf 3, wanneer een autoriteit is aangewezen als conformiteitsbeoordelingsinstantie voor overheidsinstanties, moeten deze instanties hun audits uitvoeren bij deze autoriteit.

autorité.	
Les entités de l'administration publique conservent la possibilité d'effectuer l'évaluation de la conformité, soit par l'autorité désignée comme organisme d'évaluation de la conformité, soit par le service d'inspection de l'autorité nationale de cybersécurité.	De overheidsinstanties behouden de mogelijkheid om een conformiteitsbeoordeling te laten uitvoeren ofwel door de autoriteit die is aangewezen als conformiteitsbeoordelingsinstantie, of door de inspectiedienst van de nationale cyberbeveiligingsautoriteit.
Article 64	Artikel 64
Cet article établit les règles spécifiques relatives aux services d'inspection compétents pour les entités de l'administration publique.	Dit artikel bevat specifieke regels voor de inspectiediensten die bevoegd zijn voor de overheidsinstanties.
En l'absence de désignation par le Roi, le service d'inspection de l'autorité nationale de cybersécurité est compétent pour exercer les tâches de supervision déterminées par le présent projet de loi. En tous les cas, l'autorité compétente pour le contrôle doit jouir d'une indépendance opérationnelle vis-à-vis des entités supervisées.	Bij gebrek aan een aanwijzing door de Koning is de inspectiedienst van de nationale cyberbeveiligingsautoriteit bevoegd om de toezichthoudende taken uit te voeren die dit wetsontwerp bepaalt. In elk geval moet de voor het toezicht bevoegde autoriteit operationeel onafhankelijk zijn van de instanties waarop zij toezicht houdt.
Article 65	Artikel 65
Conformément à cette disposition, quelle que soit l'autorité compétente pour le contrôle vis-à-vis des entités de l'administration publique, les dispositions relatives aux situations de conflits d'intérêts lui sont applicables.	Volgens deze bepaling zijn de bepalingen inzake belangenconflicten van toepassing ongeacht de voor het toezicht bevoegde autoriteit ten aanzien van overheidsinstanties.
TITRE 6	TITEL 6
<i>Traitement des données à caractère personnel</i>	<i>Verwerking van persoonsgegevens</i>
CHAPITRE 1er	HOODSTUK 1
Principes relatifs au traitement	Beginnelsen betreffende de verwerking
Article 66	Artikel 66
Cette disposition rend applicable les définitions du règlement européen 2016/679 (ci-après, le « RGPD ») au titre 6 du projet de loi.	Volgens deze bepaling zijn de definities van Europese Verordening 2016/679 (hierna de "AVG") van toepassing op titel 6 van het wetsontwerp.
A noter qu'il ne s'agit pas ici d'une répétition des dispositions du RGPD (interdite car le RGPD, en tant que règlement européen, est	Het gaat hier niet om een herhaling van de bepalingen van de AVG (wat verboden is omdat de AVG, als Europese verordening, rechtstreeks

d'application directe en droit nationale, de sorte que les obligations légales du RGPD ne peuvent être répétées en droit national) mais de l'utilisation des définitions du règlement pour assurer la cohérence dans les notions utilisées.	van toepassing is in het nationale recht, zodat de wettelijke verplichtingen van de AVG niet mogen worden herhaald in het nationale recht). De definities van de verordening worden evenwel gebruikt met het oog op de samenhang tussen de gebruikte begrippen.
Article 67	Artikel 67
Cette disposition énumère les finalités sur base desquelles des données à caractère personnel (délimitées au sein de l'article suivant) peuvent être traitées.	Deze bepaling somt de doeleinden op waarvoor persoonsgegevens (gedefinieerd in het volgende artikel) mogen worden verwerkt.
Article 68	Artikel 68
Cet article détermine, pour chaque finalité, les types de données à caractère personnel qui peuvent être traitées.	Dit artikel bepaalt, voor elk doeleinde, de soorten persoonsgegevens die mogen worden verwerkt.
La détermination des données à caractère personnel pouvant être traitées est systématiquement liée avec une finalité afin d'encadrer les traitements de données à caractère personnel effectués en exécution du projet de loi.	De persoonsgegevens die mogen worden verwerkt, worden systematisch gekoppeld aan een doeleinde om de verwerking van persoonsgegevens in uitvoering van het wetsontwerp te regelen.
Article 69	Artikel 69
Cet article détermine les personnes concernées par les traitements.	Dit artikel bepaalt de personen die betrokken zijn bij de verwerkingen.
Article 70	Artikel 70
Cette disposition détermine les responsables de traitement dans le cadre de l'exécution du projet de loi.	Deze bepaling verduidelijkt wie de verwerkingsverantwoordelijken zijn in het kader van de uitvoering van het wetsontwerp.
Par principe, chaque personne est responsable des traitements qu'elle effectue. Cela signifie, par exemple, que l'autorité nationale de cybersécurité est responsable de traitement dans le cadre de l'enregistrement des entités car c'est auprès de cette entité que ces enregistrements sont effectués, ou encore qu'un service d'inspection sectoriel est responsable des traitements qu'il effectue dans le cadre de la supervision des mesures spécifiques à son secteur visées à l'article 33, notamment lors d'une audition.	In principe is elke persoon verantwoordelijk voor de verwerkingen die hij uitvoert. Dit betekent bijvoorbeeld dat de nationale cyberbeveiligingsautoriteit verantwoordelijk is voor de verwerkingen in het kader van de registratie van entiteiten omdat zij de registraties uitvoert, of nog dat een sectorale inspectiedienst verantwoordelijk is voor de verwerkingen die hij uitvoert in het kader van het toezicht op de in artikel 33 bedoelde specifieke maatregelen voor zijn sector, met name bij een verhoor.

