FEDERAL OVERSEAS SERVICES

KANSELARIJ VAN DE EERSTE MINISTER

[2024/202344]

APRIL 26, 2024. — Wet tot vaststelling van een kader voor de cyberbeveiliging van newerk- en informatiesystemen van alge-meen belang voor de openbare veiligheid (1)

FILIP, Koning der Belgen,

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

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij crash-free follow:

TITEL 1. — ***Definitions in algemene bepalingen***

HOOFDSTUK 1. — *Onderwerp en toepassingsgebied*

Afdeling 1. — Onderwerp

Item 1. Deze wet regelt in material bedoeld in item 74 van de Grondwet.

Art. 2. Deze wet voorziet met name in omzetting van de Europese Richtlijn (EU) 2022/2555 van the European Parliament on December 14, 2022 betreffende maatregelen voor een hoog gezamenlijk level van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 in Richtlijn (EU) 2018/1972 in tot trekking van Richtlijn (EU) 2016/1148. Deze richtlijn wordt hierna de ÿNIS2-richtlijnÿ genoemd.

Afdeling 2. — Toepassingsgebied

Art. 3. § 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 est deze wet van toepassing oppublike of private entities van een in bijlage I of II bedoelde soort die: 1o een middelgrote onderneming

zijn krachtens artikel 2 van de
bijlage bij Aanbeveling nr. 2003/361/EG; of

2o een onderneming die de ceilings overschrijdt zoals bepaald in
lid 1 of the following articles and of these articles.

Article 3, lid 4, van de bijlage bij Aanbeveling nr. 2003/361/EG does not allow your feet to pass wet. § 2. In het kader van

de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling nr. 2003/361/EG Houdt de nationale cyberbeveiliging-sautoriteit rekening met de mate van onafhankelijkheid van een entity ten opzichte van haar partnerondernemingen de verbonden onderne-mingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten in the course of which the services are released.

On the basis of this, the national cyber security authority is based on the fact that it is an entity that does not accept the wording and that it is middelgrote on the basis of which the article 2 is based on the Aanbeveling nr. 2003/361/EG, noch of ceilings for middelgrote onderneming als bepaald in lid 1 van dat article overschrijdt, indienne die entity, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt de niet zou worden geacht die Ceilings you overwrite it all by rekening the words you have written and this has happened.

De Koning kan de criteria bepalen op base waarvan de mate van onafhankelijkheid van een entity ten opzichte van haar partneronder-nemingen de verbonden ondernemingen wordt beoordeeld.

§ 3. On verminder article 6 is deze wet ook van epassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen: 1o de diensten worden verleend door:

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

(b) verleners van vertrouwensdiensten; *c)*

registers your top level domeinnamen in domeinnaamsysteem-dienstverleners;

2o de entity wordt geïdentificeerd als een essentiële of belangrijke entity overeenkomstig hoofdstuk 4 van deze titel; 3o of entity is

een overheidsinstantie: *a)* die van de Federale

Staat afhangt; *b)* die van deelgebieden afhangt,

geïdentificeerd overeenkomstig artikel 11, § 2; *c)* die een hulpverleningszone is in de zin van artikel 14

van de wet van 15 mei 2007 betreffende de civiele veiligheid de Brusselse

Hoofdstedelijke Services for Brandweer in Dringende Medische Hulp in de zin van de ordantie van 19 Juli 1990 houdende oprichting van

FEDERAL PUBLIC SERVICE

CHANCERY OF THE PRIME MINISTER

[2024/202344]

APRIL 26, 2024. — Law establishing a framework for the cybersecurity of networks and information systems of general interest for public security (1)

PHILIPPE, King of the Belgians,

To all, present and future, Greetings.

The House of Representatives has adopted and We sanction the following:

TITLE 1. — ***Definitions and general provisions*** CHAPTER

1. — *Purpose and scope of application*

Section 1. — Purpose

Article 1. This law regulates a matter referred to in Article 74 of the Constitution.

Art. 2. This law aims in particular to transpose European Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a

common high level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. This Directive is hereinafter referred to as the ÿNIS2 Directiveÿ.

Section 2. — Scope of application **Art.**

3. § 1. Within the limits of Article 4 and without prejudice to Article 6, this law applies to public or private entities of a type referred to in Annex I or II and which constitute: 1o a medium-sized enterprise under

Article 2 of the Annex to Recommendation No. 2003/361/EC; or 2o an enterprise which exceeds the ceilings provided for in

paragraph 1
from the same article of this annex.

Article 3, § 4, of the Annex to Recommendation No. 2003/361/EC does not apply for the purposes of this Act.

§ 2. In applying Article 6(2) of the Annex to Recommendation No 2003/361/EC, the national cybersecurity authority shall take into account the degree of independence enjoyed by an entity from its partners and affiliated undertakings, in particular with regard to the networks and information systems it uses to provide its services and with regard to the services it provides.

On the basis of paragraph 1, the national cybersecurity authority shall consider that such an entity does not constitute an average undertaking under Article 2 of the Annex to Recommendation No 2003/361/EC, or does not exceed the ceilings applicable to an average undertaking provided for in paragraph 1 of that Article, if, after taking into account the degree of independence of that entity, it would not have been considered as constituting an average undertaking or exceeding those ceilings if only its own data had been taken into account.

The King may determine the criteria on the basis of which the degree of independence enjoyed by an entity with respect to its partners and related companies is assessed.

§ 3. Without prejudice to Article 6, this Law also applies to entities of a type referred to in Annex I or II, regardless of their size, in one of the following cases: 1o the services are provided by: *a)* providers of

public electronic communications

networks or publicly available electronic communications services; *b)* trust service providers; *c)* top-level domain name registries and

domain name system service providers;

2o the entity is identified as an essential or important entity in accordance with Chapter 4 of this Title;

3. the entity is a public administration entity: *a)* which depends

on the federal State; *b)* which

depends on the federated entities, identified in accordance with Article 11, § 2;

(c) which is an emergency zone within the meaning of Article 14 of the Law of 15 May 2007 on civil security or the Fire and Emergency Medical Aid Service of the Brussels-Capital Region within the meaning of the Ordinance of 19 July 1990 establishing a Fire Service

de Bruxellese Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

§ 4. On the basis of article 6, it is already wet to pass through the site, it is important to note that the words identified by the operators of the infrastructure are wetted on July 1, 2011, and are therefore intended to be used in the future.

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

§ 6. In order to take into account possible sectoral overloading in the national cyberbeveiligingsauthority by Koning, it must be vastly extended by the Ministerraad, and the sectors in/of deelsectors may be taken into account by I of II of the best sectors in/of deelsectors which may be used.

Art. 4. § 1. Deze wet is before passing in article 3 bedoelde entiteiten die sevestigd zijn in België en die hun stensten verlenen of hun activiteiten verrichten in de Europese Unie. §2 .

2o DNS service providers, registers for top level data centers, full domain name registrations, data center service providers, data center service providers, data center service providers, data center service providers, network service providers, network providers Beveiligingsdiensten, alsook op aanbieders van onlinemarktplaatsen, onlinezoekmachines of platformen voor socialenetwerkdiensten, wanneer zij hun hoofdvesti-ging in België hebben, overeenkomstig de paragraphs 4 en 5.

§ 3. Indian entity bedoeld in paragraph 2, 2o , The European Union is not yet in possession of the European Union, but it may not be the same in the European Union. De vertegenwoodiger is gevestigd in een van de lidstaten waar de diensten worden verleend.

§ 4. You must pass through wet and dry conditions in paragraph 2, 2 and , 2 , you should be aware of the fact that you are in possession of cyber security risks.

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

Indian de plaats waar deze activiteiten plaatsvinden niet kan worden bepaald, worden de in paragraaf 2, 2o bedoelde entiteiten geacht hun hoofdvestiging en België te hebben wanneer hun vestiging met het grootste aantal werknemers zich daar bevindt. § 5. For the

passage of wet words in paragraph 2, 2o bedoelde entiteiten geacht hun , hoofdvestiging in België te hebben, wanneer zij niet gevestigd zijn in de Europese Unie maar hun diensten verlenen in de Unie en hun vertegenwoordiger in de Europese Unie in België gevestigd is. § 6. De aanwijzing van een

juridische stappen die bedoeld in paragraph 2, , 2o tegen de entity it zelf kunnen worden ingesteld.

Art. 5. § 1. Deze wet doet geen afbreuk aan de toepassing van Verordening (EU) 2016/679 van het European Parliament on April 27, 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die Please note that you are not allowed to do any trekking before Richtlijn 95/46/EG (algemene verordening gegevensbescherming), aan de wet-telijke en reglementaire bepalingen die deze verordening aanvullen de verduidelijken de anan de wet van 30 Juli 2018 betreffende de bescher-ming van natuurlijke personen met betrekking tot of verwerking van persoonsgegevens. Article 2 The electronics that are classified in electronics are subject to excessive humidity. § 3. Deze wet doet geen afbreuk aan de regels die van

toepassing zijn op nucleaire documenten in de zin van de wet van April 15, 1994 betreffende de bescherming van de volking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betref-fende het Federaal Agentschap for Nuclear Control.

and urgent medical aid from the Brussels-Capital Region.

§ 4. Without prejudice to Article 6, regardless of their size, this law applies to entities identified as operators of critical infrastructure within the meaning of the law of 1 July 2011 on the security and protection of critical infrastructure.

§ 5. Regardless of their size, this law applies to entities providing domain name registration services.

§ 6. After consultation with any relevant sectoral authorities and the national cybersecurity authority, the King may, by decree deliberated in the Council of Ministers, add other sectors and/or sub-sectors to Annex I or II or expand existing sectors and/or sub-sectors.

Art. 4. § 1. This law applies to the entities referred to in Article 3 which are established in Belgium and which provide their services or carry out their activities within the European Union.

§ 2. By way of exception to paragraph 1, this Act applies to: 1o

providers of public electronic communications networks or providers of publicly available electronic communications services, when they provide these services in Belgium; 2o providers of DNS services, top-level domain name

registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms, when they have their principal establishment in Belgium, in accordance with paragraphs 4 and 5. § 3. If an entity referred to in paragraph 2, 2o is not established in the European Union but provides services there, it shall appoint a representative in the Union. The representative shall be established in one of the

Member States ,

members where services are provided.

§ 4. For the application of this law, the entities referred to in paragraph 2, 2o have their principal establishment in Belgium when they mainly take decisions there relating to cybersecurity risk management measures.

If the place where these decisions are taken cannot be determined or is not located in the European Union, the entities referred to in paragraph‧2, 2o are deemed to have their principal establishment in Belgium when they carry out their cybersecurity operations there.

If the place where these operations are carried out cannot be determined, the entities referred to in paragraph 2, 2o are deemed to have their principal establishment in Belgium when their establishment with the largest number of

employees is located there. § 5. The entities referred to in paragraph 2, 2o are deemed to have their principal establishment in Belgium, for the application of this law, when they are not established in the European Union but provide their services in the Union and their representative in the European Union is

established in Belgium. § 6. The designation of a representative paragraph 2, 2o be , by an entity referred to in is without prejudice to legal acti brought against the entity itself.

Art. 5. § 1. This law does not prejudice the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), nor the legal and regulatory provisions which supplement or clarify said regulation, nor the law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

§ 2. This Act is without prejudice to the Act of 11 December 1998 on classification, security clearances, security certificates, security notices and regulated public service and does not apply to communication and information systems approved to use classified information in electronic form in accordance with the aforementioned Act. § 3. This Act is without prejudice to the rules applicable to nuclear documents, within the meaning of the Act of 15 April 1994 on the protection of the

population and the environment against the dangers resulting from ionising radiation and relating to the Federal Agency for Nuclear Control.

§ 4. Behoudens de artikelen 8 en 38 en titel 2 est deze wet niet van toepassing op: 1o de inlichtingen- en

veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 November 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten; 2o het Coördinatieorgaan voor dreigingsanalyse opgericht

bij artikel 5 van de wet van 10 Juli 2006 reffende de analysis van de reiging; 3o the Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot

bepaling van de algemene structure van le Ministerie van Landsverdediging en tot vaststelling van de voegdheden van bepaalde auriteiten; 4o de politiediensten en de algemene inspectie bedoeld in artikel 2, 2o en 3o van de wet van December 7, 1998 tot organization van een

,

integrated politics, structure and twee levels;

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

6o de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5o ; 7o de netwerk- en

informatiesystemen van Belgische diplomatieke en consulaire missies in landen buiten de Europese Unie; 8o de inrichtingen van

class I in de zin van artikel 3.1 van het koninklijk besluit van 20 Juli 2001 houdende algemeen reglement op de becherming van devolking, van de werknemers en leefmilieu tegen het gevaar van de ioniserende stralingen.

In the end, 8° is the wet part of the element of a nuclear installation best used by your industrial electrical product which is the source of your electrical transmission.

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

1o het NCCN;

2o de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16. § 6.

De paragrafen 4 en 5 zijn niet van toepassing wanneer een van Deze entities optreedt als verlener van vertrouwensdiensten.

Art. 6. § 1. Indian sectors specified by the European Union vereist dat entiteiten die tot het toepassingsgebied van deze wet behoren, maatregelen nemen voor het beheer van cyberbeveiligingsrisico's of significante incidenten melden en melden en indienne deze eisen ten minste gelijkwaardig zijn aan de in deze wet Be careful not to worry about it being wet or wet, nor to pass through other parts.

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

§ 2. De in paragraaf 1, eerste lid, bedoelde eisen worden geacht It should be noted that there are some spills when it is wet:

1o de maatregelen voor het beheer van cyberbeveiligingsrisico's ten minste gelijkwaardig zijn aan de maatregelen bedoeld in artikel 30; of 2o het sectors specifieke rechtsinstrument

van de Europese Unie in onmiddellijke toegang voorziet, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten voor national CSIRT en wanneer de eisen voor het melden van significante incidenten ten minste gelijkwaardig zijn aan de verplichtingen bedoeld in de article-len 34 to 37.

§ 3. De be palingen van de titels 3 tot tot 5 zijn niet van toepassing op entiteiten die behoren tot de sectoren van het bankwezen en de

infrastructure for financial markets in the future I die on the passage of the financial sector in the Verordening (EU) 2022/2554 in the European Parliament on December 14, 2022 to be digitally operational for the financial sector to be implemented by the Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 and (EU) 2016/1011, includes the activities of the Central Bank of Belgium.

§ 4. From title 3 to title 1, from title 4 to title 5 without passing:

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

§ 4. Subject to Articles 8 and 38 and Title 2, this law does not apply:

1o to the intelligence and security services referred to in Article 2 of the law of 30 November 1998 on the organization of intelligence and security services; 2o to the

Coordination Body for Threat Analysis created by Article 5 of the law of 10 July 2006 on threat analysis;

3o to the Ministry of Defence referred to in Article 1 of the Royal Decree of 2 December 2018 determining the general structure of the Ministry of Defense and establishing the powers of certain authorities;

4o to the police services and the general inspectorate referred to in Article 2, 2o and 3o of the law ,of 7 December 1998 organizing an integrated police service, structured at two levels;

5o to the judicial authorities, understood as the organs of the judicial power, including the public prosecutor; 6o to

the Federal Public Service Justice created by the Royal Decree of 23 May 2001 establishing the Federal Public Service Justice, when it manages databases for the judicial authorities referred to in 5o ;

7th to the networks and information systems of diplomatic missions and Belgian consular offices in countries outside the European Union;

8o to class I establishments within the meaning of article 3.1 of the decree Royal Decree of 20 July 2001 establishing general regulations for the protection of the population, workers and the environment against the danger of ionising radiation.

By way of derogation from paragraph 1, 8o, this law is applicable to the elements of a nuclear installation intended for the industrial production of electricity and which are used for the transport of electricity.

§ 5. The provisions of Title 3, Title 4 and Title 5 do not apply: 1o to the NCCN; 2o to the national cybersecurity

authority referred to in Article 16. § 6. Paragraphs 4 and 5 do not apply when

one of these entities act as a trusted service provider.

Art. 6. § 1. Where a sectoral legal instrument of the European Union requires entities falling within the scope of this Act to adopt cybersecurity risk management measures or to notify significant incidents and where such requirements have an effect at least equivalent to that of the obligations provided for in this Act, the relevant provisions of this Act shall not apply to such entities.

Where a sectoral legal instrument of the European Union referred to in paragraph 1 does not cover all entities in a specific sector falling within the scope of this Law, the relevant provisions of this Law shall apply to entities not covered by that sectoral legal instrument of the European Union.

§ 2. The requirements referred to in paragraph 1, subparagraph 1, are considered to have an effect equivalent to the obligations of this law when: 1o the cybersecurity risk

management measures have an effect at least equivalent to that of the measures referred to in Article 30; or 2o the sectoral legal instrument of the

European Union provides for immediate access, where appropriate automatic and direct, to incident notifications for the national CSIRT and when the requirements relating to the notification of significant incidents are at least equivalent to the obligations referred to in Articles 34 to 37.

§ 3. The provisions of Titles 3 to 5 do not apply to entities in the banking and financial market infrastructure sectors.

within the meaning of Annex I which fall within the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) No 2016/1011, including the activity of central securities depository carried out by the National Bank of Belgium.

§ 4. The provisions of Title 3, Chapter 1, Title 4 and Title 5 do not do not apply:

1o to the National Bank of Belgium, except for its activity

activiteit van central effectenbewaarinstelling waarop paragraaf 3 van toepassing is;

2. The financial institution of the Nationale Bank of Belgium has been canceled since *February* 22, 1998.

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

1o de gelijkwaardige sectorspecifieke rechtsinstrumenten bedoeld in article 6, § 1, eerste lid, nader bepalen; 2. There

are extensive rules and regulations that must be taken into account in the coordination of information technology, including information about significant incidents, which are included in article 6, § § 3 and 4, and are subject to national cyber security regulations. of authority belast met het beheer van cyberrisico's.

HOOFSTUK 2. — *Definitions* **Art. 8.**

To pass the toes with wet words, you should read:

1o ÿnetwerk- en informatiesysteemÿ: *a)*

een elektronische-communicatienetwerk in de zin van article 2, 3o van de , wet van 13 June 2005 betreffende de elektronische communicatie; *b)* .

controle op afstand de la verkrijgen van werkingsgegevens en real time mogelijk maken; of *c)* digitale gegevens die worden opgeslagen, verwerkt, opgehaald de verzonden met behulp van de in punten *a)* en *b)* bedoelde elementen met het oog op de working, het gebruik, de bescherming en het onderhoud ervan;

2o ÿbeveiliging the netwerk- en informatiesystemenÿ: the vermogen of the netwerk- en informatiesystemen om op een bepaald level van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticity, integriteit de vertrouwelijkheid van opgeslagen, verzonden de verwerkte access to the door of via two netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

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

4o ÿnational cyberbeveiligingsstrategieÿ: even if we change our strategies we prioritize them when it comes to cyber-beveiliging in governance and how we prioritize them in
België te verwezenlijken;

5o ÿincidentÿ: een gebeurtenis die de beschikbaarheid, authenticity, integriteit de vertrouwelijkheid van opgeslagen, verzonden de ver-werkte gegevens de van de diensten die worden aangeboden door de toegankelijk zijn via netwerk- en informatiesystemen, en gevaar brengt; 6o ÿbijna-incidentÿ:

een gebeurtenis die de beschikbaarheid, authen-ticiteit, integrity of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes est voorkomen de zich niet heeft voorgedaan; 7o ÿgrootschalig

cyberbeveiligingsincidentÿ: een incident dat leidt tot een verstoringslevel dat the groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie; 8o ÿincidental handlingÿ: all actions in

procedures that have occurred in the event of an incident; 9o ÿrisicoÿ: de mogelijkheid van verlies de verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van

een dergelijk verlies de een dergelijke verstoring en de waarschijn-lijkheid dat een dergelijk incident zich voordoet; 10o ÿcyberdreigingÿ: een cyberdreiging bedoeld in article 2, point 8), van de cyberbeveiligingsverordening;

central securities depository to which paragraph 3 applies;

2o to financial institutions subject to the supervision of the National Bank of Belgium under Articles 8 and *12bis* of the law of 22 February 1998 establishing the organic status of the National Bank of Belgium which do not fall under paragraph 3.

