Public consultation on the preliminary draft for the law establishing a framework for the cybersecurity of network and information systems of general interest for public security ("NIS2 law"), as well as on its draft implementing Royal Decree.

How to react to the present document?

Until the 21st of December 2023

With the reference "(Consult-2023-NIS2)"

Indicate the name of the legal entity or individual responding.

Answers are exclusively expected by electronic means at the following address: **nis@ccb.belgium.be**

Your comments should refer themselves to the articles, paragraphs, and/or sections they relate to.

The present public consultation is being conducted at the request of the Prime Minister. Accordingly, it should be noted that any information submitted in response to this consultation will be deemed to be intended directly for him and may be provided to him in full, in the state in which it was submitted, without further processing or verification.

Annex 1 : Preliminary draft for the law establishing a framework for the cybersecurity of network and information systems of general interest for public security (in French and Dutch).

Annex 2: Draft explanatory memorandum (in French and Dutch).

Annex 3: Draft implementing Royal Decree (in French and Dutch).

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 werkterrein 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 gespecifieerd 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 ses annexes et la taille de l'entité comme critères	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 binnen een van de bijlagen ervan en de omvang van de

pour déterminer si celle-ci entre ou non dans le champ d'application.	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 matière de la cybersécurité dans un domaine spécifique mais impose la prise de mesures minimales destinées à assurer un niveau élevé commun de	De inhoud van de richtlijn regelt de aangelegenheid cyberbeveiliging niet op een specifiek gebied, maar legt minimummaatregelen op voor een hoog

cybersécurité dans l'ensemble de l'Union pour certaines entités fournissant des services essentiels.	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 1er 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 infrastructuren 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 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	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 niveau voor bepaalde kritieke entiteiten is in de eerste plaats een middel om de bevolking en ondernemingen van ons land te beschermen. De

échanges économiques au sein du marché intérieur n'est qu'une conséquence indirecte de ces mesures de protection. (…)	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 1er	TITEL 1
Définitions et dispositions générales	*Definities en algemene bepalingen*
CHAPITRE 1er	HOOFDSTUK 1
Objet et champ d'application	**Onderwerp en toepassingsgebied**
Section 1ère	**Afdeling 1**
Objet	*Onderwerp*

Article 1er	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 1er 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 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	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 ondernemingen genieten. Meer bepaald kunnen de lidstaten rekening houden met het feit dat een entiteit onafhankelijk is van haar partnerondernemingen of verbonden

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 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 toezichthoudend 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 des droits de vote des actionnaires ou associés de celle-ci.	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 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 1er 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 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.	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 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 1er 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 1er).	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 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.	De bepaling verduidelijkt dat de wet geen afbreuk doet aan de toepassing van de AVG, 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.

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.	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 voortspruitende 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.
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.	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.
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 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.	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 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 l'électricité demeurent eux soumis à la présente loi.	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 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-	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

ci, comme le mentionne le considérant 8 de la directive.	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 1er « Définitions et dispositions générales », 2 « Autorités compétentes et coopération au niveau national », 6 « 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).	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 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 inclues 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 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.	Deze paragraaf bepaalt dat entiteiten die behoren tot de sectoren van het bankwezen en de infrastructuur voor de financiële markt die 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 1er dans le	Paragraaf 4 implementeert de in de eerste paragraaf bedoelde afwijking ook in het

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.	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 *de jure*, 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 *de jure* 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, § 1er, alinéa 1er, 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 ne pas exercer à titre principal ses activités dans le domaine de la sécurité nationale ou de la sécurité publique.	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 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 classiques.	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 "aanbestedende 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	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

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.	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'essentielles.	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) disparait 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 "digitaledienstverleners" (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'essentielles 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 ; 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 *infra*).	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 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 *infra*).