CHAPITRE 2	HOOFDSTUK 2
Durée de conservation	Bewaartermijn
Article 71	Artikel 71
Cette disposition fixe la durée de conservation des données à caractère personnel traitées dans le cadre du projet de loi à 5 ans après la fin du dernier traitement effectué, sans que cette durée de conservation ne puisse dépasser 10 ans à partir du premier traitement effectué.	Volgens deze bepaling bedraagt de bewaartermijn van de persoonsgegevens die in het kader van het wetsontwerp worden verwerkt, 5 jaar na afloop van de laatste verwerking en maximaal 10 jaar vanaf de eerste verwerking.
CHAPITRE 3	HOOFDSTUK 3
Limitation des droits des personnes concernées	Beperking van de rechten van de betrokkenen
Article 72	Artikel 72
Cette disposition met en œuvre l'article 23 du RGPD. Afin d'assurer l'exécution des contrôles et de la supervision organisés par le projet de loi, il peut être dérogé à certains droits des personnes concernées. Les droits en question sont le droit à la transparence des informations et des communications ; le droit à l'accès aux informations lors de la collecte de données ; le droit d'accès ; le droit de rectification ; le droit à la limitation du traitement et l'obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel (voir les articles 12 à 16, 18 et 19 du RGPD).	Deze bepaling geeft uitvoering aan artikel 23 van de AVG. Met het oog op de uitvoering van de in het wetsontwerp geregelde controles en toezicht kan worden afgeweken van sommige rechten van betrokkenen. De rechten in kwestie zijn het recht op transparante informatie en communicatie; het recht op toegang tot informatie bij de gegevensverzameling; het recht van inzage; het recht op rectificatie; het recht op beperking van de verwerking en de kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens (zie de artikelen 12 tot 16, 18 en 19 van de AVG).
L'article permet, sous des conditions et limitations qu'il détermine, de déroger aux droits des personnes précités.	Het artikel maakt het mogelijk om, onder de voorwaarden en beperkingen die het bepaalt, af te wijken van de rechten van voornoemde personen.
L'exemption ne vaut que pour la finalité de contrôle et de supervision des entités essentielles et importantes, pour les catégories de données concernées par cette finalité.	De vrijstelling geldt alleen voor het doeleinde op het gebied van controle en toezicht ten aanzien van essentiële en belangrijke entiteiten, voor de gegevenscategorieën waarop dit doeleinde betrekking heeft.
L'exemption ne s'applique que pendant la période au cours de laquelle une personne concernée fait l'objet d'un contrôle, ou en tous les cas au cours de laquelle ses données sont	De vrijstelling geldt alleen voor de periode waarin een betrokkene onderworpen is aan een controle, of in elk geval waarin zijn gegevens worden verwerkt in het kader van die controle.