Art. 7. The King may, by decree deliberated in the Council of Ministers:

1o specify the equivalent sectoral legal instruments referred to in Article 6, § 1, first

paragraph ; 2o define specific rules relating to the coordination of the exchange of information, including requirements relating to the notification of significant incidents, between the entities referred to in Article 6, § § 3 and 4, the sectoral authority concerned, the national cybersecurity authority and the authority responsible for cyber risk managemer

CHAPTER 2. — *Definitions* **Art.**

8. For the purposes of this law, the following terms shall be understood to mean:

1o ÿnetwork and information systemÿ: *a)* an

electronic communications network within the meaning of Article 2, 3o of the Law of 13 June 2005 on electronic communications; *b)* any device or set of interconnected or related

devices, one or more elements of which ensure, in execution of a program, automated processing of digital data, including the digital, electronic or mechanical components of this device allowing in particular the automation of the operational process, remote control, or the obtaining of operating data in real time; or

(c) digital data stored, processed, retrieved or transmitted by the elements referred to in points *(a)* and *(b)* for the purpose of their operation, use, protection and maintenance;

2. ÿsecurity of networks and information systemsÿ: the ability of networks and information systems to withstand, at a given level of trust, any event likely to compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of the services that these networks and information systems offer or make accessible; 3. ÿcybersecurityÿ: cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the

European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification of information and communications technologies, and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation), hereinafter the ÿCybersecurity Regulationÿ; 4th “National Cybersecurity Strategy”: the coherent framework providing strategic objectives and priorities in the field of cybersecurity and governance

with a view to achieving them in

Belgium;

5o ÿincidentÿ: an event compromising the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of the services that information networks and systems offer or make accessible; 6o ÿmissed incidentÿ: an event which could have compromised the

availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of the services that information networks and systems offer or make accessible, but which could have been prevented or did not occur; 7o ÿmajor cybersecurity incidentÿ: an incident which causes disruptions beyond the response capabilities of the single Member State of the European Union

concerned or which has a significant impact on at least two Member States of the European Union;

8o ÿincident handlingÿ: all actions and procedures aimed at preventing, detecting, analysing, containing, responding to and remedying an incident; 9o ÿriskÿ: the

potential for loss or disruption following an incident, to be expressed as a combination of the magnitude of such loss or disruption and the probability of such an incident occurring; 10o ÿcyber threatÿ: a cyber threat as referred to in Article 2(8)

of the
cybersecurity regulation;

11o ÿsignificant cyber-dreigingÿ: cyber-dreiging waarvan op base van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit de gebruikers van de servicing van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

12o ÿICT-productÿ: een ICT-product als bedoeld in article 2, 12), van of cyberbeveiligingsverordening;

13o ÿICT-dienstÿ: een ICT-dienst als bedoeld in artikel 2, 13), van de cyber surveillance ordering;

14o ÿICT-procesÿ: een ICT-proces als bedoeld in article 2, 14), van de cyber surveillance ordering;

15o ÿkwetsbaarheidÿ: een zwakheid, vatbaarheid of gebrek van ICT-producen de ICT-diensten die een cyberdreiging kan worden uitgebuit; 16o ÿnormÿ:

een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 of the European Parliament on October 25, 2012 for European standardization, to be followed by the Richtlijnen 89/686/EEG in 93/15/EEG by the Raad also by the Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG of the European Parliament in de Raad, hierna ÿVerordening (EU) nr. 1025/2012ÿ;

17o ÿinternet connectionÿ: network connectivity is facilitated by more than one network (autonomous system) currently available, for which it is possible to connect the Internet to the Internet, which is all interconnected by your autonomous system and which does not exist on the internet network. If you have a deelnemende autonomous system, you can use the auto-noom system to open it, but you will have to use other systems; 18o ÿdomeinnaamsysteemÿ of ÿDNSÿ: een hierarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internet diensten en -bronnen te identificeren,

waardoor eindgebruikers appraten en staat worden gestureld routing- en connectivityitsdiensten op het internet te gebruiken om die they are in good condition;

19o ÿDNS-dienstverlenerÿ: een entity die de volgende diensten verleent:

a) openbare recursieve domeinnaamomzettingsdiensten voor internet users; of

b) .

20o ÿregister your topleveldomeinnamenÿ: a specific entity that is listed in the topleveldomeinnaam is authorized to be registered with the topleveldomeinnaam, and is included in the registration of the topleveldomeinnamen with the topleveldomeinnaam and the technical exploitation of the topleveldomeinnaam, puts in charge of exploitation of naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd de worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend your eigen gebruik worden aangewend door een register;

21o ÿentiteit die domeinnaamregistratiediensten aanbiedtÿ: een regis-trator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

22o ÿdigital servicesÿ: een services in de zin van article 1, lid 1, point *b),* van Richtlijn (EU) 2015/1535 van het European Parliament in de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regulations betreffende de services van de informatiemaatschappij;

23o ÿvertrouwensdienstÿ: een vertrouwensdienst in de zin van article 3, 16, van Verordening (EU) nr. 910/2014 of the European Parliament in the European Parliament on July 23, 2014 for electronic identification in the form of electronic transactions in the internal market in accordance with Richtlijn 1999/93/EG, hierna de ÿeIDAS-verordeningÿ genoemd;

24o ÿverlener van vertrouwensdienstenÿ: een verlener van vertrou-wensdiensten in de zin van artikel 3, 19, van de eIDAS-verordening; 25o ÿgekwalificeerde vertrouwensdienstÿ: een gekwalificeerde vert-rouwensdienst in de zin van artikel 3, 17, van de eIDAS-verordening;

11o ÿsignificant cyber threatÿ: a cyber threat which, given its technical characteristics, may be considered likely to have a serious impact on the networks and information systems of an entity or the users of the entity's services, causing considerable material, bodily or moral damage; 12o ÿICT productÿ: an ICT product within the meaning of Article 2,

12), of the cybersecurity regulation;

13o ÿICT serviceÿ: an ICT service within the meaning of Article 2, 13), of the cybersecurity regulation;

14o ÿICT processÿ: an ICT process within the meaning of Article 2, 14), of the cybersecurity regulation;

15o “vulnerability”: a weakness, susceptibility or flaw in products ICT or ICT services that can be exploited by a cyber threat;

16o ÿstandardÿ: a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Directives 89/686/EEC and 93/15/EEC of the Council and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council hereinafter ÿRegulation (EU) No 1025/2012ÿ;

17o ÿInternet exchange pointÿ: a network structure that allows the interconnection of more than two independent networks (Autonomous Systems), primarily for the purpose of facilitating the exchange of Internet traffic, that provides interconnection only for Autonomous Systems and that does not require Internet traffic passing between any pair of participating Autonomous Systems to transit a third Autonomous System, nor does it otherwise modify or alter such traffic;

18o ÿDomain Name Systemÿ or ÿDNSÿ: a hierarchical and distributed naming system that enables the identification of Internet services and resources, thereby enabling the use of Internet routing and connectivity services by end-user devices to access those services and resources; 19o ÿDNS service providerÿ: an entity that provides:

(a) accessible recursive domain name resolution services public information intended for Internet end users; or

(b) authoritative domain name resolution services for use by third parties, with the exception of root name servers; 20o ÿtop-level domain name registryÿ: an entity to which a specific top-level domain has been delegated and which is responsible for the administration of the top-level domain, including the registration of domain names under the top-level domain and the technical operation of the top-level domain, including the operation of its name servers, the maintenance of its databases and the distribution of the top-level domain's zone files on the name servers, whether these operations are carried out by the entity itself or are subcontracted, but excluding situations where top-level domain names are used by a registry solely for its own use;

21o ÿentity providing domain name registration servicesÿ: a registrar or an agent acting on behalf of registrars, such as a provider or reseller of anonymization or proxy registration services;

22o ÿdigital serviceÿ: a service within the meaning of Article 1, paragraph 1, point *(b),* of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services;

23o ÿtrust serviceÿ: a trust service within the meaning of Article 3, 16, of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter the ÿeIDAS Regulationÿ; 24o ÿtrust service providerÿ: a service provider trusted within the meaning of Article 3, 19, of the eIDAS Regulation;

25o ÿqualified trust serviceÿ: a qualified trust service at meaning of Article 3, 17, of the eIDAS Regulation;

26o ÿgekwalificeerde verlener van vertrouwensdienstenÿ: een gekwalificeerde verlener van vertrouwensdiensten in de zin van artikel 3, 20, van de eIDAS-verordening;

27o ÿonlinemarktplaatsÿ: een onlinemarktplaats in de zin van arti-kel I.8, 41o van het Wetboek van economisch recht;

28o ÿonlinezoekmachineÿ: een onlinezoekmachine als bedoeld in articles 2, 5), van Verordening (EU) 2019/1150 van het Europees Parliament in de Raad on June 20, 2019 ter bevordering van billijkheid en transparent voor zakelijke gebruikers van onlinetussenhandels-diensten;

29o ÿcloudcomputing servicesÿ: digital services of the administration are in full swing and are supported by the elastische pool of the computer network at the moment, and they also want to pay over all locations to be paid for;

30o ÿdata center serviceÿ: the structure of the network is best served by the centralized accommo-date, interconnection and exploitation by IT- and netwerkapparatuur die support op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met facilitates energy distribution and control infrastructure;

31o ÿnetwerk for inhoud controlÿ: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaar-heid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

32o ÿplatform for social network servicesÿ: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video's en aanbevelingen;

33o ÿvertegenwoordigerÿ: een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om opt te treden names een DNS-dienstverlener, een register voor topleveldo-meinnamen, een entity it domeinnaamregistratiediensten verleent, een Aanbieder van cloudcomputing diensten, een aanbieder van data-center diensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, een aanbieder van een onlinemarkt-plaats, van een onlinezoekmachine van een platform your social network services do not exist in the United Europe, in the national cyber-beveiling authority you can contact people in places where they do not need to be trekked until they are wet;

34o ÿoverheidsinstantieÿ: een administratieve overheid bedoeld in Article 14, § 1, hereinafter referred to as Article 14, § 1. State die aan de volgende criteria voldoet:

(a) zij is neither industrial nor commercial; *b)* .

bijlagen;

c) zij is a private legal entity. 35o ÿopenbaar electronic-communicatienetwerkÿ: een openbaar electronic communication network is available in article 2, 10 o , van de wet from June 13, 2005 to be used in electronic communication;

36o ÿelectronische-communicatiedienstÿ: een elektronische-van de wet van communicatiedienst in de zin van article 2, 5o june 13, , 2005 betreffende de elektronische communicatie;

37o ÿentityÿ: een natuurlijke de rechtspersoon die als zodanig est opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

38o ÿaanbieder van beheerde dienstenÿ: een entity diensten verleent die verband houden met de installation, het beheer, de exploitation of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesyste-men, via bijstand of activity administratie bij de klanten ter plaatse de op afstand;

39o ÿaanbieder van beheerde beheerde dienstenÿ: een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;

26o “qualified trust service provider”: a qualified trust service provider within the meaning of Article 3, 20, of the eIDAS Regulation;

27o ÿonline marketplaceÿ: an online marketplace within the meaning of the Code of of Article I.8, 41o , Economic Law; 28o ÿonline search engineÿ: an online search engine within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 promoting fairness and transparency for businesses using online intermediation services;

29o ÿcloud computing serviceÿ: a digital service that enables on-demand administration and broad remote access to a modular and variable set of computing resources that can be shared, including when these resources are distributed across different locations;

30o ÿdata center serviceÿ: a service that encompasses structures, or groups of structures, dedicated to the centralized hosting, interconnection and operation of computer and network equipment providing data storage, processing and transport services, as well as all electricity distribution and environmental control facilities and infrastructure; 31o ÿcontent delivery networkÿ: a network of geographically distributed servers designed to ensure high availability, accessibility or rapid delivery of digital content and services to Internet users on behalf of content and service providers;

32o ÿsocial networking services platformÿ: a platform that allows end users to connect, share, discover and communicate with each other across multiple devices, including through online conversations, posts, videos and recommendations;

33o ÿrepresentativeÿ: a natural or legal person established in the European Union who is expressly designated to act on behalf of a DNS service provider, a top-level domain name registry, an entity providing domain name registration services, a cloud computing provider, a data center service provider, a content delivery network provider, a managed service provider, a managed security service provider or a provider of online marketplaces, online search engines or social networking service platforms not established in the European Union, who may be contacted by the national cybersecurity authority in place of the entity itself regarding the obligations incumbent on that entity under this Law; 34o ÿpublic administration entityÿ: an administrative authority referred to in Article 14, § 1, paragraph 1, of the coordinated laws on the Council of State which meets the following criteria: *a)* it is not of an industrial or commercial nature; *b)* it does not carry out as its principal activity an activity listed in the entity type column of another sector or sub-sector of one of the annexes to the law;

(c) it is not a legal entity under private law. 35o ÿpublic electronic communications networkÿ: a network of the public electronic communications within the meaning of Article 2, , 10th law of June 13, 2005 relating to electronic communications;

36o ÿelectronic communications serviceÿ: an electronic communications service of electronic communications within the meaning of Article , the law of 2, 5o of June 13, 2005 relating to electronic communications;

37o ÿentityÿ: a natural or legal person constituted and recognized as such under the national law of its place of incorporation, and having, in its own name, the capacity to hold rights and obligations; 38o ÿmanaged service providerÿ: an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure or applications or other information networks and systems, through active assistance or administration, either at customers' premises or remotely;

39o ÿmanaged security services providerÿ: a managed services provider that performs or provides assistance for activities related to cybersecurity risk management;

40o ÿonderzoeksorganisatieÿ: een entity die als hoofddoel heeft het verrichten van toegepast onderzoek de experimentele ontwikkeling met het op de exploitation van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;

41o ÿAanbeveling nr. 2003/361/EGÿ: de Aanbeveling van de Com-missie van 6 mei 2003 betreffende definitie van kleine, middelgrote en micro-ondernemingen; 42o ÿwet

van 13 juni 2005ÿ: de wet van 13 juni 2005 betreffende de electronic communications;

43o ÿwet van 1 juli 2011ÿ: de wet van 1 juli 2011 betreffende de be aware of the need for infrastructure infrastructure;

44o ÿkoninklijk was on April 18, 1988ÿ: het koninklijk was on April 18, 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering; 45o ÿnationale

cyberbeveiligingsautoriteitÿ: de authoriteit bedoeld in article 16; 46o ÿnational CSIRTÿ:

het nationale computer security incident response team; 47o ÿEnisaÿ: het Agentschap van

de Europese Unie voor cyberbevei-liging opgericht jj de cyberbeveiligingsverordening; 48o ÿNCCNÿ: the Centrum

opened on April 18, 1988; 49o ÿVerordening (EU) 2016/679ÿ: Verordening (EU) 2016/679

of the European Parliament on April 27, 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gege-vens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

50o ÿgegevensbeschermingsautoriteitÿ: toezichthoudende auriteit in de zin van artikel 4, 21o van Verordening (EU) 2016/679; 51o ÿnationale

accreditatie-instantieÿ: de instantie bedoeld in article 2, point 11, van Verordening (EG) nr. 765/2008 of the European Parliament on July 9, 2008, the vast majority of its publications have been accredited in the market and have been transferred to the production and training of Verordening (EEG) nr. 339/93, hierna ÿVerordening (EG) nr. 765/2008ÿ;

52o ÿbeveiligingsbeleid voor de netwerk- en informatiesystemen (ÿIBBÿ)ÿ: het beleid vastgelegd in een document bedoeld in article 30, but de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen door een essentiële of belangrijke entity;

53o ÿconformiteitsbeoordelingsinstantieÿ: de instantie bedoeld in article 2, point 13, van Verordening (EG) nr. 765/2008;

54o ÿsectoral overheidÿ: de overheid bedoeld in article 15, § 2; 55o

ÿCSIRT-netwerkÿ: the network of national CSIRT's operating bij article 15 from NIS2-richtlijn; 56o

ÿsamenwerkingsgroepÿ: of samenwerkingsgroep opgericht bij article 14 from NIS2-richtlijn;

57o ÿsignificant incidentÿ: a significant incident occurred when the sector of deelsectors was transferred to the bank I and II was transferred to the following: 1o een ernstige operationele verstoring van een de servicio

in de sectoren of deelsectoren van de bijlagen I en II of financial transactions your betrokken entity heeft veroorzaakt of kan veroorzaken; of

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

58o ÿcybercrisisÿ: elk cyberbeveiligingsincident dat wegens zijn aard de gevolgen: 1o

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

2o een dringende besluitvorming vereist; 3o en de

gecoördineerde inzet van verscheidene departementen en organismen vergt. 59o ÿInstituutÿ: the Belgian

Institute for post-diensten en telecom-municatie zoals bedoeld in article 13 van de wet van 17 Januari 2003 met betrekking tot het statutut van de regulator van de Belgische post-en telecommunicatiesector.

HOOFSTUK 3. — *Categories of entities* **Art. 9.**

Essential items: 1 item of items in

the item 2, lid 1, item 1, item 1, item 1, item 1, item 1, item 2, item 1, item 1 2003/361/EG;

40o ÿresearch organizationÿ: an entity whose primary objective is to carry out applied research or experimental development activities with a view to exploiting the results of this research for commercial purposes, excluding educational establishments;

41st ÿrecommendation no 2003/361/ECÿ: the Recommendation of the Commission of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;

42o ÿlaw of 13 June 2005ÿ: the law of 13 June 2005 relating to electronic communications;

43o ÿLaw of 1 July 2011ÿ: the law of 1 July 2011 relating to the security and protection of critical infrastructures; 44o ÿRoyal Decree of

18 April 1988ÿ: the Royal Decree of 18 April 1988 establishing the Governmental Centre for Coordination and Crisis;

45o “national cybersecurity authority”: the authority referred to in Article 16;

46th “National CSIRT”: the National Incident Response Center computer security;

47o ÿENISAÿ: the European Union Agency for Cybersecurity established by the Cybersecurity Regulation; 48o ÿNCCNÿ: the

Centre established by the Royal Decree of 18 April 1988;

49o ÿRegulation (EU) 2016/679ÿ: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); 50o ÿData Protection Authorityÿ: Supervisory Authority within

the meaning of Regulation (EU) 2016/679; 51o ÿnational accreditation bodyÿ: of article 4, 21o , the body referred to in Article 2,

point 11, of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Council Regulation (EEC) No 339/93, hereinafter ÿRegulation (EC) No 765/2008ÿ; 52o ÿsecurity policy for information systems and networks (ÿPSIÿ)ÿ: the policy recorded in a document referred to in Article

30, setting out the security measures for networks and information systems to be adopted by an essential or important entity;

53o ÿconformity assessment bodyÿ: the body referred to in Article 2, point 13, of Regulation (EC) No 765/2008;

54o “sectoral authority”: the authority referred to in Article 15, § 2;

55o “CSIRT network”: the network of national CSIRTs established by Article 15 of the NIS2 Directive;

56o ÿcooperation groupÿ: the cooperation group established by Article 14 of the NIS2 Directive;

57o ÿsignificant incidentÿ: any incident having a significant impact on the provision of one of the services provided in the sectors or

sub-sectors listed in Annex I and II of the law and which:

1o has caused or is likely to cause serious operational disruption of one of the services provided in the sectors or sub-sectors listed in Annex I and II or financial losses for the entity concerned; or

2o has affected or is likely to affect other natural or legal persons by causing considerable material, bodily or moral damage.

58o ÿcyber crisisÿ: any cybersecurity incident which, by its nature or consequences: 1o

threatens the vital interests of the country or the essential needs of the population;

2o requires urgent decisions; 3o

requires coordinated action by several departments and organizations. 59o ÿInstituteÿ: the

Belgian Institute for Postal Services and Telecommunications as referred to in Article 13 of the Law of 17 January 2003 on the status of the regulator of the Belgian postal and telecommunications sectors.

CHAPTER 3. — *Categories of entities*

Art. 9. Essential entities are: 1. entities of a

type referred to in Annex I which exceed the ceilings applicable to medium-sized enterprises provided for in Article 2, paragraph 1, of the Annex to Recommendation No. 2003/361/EC;

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

3o de aanbieders van openbare elektronische-communicatienetwerken uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG;

4o of overheids instanties die van de Federale Staat affhangen;

5o of entities listed in article 3, § 4; 6o alle andere

entiteiten van een in bijlage I of II bedoelde soort die worden geïdentificeerd als essentialiële entiteiten overeenkomstig arti-kel 11.

Art. 10. Zijn belangrijke entiteiten: 1o de

entiteiten van een in bijlage I of II bedoelde soort die niet als
Essentially these words should be used on the basis of article 9;

2o de entiteiten die worden geïïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.

HOOFSTUK 4. — *Identification* **Art. 11.**

§ 1. Onverminderd article 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief de op voorstel van de eventuale betrokken sectorale overheid, een entity als een een essentiële of belangrijke entity, ongeacht haar omvang, en de volgende gevallen:

1o de entiteit est de enige aanbieder, en België, van minstens één dienst die essentieel est voor de instandhouding van kritieke maatschappelijke de economic activiteiten, met name in een van de sectorsen deelsectoren van de bijlagen I en II van de wet; 2o een verstoring van de door de entity verleende dienst kan

aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging de volksgezondheid;

3. If you change the door of your entity, you will have to deal with the impact of the system;

4o de entity is kritiek vanwege het specifieke belang ervan op nationalaal of regionalaal level your de specifieke sector of het specifieke type dienst, of your andere onderling afhankelijke sectoren in België.

§ 2. Wat betreft de entititeiten die van deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstan-ties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschap-pelijke de economische activity.