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 *infra*).	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 *infra*).
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 1er, 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 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.	Paragraaf 2 bepaalt dat de nationale cyberbeveiligingsautoriteit ook de overheidsinstanties van de deelgebieden identificeert die, na een risicobeoordeling, 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 concerné 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 betrekt 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 actualiseringen 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	De kennisgeving aan het Nationaal Crisiscentrum van de in dit artikel bedoelde identificaties en

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.	actualiseringen 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
Cette disposition prévoit que l'entité concernée doit transmettre toutes les informations utiles à son éventuelle identification, à la demande de l'autorité nationale de cybersécurité ou de l'autorité sectorielle lorsque cette dernière est à l'origine de la procédure.	Volgens deze bepaling moet de betrokken entiteit alle informatie bezorgen die nuttig is voor haar eventuele identificatie, op verzoek van de nationale cyberbeveiligingsautoriteit of de sectorale overheid indien die laatste aan de oorsprong van de procedure ligt.

CHAPITRE 5	HOOFDSTUK 5
Enregistrement des entités	**Registratie van de entiteiten**
Article 13	Artikel 13
Cet article organise l'enregistrement des entités essentielles et importantes auprès de l'autorité nationale de cybersécurité et détermine les informations qui doivent être renseignées par ces entités.	Dit artikel regelt de registratie bij de nationale cyberbeveiligingsautoriteit van essentiële en belangrijke entiteiten, en bepaalt welke informatie door deze entiteiten moet worden verstrekt.
Pour la première fois, cet enregistrement devra être effectué dans les cinq mois de l'entrée en vigueur du présent projet de loi. Ce délai se justifie en raison du délai imposé par la directive NIS2 à l'article 3, § 3 (le 17 avril 2025) . La fixation des modalités pratiques relatives à la communication de ces informations est confiée à l'autorité nationale de cybersécurité. Par rapport à ces modalités pratiques, on peut noter que la directive NIS2 précise que « les États membres devraient pouvoir mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes » et que, « lorsque des registres existent au niveau 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.	Deze registratie moet voor het eerst gebeuren binnen vijf maanden na de inwerkingtreding van dit wetsontwerp. Deze termijn wordt gerechtvaardigd door de termijn die is opgelegd in artikel 3, lid 3, van de NIS2-richtlijn (17 april 2025). Het vaststellen van de praktische modaliteiten voor het verstrekken van deze informatie wordt toevertrouwd aan de nationale cyberbeveiligingsautoriteit. Met betrekking tot deze praktische modaliteiten wordt opgemerkt dat de NIS2-richtlijn het volgende bepaalt: "*de lidstaten [moeten] nationale mechanismen kunnen instellen voor entiteiten om zich te registreren"* en "*indien er 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.

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. Ensuite, l'autorité sectorielle concernée communique les informations collectées à l'autorité nationale de cybersécurité. 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.	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. Vervolgens bezorgt de betrokken sectorale overheid de ingezamelde informatie aan de nationale cyberbeveiligingsautoriteit. 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	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

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.	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
Autorités compétentes et coopération au niveau national	*Bevoegde autoriteiten en samenwerking op nationaal niveau*
CHAPITRE 1ER	HOOFDSTUK 1
Autorités compétentes	**Bevoegde autoriteiten**
Section 1re	**Afdeling 1**

Désignation des autorités compétentes	*Aanwijzing van de bevoegde autoriteiten*
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 *infra*).	De rol en de taken van de nationale cyberbeveiligingsautoriteit worden beschreven in de volgende artikelen (zie *infra*).
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 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.	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 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	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

autorités compétentes dans le cadre de la directive NIS2 et de la directive CER devraient coopérer de manière étroite.	autoriteiten die in het kader van de NIS2-richtlijn en de CER-richtlijn bevoegd zijn, nauw moeten samenwerken.
Section 2	**Afdeling 2**
L'autorité nationale de cybersécurité	*De nationale cyberbeveiligingsautoriteit*
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 directive NIS2) ;	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 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,	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