traitées dans le cadre dudit contrôle. Cette période ne peut durer plus d'un an, deux en comptant les actes préparatoires.	Deze periode mag niet langer duren dan één jaar, of twee jaar als men rekening houdt met de voorbereidende werkzaamheden.
De plus, si un responsable de traitement ne respecte pas les conditions de l'exemption, il ne peut en bénéficier et risque donc d'effectuer un manquement au RGPD.	Indien een verwerkingsverantwoordelijke de voorwaarden van de vrijstelling niet naleeft, kan hij er bovendien geen gebruik van maken en loopt hij dus het risico dat hij de AGV overtreedt.
Article 73	Artikel 73
Dans le cadre de l'exemption visée à l'article précédent, le responsable doit tout de même fournir des informations aux personnes concernées, autant que possible et tant que cela ne compromet pas la finalité pour laquelle l'exemption est possible, à savoir le contrôle et l'inspection des entités dans le cadre du projet de loi.	In het kader van de in het vorige artikel bedoelde vrijstelling moet de verantwoordelijke de betrokkenen wel informatie bezorgen, voor zover mogelijk en zolang dit het doeleinde waarvoor de vrijstelling mogelijk is niet in het gedrang brengt, namelijk de controle en inspectie van de entiteiten in het kader van het wetsontwerp.
Cet article dispose que l'exemption visée à l'article précédent doit être levée lors de la fin du contrôle, de la supervision ou des actes préparatoires ou lorsque l'exemption n'est plus nécessaire pour le contrôle. En tous les cas, le délégué à la protection informe les personnes concernées à la levée de l'exemption.	Dit artikel bepaalt dat de in het vorige artikel bedoelde vrijstelling moet worden opgeheven op het einde van de controle, het toezicht of de voorbereidende werkzaamheden of wanneer de vrijstelling niet meer nodig is voor de controle. In elk geval informeert de functionaris voor gegevensbescherming de betrokkenen dat de vrijstelling is opgeheven.
CHAPITRE 5	HOOFDSTUK 5
Limitations aux obligations de notification des violations de données à caractère personnel	Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens
Article 74	Artikel 74
L'article introduit une autre dérogation, plus limitée, concernant l'article 34 du RGPD et l'obligation de notification individuelle en cas de violation de données personnelles. Ce n'est qu'avec l'autorisation de l'autorité nationale de cybersécurité, et seulement dans la mesure nécessaire pour préserver les finalités visées à l'article 74, § 2, du projet de loi, que cette notification individuelle ne serait plus obligatoire.	Het artikel voorziet in een andere, beperktere afwijking met betrekking tot artikel 34 van de AVGen de verplichte individuele kennisgeving in geval van een inbreuk in verband met persoonsgegevens. Deze individuele kennisgeving zou niet meer verplicht zijn mits toestemming van de nationale cyberbeveiligingsautoriteit en alleen voor zover nodig om de in artikel 74, § 2, van het wetsontwerp bedoelde doeleinden te vrijwaren.
TITRE 7	TITEL 7

<i>Dispositions finales</i>	<i>Slotbepalingen</i>
CHAPITRE 1 ^{er}	HOOFDSTUK 1
Dispositions transitoires	Overgangsbepalingen
Article 75	Artikel 75
Cette disposition habilite le Roi à fixer le délai endéans lequel l'évaluation périodique de la conformité doit, pour la première fois, être effectué par les entités essentielles (nous renvoyons au commentaire de l'article 39 pour plus de détails sur l'évaluation périodique de la conformité). Etant donné que le Roi fixe les modalités de cette évaluation ainsi que les cadres de référence utilisés, il doit lui revenir également de fixer un délai permettant aux entités essentielles de se mettre en conformité avec cette nouvelle obligation.	Deze bepaling machtigt de Koning om de termijn vast te stellen waarbinnen essentiële entiteiten de regelmatige conformiteitsbeoordeling voor het eerst moeten uitvoeren (we verwijzen naar de commentaar bij artikel 39 voor meer informatie over de regelmatige conformiteitsbeoordeling). Aangezien de Koning de modaliteiten van deze beoordeling en de gebruikte referentiekaders vaststelt, komt het Hem ook toe een termijn te bepalen waarbinnen de essentiële entiteiten aan deze nieuwe verplichting moeten voldoen.
CHAPITRE 2	HOOFDSTUK 2
Dispositions modificatives	Wijzigingsbepalingen
Section 1 ^{ère}	Afdeling 1
<i>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</i>	<i>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</i>
Les articles 76 et 77 visent à adapter la loi du 15 avril 1994 et n'appellent pas de commentaire particulier.	De artikelen 76 en 77 passen de wet van 15 april 1994 aan en behoeven geen verdere commentaar.
Section 2	Afdeling 2
<i>Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique</i>	<i>Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België</i>
Les articles 78 à 80 visent à adapter la loi du 22 février 1998 et n'appellent pas de commentaire particulier.	De artikelen 78 tot 80 passen de wet van 22 februari 1998 aan en behoeven geen verdere commentaar.
Section 3	Afdeling 3
<i>Modification de la loi du 2 août 2002 relative à</i>	<i>Wijziging van de wet van 2 augustus 2002</i>