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

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

In general, there are some advices about sectoral overheid in the Indian national cyberbelieving authority which have to do with your handhaven, the same word of advice is given to you by the Strategic Committee of the Inlichtingen in Veiligheid, you can choose the right one for 22 December 2020 to be completed by the National Veiligheidsraad, the Strategic Committee of the Veiligheid and the Coördinatiecomité of the Veiligheid die and bindend advices uitbrengen.

§ 4. De nationale cyberbeveiligingsautoriteit evaluert en actuali-seert, in voorkomend geval, minstens om de twee jaar de identificatie van essential en belangrijke entiteiten volgens de modaliteiten bedoeld in de paragraphs 1 tot 3.

National Cyber Security Authority identifies and updates the essential entities of the NCCN and possible sectoral changes.

The National Cyber Security Authority identifies and updates its entities in the event of a possible sectoral authority.

§ 5. In this case, in paragraph 1 of the Koning, there is a vast influence in the Ministerraad, and an entity that is in its original sector, which is an essential part of the legal entity.

2o qualified trust service providers and top-level domain name registries and DNS service providers, regardless of their size; 3o providers of public electronic communications networks or publicly available electronic

communications services which are at least medium-sized enterprises, pursuant to Article 2 of the Annex to Recommendation No 2003/361/EC;

4o public administration entities which depend on the federal State; 5o the entities referred

to in Article 3, § 4; 6o any other entity of a type

referred to in Annex I or II which is identified as an essential entity in accordance with Article 11.

Art. 10. Significant entities are: 1o entities of a

type referred to in Annex I or II which are not
qualified as essential entities on the basis of Article 9;

2o entities identified as significant entities in accordance with Article 11.

CHAPTER 4. — *Identification* **Art. 11.**

§ 1. Without prejudice to Article 6, on its own initiative or on the proposal of the relevant sectoral authority, the national cybersecurity authority shall identify an entity as an essential or important entity, regardless of its size, in the following cases:

1o the entity is the sole provider, in Belgium, of at least one service essential to the maintenance of critical societal or economic activities, in particular in one of the sectors or sub-sectors listed in Annexes I and II of the law;

2o a disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; 3o a disruption of the service provided by the entity could

induce a significant systemic risk, in particular for sectors where such an interruption could have a cross-border impact;

4o the entity is critical because of its specific importance at national or regional level for the sector or type of service in question, or for other interdependent sectors, in Belgium.

§ 2. With regard to entities that depend on federated entities, the national cybersecurity authority identifies public administrations which, following a risk-based assessment, provide services whose disruption could have a significant impact on critical societal or economic activities. § 3. As part of the identification referred to in paragraphs 1 and 2, the national cybersecurity authority first submits a draft decision to the entity

concerned and then to any federated entities concerned and sectoral authorities, which issue an unpublished opinion within sixty days.

In the absence of an opinion given within the period referred to in paragraph 1, it may to have ignored the absence of notice.

In the event of an unfavorable opinion from a sectoral authority and if the authority

National Cybersecurity Authority wishes to maintain its draft decision, the draft decision, accompanied by the opinion, is submitted to the Strategic Intelligence and Security Committee, created by the Royal Decree of 22 December 2020 establishing the National Security Council, the Strategic Intelligence and Security Committee and the Intelligence and Security Coordination Committee, which issues a binding opinion. § 4. The National Cybersecurity Authority assesses and, where appropriate, updates the identification of essential and important entities at least every two years,

in accordance with the procedures referred to in paragraphs 1 to 3.

The National Cybersecurity Authority sends the identifications and updates of essential entities to the NCCN and to the relevant sectoral authority, if any.

The national cybersecurity authority sends the identifications and updates of important entities to the relevant sectoral authority, if any.

§ 5. In the cases referred to in paragraph 1, the King may, by decree deliberated in the Council of Ministers, designate as an essential or important entity an entity which is not part of the sectors referred to in
annex.

Art. 12. In the case of identification in this article 11, the information is subject to your possible identification.

HOOFSTUK 5. — *Registration of entities* **Art. 13.** § 1.

Binnen vijf maanden na de inwerkingtreding van de wet of de in item 11 bedoelde identificatie registreren enssentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zich bij de nationale cyberbeveiligingsautoriteit volgens de door deze auriteit Extensive practical methods relating to computer operations:

1o hun naam, also ok hun registratienummer bij de Kruispuntbank van Ondernemingen (KBO) of een gelijkwaardige registratie in de
United Europe;

2o your addresses in your current contact details, address your e-mail addresses, your IP address in your telephone number;

3o indian van toepassing, of relevant sector in deelsector bedoeld in bijlage I of II, in

4o indian van toepassing, een lijst van de lidstaten waar zij diensten
Verlenen die binnen het passingsgebied van deze wet vallen.

De Koning kan deze lijst met informatie aanvullen. §2. sectoral

overheid.

From Paragraph 1, please refer to the article below, which means that your computer is subject to a wide range of practical methods.

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

§ 4. De betrokken sectorale overheid bezorgt de krachtens de paragraphs 2 en 3 verzamelde informatie aan de nationale cyberbevei-ligingsautoriteit.

National cyber security authorities do not need to be authorized to do so in any sector where they are subject to change.

Art. 14. § 1. Binnen twee maanden na de inwerkingtreding van de wet verstrekken DNS-dienstverleners, registers voor topleveldomeinname, entitiiteiten die domeinnaamregistratiediensten verlenen, anbieders van cloudcomputingdiensten, ananbieders van datacentrumdiensten, ananbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van online marktplaatsen, van onlinezoekmachines en van platforms voor sociale netwerkdiensten de nationale cyberbe-veiligingsautoriteit volgens de modaliteiten bedoeld in artikel 13, § 1, eerste lid, ten minste of following information:

1o hun naam; 2o

hun relevante sector, deelector en soort entiteit bedoeld in bijlage I of II, waar van toepassing; 3o het adres van hun

hoofdvestiging en hun andere wettelijke vestigingen in de Unie de, indienne deze niet in de Unie zijn gevestigd, van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger; 4o current contact information, including e-mail address in telephone numbers in, indian

text message, deze van hun op grond van artikel 4, § 3, aangewezen vertegenwoordiger;

5o de lidstaten waar ze hun diensten verlenen die tot het passings-
gebied van deze wet behoren; in 6o hun
IP-bereiken.

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

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

Art. 12. As part of the identification referred to in Article 11, the entity concerned shall transmit all information useful for its possible identification, at the request of the national cybersecurity authority or the sectoral authority.

CHAPTER 5. — *Registration of entities* **Art. 13.** § 1.

Within five months of the entry into force of the law or the identification referred to in Article 11, essential entities, important entities and entities providing domain name registration services shall register with the national cybersecurity authority in accordance with the practical arrangements set by that authority and shall provide it with the following information:

1o their name and their registration number with the Crossroads Bank for Enterprises (CBE) or an equivalent registration in the European Union; 2o their updated address and contact details, including their email address, IP

ranges and telephone number; 3o where applicable, the sector and subsector concerned referred to in Annex I or II; and 4o where applicable, a list of the Member States in which they provide

services falling within the scope of this Law.

The King may supplement this list of information. § 2. By way

of derogation from paragraph 1, subparagraph 1, where the entity referred to in the aforementioned paragraph already communicates to the relevant sectoral authority some of the information referred to in the aforementioned paragraph, by virtue of a legal obligation, the entity shall supplement this information with that sectoral authority.

The entity referred to in paragraph 1, subparagraph 1, shall communicate the information within five months of the entry into force of the law, in accordance with the practical arrangements set by the

aforementioned authority. § 3. The entities referred to in paragraph 1, subparagraph 1, shall communicate without delay any changes to the information they have communicated in accordance with paragraph 1, subparagraph 1, and paragraph 2, subparagraph 1, and, in any event, within two weeks of the date of the change. § 4.

The sectoral authority concerned shall communicate the information collected under paragraphs 2 and 3 to the national cybersecurity authority.

The national cybersecurity authority takes the necessary measures to ensure that sectoral authorities can consult the data communicated for the sectors that concern them.

Art. 14. § 1. Within two months of the entry into force of the law, DNS service providers, top-level domain name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms shall provide the national cybersecurity authority, in accordance with the procedures referred to in Article 13, § 1, paragraph 1, at least the following information:

1o their

name; 2o their sector, sub-sector and type of entity concerned, referred to in Annex I or II, as applicable;

3o the address of their principal establishment and of their other legal establishments in the Union or, if they are not established in the Union, of their representative designated in accordance with Article 4, § 3; 4o their updated contact details, including email addresses

and telephone numbers and, where applicable, those of their representative designated in accordance with Article 4, § 3;

5o the Member States in which they provide their services falling within the scope of this law; and

6o their IP ranges. § 2.

The entities referred to in paragraph 1 shall notify the national cybersecurity authority of any change to the information they have communicated under paragraph 1 without delay and, in any event, within three months of the date of the change.

§ 3. By way of derogation from paragraph 1, the data referred to in the same paragraph, relating to qualified trust service providers in Belgium, which have already been communicated to the supervisory body concerned

For eIDAS-verordening bedoelde toezichthoudende organaan, door dat orgaan doorsgestuurd naar de nationale cyberbeveiligingsautoriteit, volgens de door de Koning vastgestelde modaliteiten.

TITLE 2. — ***Bevoegde auriteiten en samenwerking op nationale level***

HOOFDSTUK 1. — *Bevoegde auriteiten*

Afdeling 1. — Aanwijzing van de voegde auriteiten **Art. 15.**

§ 1. De Koning wijst de nationale cyberbeveiligingsautoriteit
a year.

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

In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van den het kader van de wet van 1 Juli 2011 aangewezen sectorale overheden en sectorale inspectionien-
sten.

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

In order to ensure that the sector is overheated and the sector is inspected

sten aan.

Afdeling 2. — National cyberbeveiligingsauthority **Art. 16.**

The national cyberbeveiliging authority is the last one to be implemented in coördinatie of the uitvoering van deze wet, het toezicht op de uitvoering ervan door de ssentiële en belangrijke entiteiten, alsook met het beheer van cybercrises en cyberbeveiligingsincidenten overeenkomstig artikel 18.

The national cyber security authority is responsible for taking the necessary authority into account, the national CSIRT, the central national contact point for the use of the wet, the green field in Belgium in the same network of companies, the CSIRT network in the European network. verbindings-
organisaties voor cybercrises (EU-CyCLONe) bedoeld in article 16 van de NIS2-richtlijn.

Onderafdeling 1. — Taken met betrekking tot de rol
van bevoegde autoriteit belast met cyberbeveiliging **Art. 17.** De nationale
cyberbeveiligingsautoriteit heeft de volgende taken:

1. If you have any coördinatie you have to be authorized to do so when your feet pass through wet weather, you also have to be authorized to contact them by cyberbeyond your control.

Belgium; 2o het opvolgen en coördineren van en toezien op de uitvoering van de nationale cyberbeveiligingsstrategie bedoeld in article 28;

3. How to identify the essential items in this article above; 4o het toezien op de uitvoering van de wet

door de essential en
belangrijke entiteiten overeenkomstig titel 4;

5o het zorgen voor dinatie tussen de overheden en de private sector de wetenschappelijke wereld; 6o het

formularen van voorstellen tot aanpassing van het telijk en regelgevend kader op het vlak van cyberbeveiliging; 7o het opstellen,

verse preiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor de cyberbeveiliging van de verschillende soorten informatiesystemen;

8o het coördineren van de Belgische vertegenwerdiging in international fora voor cyberbeveiliging, van de opvolging van international verplichtingen van voorstellen van het nationale standpunt op dit vlak; 9o het fungeren als

central contactpunt dat een verbindingsfunctie vervult om, in het kader van deze passing van deze wet, te zorgen voor grensoverschrijdende samenwerking van de Belgische auriteiten met de voegde auriteiten van etere lidstaten van de Europese
Unie en voorkomend geval met de Europese Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde Belgische auriteiten;

in Article 17 of the eIDAS regulation are transmitted by this body to the national cybersecurity authority, according to the procedures set by the King.

TITLE 2. — ***Competent authorities and cooperation at national level***

CHAPTER 1. — *Competent authorities*

Section 1. — Designation of competent authorities **Art.**
15. § 1. The King designates the national cybersecurity authority.

§ 2. After consulting the national cybersecurity authority, the King may, by decree deliberated in the Council of Ministers, designate a sectoral authority and, where appropriate, a sectoral inspection service responsible, for a specific sector or sub-sector, for supervising the implementation of the additional sectoral or sub-sectoral cybersecurity risk management measures referred to in Article 33.

In the context of the designation referred to in paragraph 1, the King takes into account the identity of the sectoral authorities and sectoral inspection services designated under the law of 1 July 2011.

The King may, by decree deliberated in the Council of Ministers, create sectoral authorities, composed of representatives of the federal State, the Communities and the Regions, in accordance with the procedures provided for in Article 92ter of the special law of 8 August 1980 on institutional reforms.

By way of derogation from paragraph 1, this law itself designates the sectoral authorities and inspection services created and governed by the law.

Section 2. — The National Cybersecurity Authority **Art. 16.** The

National Cybersecurity Authority is responsible for monitoring and coordinating the implementation of this Act, ensuring the implementation of this Act by essential and important entities and managing cyber crises and cybersecurity incidents in accordance with Article 18. In this capacity, the National Cybersecurity Authority carries out the tasks of competent authority for essential and important

entities, national CSIRT, single national point of contact for the implementation of this Act and representing Belgium within the cooperation group, the CSIRT network and the European Cyber Crisis Preparedness and Response Network (EU-CyCLONe) referred to in Article 16 of the NIS2 Directive.

Subsection 1. — Tasks relating to the role of
competent authority responsible for cybersecurity **Art. 17.** The tasks of the
national cybersecurity authority are as follows:

1. ensure coordination between the competent authorities in the context of the application of this law, as well as between the different services and authorities concerned with cybersecurity in Belgium;

2. supervise, coordinate and ensure the implementation of the strategy national cybersecurity policy referred to in Article 28;

3. identify essential and important entities in accordance with Article 11; 4. supervise

the implementation of the law by essential and important entities in accordance with Title 4; 5. ensure

coordination between public authorities and the sector
private or the scientific world;

6. formulate proposals for the adaptation of the legal framework and regulatory in cybersecurity;

7o develop, disseminate and ensure the implementation of standards, directives and norms for the cybersecurity of different types of information systems; 8o coordinate

Belgian representation at international forums on cybersecurity, the monitoring of international obligations and the presentation of the national point of view on the matter;

9o serve as a single point of contact exercising a liaison function aimed at ensuring, within the framework of the application of this law, cross-border cooperation between the Belgian authorities and the competent authorities of the other Member States of the European Union and, where appropriate, with the European Commission and ENISA, as well as guaranteeing intersectoral cooperation with the other competent Belgian authorities;

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

11o het informen en sensitizeen van gebruikers van informatie-en communicatiesystemen; 12o het

toekennen van subsidies foor projects en activiteiten round cyberbeveiliging, binnen de grenzen van haar begrotingskredieten en volgens de voorwaarden bepaald door de Koning;

13o to facilitate the organization of all possible cyber-related activities for your personal needs;

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

Onderafdeling 2. — Taken met betrekking tot het cybercrisisbeheer

Art. 18. Onverminderd de articles 8 en 9 van de wet van May 15, 2007

Betreffende de civiele veiligheid en de uitvoeringsbesluiten ervan en onverminderd de bevoegdheden van het NCCN vervult de nationale cyberbeveiligingsautoriteit de volgende taken et betrekking tot het cybercrisisbeheer: 1o in samenwerking met het NCCN, het vaststellen van de

capaci-teiten, middelen en procedures die in geval van een cybercrisis kunnen worden ingezet;

2o het opvolgen van de opmaak, actualisering en operationalisering van het nationale plan voor cyberbeveiligingsincidenten en cybercrisis-response bedoeld in article 29, in samenwerking met het NCCN;

3o het vervullen van de rol van coördinator bij het beheer van cybercrises en cyberbeveiligingsincidenten, en voorkomend geval over-eenkomstig het in 2o bedoelde plan.

Onderafdeling 3. — Taken en voorschriften met betrekking tot de rol van national CSIRT **Art. 19.** § 1. The

national CSIRT has taken the following steps: 1. The monitors and

analyzers of the cyber-dreigingen are aware of the incident at the national level, at the national level, and the verlenen of the bijna-realtime are essential. monitor your network - in computer systems;

2o het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigen en het verspreiden van de informatie onder de betrokken essentiële en belangrijke entiteiten en aan de voegde auriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaar-heden en incidentsen, in bijna-realtime indian mogelijk;

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

4. Verify the analysis of forensics that involves dynamic risk-taking in incident analysis and situational analysis with betrekking before cyberbeveiliging; 5. Opinion of the essential nature of the entity: the proactive scan of the network and the

information system of the active entity with the most significant information on the subject; 6o het deelnemen aan het CSIRT-netwerk, het doeltreffend, efficiënt en veilig samenwerken en dit netwerk en, in overeenstemming met zijn capaciteiten en

bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van dit netwerk op hun verzoek;

7o indian van toepassing, het optreden als coördinator ten behoeve van het in article 22 bedoelde proces van gecoördineerde bekendma-king van kwetsbaarheden; 8o het bijdragen aan de uitrol van elige

instrumenten por het delen van informatie;

9o het proactive en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen als deze scan wordt uitgevoerd om kwetsbare de onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informen en deze negatieve gevolgen heeft voor de werking van deiensten van de entities;

10o het opsporen, observeren en analyzen van computerbeveili-gingsproblemen;

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

10o coordinate the assessment and certification of the security of

information and communication systems;

11o inform and raise awareness among users of information and communication systems; 12o grant subsidies for

projects and activities relating to cybersecurity, within the limits of its budgetary appropriations and according to the conditions established by the King;

13o facilitate and encourage the organization of cybersecurity training for staff members of essential or important entities; 14o establish a list of essential and important entities as well

as entities providing domain name registration services. Subsequently, review this list and, where appropriate, update it regularly and at least every two years.

Subsection 2. — Tasks relating to the role of cyber crisis management **Art. 18.** Without

prejudice to Articles 8 and 9 of the Law of 15 May 2007 on civil security and their implementing decrees and without

Without prejudice to the powers of the NCCN, the tasks of the National Cybersecurity Authority relating to the role of cyber crisis management are as follows:

1o in collaboration with the NCCN, identify the capacities and means and the procedures that can be deployed in the event of a cyber crisis;

2o supervise, in collaboration with the NCCN, the drafting, updating and operationalization of the national plan for responding to cyber crises and cybersecurity incidents referred to in Article 29; 3o ensure the role of coordinator in the management of

cyber crises and cybersecurity incidents, where appropriate in accordance with the plan referred to in 2o

.

Subsection 3. — Tasks and

obligations relating to the role of national CSIRT

Art. 19. § 1. The tasks of the national CSIRT are as follows: 1o to monitor and

analyze cyber threats, vulnerabilities and incidents at the national level and, upon request, provide assistance to the essential and important entities concerned to monitor their networks and information systems in real or near real time;

2o activate the early warning mechanism, the dissemination of alert messages, announcements and dissemination of information on cyber threats, vulnerabilities and incidents to the relevant critical and important entities as well as to the competent authorities and other relevant stakeholders, if possible in near real time; 3o respond to incidents and provide assistance to the relevant critical and important entities, where

appropriate; 4o gather and analyse forensic data, and provide dynamic risk and incident analysis and cybersecurity situational awareness; 5o carry

out, at the request of a critical or important entity, a proactive scan of the relevant entity's networks and information systems to detect vulnerabilities that may have a significant impact; 6o participate in the CSIRT

network, cooperate effectively, efficiently and securely within this network and provide mutual assistance according to its capabilities and skills to other members of the CSIRT network at their request; 7o where applicable, act as coordinator for the purposes of the coordinated vulnerability

disclosure process under Article 22;

8o contribute to the deployment of secure information sharing tools; 9o carry out a proactive

and non-intrusive scan of publicly accessible networks and information systems when this scan is carried out with the aim of detecting vulnerable or insecurely configured networks and information systems and informing the entities concerned and it does not have a negative effect on the operation of the entities' services;

10o detect, observe and analyze IT security problems; 11o establish cooperative

relationships with relevant stakeholders in the
private sector, with a view to achieving the objectives of this law;

12o het vergemakkelijken van de in punt 11o bedoelde samenwerking door de invoering en het gebruik te bevorderen van gemeenschappe-lijke de gestandaardiseerde praktijken, classificatieschema's en taxono-mieën met betrekking tot: *a)* procedures

voor de incidentenbehandeling; *b)* crisisbeheer; in

c) of gecoördineerde

bekendmaking van kwetsbaarheden uit hoofde van artikel 22;

13o het samenwerken en in voorkomend geval uitwisselen van relevante informatie overeenkomstig artikel 27 met detzelfde artikel bedoelde gemeenschappen;

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

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

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

Art. 20. For the national CSIRT, we have the following: 1. We need to know more about

communication, information and infrastructure, and more relevant information;

2o a high mate can be used to communicate with you through various channels that can be contacted and sent to you; of communication channels two specific ones in connection with the gebruikersgroep and samenwerkingspartners;

3o beschikken over locations in informaticesystemen die zich op watch out for localities;

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

5% of the total amount of time it takes to get out of the action; 6o beschikken over voldoende

personeel om te allen tijde de beschikbaarheid van zijn fiensten te garanderen, en ervoor zorgen dat zijn pereel naar behoren wordt opgeleid;

7o uitgerust zijn put redundante systemsen en reservewerkruimten om de continuïteit van zijn diensten te waarborgen.