l'autorité chargée de la gestion des incidents et crises de cybersécurité majeurs ;	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).
Sous-section 1re	*Onderafdeling 1*
Tâches relatives au rôle d'autorité compétente chargée de la cybersécurité	*Taken met betrekking tot de rol van bevoegde autoriteit belast met cyberbeveiliging*
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 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.	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 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	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

développera une connaissance spécifique aux différentes entités actives dans les secteurs visés par la loi.	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.
Sous-section 2	*Onderafdeling 2*
Tâches relatives au rôle de gestion des crises cyber	*Taken met betrekking tot het cybercrisisbeheer*
Article 18	Artikel 18
Cet article transpose l'article 9, § 1er 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 crises.	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 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.
Sous-section 3	*Onderafdeling 3*

Tâches et obligations relatives au rôle de CSIRT national	*Taken en voorschriften met betrekking tot de rol van nationaal CSIRT*
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 prioritiser 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 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.	Bij het niet-intrusief scannen van openbaar 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 informaticasystemen. 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, § 1er, 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.
L'article précise que le CSIRT national prendra toutes les mesures adéquates, proportionnelles et prudentes afin de réaliser ses missions légales. 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	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

judiciaire. Par ailleurs, les compétences du CSIRT national ne peuvent violer le secret de l'information ni le secret de l'instruction.	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.
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 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi 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).	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).
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 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.	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 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,	Aangezien deze incidenten essentiële spelers in sleutelsectoren, waaronder overheden, treffen,

ces incidents constituent des menaces graves pour la sécurité publique.	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 politionele 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 droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.	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 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 zwakheid, 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 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.	In bepaalde omstandigheden kunnen ethische hackers echter de rol van "digitale klokkenluider" vervullen voor kwetsbaarheden 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, § 1er 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 potentielle vulnérabilité.	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 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	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.

également communiquées dans un seul signalement.	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 site internet une liste indicative des techniques pouvant être considérées comme nécessaires et proportionnées.	Om ethische hackers bij deze evaluatie te helpen, zal het nationale CSIRT op zijn website een indicatieve lijst van technieken publiceren die als noodzakelijk en evenredig kunnen worden beschouwd.
Dans un tel cadre, peuvent être considérées notamment comme des actions nécessaires pour vérifier l'existence d'une vulnérabilité et pour la rapporter : - 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);	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: - - 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);

- 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.	- - 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 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.	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 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	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

réputation de l'organisation responsable et entamer la confiance des utilisateurs dans les technologies concernées.	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.

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. 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.	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. 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.
Section 2	**Afdeling 2**
Les éventuelles autorités sectorielles	*De eventuele sectorale overheden*
Article 24	Artikel 24
Cet article octroie des compétences aux éventuelles autorités sectorielles, en plus des tâches et compétences visées aux différents articles du présent projet de loi.	Dit artikel verleent bevoegdheden aan de eventuele sectorale overheden, naast de taken 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 1er 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 national, 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 1er. 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, *initio*, de la directive NIS2, selon lequel les autorités compétentes en vertu des directives 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 *de facto* des entités essentielles au sens du présent projet de loi.	Paragraaf 4 voorziet in de omzetting van artikel 13, lid 5, *initio*, van de NIS2-richtlijn, volgens hetwelke de autoriteiten die bevoegd zijn uit 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 *de facto* immers essentiële entiteiten zijn als bedoeld in dit wetsontwerp.
Le paragraphe 5 transpose l'article 13, § 5, *in fine*, 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	De paragraaf 5 voorziet in de omzetting van artikel 13, lid 5, *in fine*, 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

télécommunications échangent régulièrement des informations pertinentes.	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 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.	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, veiligheidsadviezen en de publiek gereguleerde 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 Contrôle, 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	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,

conformité ou à la supervision dans le cadre de la présente loi.	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 se fait au travers d'accords de partage d'informations en matière de cybersécurité.	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-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 « *prévoyant des objectifs stratégiques et des priorités dans le domaine de la cybersécurité et de la gouvernance pour les atteindre* » (directive NIS2, considérant 48).	De strategie bestaat uit een samenhangend kader "*met strategische doelstellingen en prioriteiten op het gebied van cyberbeveiliging en de governance om deze te verwezenlijken*" (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 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.	Paragraaf 1 bepaalt dat deze strategie wordt aangenomen bij de Ministerraad en minstens om de 5 jaar wordt bijgewerkt, na advies van de 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
Mesures de gestion des risques en matière de cybersécurité et obligations d'information	*Maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen*
CHAPITRE 1ER	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	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