<i>la surveillance du secteur financier et aux services financiers</i>	<i>betreffende het toezicht op de financiële sector en de financiële diensten</i>
L'article 81 vise à adapter la loi du 2 août 2002 et n'appelle pas de commentaire particulier.	Artikel 81 past de wet van 2 augustus 2002 aan en behoeft geen verdere commentaar.
Section 4	Afdeling 4
<i>Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges</i>	<i>Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector</i>
Les articles 82 et 83 visent à adapter la loi du 17 janvier 2003.	De artikelen 82 en 83 passen de wet van 17 januari 2003 aan.
Un des secteurs visés par la directive NIS 2 est le secteur des infrastructures numériques.	Een van de in de NIS 2-richtlijn bedoelde sectoren is de sector van de digitale infrastructuur.
Lors de la transposition de la directive NIS 2 en droit belge, il a été décidé que l'IBPT serait l'autorité sectorielle pour l'ensemble des entités de ce secteur, à l'exception des prestataires de services de confiance, pour lesquelles l'autorité sectorielle reste le ministre de l'Economie (et le SPF Economie par délégation).	Bij de omzetting van de NIS 2-richtlijn in Belgisch recht is beslist dat het BIPT de sectorale overheid zou zijn voor alle entiteiten van deze sector, met uitzondering van de verleners van vertrouwensdiensten, waarvoor de sectorale overheid de Minister van Economie blijft (en de FOD Economie bij delegatie).
Comme il a été considéré que les fournisseurs de services d'informatique en nuage (« cloud »), les fournisseurs de services de centres de données (« data center ») et les fournisseurs de réseaux de diffusion de contenu, qui sont des entités du secteur des infrastructures numériques, relèvent de la compétence du ministre qui a l'Economie dans ses attributions, ce dernier est impliqué pour ces entités de la manière suivante.	Aangezien werd geoordeeld dat de Minister van Economie bevoegd is voor de aanbieders van cloudcomputingdiensten ("cloud"), de aanbieders van datacentra ("data center") en de aanbieders van netwerken voor de levering van inhoud, die entiteiten zijn van de sector van de digitale infrastructuur, is genoemde minister betrokken bij deze entiteiten zoals hierna uiteengezet.
D'abord, ce ministre reste compétent pour la réglementation de ces entités.	In de eerste plaats blijft deze minister bevoegd voor de regelgeving wat deze entiteiten betreft.
Ensuite, ce ministre est aussi visé dans la loi relative au statut de l'IBPT. Ainsi, l'article 14 de cette loi prévoit que le ministre qui a l'Economie dans ses attributions peut demander un avis à l'IBPT, dans la limite de ses attributions.	Vervolgens wordt deze minister ook genoemd in de wet betreffende het statuut van het BIPT. Zo bepaalt artikel 14 van deze wet dat de Minister van Economie een advies kan vragen aan het BIPT, binnen de grenzen van zijn bevoegdheden.
L'article 19 de cette même loi prévoit que les décisions du Conseil sont notifiées aux	Artikel 19 van diezelfde wet bepaalt dat de beslissingen van de Raad worden meegedeeld

personnes directement et personnellement concernées, au ministre, ainsi qu'au ministre qui a l'Economie dans ses attributions, dans la limite de leurs attributions respectives.	aan de personen die rechtstreeks en persoonlijk betrokken zijn, aan de minister en aan de Minister van Economie, binnen de grenzen van hun respectievelijke bevoegdheden.
Section 5	Afdeling 5
<i>Modification de la loi du 13 juin 2005 relative aux communications électroniques</i>	<i>Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie</i>
Les articles 84 à 87 visent à adapter la loi du 13 juin 2005 et n'appellent pas de commentaire particulier	De artikelen 84 tot 87 passen de wet van 13 juni 2005 aan en behoeven geen verdere commentaar.
Section 5	Afdeling 5
<i>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</i>	<i>Wijzigingen van de wet van 21 november 2017 over de infrastructuur voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU</i>
Les articles 88 et 89 visent à adapter la loi du 21 novembre 2017 et n'appellent pas de commentaire particulier.	De artikelen 88 en 89 passen de wet van 21 november 2017 aan en behoeven geen verdere commentaar.
CHAPITRE 3	HOOFDSTUK 3
Disposition abrogatoire	Opheffingsbepaling
Article 90	Artikel 90
Cet article abroge 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, que le projet de loi vient remplacer.	Dit artikel voorziet in de opheffing 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, die door het wetsontwerp vervangen wordt.
CHAPITRE 4	HOOFDSTUK 4
Entrée en vigueur	Inwerkingtreding
Article 91	Artikel 91
Cet article fixe la date d'entrée en vigueur du projet de loi au 18 octobre 2024, conformément à l'article 41, § 1 ^{er} , alinéa 2, de la directive NIS2.	Dit artikel legt de datum van inwerkingtreding van het wetsontwerp vast op 18 oktober 2024, overeenkomstig artikel 41, § 1, tweede lid, van de NIS2-richtlijn.