Art. 21. § 1. In the case of those who use the CSIRT, the national CSIRT will pass on the terms of articles 19 and 20, which will be published in detail. Deze gelen moeten evenredig zijn met die deelstellingen, en in overeenstemming met de beginselen van objectivity, transparantie en non-discriminatie.

§ 2. Indian dat strikt noodzakelijk is voor de uitvoering van zijn kan het nationale CSIRT taken opgesomd in article 19, § 1, 1o tot 5o , van de wet van identificatiegegevens bedoeld in article 2, eerste lid, , 5o 17 januari 2003 met betrekking tot het statutut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens bedoeld in article 2, 93o, from the wet van June 13, 2005 verkrijgen van een operator in de zin van article 2, , van 11o de voormelde wet van 13 June 2005, die deze gegevens bewaart.

You should be informed of the fact that you are in possession of those who are responsible for the political action taken by you and your authority, and your words are taken into account by your decision: 1st , the finality of the decision,

the finality of your decision, the decision to take into account the fact that it is possible to do so. die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminale feiten;

2o het voorkomen van ernstige bedreigingen voor de openbare veiligheid; 3. There are

some problems with electronic problems. communicatienetwerken of -diensten of informatiesystemen.

The national CSIRT can be used to operate the operator at the end of the day.

12o facilitate the cooperation referred to in 11o by encouraging the adoption and use of common or standardized practices, classification systems and taxonomies with regard to:

(a) incident management procedures; *(b)* crisis

management; and *(c)*

coordinated disclosure of vulnerabilities under Article 22;

13o cooperate and, where appropriate, exchange relevant information in accordance with Article 27 with the communities referred to in the same Article; 14o participate in peer reviews

organised in accordance with in Article 19 of the NIS2 Directive.

After consulting the national CSIRT, the King may, by deliberate decree in Council of Ministers, entrust him with additional tasks.

§ 2. When carrying out the tasks referred to in paragraph 1, the national CSIRT may give priority to certain tasks on the basis of a risk-based approach.

Art. 20. The obligations of the national CSIRT are as follows:

1o have a suitable, secure and resilient communication and information infrastructure enabling it to exchange information with essential and important entities and other stakeholders; 2o ensure a high level of availability of its

communication channels by avoiding single points of failure and have multiple means of being contacted and contacting others at any time; clearly specify the communication channels and make them known to partners and collaborators;

3. have premises and information systems located on secure sites;

4. be equipped with an appropriate system for managing and routing requests in order, in particular, to facilitate effective and efficient transfers;

5o guarantee the confidentiality and reliability of its operations;

6. be provided with adequate staff to ensure permanent availability of its services and ensure that its staff receive appropriate training;

7o be equipped with redundant systems and a backup workspace to ensure the continuity of its services.

Art. 21. § 1. In exercising its powers, the national CSIRT shall take all appropriate measures to achieve the objectives defined in Articles 19 and 20. These measures must be proportionate to these objectives and respect the principles of objectivity, transparency and non-discrimination.

§ 2. When this proves strictly necessary for the performance of its tasks listed in Article 19, § 1, 1o to 5o, the national CSIRT may obtain from an operator referred to in Article 2, 11o of the Law of 13 June 2005, identification data referred to in Article 2, paragraph 1, 5o of the Law of 17 January 2003 relating to the status of the regulator of the Belgian postal and telecommunications sectors or electronic communications metadata within the meaning of Article 2, 93o of the aforementioned Law of 13 June 2005 retained by the latter.

Without undermining or interfering with the powers of persons exercising judicial police duties or of judicial authorities, the purposes pursued by the aforementioned tasks are:

1o without a criminal purpose, the prevention, research and detection of offences committed online or via an electronic communications network or service, including acts which constitute serious crime;

2. the prevention of serious threats to public safety;

3. the examination of network or service security failures electronic communications or information systems.

The national CSIRT may determine the time limit within which the opera-The operator responds to his request, depending on its urgency.

§ 3. Indian het nationale CSIRT een operator een verzoek om identificatiegegevens bedoeld in article 2, eerste lid, 5o van de wet van 17 januari 2003 met betrekking tot het statutut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hierarchische meerdere.

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

In order to do so, you will be able to check the national CSIRT optreden zone of your bedoeld control in the right place, and to take advantage of the rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het eerste lid bedoelde overheid gestures om een latere controle mogelijk te maken.

Indian de gegevensbeschermingsautoriteit, na de in het tweede lid bedoelde controle, weigert de geldigheid van het in het eerste lid bedoelde verzoek om elektronische-communicatiemetagegevens te bevestigen, stelt het nationale CSIRT de betrokken operator daarvan onverwijld in kennis en verwijdert het de ontvangen metagegevens. § 5. The general director of the national CSIRT is the person who has the right to contact you in

this article.

§ 6. Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de totegang von elektronische-communicatiegegevens als de uitvoering van zijn taken van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd. § 7. On verminderd de articles 28quinquies, § 1, en 57, § 1, van het Wetboek van

strafvordering mag het nationale CSIRT, om die doelstel-lingen te verwezenlijken, alle beschikbare gegevens bezitten, onthullen de verspreiden, de er enig gebruik van maken, Please note that the computer system is already in use and is not subject to any restrictions.

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

The general director of the national CSIRT is responsible for the publication of this article. Daartoe werkt hij internal procedures uit.

Art. 22. § 1. In this case, the coordinator meets the oog op een gecoördineerde bekendmaking van kwetsbaarheden treedt the national CSIRT op als betrouwbare tussenpersoon en vergemakkelijkt het, waar nodig, de interactie tussen de natuurlijke de rechtspersoon die een mogelijke These products are supplied by the manufacturer of the ICT products, which are then supplied by the manufacturer.

In this case we have taken the national CSIRT with the name:

1o het identificeren van en contact opnemen met de trokken entiteiten; 2o het bijstaan van de natuurlijke

de rechtspersonen die een kwetsbaarheid melden; in 3o het onderhandelen over tijdschema's voor de bekendmaking, en het

beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.

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

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

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

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

§ 3. When the national CSIRT addresses a request to an operator under the law of of identification data referred to in Article 2, paragraph 1, 5o of January 17, , 2003 relating to the status of the regulator of the Belgian postal and telecommunications sectors, this request is authorized by the hierarchical superior.

§ 4. When the national CSIRT sends an operator a request for electronic communications metadata within the meaning of Article 2, 93o of the law of June 13, 2005 other than those referred to in paragraph 3, this request is subject to prior control by the data protection authority.

In the event of a duly justified urgent situation, the national CSIRT may dispense with the prior check referred to in paragraph 1 and request the data directly. This request shall be sent without delay to the authority referred to in paragraph 1 to allow for a subsequent check.

Where, following the check referred to in paragraph 2, the data protection authority refuses to confirm the validity of the request for electronic communications metadata referred to in paragraph 1, the national CSIRT shall notify the operator concerned without delay and delete the metadata received.

§ 5. The Director General of the National CSIRT expressly designates the persons authorized to process the electronic communications data referred to in this article.

§ 6. The national CSIRT informs, as far as possible, the natural persons concerned of access to their electronic communications data when this is no longer likely to compromise the proper conduct of its tasks or an ongoing investigation and when these persons can be identified.

§ 7. Without prejudice to Articles 28quinquies, § 1, and 57, § 1, of the Code of Criminal Procedure, to achieve these objectives, the national CSIRT is authorized to hold, disclose, disseminate or make use of all available information, even if this information comes from unauthorized access to a computer system by a third party.

§ 8. In carrying out its missions, the national CSIRT exercises the prudence that one is entitled to expect from a public authority, always ensuring as a priority not to disrupt the operation of the computer system and taking all reasonable precautions to ensure that no material damage is caused to the computer system.

The Director General of the National CSIRT ensures, through the adoption of internal procedures, compliance with the conditions referred to in this article.

Art. 22. § 1. In its role as coordinator for the purposes of coordinated vulnerability disclosure, the national CSIRT acts as a trusted intermediary by facilitating, if necessary, interactions between the natural or legal person reporting a potential vulnerability and the manufacturer or supplier of the potentially vulnerable ICT products or ICT services, at the request of either party.

In this context, the tasks of the national CSIRT consist in particular of: 1o identifying and

contacting the entities concerned;

2. provide assistance to individuals or legal entities reporting a vulnerability; and

3. Negotiate disclosure deadlines and manage vulnerabilities that affect multiple entities.

§ 2. Any natural or legal person may report, even anonymously when requested, to the national CSIRT the existence of a potential vulnerability.

The report is made in writing, according to the procedure detailed on the national CSIRT website.

This reporting is without prejudice to the application of the law of 28 November 2022 on the protection of persons who report violations of Union or national law observed within

of a private sector legal entity or legal provisions on the protection of individuals who report breaches of Union or national law within a public sector legal entity.

§ 3. The national CSIRT shall ensure that diligent follow-up measures are taken with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability, provided that this person so requests and complies with the conditions referred to in Article 23.

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

From tot deze informatie wordt beperkt tot personen die daartoe door de uitvoering van de taken opgesomd en dit article.

§ 4. Met in the information system observed in article 21, § § 1 in 4, kan het nationale CSIRT de beveiliging van een netwerk- en informatiesysteem observeren, onderzoeken en testen om te bepalen de er sprake est van een mogelijke kwetsbaarheid de om de door de melder this method is not used.

§ 5. Wanneer een gemelde kwetsbaarheid significante volgen kan hebben voor entiteiten in meer dan één lidstaat, werkt het national CSIRT, in voorkomend geval, samen met andere als coördinator aangewezen CSIRT's binnen het CSIRT-netwerk. § 6. The general director of the national CSIRT is responsible for the publication of these articles. Daartoe werkt hij internal procedures uit.

Art. 23. § 1. In the following procedure, we refer to article 22 of the articles *314bis,* 458, *550bis* and 550ter in the article 145 of June 13, 2005, at the latest:

1o zij zonder bedriegliijk opzet de het oogmerk om te schaden hebben gehandeld; 2o zij onverwijld en uiterlijk binnen vierentwintig uur na de ontdek-king van een mogelijke kwetsbaarheid een vereenvoudigde kennisge-ving met de identificatie van het betrokken systeem en een eenvoudige beschrijving van de mogelijke kwetsbaarheid hebben gestuurd naar de organizatie verantwoordelijk is your system in the national CSIRT;

3. You can find out more about this and we have two more than one month of organizing your system, in which you have to take advantage of the fact that you have already organized a wide range of organizing activities. meldingsmodaliteiten, in national law CSIRT, overeenkomstig de in article 22, § 2, bedoelde procedure;

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

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

6o zij, wat betreft de netwerken en systemen van de in article 5, § § 4 en 5, bedoelde organizations en van de rechterlijke instanties, en de informatie die door hen de names hen wordt verwerkt, vóór het plegen van die daden een schriftelijke overeenkomst hebben gesloten met de bevoegde Dienst over de te haunteren modaliteiten en methodo-logie in het kader van het onderzoek naar mogelijke kwetsbaarheden. § 2. Personen die informatie melden over een mogelijke kwetsbaar-heid waarvan zij in het kader van hun beroep kennis hebben gekregen, worden niet geacht hun beroepsgeheim te hebben geschonden en kunnen op generlei wijze aansprakelijk worden gesteld voor de overdracht van informatie die noodzakelijk was om een mogelijke kwetsbaarheid aan het nationale CSIRT te melden.

§ 3. For further information, please refer to the following instructions: gelden.

Afdeling 3. — De eventuale sectorale overheden **Art. 24.** We are also aware of the sectoral overheid: 1o sectorale oefeningen organizer, coördineren of eraan deelnemen,
Please note that the contents of this item are 30 to 33;

2o when an incident occurs in the sector it is analyzed in advance; 3o deelnemen aan de werkzaamheden van de samenwerkingsgroep voor de onderwerpen die betrekking hebben op haar bevoegdheden; 4o de entiteiten die onder haar sector vallen sensitizeen.

HOOFSTUK 2. — *Samenwerking op nationalaal level* **Art. 25.** § 1.

De authoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.

The National CSIRT preserves the completeness, integrity, long-term storage and confidentiality of information transmitted through reporting.

Access to this information is limited to persons authorized by the Director General of the National CSIRT, except when sharing this information is necessary for the performance of the tasks listed in this Article. § 4.

While respecting the conditions listed in Article 21, § § 1 and 4, the national CSIRT may observe, study or test the security of a network and information system in order to determine the existence of a potential vulnerability or to verify the methods used by the reporting party. § 5. Where the reported vulnerability is likely to have a significant impact on entities in several Member States, the national CSIRT shall cooperate, where appropriate, with other CSIRTs designated as coordinators within the CSIRT network.

§ 6. The Director General of the National CSIRT ensures, through the adoption of internal procedures, compliance with the conditions referred to in this article.

Art. 23. § 1. In the context of the procedure referred to in Article 22, the authors of the report do not commit an offense under Articles *314bis,* 458, *550bis,* 550ter of the Penal Code and Article 145 of the Law of June 13, 2005, provided:

1. that they acted without fraudulent intent or intention to harm;

2. that they have sent a simplified notification which includes the identification of the system concerned and a simple description of the potential vulnerability, without delay and at the latest within twenty-four hours of the discovery of a potential vulnerability, to the organization responsible for the system and to the national CSIRT;

3. that they have sent a complete notification, without delay and at the latest within seventy-two hours of the discovery of a potential vulnerability, to the organization responsible for the system, where applicable in compliance with the reporting procedures established by this organization, and to the national CSIRT, in accordance with the procedure referred to in Article 22, § 2;

4o that they have not acted beyond what was necessary and proportionate to verify the existence of a vulnerability and to report it; 5o that they have not publicly disclosed information relating to the vulnerability discovered and the vulnerable systems, without the agreement of the national CSIRT;

6o with regard to the networks and systems of the organisations referred to in Article 5, §§ 4 and 5, and of judicial bodies as well as the information processed by them or on their behalf, that they have, before committing these acts, concluded a written agreement with the competent service on the methods and methodology to be used in the context of the search for potential vulnerabilities.

§ 2. When individuals report information about a potential vulnerability that they have become aware of in their professional context, they are not considered to have breached their obligation of professional secrecy and do not incur any liability of any kind regarding the transmission of necessary information.

to report a potential vulnerability to the national CSIRT.

§ 3. Any other possible liability of the reporting persons arising from acts or omissions which are not necessary for the completion of the procedure referred to in Article 22 and do not comply with the conditions of paragraph 1 shall continue to be governed by the applicable law.

Section 3. — Possible sectoral authorities

Art. 24. Without prejudice to other provisions, the sectoral authority may: 1o organize, coordinate or participate in sectoral exercises,
as regards the measures referred to in Articles 30 and 33;

2nd analyze and manage the consequences of an incident for the sector;

3. participate in the work of the cooperation group with regard to subjects which affect its competences; 4. raise awareness among entities within its sector.

CHAPTER 2. — *Cooperation at national level* **Art. 25.** § 1.

The authorities referred to in Chapter 1 of this Title shall cooperate with each other in order to comply with the obligations set out in this law.

§ 2. Please note that you are not required to operate under any conditions in paragraph 1 of the national authority at the same level as the NCCN, the administrative authority of the State, the administrative authority overheden, and the national authority of the Verordening (EG) nr. 300/2008 in nr. 2018/1139, of toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 of the European Parliament in the European Parliament on July 23, 2014 for electronic identification in the form of electronic transactions in the internal markets of the Bank of Belgium 1999/93/EG, of the National Bank of België, of the Authority for Financial Services in Markten, the Institute, of wet crashes on July 1, 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 Novem-ber 1998 houdende regeling van de inlichtingen- en veiligheidsdien-sten, de politiediensten bedoeld in de wet van 7 December 1998 tot organization van een geïntegreerde politiedienst, gestructureerd op tweelevels, en de gegevensbeschermingsautoriteiten. § 3. Of the essential nature of the information and of the authoritative authority, 1 of the titles we are working with you also have the right to use the information system over the network.

§ 2. Depending on the needs necessary for the implementation of this law, the authorities referred to in paragraph 1 shall also cooperate, at national level, with the NCCN, the administrative services of the State, the administrative authorities, including the national authorities under Regulations (EC) No 300/2008 and No 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, the National Bank of Belgium, the Financial Services and Markets Authority, the Institute, the competent authorities under the Law of 1 July 2011, the judicial authorities, the intelligence and security services referred to in the Organic Law of 30 November 1998 on Intelligence and Security Services, the police services covered by the law of December 7, 1998 organizing an integrated police service, structured at two levels and with data protection authorities.

§ 3. Essential and important entities and the authorities referred to in Chapter 1 of this Title shall collaborate at all times through an adequate exchange of information concerning the security of information systems and networks.

§ 4. From 1 to 2 December 2011, the authority to be authorized by the authority to be authorized by the authorities on 1 July 2011 is subject to regulatory information which is subject to the protection of infrastructure, over risks, cyber-related incidents, and also over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor exploiten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen. § 5. De in hoofdstuk 1 van deze titel bedoelde authoritative en de auriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 of the European Parliament in the European Parliament on July 23,

2014 for electronic identification in the form of electronic transactions in the internal markets of the European Parliament in 1999/93/EG, Verordening (EU) 2022/2554 in the European Parliament Last December 14, 2022, the digital operation of our financial sector will be fully implemented by Verorde-Ningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 in (EU) 2016/1011 on June 13, 2005, the regulations governing relevant information technology are subject to the latest cyber-related incidents. § 6. National cyber security authority has a coordinating platform and an evaluation platform based on articles 15 and 15 of which are authoritative in the NCCN data processing system and are therefore opted for in the future.

§ 4. The authorities referred to in Chapter 1 of this Title and the competent authorities under the Law of 1 July 2011 shall cooperate and regularly exchange information on the identification of critical infrastructures, risks, cyber threats and incidents, as well as on non-cyber risks, threats and incidents affecting operators of infrastructures identified as critical infrastructures under the Law of 1 July 2011 and on the measures taken to address these risks, threats and incidents.

§ 5. The authorities referred to in Chapter 1 of this Title and the competent authorities under Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 and the Law of 13 June 2005, shall regularly exchange relevant information, including with regard to incidents and cyber threats concerned.

§ 6. The National Cybersecurity Authority shall establish a coordination and evaluation platform so that the authorities referred to in Article 15 and the NCCN exchange information and coordinate in the context of the implementation of this Act.

HOOFSTUK 3. — *Vertrouwelijkheid en informatie-uitwisseling* **Art.**

26. § 1. Dit article dot geen afbreuk aan de toepassing van de wet van April 15, 1994 betreffende de becherming van de volking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de wet on April 11, 1994, it was opened to the best of the national open air network.

CHAPTER 3. — *Confidentiality and exchange of information*

Art. 26. § 1. This article does not prejudice the application of the law of 15 April 1994 relating to the protection of the population and the environment against the dangers resulting from ionizing radiation and relating to the Federal Agency for Nuclear Control, the law of 11 April 1994 relating to the publicity of the administration or other legal provisions guaranteeing the confidentiality of information linked to the essential interests of national public security.

§ 2. Eenieder die beroepshalve zijn medewerking diente verlenen aan de conformiteitsbeoordeling de het toezicht est tot geheimhouding verplicht. Diegene dit geheim schendt, wordt gestraft met de straffen bepaald in article 458 van het Strafwetboek.

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

Deze personen verkrijgen het akkoord van deze authoriten bedoeld in article 5, § 4, wanneer deze auriteiten bij het geheim betrokken zijn. § 3. De

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

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

§ 2. Any person who is called upon to provide professional assistance in conformity assessment or supervision is bound by secrecy. Anyone who violates this secrecy shall be punished by the penalties provided for in Article 458 of the Criminal Code.

Persons who are custodians, by status or profession, of the secrets entrusted to them are authorized to make these secrets known for the execution of this law.

These persons shall obtain the agreement of the authorities referred to in Article 5, § 4, when these authorities are concerned by

secrecy. § 3. The authorities referred to in Chapter 1 of this Title, essential or important entities, or their subcontractors, shall limit access to information under this law to persons who need to know and have access to it for the exercise of their functions or their mission in connection with the execution of this law.

§ 4. Information provided to the authorities referred to in Chapter 1 of this Title by essential or important entities may be exchanged with authorities of the European Union, with Belgian or foreign authorities, when this exchange is necessary for the application of legal provisions.