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* ».	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 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* » (considérant 82, directive NIS2). Ces considérations, fondamentales dans l'évaluation des mesures à adopter, reprises dans l'article 21, § 1er, de la directive NIS2, sont transposées au sein du présent article.	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 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*" (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.
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.	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.
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.	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.
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.	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.
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, « *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*	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*

exploitant les vulnérabilités touchant les produits et les services de tiers » (considérant 85).	*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, § 1er, 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 1er 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 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).	Deze verplichting voor aanbieders van 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	Dit artikel voorziet in de omzetting van artikel 20 van de NIS2-richtlijn, volgens hetwelke de

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.	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, § 1er, 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 1er, 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 et pour les membres du personnel au service des personnes publiques.	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 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, § 1er, alinéa 1er, du présent projet de loi, évoqué *supra*.	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, § 1er, dispose que ce sont les entités qui prennent les mesures techniques, opérationnelles et organisationnelles. Le	Dat blijkt uit de NIS2-richtlijn. Artikel 21, lid 1, bepaalt dat de entiteiten technische, operationele en organisatorische maatregelen moeten nemen. Volgens

considérant 77 explique que, « *dans une large mesure, il incombe aux entités essentielles et importantes de garantir la sécurité des réseaux et des systèmes d'information* », le considérant 83 indique que « *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* » et le considérant 89 que « *les entités essentielles et importantes devraient adopter une vaste gamme de pratiques de cyberhygiène de base,* […] ».	overweging 77 ligt "*de verantwoordelijkheid voor het waarborgen van de beveiliging van netwerk- en informatiesystemen* […] *voor een groot deel bij de essentiële en belangrijke entiteiten*". Overweging 83 wijst erop dat "*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*" en overweging 89 voegt hieraan toe dat essentiële en belangrijke entiteiten "*een breed scala aan basispraktijken op het gebied van cyberhygiëne* [moeten] *toepassen,* […]".
L'objectif du présent article est d'expliciter cette responsabilité incombant aux entités essentielles et importantes, nonobstant l'application de l'article 31, § 1er, alinéa 1er.	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	Voor sommige (deel)sectoren kunnen, naargelang hun specifieke kenmerken,

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.	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 1re	**Afdeling 1**
Notification obligatoire	*Verplichte melding*
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, §§ 1er 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 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.	In de eerste plaats is het belangrijk te 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*	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*

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.	*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 à 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.	Significante 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 utiliser 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 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.	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 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 mogelijkerwijs 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 « *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* » (directive NIS2, considérant 101).	Onder significante incidenten moeten incidenten worden verstaan die "*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*" (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 de notification en fonction du degré d'impact ou d'urgence de l'incident.	Paragraaf 3 machtigt de Koning om, bij besluit vastgesteld na overleg in de Ministerraad en na de nodige raadplegingen, precieze meldingsdrempels te bepalen naargelang de impact of dringendheid van het incident.
La paragraphe 4 indique que la notification doit, le cas échéant, se fait 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 socialenetwerkdiensten).
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 *supra*, 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 24 heures lorsque l'incident a un impact sur la fourniture de leurs services de confiance ;	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 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 « *devrait inclure uniquement les informations nécessaires pour porter l'incident*	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 "*mag*