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

Art. 27. § 1. Binnen het toepassingsgebied van deze wet valley, kunnen op vrijwillige basis onderling, binnen gemeenschappen, relevante informatie over cyber-beveiliging uitwisselen, mit inbegrip van informatie over cyberdreigin-gen, bijna-incidenten, kwetsbaarheden, technieken en procedures, indicatoren voor anantasting, vijandige tactieken, dreigingsactorspeci-fieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyber attacks detect you, wanneer dat uitwisselen van informatie:

1o beoogt incidentsen te voorkomen, te detecteren, erop te reageren de ervan te herstellen de gevolgen ervan te beperken; 2o het level van de

cyberbeveiliging verhoogt, met name door de bewustword met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beper-ken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en openbaarmaking van kwetsbaarheden, het opsporen van dreigin-gen, beheersings- en preventietechnieken, beperkingsstrategieën de respons- en herstelfasen te ondersteunen de gezamenlijk onderzoek naar cyberdreigingen door pubke en private entity te bevorderen. § 2. De informatie-uitwisseling bedoeld in paragraaf 1 wordt uitgevoerd door middel van informatie-uitwisselingsregelingen op het gebied van

cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie. § 3. The national cyberbeveiliging authority facilitates extensive information in paragraph 2 of the information technology regulations that apply to cyberbeveiliging. In order to control the operational elements, you

need to take into account the specification of ICT-platforms in automatic automation, and you need to know how to use information-processing regulations. National cyber security authorities and possible sectoral overrides can be made available in paragraph 1.

§ 4. Of the essential elements of national cyberbeveiliging authority in Kennis van Hun deelname aan de in paragraaf 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indienne van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

HOOFSTUK 4. — *National cyberbeveiligingsstrategie* **Art. 28.** § 1.

De in Raad vergaderde ministries keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de vijf jaar bij op base van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in article 15 bedoelde auriteiten, het NCCN en, en voorkomend geval, of gegevensbeschermingsautoriteiten.

Deze strategy bepaalt de strategische doelstellen, de middelen die nodig zijn om die doelstellingen te behalen, en pasende beleids- en regelgevingsmaatregelen, om een hoog level van cyberbeveiliging te bereiken en te handhaven.

§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:

1st of priority actions for the national cyber-strategy strategy, with the name included in the two sectors I and II of the sector;

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

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

4o a relevant mechanism activated by a large number of players in Belgium;

The information exchanged shall be limited to what is relevant and proportionate to the purpose of the exchange, in particular in compliance with Regulation (EU) 2016/679. This exchange of information shall preserve the confidentiality of the information concerned and protect the security and commercial interests of essential or important entities.

Art. 27. § 1. On a voluntary basis, entities falling within the scope of this Act and, where applicable, other relevant entities not falling within the scope of this Act may exchange, among themselves, within communities, relevant cybersecurity information, including information relating to cyber threats, incidents avoided, vulnerabilities, techniques and procedures, indicators of compromise, adversary tactics, as well as specific information on threat actors, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks, where such sharing of information:

1o aims to prevent, detect, respond to, recover from or mitigate the impact of incidents; 2o strengthens the level of

cybersecurity, including by raising awareness of cyber threats, limiting or preventing their ability to spread, supporting a range of defence capabilities, addressing and disclosing vulnerabilities, implementing threat detection, containment and prevention techniques, mitigation strategies or response and recovery steps, or encouraging collaborative research on cyber threats between public and private entities.

§ 2. The exchange of information referred to in paragraph 1 is implemented by means of cybersecurity information sharing agreements, taking into account the potentially sensitive nature of the information shared.

§ 3. The national cybersecurity authority shall facilitate the establishment of cybersecurity information sharing agreements referred to in paragraph 2. These agreements may specify the operational elements, including the use of specialized ICT platforms and automation tools, the content and conditions of the information sharing agreements. The national cybersecurity authority and any sectoral authorities may impose conditions for the use of the information they make available to the communities referred to in paragraph 1.

§ 4. Essential and important entities shall notify the national cybersecurity authority of their participation in the cybersecurity information sharing agreements referred to in paragraph 2, when they conclude such agreements or, where applicable, when they withdraw from such agreements, once the withdrawal takes effect.

CHAPTER 4. — *National cybersecurity strategy* **Art. 28.** § 1. The ministers

meeting in Council shall adopt the national cybersecurity strategy and update it at least every five years, on the basis of performance indicators, after consulting the National Security Council, the authorities referred to in Article 15, the NCCN and, where appropriate, the data protection authorities.

This strategy defines the strategic objectives, the resources needed to achieve these objectives, as well as the appropriate political and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

§ 2. The national cybersecurity strategy includes,
among others:

1. the objectives and priorities of the national cybersecurity strategy, covering in particular the sectors referred to in Annexes I and II;

2. a governance framework aimed at achieving the objectives and priorities referred to in 1. , including the tasks and responsibilities of public authorities and other relevant actors as well as the policies referred to in paragraph 3;

3o a governance framework specifying the roles and responsibilities of the stakeholders in Belgium, and on which cooperation and coordination in Belgium between the authorities referred to in Chapter 1 of this Title are based, as well as cooperation and coordination between these authorities and the competent authorities under sectoral legal instruments of the European Union;

4o a mechanism to identify relevant assets and a risk assessment in Belgium;

5. Inventories are taken into account when they are taken into account, are responsible for any incident, and are included in the same information published in the private sector;

6o een lijst van de verschillende belanghebbenden en auriteiten die betrokken zijn bijn uitvoering van de nationale cyberbeveiligingsstra-tegie; 7 o een beleidskader voor

versterkte coördinatie tussen de auriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de wet van

July 1, 2011 bevoegde authoriten, met als doel het delen van informatie over risico's, cyberdreigingen en incidentsen, alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken; 8o een plan, put

inbegrip vanodzakelijke maatregelen, om het algemene level van cyberbeveiligingsbewustzijn bij de burgers te verbeteren; 9o een overzicht van de onderwijs-,

bewustmakings- en opleidings-programma's met betrekking tot de nationale cyberbeveiligingsstrate-gie; 10o een overzicht van de plannen voor onderzoek en

ontwikkeling
puts betrekking tot of national cyberbeveiligingsstrategie.

§ 3. The following words are included in the genome of the national cyberbeveiling strategy:

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

2o inzake the specific opnemen van cyberbeveiligingsgerela-teerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrach-ten, onder meer met betrekking àtt cyberbeveiligingscertificering, versleuteling en het gebrik van open-source-cyberbeveiligings producten; 3. If you are using the kwetsbaarheden, you should also take into account

the handling and control of the kwetsbaarheden overeenkomstig article 22; 4o inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet,

en voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatie cables; 5. You must be aware of the integration of relevant technological advances and the fact that you have advanced knowledge of cyber-believing; 6o you have to be aware of the

fact that you are in control of the cyberbelieving, cyberbeveiligings are available, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controls op het gebied

van cyber hygiene, gericht op burgers, belang-hebbenden en entities;

7. If you are learning about academics in your online education system, you will be able to use the tools for your cyber security and network infrastructure; 8o take into account the relevant procedures in the hands of your information systems, which are

responsible for the control of your cyber security information systems;

9 o you have the right to use digital media on the basis of cyber hygiene in small and medium-sized cases, with the name given to you by the passing of the wet and dry, which means that you need to know the richness of your products and your specific needs. behoeften; 10% of your behavior in cyber activities.

HOOFSTUK 5. — *The national plan for cyber-related incidents in cyber-crisis responses* **Art. 29.**

§ 1. De Koning stelt, bij besluit vastgesteld na overleg in de Ministerraad, een national plan voor cyberbeveiligingsincidenten en cybercrisisrespons op. Dit plan is a national plan in de zin van artikel 9, § 2, van de wet van 15 mei 2007 betreffende de civiele veiligheid. § 2. On the basis of the elements of the national plan, the

national plan for cyber-emergencies in the cyber crisis is responsible for ten minutes: 2o taken into account by cybercrisis authorities;

5o an inventory of measures ensuring the preparation, response and recovery of services after an incident, including cooperation between the public and private sectors;

6o a list of the different actors and authorities concerned by the implementation implementation of the national cybersecurity strategy;

7o a policy framework aimed at enhanced coordination between the authorities referred to in Chapter 1 of this Title and the competent authorities under the Law of 1 July 2011 for the purposes of sharing information relating to risks, threats and incidents in the cyber and non-cyber domains and the exercise of supervisory tasks, where appropriate; 8o a plan including the necessary measures to improve the

general level of awareness of citizens about cybersecurity;

9o an overview of education, awareness and training programs related to the national cybersecurity strategy; 10o an overview of research and development plans in

relation to the national cybersecurity strategy.

§ 3. Policies, integral parts of the national cybersecurity strategy, are adopted and cover the following elements:

1. cybersecurity in the supply chain of ICT products and services used by entities for the provision of their services;

2o the inclusion and specification of cybersecurity-related requirements for ICT products and services in public procurement, including regarding cybersecurity certification, encryption and the use of open source cybersecurity products;

3o vulnerability management, including the promotion and facilitation of coordinated vulnerability disclosure in accordance with Article 22; 4o maintaining the general availability,

integrity and confidentiality of the public core of the open internet, including, where appropriate, the cybersecurity of submarine communications cables;

5o the promotion of the development and integration of relevant advanced technologies aimed at implementing cutting-edge measures in cybersecurity risk management;

6o the promotion and development of cybersecurity education and training, cybersecurity skills, cybersecurity awareness-raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, for citizens, stakeholders and entities;

7o support for university and research institutions aimed at developing, improving and promoting the deployment of cybersecurity tools and securing network infrastructures;

8o the establishment of relevant procedures and appropriate information sharing tools aimed at supporting the voluntary sharing of cybersecurity information between entities; 9o the strengthening of the

cyber resilience and cyber hygiene values of small and medium-sized enterprises, in particular those excluded from the scope of this law, by providing easily accessible guidance and support to meet their specific needs; 10o the promotion of active cyber protection.

CHAPTER 5. — *The national plan for responding to cyber crises and cybersecurity incidents* **Art.**

29. § 1. The King shall establish, by decree deliberated in the Council of Ministers, a national plan for responding to cyber crises and cybersecurity incidents. This plan constitutes a national plan within the meaning of Article 9, § 2, of the law of 15 May 2007 on civil security.

§ 2. Without prejudice to the elements to be contained in national plans, the national plan for responding to cyber crises and cybersecurity incidents shall contain at least the following elements:

1. the objectives of national preparedness measures and activities;

2. the tasks and responsibilities of cyber crisis management authorities;

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

4o de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en pleidingsactiviteiten;

5o of relevant published in private belanghebbenden in built infrastructure;

6o of national procedures in regelingen tussen of betrokken national aurititeiten in instanties om de effectieve deelname van België aan het gecoördineerde beheer van cybercrises en cyberbeveili-gingsincidenten op het vel de Europese Unie en de ondersteuning daarvan te waarborgen.

TITLE 3. — *How to deal with cyber-related risks and reports*

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

Art. 30. § 1. Of essential nature entities do not passende in even redige technische, operationele in organizersche maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesys-temen die zij voor hun activiteiten de voor het verlenen van hun diensten gebruiken, te Be there in the event of an incident that you will be affected by any incident that may occur in your future.

§ 2. Rekening houdend met de stand van de techniek en, indienne van toepassing, de beveiligingslevel van de netwerk- en informa-tiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entity aan risico's est blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, et inbegrip van de maatschap-pelijke en economische gevolgen.

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

risicoanalysis in beveiliging van informatiesystemen;

2o incidental handling; 3o

bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplan-nen en crisisbeheer; 4o de

beveiliging van de toeleveringsketen, et inbegrip van beveiligingsgerelateerde aspecten et betrekking tot de relaties tussen elke entity en haar rechtstreekse leveranciers of dienstverleners;

5o beveiliging bij het verwerven, ontwikkelen en onderhouden van kwetsbaarheden; 6o beleid en procedures om de effectiveness van maatregelen voor het beheer van cyberbeveiligingsrisico's

te beoordelen;

7. Basis of practice for cyber hygiene in operation het gebied van cyberbeveiliging;

8o beleid en procedures inzake het gebruik van cryptografie en, in pre-commanded, encrypted;

9o benevolent aspects of people who are involved in their actions;

10o wanneer gepast, het gebruik van multifactorauthenticatie- of continu-authenticatieoplossingen, beveiligde spraak-, video- en tekst-communicatie en beveiligde noodcommunicatiesystemen binnen de entity;

11o een beleid voor de gecoördineerde bekendmade van kwetsbaar-heden.

§ 4. Wanneer essentiële en belangrijke entitiiteiten nagaan welke maatregelen bedoeld in paragraaf 3, 4o , passend zijn, houden zij rekening met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbehavioral applications of the levers in the service, including the monitoring of the procedure-

res.

Deze maatregelen moeten passend zijn en het licht van de resultaten van de op de level van de Europese Unie gecoördineerde beveili-gingsrisicobeoordelingen van kritieke toeleveringsketens.

3. cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;

4o national preparedness measures, including exercises and training activities; 5o public and sector

stakeholders and infrastructure private parties concerned;

6o national procedures and arrangements between the competent national authorities and bodies aimed at ensuring Belgium's effective participation and support in the coordinated management of cyber crises and cybersecurity incidents at European Union level.

TITLE 3. — *Cybersecurity risk management measures and information obligations*

CHAPTER 1. — *Cybersecurity risk management measures* **Art. 30.** § 1. Essential and

important entities shall take appropriate and proportionate technical, operational and organizational measures to manage risks that threaten the security of the networks and information systems that these entities use in the course of their activities or the provision of their services, as well as to eliminate or reduce the consequences that incidents have on the recipients of their services and on other services.

§ 2. The measures referred to in paragraph 1 shall ensure, for networks and information systems, a level of security appropriate to the existing risk, taking into account the state of knowledge and, where appropriate, applicable European and international standards, as well as the cost of implementation. When assessing the proportionality of these measures, due account shall be taken of the degree of exposure of the entity to risks, the size of the entity and the likelihood of incidents occurring and their severity, including their societal and economic consequences.

§ 3. The measures referred to in paragraph 1 are based on an "all-risks" approach which aims to protect networks and information systems as well as their physical environment against incidents, and they relate at least to:

1. policies relating to risk analysis and information systems security;

2o incident management; 3o

business continuity, for example backup management and business recovery, and crisis management; 4o supply chain security,

including security aspects concerning the relationships between each entity and its direct suppliers or service providers; 5o security of the acquisition, development and maintenance of networks and

information systems, including the treatment and disclosure of vulnerabilities;

6o policies and procedures to evaluate the effectiveness of cybersecurity risk management measures;

7o basic cyber hygiene practices and cybersecurity training;

8o policies and procedures relating to the use of cryptography and, where applicable, encryption; 9o human resources security,

control policies access and asset management;

10o the use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications and secure emergency communication systems within the entity, as needed;

11th a policy of coordinated disclosure of vulnerabilities.

§ 4. When essential and important entities consider which of the measures referred to in paragraph 3, 4o are appropriate, they shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of the products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

These measures must be appropriate in the light of the results of coordinated assessments at European Union level of risks to the security of critical supply chains.

§ 5. It is the essential part of the network and the risk analysis that is based on the fact that it is based on the entire network and information systems and on the basis of which the system is incidental to the work, on the basis of the IBB system. dat minstens de in paragraaf 3 bedoelde aspecten bevat.

§ 6. An essential part of the vast majority of the text does not have to be in paragraph 3 of the rules, but it cannot be changed or corrected in any way.

Art. 31. § 1. Of the best organs of the essentials in the list of essential elements which may be used for cyber-behaviour, there are two elements that do not belong to the article 30, but this is not the case for the use of the door. Deze entities op dat article.

Said article does not have to be published without prior notice of the regulations that have been given to you over the instants, but you also have the right to be authorized by them.

§ 2. Of the best organs of the essentials in the list of elements that can be used in the future, it is important to know that your risk is identified by the risk that it is used by cyber security. If you keep the door of the entity's words out, you will be able to do so.

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

Art. 33. If there is a national cyberbeveiling authority, if there is any sectoral overreach in the country, it may be vastly overruled by the Minister, and even then it will be possible for you to be able to do so.

HOOFSTUK 2. — *Melding van incidents*

Afdeling 1. — Verplichte melding **Art. 34.**

§ 1. Of the essential nature of these entities, a significant incident occurs at the national CSIRT, but these procedures are subject to a protocol established by the national CSIRT and the NCCN. Deze entities report on more information about the national CSIRT in state and where possible

grensoverschrijdende volgen van het incident you bepalen.

In the event of a significant incident in the future, it may be possible to change the distribution of sectors I to II.

Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen onmiddellijk aan de possibleevoegde sectorale overheden. These are the essential parts of the wording and the contents of the NCCN.

§ 2. Indian van toepassing delen de betrokken entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indian nodig stars of entities die ontvangers ook in kennis van de significante cyberdreiging zelf. § 3. Na raadpleging van de nationale cyberbeveiligingsautoriteit, de sectorale overheden, het NCCN en deelgebieden kan

de Koning, bij besluit vastgesteld na overleg en de Ministerraad, precieze meldings-drempels bepalen naargelang de impact dringendheid van this incident.

§ 4. Een melding leidt niet tot blootstelling van de entity aan een high-level speech.

Art. 35. § 1. For article 34, § 1, please refer to the CSIRT national entity : waarschuwing waarin, indian van toepassing, wordt

aangegeven de het significante incident vermoedelijk door een onrechtmatige of kwaad-willige handeling is veroorzaakt, dan wel grensoverschrijdende gevol-gen zou kunnen hebben; 2o onverwijld en in elk geval binnen tweeënzeventig uur nadat zij kennis hebben gekregen van het significante incident, een incidentmel-ding met, indien van toepassing, een update van de in 1o

bedoelde informatie, een initiële beoordeling van het significant incident, met inbegrip van de ernst en de gevolgen ervan en, indian beschikbaar, from indicatoren voor aantasting;

§ 5. Each essential and important entity shall carry out a risk analysis based on an "all-risks" approach which aims to protect networks and information systems as well as their physical environment against incidents and shall draw up, on the basis of this analysis, a PSI covering at least the aspects referred to in paragraph 3.

§ 6. Where an essential or important entity finds that it is not complying with the measures referred to in paragraph 3, it shall take, without undue delay, all necessary appropriate and proportionate corrective measures.

Art. 31. § 1. The management bodies of essential and important entities approve the cybersecurity risk management measures that these entities take in order to comply with Article 30, supervise their implementation and are responsible for the violation of said Article by these entities.

This Article is without prejudice to the rules on liability applicable to public institutions, as well as the liability of civil servants and elected or appointed officials.

§ 2. Members of the management bodies of essential and important entities undergo training to ensure that their knowledge and skills are sufficient to determine risks and assess cybersecurity risk management practices and their impact on the services provided by the entity.

Art. 32. The essential or important entity is responsible for the risk analysis carried out as well as for the choice and implementation of the measures referred to in Article 30, § 1.

Art. 33. After consultation with the national cybersecurity authority, any relevant sectoral authority and the relevant federated entities, the King may, by decree deliberated in the Council of Ministers, impose additional appropriate and proportionate cybersecurity risk management measures.

CHAPTER 2. — *Notification of incidents*

Section 1. — Mandatory notification

Art. 34. § 1. Essential and important entities shall notify any significant incident without undue delay to the national CSIRT, in accordance with the terms established in a protocol concluded between it and the NCCN. These entities shall report, among other things, any information that allows the national CSIRT to determine whether the incident has a transboundary impact.

Where appropriate, the entities concerned shall notify, without undue delay, the recipients of their services of any significant incidents likely to harm the provision of services relating to the sectors or sub-sectors.

sectors listed in Annex I and II.

The national CSIRT immediately communicates the notifications referred to in paragraph 1 to any competent sectoral authorities.

Notifications from critical entities are also forwarded to the NCCN. § 2. Where appropriate, the

relevant entities shall, without undue delay, inform the recipients of their services that are potentially affected by a significant cyber threat of any measures or corrections that these recipients may apply in response to this threat. Where appropriate, the entities shall also inform these recipients of the significant cyber threat itself.

§ 3. After consultation with the national cybersecurity authority, sectoral authorities, the NCCN and federated entities, the King may determine, by decree deliberated in the Council of Ministers, precise notification thresholds depending on the degree of impact or urgency of the incident.

§ 4. The mere fact of notifying an incident does not increase the liability of the entity that originated the notification.