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 » (considérant 102, directive NIS2). Cette alerte 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 importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard* » (même considérant).	*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*" (overweging 102, NIS2-richtlijn). Deze waarschuwing mag "*de middelen van de meldende entiteit"* niet afleiden van "*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*" (dezelfde overweging).
La notification d'incident visée 2° (voir *supra*) 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 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.	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 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	Het voortgangsverslag bevat de informatie die in het eindverslag zou moeten staan, en waarover

l'entité au moment de la communication du rapport d'avancement.	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 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.	Bovendien moet het nationale CSIRT aanvullende technische ondersteuning verlenen 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 rechtshandhavingsinstanties.
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 communiquées.	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 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	In uitvoering van de NIS2-richtlijn moet de nationale cyberbeveiligingsautoriteit

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, § 1er, et à l'article 38, § 1er, du projet de loi, afin de les communiquer à l'ENISA tous les 3 mois.	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 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**
Notification volontaire	*Vrijwillige melding*
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 *doivent* être notifiés), les cybermenaces et les incidents évités.	In de eerste plaats kunnen essentiële en belangrijke entiteiten (niet significante) incidenten (significante incidenten *moeten* 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 *supra*. 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
Supervision et sanctions	*Toezicht en sancties*
CHAPITRE 1ER	HOODSTUK 1
Supervision	**Toezicht**
Section 1re	**Afdeling 1**
Evaluation périodique de la conformité	*Regelmatige conformiteitsbeoordeling*
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, of 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 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.	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, 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	Deze conformiteitsbeoordelingsinstantie moet essentiële entiteiten adequaat kunnen beoordelen op basis van door de Koning

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 agréation 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 1er, 1°. L'agréation permet également d'ajouter des conditions particulières, nécessaires pour la sécurité d'un ou plusieurs secteurs spécifiques.	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'agréation, 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, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui effectuerons 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.	Wanneer de conformiteitsbeoordeling betrekking heeft op kritieke entiteiten of overheidsinstanties, moeten de 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, § 1er, de la directive NIS2, ces entités ne sont soumises qu'à un contrôle *ex post* 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 1er, 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	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

lorsque ce dernier constate des manquements aux obligations créées par le présent projet de loi.	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**
Dispositions générales relatives au service d'inspection	*Algemene bepalingen betreffende de inspectiedienst*
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 « *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*. » (considérant 30, directive NIS2) et « *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*	Deze drie juridische teksten zijn nauw met elkaar verweven. Om die reden "*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.*" (overweging 30, NIS2-richtlijn) en "*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*

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] » (considérant 28, directive NIS2).	*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.*" (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, « *afin de garantir le respect par les entités des obligations qui leur incombent en vertu de la présente directive, les 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).	Volgens de NIS2-richtlijn moeten lidstaten "*om ervoor te zorgen dat entiteiten hun in deze richtlijn vastgelegde verplichtingen nakomen, (…) 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).
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 omzettingswet 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*	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."*

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).	(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 autorités belges doit se faire de manière proportionnée à leurs ressources et rentrer dans le cadre de leurs compétences.	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 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 échant, 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	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

d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt quelconque.	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**
La supervision des entités par le service d'inspection	*Het door de inspectiedienst uitgeoefende toezicht op de entiteiten*
Article 48	Article 48
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 judicaire. Ils ne peuvent faire usage de la contrainte à l'encontre des personnes contrôlées et ne peuvent, dès lors, forcer l'accès aux informations, *a fortiori* aux informations protégées par l'article 458 du Code pénal.	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, *a fortiori* tot de informatie die door artikel 458 van het Strafwetboek beschermd is.
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	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

qu'elles puissent mener à bien leurs tâches de contrôle et d'imposition de mesures administratives.	toezicht bevoegde autoriteiten met het oog op de uitvoering van hun toezichthoudende taken en het opleggen van administratieve maatregelen.
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 détermine la procédure et les éléments à fournir au juge d'instruction. Les autorités compétentes peuvent aussi 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.	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 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	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

l'Autorité de protection des données sans retard injustifié.	Gegevensbeschermingsautoriteit daarvan onverwijld in kennis stellen.
Pour finir, les contrôles auprès des entités importantes ne peuvent s'organiser que de manière *ex post*.	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 d'apporter son entière collaboration aux autorités compétentes pour le contrôle.	Dit artikel bepaalt dat de gecontroleerde 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 inexactes 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 1re	**Afdeling 1**
Procédure	*Procedure*