Art. 35. § 1. For the purposes of the notification referred to in Article 34, § 1, paragraph 1, the entities concerned submit to the national CSIRT:

1o without undue delay and in any event within twenty-four hours of becoming aware of the significant incident, an early warning which, where appropriate, indicates whether it is suspected that the significant incident was caused by unlawful or malicious acts or whether it could have a cross-border impact;

2o without undue delay and in any event within seventy-two hours of becoming aware of the significant incident, an incident notification which, where appropriate, updates the information referred to in 1o and provides an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available;

3o op verzoek van the national CSIRT of possible future sectoral overheid, een tussentijds verslag over relevant updates of the situation; 4o iterlijk één maand na de indience van

de in 2o bedoelde incidentmelding, een eindverslag waarin het volgende est opgenomen: *a)* een gedetailleerde beschrijving van het incident, et inbegrip van

from ernst to from gevolgen ervan;

b) het soort bedreiging de grondoorzaak die waarschijnlijk tott het incident heeft geleid; *c)* toegepaste in the open

risicobeperkende maatregelen; *d)* in the event of an incident; 5o Indian

het incident nog aan de gang is op het moment dat het in 4o bedoelde eindverslag moet

worden ingediend, dienen de betrokken entiteiten op dat moment een voortgangsverslag in, en binnen één maand nadat zij het incident definitief hebben afgehandeld, een eindverslag. § 2. In afwijking van paragraaf 1, 2o

, melts a victim of

However, there are significant incidents that may occur when the incident occurs, and in this case, the national CSIRT is responsible for this.

§ 3. Het nationale CSIRT bezorgt de in de paragraphe 1 en 2 bedoelde meldingen onmiddellijk aan de eventuale bevoegde sectorale overhe-den. Meldingen van essential entiteiten worden ook ookstuurd naar het NCCN.

Art. 36. § 1. Het nationale CSIRT verstrekt onverwijld en zo gelijk binnen vierentwintig uur na ontvangst van de in article 35, § 1, 1°, bedoelde vroegtijdige waarschuwing een antwoord aan de meldende entity, met inbegrip van een eenste feedback sur het significante incident en, op verzoek van de entity, richtsnoeren de operationeel eel voor de uitvoering van mogelijke risicobeperkende maatregelen.

§ 2. Het nationale CSIRT verleent aanvullende technische ondersteu-ning indian de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat the significant incident of a criminal act is, geeft the national CSIRT and ook richtsnoeren voor het melden van het significante incident aan de rechtshandhavingsinstanties.

Art. 37. § 1. In your opinion, in the name of the significant incident being trekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig artikel 35 est vangen. Please note that the national CSIRT, the United Kingdom, the national law, commercial benevolent interests of the entity, and the rights of the computer industry are also responsible. § 2. Wanneer publishke bewustmaking nodig is om a significant incident te voorkomen of a lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in

het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entity, het NCCN, de eventuale betrokken sectorale Over-heid by the minister, he published the significant incident informed of the entity's verlangen dat zij dit doet.

§ 3. From the national cyberbeveiling authority it is possible to verify the eventuality of sectoral controls, and to comply with article 34, § 1, hereinafter the central contact point has been established.

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

§ 5. Het nationale CSIRT verstrekt de uit hoofde van de wet van 1 July 2011 bevoegde authoritative informatie over significant incident, incidenten, cyberdreigingen en bijna-incidenten die overeenkom-stig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld Door operator of infrastructure that has been wetted by July 1, 2011 and the infrastructure has been identified.

Afdeling 2. — Vrijwillige melding **Art. 38.**

§ 1. Name of article 34 bedoelde meldingsverplichtingen
Please refer to the national CSIRT word at the door:

1o essential in the following entities: incidents, cyber-related incidents and other incidents;

3o at the request of the national CSIRT or any relevant sectoral authority, an interim report on relevant situation updates; 4o a final report no later than one month after the submission of the incident

notification referred to in 2o , including the following: *a)* a detailed description of the incident, including its severity and impact; *b)* the type of threat or root cause that likely

triggered the incident; *c)* the mitigation measures implemented and in progress; *d)* where

applicable, the transboundary impact of the incident;

5o in the event of an incident in progress at the time of presentation of the final report referred to in 4o, the entities concerned shall provide at that time a progress report and then a final report within one month of the final processing of the incident.

§ 2. By way of derogation from paragraph 1, 2o, a trust service provider shall notify the national CSIRT of significant incidents that have an impact on the provision of its trust services, without undue delay and in any event within twenty-four hours of becoming aware of the significant incident. § 3. The national CSIRT shall immediately communicate the notifications referred to in paragraphs 1

and 2 to any relevant sectoral authorities. Notifications from essential entities shall also be transmitted to the NCCN.

Art. 36. § 1. The national CSIRT shall provide, without undue delay and if possible within twenty-four hours of receiving the early warning referred to in Article 35, § 1, 1o, a response to the entity issuing the notification, including initial feedback on the significant incident and, at the request of the entity, operational guidance or advice on the implementation of possible mitigation measures.

§ 2. The National CSIRT provides additional technical support if requested by the relevant entity. Where there is reason to suspect that the incident is criminal in nature, the National CSIRT also provides guidance on how to notify the significant incident to law enforcement authorities.

Art. 37. § 1. Where appropriate, and in particular if the significant incident concerns two or more Member States, the national CSIRT shall inform the other affected Member States and ENISA of the significant incident without undue delay. Information of the type received in accordance with Article 35 shall then be shared. In doing so, the national CSIRT shall, in accordance with European Union or national law, safeguard the security and commercial interests of the entity and the confidentiality of the information communicated.

§ 2. Where public awareness is necessary to prevent a significant incident or to address an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, the National CSIRT may, after consulting the relevant entity, the NCCN, any relevant sector authority and the relevant Minister, inform the public of the significant incident or require the entity to do so.

§ 3. At the request of any relevant sectoral authority, the national cybersecurity authority shall forward the notifications received pursuant to Article 34, § 1, first paragraph , to the single points of contact of the other affected Member States.

§ 4. The national cybersecurity authority shall submit to ENISA every three months a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats and avoided incidents notified in accordance with Article 34, § 1, first paragraph , and Article 38, § 1.

§ 5. The national CSIRT provides the competent authorities under the law of 1 July 2011 with information on significant incidents, incidents, cyber threats and avoided incidents notified in accordance with Article 34, § 1, paragraph 1, and Article 38, § 1, by operators of infrastructures identified as critical infrastructures under the law of 1 July 2011.

Section 2. — Voluntary notification

Art. 38. § 1. In addition to the notification obligations referred to in Article 34, may be notified voluntarily to the national CSIRT by:

1o essential and important entities, incidents, cyber-naces and incidents avoided;

2o and there in 1o bedoelde entiteiten, ongeacht of zij tot het toepassingsgebied van deze wet behoren: significante incidentsen, cyberdreigingen en bijna-incidenten. §

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

And you can even hear the words you hear when you see them Verplichte meltingen boven die van vrijwillige meltingen.

On the other hand, you will be able to find out what you are looking for, and then you will be able to find out more about it, and you will be able to find out more about it and do not hesitate to contact us directly. zijn onderworpen indian zij de melding niet had ingediend.

TITEL 4. — *Toezicht en sancties*

HOOFDSTUK 1. — *View*

Afdeling 1. — Regelmatige conformiteitsbeoordeling

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

1o of our opted for you in article 40 bedoelde regelmatige conformiteitsbeoordeling, op basis van een van de door de Koning bepaalde referentiekaders; 2o of our

onderwerpen zij zich aan een inspectie door de nationale cyberbeveiligingsautoriteit, op base van de door de Koning bepaalde nadere regels.

In the event of an inspection by the National Cyber Security Authority, you will be able to verify the position of the sectoral beneficiary over the wording of the future bedoeld inspections carried out by the National Cyber Security Authority. cyberbeveiligingsauto-riteit.

Koning Indian meerdere referentiekaders bepaalt, kiezen essen-Tiële entititeiten aan welk referentiekader zij zich onderwerpen.

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

You will be able to enter the wording of the operator of the infrastructure in the wet on July 1, 2011 in the immediate future of conformity by the nature of the conformity person in question. § 2. De inspection of the national cyber security authority can be used to create conformity information in accordance with paragraph 1 of the law, which is

subject to review.

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

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

Art. 43. There is a need to comply with the instructions given by the overeenkomstig article 40 and by the national cyberbeveili-gingsauthority, which is required by the authority, which is currently in force.

Afdeling 2. — Algemene bepalingen betreffende de inspectiondienst **Art. 44.** § 1. De

inspections of the national cyberbeveiligings-authority must be controlled by those who are essential in the event of an incident.

In this case, it is possible to see the sectoral surveillance over the wording of two controls that are currently being used, on the basis of the National Cyber Security Authority, of the possible inspection of the National Cyber Security Authority.

2o entities other than those referred to in 1o , regardless of whether or not they fall within the scope of this law, significant incidents, cyber threats and incidents avoided.

§ 2. The voluntary notifications referred to in paragraph 1 are treated in the same way as the mandatory notifications referred to in section 1 of this chapter.

Mandatory notifications may nevertheless be processed priority over voluntary notifications.

Without prejudice to the prevention, detection, investigation and prosecution of criminal offences, a voluntary report shall not have the direct effect of initiating an inspection referred to in Article 44 or of imposing on the reporting entity additional obligations to which it would not have been subject had it not submitted the notification.

TITLE 4. — *Supervision and sanctions*

CHAPTER 1. — *Supervision*

Section 1. — Periodic assessment of conformity

Art. 39. Essential entities shall submit to a periodic assessment of the conformity of the implementation of the cybersecurity risk management measures referred to in Article 30, based on the procedures and reference frameworks determined by the King:

1. Either by choosing a periodic assessment of conformity referred to in Article 40, on the basis of one of the reference frameworks determined by the King;

2. Or by submitting to an inspection by the national authority of cybersecurity, based on the terms determined by the King.

By way of derogation from paragraph 1, and at the request of the sectoral authority concerned, the inspections referred to in paragraph 1, 2o are carried out jointly, under the direction of the national cybersecurity authority or are delegated to the relevant inspection service with the agreement of the national cybersecurity authority.

When the King determines several frames of reference, the essential entities choose the frame of reference to which they submit.

Art. 40. § 1. The periodic assessment of conformity referred to in Article 39, paragraph 1, 1o is carried out by a conformity assessment body approved by the national cybersecurity authority according to the conditions set by the King.

For the control of entities identified as operators of critical infrastructure within the meaning of the law of 1 July 2011 and public administration entities, the conformity assessment body and the natural persons who assess conformity have security clearance.

§ 2. The inspection service of the national cybersecurity authority may at any time verify compliance with the approval conditions referred to in paragraph 1 by the conformity assessment bodies, in accordance with the provisions of this chapter.

Art. 41. Significant entities may, voluntarily, submit to a periodic assessment of the conformity referred to in Article 39, paragraph 1, 1o of the implementation of the cybersecurity risk management measures referred to in Article 30, § 3, on the basis of the terms and reference frameworks determined by the King.

Art. 42. Essential and important entities which submit to a periodic assessment of conformity referred to in Article 39, paragraph 1, 1o , respectively in accordance with Articles 39 and 41 are, until proven otherwise, presumed to comply with the obligations referred to in Article 30.

Art. 43. A list of conformity assessment bodies approved by the national cybersecurity authority in accordance with Article 40 is available from the national cybersecurity authority, which shall keep it up to date.

Section 2. — General provisions relating to the inspection service **Art. 44.**

§ 1. The inspection service of the national cybersecurity authority carries out checks on compliance by essential and important entities with cybersecurity risk management measures and incident reporting rules.

By way of derogation from paragraph 1, and at the request of the sectoral authority concerned, these checks are carried out jointly, under the direction of the national cybersecurity authority, or are delegated to the relevant inspection service with the agreement of the national cybersecurity authority.

De bevoegde sectorale overheid of sectorale inspectionienst of, indian geen sectorale inspectionienst is aangewezen door de wet of de Koning, de inspectionienst van de nationale cyberbeveiligingsautoriteit kan controls uitvoeren om na te gaan de essentiële en belangrijke entiteiten de bijkomende sectorale de Electorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in article 33 naleven.

The competent sectoral authority or sectoral inspection service, or, where no sectoral inspection service has been designated by law or by the King, the inspection service of the national cybersecurity authority may carry out checks on compliance by essential and important entities with the additional sectoral or sub-sectoral cybersecurity risk management measures referred to in Article 33.

§ 2. Bij het formularen van een verzoek om informatie of bewijzen vermelden of inspectioniedienst van de nationale cyberbeveiligings auto-riteit and of possible bevoegde sectorale overheid of sectorale inspec-tiedienst het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen Deze moeten worden verstrekt.

§ 2. When making a request for information or evidence, the inspection service of the national cybersecurity authority and any relevant sectoral authority or sectoral inspection service shall state the purpose of the request, the specific information or evidence requested and the time limit within which it must be provided.

De inspections of national cyber security authorities and possible sectoral inspections may be carried out by experts. § 3. De inspections of the national cyber security authority and possible sectoral inspections have priority

given to them in certain cases which may be subject to risk.

The National Cybersecurity Authority Inspectorate and any relevant sectoral authority or sectoral inspectorate may call upon experts. § 3. The National Cybersecurity Authority Inspectorate and any relevant sectoral authorities and sectoral

inspectorates may set priorities for the supervisory tasks referred to in this Title using a risk-based approach. § 4. When dealing with incidents giving rise to personal data breaches as defined in Article 4(12) of Regulation (EU) 2016/679, the National Cybersecurity Authority Inspectorate and any relevant sectoral authorities and sectoral inspectorates shall cooperate closely

§ 4. Bij de aanpak van incidenten die leiden tot inbreuken en verband met persoonsgegevens zoals definieerd in artikel 4, point 12), van Verordening (EU) 2016/679, werken de inspectionienst van de natio-nale cyberbeveiligingsautoriteit en de eventuele sectorale overheden en sectorale inspectionien-sten new samen met de gegevensbescherming-sautoriteiten, onverminderd de bevoegdheid en taken van deze laatsten.

with the data protection authorities, without prejudice to the competence and tasks of the latter.

Art. 45. § 1. De inspection of the national cyberbeveiligings-authority and possible sectoral oversight of sectoral inspections shall be carried out on July 1, 2011 by the authority of the authorities in Kennis where they are to be found. It is intended that the operator of the infrastructure should be wetted on July 1, 2011 and the infrastructure must be identified, which must be wetted. In the event of a sectoral overheid of sectoral inspections, you will be required to have the authority to inspect the national cyber security authority in advance. operator of an infrastructure that is identified by the infrastructure that is located on July 1, 2011.

Art. 45. § 1. The inspection service of the national cybersecurity authority and any relevant sectoral authority or sectoral inspection service shall inform the competent authorities under the Law of 1 July 2011 when they exercise their supervisory and enforcement powers with the aim of ensuring that an operator of an infrastructure identified as critical under the Law of 1 July 2011 complies with this Law. Where appropriate, the competent authorities under the Law of 1 July 2011 may request the inspection service of the national cybersecurity authority and any relevant sectoral authority or sectoral inspection service to exercise their supervisory and enforcement powers with regard to an operator of an infrastructure that is identified as critical infrastructure under the Law of 1 July 2011.

§ 2. De inspection of the national cyber security authority and possible sectoral inspections are subject to the relevant authority of the Verordening (EU) 2022/2554 of the European Parliament in December 14, 2022. digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verorde-ningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 in (EU) 2016/1011. De inspectioniedienst van de nationale cyberbeveiligingsautoriteit en de eventuale bevoegde sectorale over-heid of sectorale inspectionienst stellen met name het oversightforum dat is opgericht op grond van article 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbe-voegdheden uitoefenen Therefore, it is important to note that the essential parts of the product are 31 times larger than the previous ones, which are then stored in the ICT-diensten is aangewe-zen, voldoet aan deze wet.

§ 2. The National Cybersecurity Authority Inspectorate and any relevant sectoral authority or sectoral inspectorate shall cooperate with the relevant competent authorities under Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU)

2016/1011. In particular, the National Cybersecurity Authority Inspectorate and any relevant sectoral authority or sectoral inspectorate shall inform the oversight forum established under Article 32(1) of that Regulation when exercising their supervisory and enforcement powers to ensure that an essential or important entity that has been designated as a critical third-party ICT service provider under Article 31 of that Regulation complies with this Act.

Art. 46. § 1. Wanneer de netwerk- en informatiesystemen van een entity zich buiten het Belgische grondgebied bevinden, kunnen de inspectionient van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, in overleg met de nationale cyberbeveiligingsautoriteit, de bevoegde These are authorized by the authorities and are subject to the same conditions.

Art. 46. § 1. When the networks and information systems of an entity are located outside Belgian territory, the inspection service of the national cybersecurity authority and any competent sectoral authority or sectoral inspection service, in consultation with the national cybersecurity authority, may request the cooperation and assistance of the competent supervisory authorities of other Member States.

In this case, you can read it in this text:

1. the inspection of the national cyber security authority and possible sectoral inspections may be overridden by the authority to be authorized to do so;

In the context of the solicitation referred to in paragraph 1:

1. the inspection service of the national cybersecurity authority and the relevant sectoral authority or sectoral inspection service may request the competent supervisory authorities of other Member States to take supervisory or enforcement measures; 2. the inspection service of the national cybersecurity authority and the relevant sectoral authority or sectoral inspection service may request, in

2. The inspection of the national cyber security authority and possible sectoral inspections may be overridden by sectoral inspections to be authorized by the authorities and are subject to review by the authorities. handhavings are effective, efficient and consistent when you use the correct words.

a reasoned manner, the competent supervisory authorities of other Member States for mutual assistance so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

De wederzijdse bijstand bedoeld in het tweede lid, 2o , You can be trekking by checking the information on your website, including the inspections on site, by the elders of the beveiliging audits and by you. § 2. In order to be able to do so at any time in your life, we will be inspecting the national cyberbeveiliging

authority and possibly sectoral inspections over the course of the sectoral inspection even with the authority to comply with your cyberbeveiliging and lidstaten. Verlenen ze bijstand aan deze autoriteiten die daarom verzoeken, wanneer de netwerk- en informatiesystemen van de betrokken entiteit zich op Belgisch grondgebied bevinden.

In het kader van het verzoek bedoeld in het eerste lid: 1o centraliseert

de nationale cyberbeveiligingsautoriteit de informatie en raadplegingen met betrekking tot de toezichts- en handhavingsmaat-regelen die zijzelf de possible bevoegde sectorale overheid of sectorale inspectiondienst heeft genomen, en deelt deze mee aan of your authoritative authority bevoegd your cyberbeveiliging van andere lidstaten;

2o kan dit verzoek betrekking hebben op toezichts- of handhavings-maatregelen; 3o kan dit verzoek,

op een met redenen omklede wijze, betrekking hebben op wederzijdse bijstand, zodat de toezichts- of handhavings-maatregelen op een een effective, efficient in consistency wijze kunnen worden uitgevoerd.

De wederzijdse bijstand bedoeld in het tweede lid, 3o , You can be trekking by checking the information on your website, including the inspections on site, by the elders of the beveiliging audits and by you.

De autoriteit waaraan een verzoek om bijstand est gericht, mag dat verzoek niet weigeren, tenzij wordt vastgesteld dat zij niet bevoegd is om de gevraagde bijstand te verlenen, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van deze autoriteit, de het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indienne ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid de defensie van België.

Alvorens een dergelijk verzoek af te wijzen, raadpleegt voornoemde aurititeit de andere betrokken bevoegde auriteiten alsook, op verzoek van een van de betrokken lidstaten, de Europese Commissie en Enisa.

§ 3. De inspectionienst van de nationale cyberbeveiligingsautoriteit en de eventuale bevoegde sectorale overheid de sectorale inspectione-dienst kunnen en onderlinge overeenstemming gezamenlijke toezichts-acties uitvoeren, en dit onderling en/of met de bevoegde toezichthou-dende auriteiten van andere lidstaten.

§ 4. Dit artikel est niet van toepassing op diplomatieke en consular missies.

Art. 47. § 1. De leden van de inspectiondienst van de nationale cyberbeveiligingsautoriteit en van de eventuale bevoegde sectorale overheid of sectorale inspectiedienst beschikken over een legitimatie-kaart waarvan het model door de Koning wordt bepaald.

§ 2. De leden van de inspectionienst van de nationale cyberbeveili-gingsautoriteit en van de eventuale bevoegde sectorale overheid de sectorale inspectionienst en de experts deelnemen aan de inspec-tie, mogen geen enkel rechtstreeks de onrechtstreeks belang hebben en de ondernemingen de instellingen waarvoor zij met het toezicht belast zijn, waardoor hun objectiteit in het gedrang zou kunnen komen. Zij leggen de eed af bij de leidend ambtenaar van hun dienst.

De authoritéiten bedoeld in article 44, § 1, nemen de nodige maatregelen om, bij de uitvoering van hun taken, de onafhankelijkheid van hun personeelsleden te garanderen en om belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossesen.

Het begrip ÿbelangenconflictÿ heeft minstens betrekking op situaties waarin een personeelslid van de auriteiten bedoeld in artikel 44, § 1, rechtstreeks of onrechtstreeks financiële, economische de andere per-soonlijke belangen heeft die geacht kunnen worden zijn You can start and operate in the future. § 3. De personeelsleden van de authoriteiten bedoeld in article 44, § 1, krijgen noch vragen binnen de grenzen van hun bevoegdheden op direct of indirecte wijze

instructions van derden.