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 *supra* 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.	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

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.	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 après l'envoi du projet de décision.	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 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 *infra* 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	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

sanction par défaut. Une amende n'est infligée que lorsque cela est proportionné.	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 *infra*).	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 *infra*).
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 précédent.	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 vorige artikel.
Il est renvoyé *mutatis mutandis* 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 *mutatis mutandis* 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	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

présent article, par les articles 51, §§ 3 et 4, et 52, §§ 3 et 4, qui mettent en place le principe *audi alteram partem*.	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 *audi alteram partem* 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 autorités compétentes pour le contrôle ne peuvent plus imposer d'amendes pour les mêmes faits. Il s'agit là d'une application du principe *non bis in idem*.	Het artikel verduidelijkt bovendien dat, wanneer de Gegevensbeschermingsautoriteit een geldboete heeft opgelegd voor een of meer feiten, de voor het toezicht bevoegde autoriteiten geen geldboete kunnen opleggen voor dezelfde feiten. Het betreft hier een toepassing van het principe *non bis in idem*.
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.	Voornoemde 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	In geval van wanbetaling kan de voor de betaling bevoegde overheid een dwangbevel uitvaardigen via een wettelijke

de cette autorité ou d'un membre habilité à cette fin.	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 partir de la signification de la contrainte. En ce cas, les dispositions pertinentes du Code judiciaire sont applicables à ce délai.	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 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 *non bis in idem*, le paiement de l'amende administrative imposée	Teneinde het principe *non bis in idem* na te leven, doet de betaling van de administratieve

pour des faits précis éteint les possibilités de poursuites pénales pour ces mêmes faits.	geldboete die is opgelegd voor precieze feiten de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor dezelfde feiten.
Section 2	**Afdeling 2**
Mesures et amendes administratives	*Administratieve maatregelen en geldboetes*
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 1er, 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	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

à l'encontre d'une entité ne sont pas exécutées par l'entité dans le délai imparti.	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 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.	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 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
Dispositions spécifiques au secteur de l'administration publique	*Specifieke bepalingen voor de overheidssector*
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 1er, 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'agréation 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 autorité.	Zoals bepaald in paragraaf 3, wanneer een autoriteit is aangewezen als conformiteitsbeoordelingsinstantie voor overheidsinstanties, moeten deze instanties hun audits uitvoeren bij deze autoriteit.
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

Traitement des données à caractère personnel	*Verwerking van persoonsgegevens*
CHAPITRE 1er	HOODSTUK 1
Principes relatifs au traitement	**Beginselen 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 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.	Het gaat hier niet om een herhaling van de bepalingen van de AVG (wat verboden is omdat de AVG, als Europese verordening, rechtstreeks 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 traitées dans le cadre dudit contrôle. Cette période ne peut durer plus d'un an, deux en comptant les actes préparatoires.	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. 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 AVG en 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
Dispositions finales	*Slotbepalingen*
CHAPITRE 1er	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 1ère	**Afdeling 1**
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	*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*

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**
Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique	*Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België*
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**
Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	*Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten*
L'article 81 vise à adapter la loi du 2 aout 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**
Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	*Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector*
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,	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

relèvent de la compétence du ministre qui a l'Economie dans ses attributions, ce dernier est impliqué pour ces entités de la manière suivante.	digitale instrastructuur, 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 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.	Artikel 19 van diezelfde wet bepaalt dat de beslissingen van de Raad worden meegedeeld 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**
Modification de la loi du 13 juin 2005 relative aux communications électroniques	*Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie*
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**
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	*Wijzigingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU*
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	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

pour la sécurité publique, que le projet de loi vient remplacer.	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, § 1er, 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.