Het is hen verboden aanwezig te zijn een beraadslaging of besluit over files waarin zij een personlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met derde graad een personlijk of rechtstreeks belang hebben.

The mutual assistance referred to in paragraph 2, 2o , mayrelate to requests for information and control measures, including requests to carry out on-site inspections, remote controls or targeted security audits.

§ 2. In a manner proportionate to their resources and to the extent that this falls within the scope of their competences, the inspection service of the national cybersecurity authority and any competent sectoral authority or sectoral inspection service shall cooperate and provide assistance to the competent cybersecurity supervisory authorities of other Member States which so request, when the networks and information systems of the entity concerned are located in Belgian territory.

In the context of the request referred to in paragraph 1: 1. the

national cybersecurity authority shall centralise information and consultations concerning the supervisory and enforcement measures taken by itself, by any relevant sectoral authority and by any relevant sectoral inspection service and shall communicate them to the competent cybersecurity supervisory authorities of other Member States;

2. the said request may relate to supervisory or enforcement measures; 3. the said request may,

with reasons, relate to mutual assistance so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

The mutual assistance referred to in paragraph 2, 3o , mayrelate to requests for information and control measures, including requests to carry out on-site inspections, remote controls or targeted security audits.

The authority to which a request for assistance is addressed may refuse that request only if it is established that the said authority is not competent to provide the requested assistance, that the requested assistance is not proportionate to the supervisory tasks of the said authority or that the request concerns information or involves activities the disclosure or exercise of which would be contrary to the essential interests of national security, public security or the defence of Belgium. Before refusing such a request, the said authority shall consult the other competent authorities concerned and, at the request of one of the Member States concerned, the European Commission and

ENISA.

§ 3. By mutual agreement, the inspection service of the national cybersecurity authority and any competent sectoral authority or sectoral inspection service may carry out joint supervisory actions with each other and/or with the competent supervisory authorities of other Member States. § 4. This Article shall not apply to diplomatic and consular missions.

Art. 47. § 1. Members of the inspection service of the national cybersecurity authority and of any competent sectoral authority or sectoral inspection service are provided with a legitimation card, the model of which is set by the King.

§ 2. Members of the inspection service of the national cybersecurity authority and of any relevant sectoral authority or sectoral inspection service and experts called upon to participate in the inspection may not have any interest, direct or indirect, in the companies or institutions they are responsible for inspecting, which could compromise their objectivity. They shall take an oath before the leading official of their service.

The authorities referred to in Article 44, § 1, shall take the necessary measures to ensure the independence of their staff members and to prevent, identify and effectively resolve conflicts of interest when carrying out their tasks.

The concept of conflict of interest covers at least situations in which a member of staff of the authorities referred to in Article 44, § 1, has, directly or indirectly, a financial, economic or other personal interest which could be perceived as compromising his impartiality and independence in the context of his mission or functions.

§ 3. The staff members of the authorities referred to in Article 44, § 1, shall not receive or seek, within the limits of their responsibilities, directly or indirectly, instructions from third parties.

They are prohibited from being present during any deliberation or decision on matters in which they have a personal or direct interest or in which their relatives or relatives up to the third degree have a personal or direct interest.

De Koning kan ook andere situaties benoemen als belangen-conflicten.

Afdeling 3. — Het door de inspectiondienst uitgeoefende toezicht op de entiteiten **Art. 48.** §

1. It is important to note that the officer responsible for the policy is subject to article 8 of the Wetboek van Strafvor-dering beschikken de beschikken de beëdigde leden van de inspectioniedienst van de nationale cyberbeveiligingsautoriteit en de beëdigde leden van de eventuale bevoegde sectorale overheid de sectorale inspectiedienst bij of uitoefening van hun toezichtsopdracht over de volgende toezichts-bevoegdheden, en dit zowel in het kader van administratieve hande-lingen als in het kader van de vaststelling van inbreuken op deze wet:

1st you have to take all the documents of information that we do not know about the use of your information and your information, including the name of the verification of the cyber security, the results of the conformity and compliance audits of respect. onderliggende bewijzen;

2o overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor, met inbegrip van steekproefsgewijze controlse die worden uitgevoerd båartoe opgeleide professionals; 3o essential entity onderwerpen aan regelmatige

en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie, gebaseerd op door de betrokken inspectionienst de gecontroleerde entiteit verrichte risicobeoordelingen de op etere beschikbare risicogerelateerde informatie; 4o all the information inwinnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen maatregelen voor het beheer van

cyberbeveiligingsrisico's, met name betreffende het gedo-cumenteerde cyberbeveiligingsbeleid, de naleving van de verplichting om informatie in te dienen bij de nationale cyberbeveiligingsauthority of possible sectoral overheid overeenkomstig titel 1 en de uitvoering van deze wet; 5o een ad-hocaudit uitvoeren, met name in gevallen waarin dat gerechtvaardigd is vanwege een significant incident of een inbreuk op deze wet; 6o beveiligingsscans uitvoeren op base van objectieve, niet-discriminerende, eerlijke en transparent

risicobeoordelingscriteria, indian nodig in samenwerking met de betrokken entiteit;

7% of the identity of the person who is in the door of the entity that has been placed on it must be seen if it does not exist for the purpose of its operation. Please note that there are two people who have officially identified their documents;

8o in voorkomend geval, de bijstand vragen van de federale de locale politiediensten in het kader van het gebruik van geweld;

9o inwinnen informatie bij de personeelsleden bedoeld in article 9 van de wet van April 15, 1994 betreffende de bescherming van de volking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor
Nuclear Control, your operation should be handled by wet weather;

10o you should be aware of the fact that it is legally valid and that the entity has written its rights; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging est uitgereikt door de onderzoeksrechter. § 2. In het kader van deze inspection van belangrijke entiteiten worden de toezichtsbevoegdheden

bedoeld in paragraaf 1 achteraf (ÿex postÿ) uitgeoefend op base van bewijzen, aanwijzingen of informatie waaruit blijkt dat een belangrijke entiteit deze wet niet naleeft.

§ 3. If you wish to be aware of local authorities, you may be informed of the inspection of national cyber security authorities and possible sectoral inspections which may be overtaken by sectoral inspections. Dit verzoek bevat minstens de volgende gegevens: 1o de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben; 2o of possible inbreuken which you have already received; 3. All documents in the text must be taken into

account.

The best list of terms and conditions will be as long as possible. De beslissing van derzoeksrechter is met redenen omkleed. Bij gebrek aan een

The King may also designate other situations as conflicts of interest.

Section 3. — Supervision of entities by the inspection service

Art. 48. § 1. Without prejudice to the powers of judicial police officers referred to in Article 8 of the Code of Criminal Procedure, the sworn members of the inspection service of the national cybersecurity authority and the sworn members of any competent sectoral authority or sectoral inspection service have, in the exercise of their supervisory mission, the following control powers, both in the context of administrative procedures and in the context of the observation of violations of this law: 1o request access to and obtain a copy of any document or information necessary for the exercise of their supervisory mission, in particular evidence of the implementation of cybersecurity policies, such as the results of compliance

assessments or security audits or the corresponding underlying evidence;

2. carry out, on site or remotely, any examination, check and hearing, including random checks carried out by trained professionals;

3o subject essential entities to regular and targeted security audits carried out by an independent body, based on risk assessments carried out by the relevant inspection service or the audited entity, or on other available risk-related information; 4o request all information they consider necessary for the assessment of the cybersecurity risk management

measures adopted by the relevant entity, in particular the cybersecurity policies recorded in writing, compliance with the obligation to submit information to the national cybersecurity authority or any sectoral authority in accordance with Title 1 and the implementation of this Law;

5o carry out an ad hoc audit, in particular when it is justified due to of a significant incident or violation of this Act;

6o carry out security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, if necessary with the cooperation of the entity concerned; 7o take the identity of persons who are on the premises used by the entity

and whose hearing they consider necessary for the exercise of their mission. To this end, they may require these persons to present official identification documents;

8o if necessary, request assistance from the federal or local police services in the context of the use of force; 9o request information from the staff

members referred to in Article 9 of the Law of 15 April 1994 on the protection of the population and the environment against the dangers resulting from ionising radiation and relating to the Federal Agency for Nuclear Control, for the purposes of implementing the provisions of this Law; 10o enter without prior warning, upon presentation of their legitimation card, all the places used by the entity; they may only access inhabited premises with prior

authorisation issued by the investigating judge. § 2. In the context of the inspection of significant entities, the control powers referred to in paragraph 1 shall be carried out ex post, on the basis of evidence, indications or information according to which a significant entity is not complying with this

Law. § 3. To obtain authorization to enter inhabited premises, members of the inspection service of the national cybersecurity authority and of any sectoral authority or service

The competent sectoral inspection authorities shall send a reasoned request to the investigating judge. This request shall contain at least the following data:

1. the identification of the inhabited spaces to which they wish to have access; 2. any possible

breaches which are the subject of the control; 3. all documents and

information from which it appears that the use of this means is necessary.

The investigating judge shall decide within a maximum of forty-eight hours after receipt of the request. The investigating judge's decision shall be justified. In the absence of a decision within the time limit

Please note that the terms you wish to use will be correct. De inspection of the national cyber security authority of possible sectoral overheid of sectoral inspection can be established by weigeringsbe-slissing of het gebrek aan een beslissing bij de kamer van inbeschuldi-gingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewond localokalen zonder toestemming van de woner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiondienst die samen optreden. § 4. When the

word begins, the word will begin
Personally responsible:

1o dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2o dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd en de gebruikte bewoor-dingen; 3o dat

hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde person mag de documentsen in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor der later vragen om die documentsen bij het verhoor te voegen.

If the word is changed, it may be broken and it may also be necessary. The identity of a person who has passed away may be revealed.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen de het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren de er iets aan laten toevoegen.

From the inspection of the national cyber security authority to possible sectoral inspections, the inspection of the sector is subject to personal inspection, which means that it is possible to do so. Deze kopie wordt gratis verstrekt. § 5. De leden van de inspectionienst van de nationale cyberbeveili-gingsautoriteit

en van de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten de kopieën van nemen de vragen en een door hen gevraagde leesbare en verstaanbare vorm.

Indian het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiondienst van de nationale cyberbeveiligingsau-toriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, tegen een vangstbewijs dat een inventories bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen. § 6. Om de zoekactie in

een informaticasysteem of een deel hiervan die op base van paragraaf 5 werd opgestart uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiondienst van de nationale cyberbeveiligingsauthoritéit de eventuele bevoegde secto-rale overheid of sectorale inspectionienst een onderzoeksrechter vragen om opt te treden.

§ 7. Wanneer de inspectionient van de nationale cyberbeveiliging-sautoriteit de eventuele bevoegde sectorale overheid de sectorale inspectionienst er in het kader van het toezicht de handhaving kennis van krijgen dat de inbreuk door een een essentiële of belangrijke entity op de in de articles 30 en 34 tot 37 vast amounts of information are available in verband met persoonsgegevens in de zin van artikel 4, point 12, van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de gegevensbeschermingsautoriteiten daarvan onverwijld in Kennis.

Wanneer de bevoegde gegevensbeschermingsautoriteit in een andere lidstaat dan België gevestigd is, stelt de inspectionienst van de nationale cyberbeveiligingsautoriteit de eventuele bevoegde secto-rale overheid of sectorale inspectionienst de in België gevestigde bevoegde gegevensbeschermingsautoriteit in kennis van de in het eerste lid bedoelde potentiële inbreuk in verband met persoonsgege-
come.

§ 8. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit article zorgen de beëdigde leden van de authoriteiten bedoeld in artikel 44, § 1, ervoor dat de door he bruikte middelen passend en noodzakelijk zijn voor dit toezicht.

prescribed, the visit to the premises is deemed to be refused. The inspection service of the national cybersecurity authority or the relevant sectoral authority or sectoral inspection service may lodge an appeal against the decision to refuse or the absence of a decision before the indictments chamber within fifteen days of notification of the decision or the expiry of the deadline.

Visits without the occupant's permission to inhabited premises are made between 5 p.m. and 9 p.m. by at least two members of the inspection service acting jointly.

§ 4. At the start of any hearing, the person being questioned is informed: 1o that

their statements may be used as evidence in court; 2o that they may request

that all questions put to them
and the answers it gives are recorded in the terms used;

3rd that she has the right to remain silent and not to contribute to her self-incrimination.

Any person being questioned may use the documents in their possession, without this leading to the postponement of the hearing. They may, during the hearing or subsequently, require that these documents be attached to the hearing.

The hearing shall state precisely the time at which it began, was interrupted and resumed, and ended. It shall state the identity of the persons who spoke during the hearing or during any part of it.

At the end of the hearing, the person being questioned has the right to reread it or to request that it be read to them. They may request that their statements be corrected or supplemented.

The members of the inspection service of the national cybersecurity authority and of the relevant sectoral authority or sectoral inspection service who question a person shall inform them that they may request a copy of the text of their hearing.
This copy shall be issued to him free of

charge. § 5. The members of the inspection service of the national cybersecurity authority and of any competent sectoral authority or sectoral inspection service may consult all information media and the data they contain. They may have the computer system and the data it contains produced on site that they need for their examinations and findings, and take or request extracts, duplicates or copies free of charge, in a legible and intelligible form that they have requested.

If it is not possible to take copies on site, members of the inspection service of the national cybersecurity authority and of any relevant sectoral authority or sectoral inspection service may seize, against receipt containing an inventory, the computer system and the data it contains.

§ 6. To extend the searches in a computer system or part thereof, initiated on the basis of paragraph 5, to a computer system or part thereof which is located in a place other than that where the search is carried out, the inspection service of the national cybersecurity authority or the competent sectoral authority or sectoral inspection service may request the intervention of an investigating judge.

§ 7. Where the inspectorate of the national cybersecurity authority or the relevant sectoral authority or sectoral inspectorate becomes aware, in the course of supervision or enforcement, that a breach by an essential or important entity of the obligations set out in Articles 30 and 34 to 37 may give rise to a personal data breach within the meaning of Article 4(12) of Regulation (EU) 2016/679, which must be notified pursuant to Article 33 of that Regulation, they shall inform the data protection authorities without undue delay.

Where the competent data protection authority is established in a Member State other than Belgium, the inspection service of the national cybersecurity authority or the relevant sectoral authority or sectoral inspection service shall inform the competent data protection authority established in Belgium of the potential breach of personal data referred to in paragraph 1.

§ 8. When exercising their powers of control referred to in this article, the sworn members of the authorities referred to in Article 44, § 1, shall ensure that the means they use are appropriate and necessary for said control.

Art. 49. § 1. Na elke inspectione stellen delden van de inspectionienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectionient een verslag op en bezorgen ze daarvan een kopie aan de geïnspecteerde entity.

§ 2. From national cyberbeveiligingsauthority and from possible secto-ral overheid wesselen hun inspectionverslagen uit.

Art. 50. § 1. De entiteit waarop toezicht wordt uitgeoefend, verleent haar volledige medewerking aan de leden van de inspectioniedienst van de nationale cyberbeveiligingsautoriteit de van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informen over all bestaandbeveiligingsmaatregelen.

Indian nodig stelt de entiteit het nodige materiaal ter beschikking van de leden van de inspectioniedienst van de nationale cyberbeveiligingsau-toriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst, opdat ze de veiligheidsvoorschriften naleven tijdens de inspecties. § 2. De kosten van de inspectiones zijn niet ten laste van de entiteiten.

In the future, in the future, in the sector of the electorate, there is a vast influence in the Ministerial Administration and in the advice of the National Cyber Security Authority in the event of a sectoral overrun, and retributies must be paid to you for inspections. De Koning bepaalt de berekenings- en betalingsregels.

§ 3. Het feit dat iemand de uitvoering van een controle door de leden van de inspectioniedienst van de nationale cyberbeveiligingsautoriteit de van de eventuele bevoegde sectorale overheid of sectorale inspectione-dienst opzettelijk verhindert de belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee you delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door of beëdigde leden van de inspectioniedienst van de nationale cyberbeveiligingsautoriteit of van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst.

HOOFDSTUK 2. — *From administration to management and administration*

Afdeling 1. — Procedure **Art.**

51. § 1. Wanneer een de meer inbreuken op de eisen van deze wet, de uitvoeringsbesluiten ervan de eraan verbonden individuale administratieve beslissingen worden vastgesteld, kunnen de feiten opgetekend worden in een proces-verbaal door de beëdigde leden van de inspectioniedienst van de nationale cyberbeveiligingsautoriteit, van de eventuele sectorale inspectioniedienst de van de eventuele betrokken sectorale overheid, overeenkomstig artikel 44, § 1.

Mits de nationale cyberbeveiligingsautoriteit akkoord gaat, kan de sectorale overheid administratieve maatregelen en geldboetes als bedoeld in afdeling 2 opleggen aan een entity.

De nationale cyberbeveiligingsautoriteit informert de betrokken sectorale overheid wanneer zij overweegt om administratieve maatre-gelen en geldboetes als bedoeld in de articles 58 en 59 opt te leggen aan een entity.

Wanneer de authoriteiten bedoeld in het eerste en tweede lid er tijdens hun toezichtsopdracht kennis van krijgen dat een in het eerste of tweede lid bedoelde inbreuk door een essential of belangrijke entiteit een inbreuk in verband met persoonsgegevens zoals gedefinieerd in article 4, point 12), van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde gegevensbeschermingsautoriteiten daarvan onverwijld en kennis.

§ 2. Op basis van het in paragraaf 1 bedoelde proces-verbaal en, in voorkomend geval, van de relevante verslagen bedoeld in artikel 49, § 1, kan de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een ontwerp van beslissing opstellen dat minstens de referenties van het minutes dat of inbreuk vaststelt and of feiten beschrijft die aanleiding hebben gegeven tot de procedure, en een of meer overwogen administratieve maatregelen of geldboetes als bedoeld in article 58 en/of 59 bevat, alsook de termijn waarbinnen de betrokken entiteit de administratieve maatregelen to leave.

De in het eerste lid bedoelde termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de entiteit en de te nemen maatregelen. § 3. National cyber security authority of

possible sectoral action is overheid in paragraph 2 of which must be considered before the entity, with the motivation of overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te

Art. 49. § 1. After each inspection, the members of the inspection service of the national cybersecurity authority and of the relevant sectoral authority or sectoral inspection service shall draw up a report and send a copy to the inspected entity. § 2. The national cybersecurity authority and the relevant sectoral authority shall communicate their inspection reports to

each other.

Art. 50. § 1. The supervised entity provides its full cooperation to the members of the inspection service of the national cybersecurity authority and of any relevant sectoral authority or sectoral inspection service in the exercise of their functions and in particular to inform them as best as possible of all existing security measures.

If necessary, the entity shall provide members of the inspection service of the national cybersecurity authority and any relevant sectoral authority or sectoral inspection service with the necessary equipment so that they can comply with the security instructions during inspections.

§ 2. The costs of inspections are not charged to the entities.

By way of derogation from the preceding paragraph, the King may determine, by sector or sub-sector, by decree deliberated in the Council of Ministers and after consulting the national cybersecurity authority and any relevant sectoral authority, remuneration relating to inspection services. He shall set the terms of calculation and payment.

§ 3. Any person who willfully prevents or obstructs the execution of an inspection carried out by members of the inspection service of the national cybersecurity authority or of the relevant sectoral authority or sectoral inspection service, refuses to provide information requested during this inspection, or knowingly provides inaccurate or incomplete information shall be recorded in a report by the sworn members of the inspection service of the national cybersecurity authority or of the relevant sectoral authority or sectoral inspection service.

CHAPTER 2. — *Administrative measures and fines*

Section 1. — Procedure

Art. 51. § 1. When one or more breaches of the requirements imposed by this law, its implementing decrees or the individual administrative decisions relating thereto are observed, the facts may be noted in a report drawn up by the sworn members of the inspection service of the national cybersecurity authority, of the possible sectoral inspection service or of the possible sectoral authority concerned, in accordance with Article 44, § 1.

With the agreement of the national cybersecurity authority, the sectoral authority may impose on an entity administrative measures and fines referred to in Section 2.

The national cybersecurity authority shall inform the relevant sectoral authority when it intends to impose administrative measures and fines referred to in Articles 58 and 59 on an entity.

Where the authorities referred to in paragraphs 1 and 2 become aware, in the context of their supervisory duties, that a breach referred to in paragraph 1 or 2, committed by an essential or important entity, may give rise to a personal data breach within the meaning of Article 4(12) of Regulation (EU) 2016/679, which must be notified pursuant to Article 33 of that Regulation, they shall inform the competent data protection authorities without undue delay. § 2. On the basis of the report referred to in paragraph 1 and, where applicable, the relevant reports referred to in Article 49, § 1, the national cybersecurity authority or any competent

sectoral authority may draw up a draft decision containing at least the references of the report which notes the infringement and which relates the facts in respect of which the procedure is initiated and one or more administrative measures or fines referred to in Article 58 and/or 59 envisaged as well as the time limit within which the entity concerned would execute the administrative measures.

The time limit referred to in paragraph 1 is determined taking into account the operating conditions of the entity and the measures to be implemented.
artwork.

§ 3. The national cybersecurity authority or any competent sectoral authority shall send the draft decision referred to in paragraph 2 to the entity concerned, setting out, in detail, the reasons for the administrative measures and/or fines envisaged and informing it of its right, within thirty days of receipt of this information, to formulate its means of defence in writing or to request to be

dienen de te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In the end, the last word will be heard and you will not be able to do anything about it that will happen in the future and you will have to worry about it.

§ 4. If any entity has a verweer midddelen heeft kunnen aanvoeren, op het einde van de termijn bedoeld in paragraaf 3, eerste lid, of in het geval bedoeld in paragraaf 3, tweede lid, zal de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale over-heid het wep beslissing bedoeld in paragraph 2, eerste lid, handhaven, wijzigen of ervan afzien, rekening houdend met de entiteitscategorie waartoe de betrokken entiteit behoort, de verweer-middelen van deze laatste en de in article 54 bedoelde elementsen.

Art. 52. § 1. Indian de op grond van artikel 58, 1o tot 4o genomen , in 6th grade, handhavingsmaatregelen ondoeltreffend zijn, kan de natio-nale cyberbeveiligingsautoriteit of de eventuele bevoegde sectorale overheid een termijn vaststellen waarbinnen een essential entiteit wordt verzocht de Noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen de aan haar eisen te voldoen.

§ 2. Indian een essential entity geen gevolg geeft aan de maatregel(en) vermeld in de belissing bedoeld in artikel 51, § 4, stelt de auriteit die deze beslissing heeft genomen de feiten vast in een proces-verbaal.

§ 3. Op basis van het in paragraaf 2 bedoelde proces-verbaal stelt de nationale cyberbeveiligingsautoriteit of de eventuele bevoegde secto-rale overheid een ontwerp van beslissing op dat minstens een de meer overwogen administratieve maatregelen de geldboetes bedoeld in de artikelen 59 en/of 60 bevat.

§ 4. Of national cyberbelieving authority of possible sectoral action overheid in paragraph 3 bedoelde ontwerp van belissing naar de betrokken entity, met een gedetailerde motivatering voor de overwogen administratieve maatregelen en/of geldboetes, en laat haar weten dat zij Het recht heeft om, binnen dertig dagen na ontvangst van deze informatie, haar verweermiddelen schriftelijk in te dienen of your vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending van voormeld ontwerp van beslissing.

In the end, the last word will be heard and you will not be able to do anything about it that will happen in the future and you will have to worry about it.

§ 5. If any entity has to be verified, it may be used in accordance with the terms of reference in paragraph 4. Het in paragraph 3 bedoelde ontwerp van beslissing handhaven, wijzigen de ervan afzien, rekening houdend met de verweermiddelen van de trokken entiteit en de in article 54 bedoelde elementsen.

Art. 53. De processen-verbaal van de beëdigde leden van de inspection-tiedienst hebben bewijskracht tot het tegendeel is bewezen.

Art. 54. § 1. Bij het nemen van handhavingsmaatregelen in het kader van de in de articles 51 en 52 bedoelde procedures eerbiedigt de nationale cyberbeveiligingsautoriteit of de possible bevoegde secto-rale overheid de rechten van de verdediging, houdt zij rekening met de omstandigheden van elk Please note:

1o de in de articles 9 en 10 bedoelde category warartoe de betrokken entiteit behoort;

2o of ernst van de breuk en het belang van de geschonden bepalingen, waarbij onder meer het volgende in ieder geval een ernstige inbreuk vormt:

(a) heralde inbreuken; *b)* het

neet melden de niet verhelpen van significante incidentsen;

(c) he does not provide any assistance with the instructions given by the authorized authorities; *d)* het belemmeren van audits of monitoring activities iten

waartoe de inspectionienst van de nationale cyberbeveiligingsautoriteit of de possible bevoegde sectorale overheid of sectorale inspectionienst opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk;

of hearing. The information is presumed to have been received by the offender on the sixth day following the sending of the aforementioned draft decision.

By way of exception to paragraph 1, the draft decision is not sent in advance to the entity concerned in exceptional, duly justified cases where this would hinder immediate intervention to prevent or respond to an incident.

§ 4. After the entity concerned has been able to assert its means of defense, at the end of the period referred to in paragraph 3, subparagraph 1, or in the case referred to in paragraph 3, subparagraph 2, the national cybersecurity authority or any competent sectoral authority shall maintain or amend the draft decision referred to in paragraph 2, subparagraph 1 or waive it, taking into account the category of entity to which the entity concerned belongs, the latter's means of defense and the elements referred to in Article 54.

Art. 52. § 1. Where the implementing measures adopted pursuant to Article 58, 1o to 4o are ineffective, the national cybersecurity authority or any competent sectoral authority may and 6o, set a deadline within which an essential entity is invited to take the necessary measures to remedy the deficiencies or meet its requirements. § 2. Where an essential entity does not comply with the measure(s) contained in the decision referred to in Article 51, § 4, the authority

which took that decision shall record the facts in a report.

§ 3. On the basis of the report referred to in paragraph 2, the national cybersecurity authority or any competent sectoral authority shall draw up a draft decision containing at least one or more administrative measures or fines referred to in Articles 59 and/or 60 envisaged. § 4. The national cybersecurity authority or any competent sectoral authority shall send the

draft decision referred to in paragraph 3 to the entity concerned, setting out, in detail, the reasons for the administrative measures and/or fines envisaged and informing it of its right, within thirty days of receiving this information, to formulate its means of defence in writing or to request a hearing. The information shall be presumed to have been received by the offender on the sixth day following the sending of the aforementioned draft decision.

By way of exception to paragraph 1, the draft decision is not sent in advance to the entity concerned in exceptional, duly justified cases where this would hinder immediate intervention to prevent or respond to an incident.

§ 5. After the entity concerned has been able to assert its means of defense, at the end of the period referred to in paragraph 4, subparagraph 1, or in the case referred to in paragraph 4, subparagraph 2, the national cybersecurity authority or any competent sectoral authority shall maintain or amend the draft decision referred to in paragraph 3 or waive it, taking into account the means of defense of the entity concerned and the elements referred to in Article 54.

Art. 53. The minutes drawn up by the sworn members of the inspection service are authentic until proven otherwise.

Art. 54. § 1. When taking any enforcement measure in the context of the procedures referred to in Articles 51 and 52, the national cybersecurity authority or any competent sectoral authority shall respect the rights of the defence, take into account the circumstances specific to each case and, at a minimum, take due account of:

1. the category referred to in Articles 9 and 10 to which the entity concerned belongs; 2. the seriousness

of the violation and the significance of the provisions infringed, the following facts, inter alia, being considered in any event as serious: *a)* repeated violations; *b)* failure to notify significant incidents or to remedy

them; *c)* failure to remedy

deficiencies following binding instructions from the competent authorities;

(d) obstructing audits or control activities ordered by the inspection service of the national cybersecurity authority or the relevant sectoral authority or sectoral inspection service following the discovery of a breach;

e) het verstrekken van valse de heel onnauwkeurige informatie met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's de in titel 3 bedoelde melding van inciden-ten; 3o of duur van de inbreuk; 4o possible relevant eerdere inbreuken door de

betrokken entiteit;

5o Elke veroorzaakte material de immateriële schade, met inbegrip van elke financiële de economische schade, gevolgen voor etere diensten en het aantal getroffen gebruikers; 6o opzet of nalatigheid van de pleger van de inbreuk;

7o door de entity genomen maatregelen om de materiële de immateriële schade te voorkomen de te beperken; 8o de naleving van goedgekeurde

gedragscodes of goedgekeurde certificeringsmechanismen; 9o de mate waarin de aansprakelijk gesturelde natuurlijke

de rechtsper-sonen meewerken met de inspection van de nationale cyberbevei-ligingsautoriteit de met de eventuele bevoegde sectorale overheid de sectorale inspectiedienst. § 2. Indian de gegevensbeschermingsautoriteiten een administra-tieve geldboete opleggen op grond

van artikel 58, lid 2, point *i),* van Verordening (EU) 2016/679, legt de nationale cyberbeveiligingsautori-teit de eventuele bevoegde sectorale overheid geen administratieve Please note that the delivery date is correct and the order *of* the order is correct.

Art. 55. § 1. De in de articles 51 en 52 bedoelde beslissingen worden
You can then change the position by Kennis before overtaking.

§ 2. De administratieve geldboetes die worden opgelegd door een in article 51 of 52 bedoelde beslissing, moeten worden betaald binnen de zestig dagen na ontvangst van de in paragraaf 1 bedoelde aangete-kende zending.

These terms can be found in the functions of the administrative board.

De in het eerste lid bedoelde termijn wordt geacht in te gaan uiterlijk
zes dagen na de in paragraaf 1 bedoelde aangetekende zending.

§ 3. Wanneer een in article 51 of 52 bedoelde bedoelde beslissing een andere administratieve maatregel dan een administratieve geldboete oplegt, vermeldt deze belissing de termijn waarbinnen de maatregel moet worden uitgevoerd. § 4. De nationale cyberbeveiligingsautoriteit

en, desgevallend, de eventuele sectorale overheid wisselen hun in article 51 of 52 bedoelde beslissing uit.

Art. 56. § 1. Although the administrative entity is not in charge of the administration, it is not possible for the administration to be authorized to operate in the national cyberbeveiligingsauthority of the possible sectoral sectoral over-heid in the dwangbevel. uitvaardigen.

Het dwangbevelt uitgevaardigd door een wettelijke vertegen-woordiger van de nationale cyberbeveiligingsautoriteit de van de eventuele bevoegde sectorale overheid of door een daartoe gemachtigd personeelslid. § 2. Het dwangbevel wordt aan de overtreder bij

gerechtsdeurwaar-derexploot betekend. De betekening bevat een bevel om te betalen binnen achtenveertig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de belagrechter.

Het verzet est, op straffe van nietigheid, mit redenen omkleed. Het moet worden ingediend door middel van een dagvaarding van de nationale cyberbeveiligingsautoriteit de van de eventuele bevoegde sectorale overheid bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in item 50, tweede lid, en item 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuit-voerlegging hiervan, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak est gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

(e) the provision of false or manifestly inaccurate information relating to cybersecurity risk management measures or incident notifications provided for in Title 3;

3o the duration of the violation; 4o

any relevant previous violation committed by the entity concerned; 5o the material, bodily or

moral damage caused, including financial or economic losses, the effects on other services and the number of users affected; 6o whether the perpetrator of the violation acted deliberately or negligently; 7o the

measures taken by the entity to prevent or mitigate the

material, bodily or moral damage;

8o of the application of approved codes of conduct or mechanisms-approved certification measures;

9o the degree of cooperation with the inspection service of the national cybersecurity authority or with the possible sectoral authority or the possible sectoral inspection service competent of the natural or legal persons held responsible. § 2. Where the data protection authorities impose an administrative fine pursuant to Article

58(2)(i) of Regulation (EU) 2016/679, the national cybersecurity authority or the possible sectoral authority competent shall not impose an administrative fine for a violation arising from the same conduct as that which was the subject of an administrative fine pursuant to Article 58(2)(i) of that Regulation.

Art. 55. § 1. The decisions referred to in Articles 51 and 52 shall be notified to the offender by registered mail. § 2. Administrative

fines imposed by a decision referred to in Article 51 or 52 must be paid within sixty days of receipt of the registered mail referred to in paragraph 1.

This period may be increased depending on the amount of the fine.
administrative.

The period referred to in paragraph 1 is deemed to begin at the latest six days after the registered mail referred to in paragraph 1.

§ 3. Where a decision referred to in Article 51 or 52 imposes an administrative measure other than an administrative fine, that decision shall specify the time limit within which the measure must be executed.

§ 4. The national cybersecurity authority and, where applicable, any sectoral authority shall communicate to each other their decision referred to in Article 51 or 52.

Art. 56. § 1. Where the entity concerned fails to pay the administrative fine within the time limit, the decision to impose an administrative fine shall be enforceable and the national authority

cybersecurity or the relevant sectoral authority may issue a constraint.

The constraint is issued by a legal representative of the national cybersecurity authority or any competent sectoral authority or by a member of staff authorized for this purpose.

§ 2. The enforcement order is served on the offender by bailiff's writ. The service contains a demand to pay within forty-eight hours, under penalty of execution by seizure, as well as an accounting justification for the sums demanded and a copy of the enforcement order.

§ 3. The offender may file an objection to the constraint before the seizure judge.

The opposition must be justified, otherwise it will be null and void. It is made by means of a summons from the national cybersecurity authority or any competent sectoral authority served by bailiff's writ within fifteen days of service of the constraint.

The provisions of Chapter VIII of Part I of the Judicial Code are applicable to this period, including the extensions provided for in Article 50, paragraph 2, and Article 55 of this Code.

The exercise of opposition to the constraint suspends the execution of the latter, as well as the limitation period of the claims contained in the constraint, until a ruling has been made on its merits. Seizures already carried out previously retain their precautionary character.

§ 4. De nationale cyberbeveiligingsauthority of possible sectoral overheid mag bewarend beslag laten leggen en het dwangbe-vel uitvoeren met gebruikmaking van de middelen tot tenuitvoerleg-ging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

Deferred betalingen gedaan ingevolge de betekening van een
Please note that you do not have to worry about any changes.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging van bewarende maatregelen zijn ten laste van de overtreder.

These words should be taken into account when they are taken into account.
gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 57. You will be able to see all the details you need to know. Verjaring wordt alleen gestuit door onderzoekshandelingen de vervol-ging een inspectiedienst. Deze handelingen doen een new period van gelijke duur lopen, zelfs ten aanzien van personen die net betrokken zijn.

De adminstratieve maatregelen de geldboetes verjaren vijf jaar na de datum waarop ze ten uitvoer moeten worden gelegd. De verjaringster-mijn wordt geschorst in geval van beroep tegen de administratieve beslissing.

Afdeling 2. — Administratieve maatregelen en geldboetes **Art. 58.**

Administrative decisions are taken into account in accordance with the terms of article 51: 1 .

entities on this site;

2o bindende aanwijzingen vaststellen de een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen de inbreuken op deze wet te verhelpen;

3o de betrokken entiteiten gelasten een einde te maken aan gedra-gingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;

4o de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met titel 3 de voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel; 5o de betrokken entiteiten gelasten de natuurlijke de

rechtspersonen aan wie zij diensten verlenen of your wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de reiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtsper-sonen kunnen nemen als reactie op die dreiging; 6o de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit voeren;

7% of the liquids are frozen in appearance when they are soaked and wet and then they should be handled openly; 8o Wanneer de betrokken entiteit

een essential entiteit est, een controle functionsaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor het beheer van cyberbeveiligingsrisico's and inzake het melden van incidents bedoeld in title 3.

Wanneer de betrokken entiteit een essential entiteit est, omvatten de bindende aanwijzingen bedoeld in het eerste lid, 2o ook de maatrege-len die nodig zijn om een incident te voorkomen de te verhelpen, alsmede uiterste termijnen voor de uitvoering van dergelijke maatre-gelen en voor verslaggeving over de uitvoering ervan.

Art. 59. De volgende administratieve geldboetes kunnen aan titei-ten worden opgelegd op base van article 51 of 52: 1o eenieder die niet voldoet aan de in article 12 bedoelde

rapport-tageverplichtingen wordt bestraft met een geldboete van 500 tot 125,000 euro;

2. If you are an entity you choose to have your hands full, you will be able to take advantage of the transport, you can find it in the order of your vehicle, it will be possible to transport it in wet weather, the best price is between 500 and 200,000. euro; eenieder die niet voldoet aan de ze titel bedoelde toezichtverplichtingen wordt bestraft met een geldboete

3o onverminderd article 48, § 4, eerste lid, 3o , van 500 tot 200,000 euro;

4o een belangrijke entity die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen bedoeld in titel 3, wordt bestraft

§ 4. The national cybersecurity authority or any competent sectoral authority may carry out the precautionary seizure and enforce the constraint using the enforcement procedures provided for in Part Five of the Judicial Code.

Partial payments made following the service of a
constraint does not prevent the continuation of proceedings.

§ 5. The costs of serving the order as well as the costs of execution or precautionary measures shall be borne by the offender.

They are determined according to the rules established for the acts performed by bailiffs in civil and commercial matters.

Art. 57. Acts are prescribed three years after their commission. The limitation period is interrupted only by acts of investigation or prosecution by an inspection service. These acts start a new period of equal duration, even with regard to persons who are not involved in them.

Administrative measures or administrative fines are subject to a limitation period of five years from the date on which they are to be executed. The limitation period is suspended in the event of an appeal against the administrative decision.

Section 2. — Administrative measures and fines

Art. 58. The following administrative measures may be imposed on entities on the basis of Article 51:

1. issue warnings regarding violations of this
law by the entities concerned;

2. adopt binding instructions or an injunction requiring the entities concerned to remedy the deficiencies noted or the violations of this law; 3. order the entities concerned to put an end to a

conduct that violates this law and not to repeat it;

4. order the entities concerned to ensure that their cybersecurity risk management measures comply with Title 3 or to comply with the incident notification obligations set out in the same title, specifically and within a specified timeframe; 5. order the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities

likely to be affected by a significant cyber threat of the nature of the threat, as well as of any preventive or remedial measures that these natural or legal persons could take in response to this threat;

6o order the entities concerned to implement the recommendations made following a security audit within a reasonable time; 7o order the entities concerned to make public the aspects of

violations of this Act in a specific manner;

8o where the entity concerned is an essential entity, designate, for a specified period, a control officer with clearly defined tasks to supervise compliance by the entities concerned with the cybersecurity risk management and incident notification measures referred to in Title 3.

Where the entity concerned is an essential entity, the binding instructions referred to in paragraph 1, 2o also concern the measures necessary to avoid or remedy an incident, as well as the deadlines for implementing these measures and reporting on this implementation.

in operation.

Art. 59. The following administrative fines may be imposed on entities on the basis of Article 51 or 52:

1. Anyone who fails to comply with the regulations shall be punished with a fine of 500 to 125,000 euros.
does not comply with the information obligations referred to in Article 12;

2o any entity that causes negative consequences to a person acting on its behalf as a result of the execution, in good faith and within the scope of its functions, of the obligations arising from this law shall be punished with a fine of 500 to 200,000 euros; 3o

without prejudice to Article 48, § 4, paragraph 1, 3o, anyone who fails to comply with the control obligations referred to in this title shall be punished with a fine of 500 to 200,000 euros;

4o is punishable by a fine of 500 to 7,000,000 euros or 1.4 percent of the total worldwide annual turnover of the previous financial year of the company to which the significant entity belongs, whichever is the greater.

met een geldboete van 500 tot 7,000,000 euro van 1.4 per cent van de totale wereldwijde jaaromzet in het voorgaande boekjaar van derneming waartoe de belangrijke entiteit behoort, afhankelijk van welk bedrag het hoogst est; 5o an essential entity that does not have to be transferred and has to

be paid for by the cyber security risk's en/of a reporting report on the basis of title 3, the best price is 500 to 10,000,000 euros of 2 percent The total package was already in the right place, and it is important to know that it is the correct item for you to use.

high being retained, the significant entity which does not comply with the obligations relating to cybersecurity risk management measures and/or incident notification referred to in Title 3;

5o shall be punished by a fine of 500 to 10,000,000 euros or 2 percent of the total worldwide annual turnover of the previous financial year of the company to which the essential entity belongs, whichever is the higher, the essential entity which does not comply with the obligations relating to cybersecurity risk management measures and/or incident notification referred to in Title 3.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jar.

The administrative fine is doubled in the event of a repeat offense for the same facts within three years.

De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

The combination of several breaches may give rise to a single administrative fine proportional to the seriousness of all the facts.

Art. 60. Indian de gevraagde maatregelen niet binnen de gestelde termijn n worden ondernomen, kunnen an essential entity op grond van artikel 52 de volgende administratieve maatregelen worden opgelegd: 1o de nationale cyberbeveiligingsautoriteit verzoeken een certifice-ring

de vergunning You should also choose to be trekking early and this is one of the relevant activities of the trekking entity.

Art. 60. If the requested measures are not taken within the specified time limit, the following administrative measures may be imposed on essential entities on the basis of Article 52:

1. request the national cybersecurity authority to temporarily suspend a certification or authorization concerning all or part of the relevant services provided or relevant activities carried out by the entity concerned;

2o een natuurlijke persoon met leidinggevende verantwoordelijkhe-den op het-level van de algemeen director of de wettelijke vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leiding-gevende functions in the entity it uit oefenen.

2. temporarily prohibit any natural person exercising managerial responsibilities at the level of general manager or legal representative in the entity concerned from exercising managerial responsibilities in this entity.

De in het eerste lid bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen de te voldoen aan de vereisten van de bevoegde autoriteit die deze handhavingsmaatregelen heeft opgelegd.

The temporary suspensions or prohibitions referred to in paragraph 1 shall only be applied until the entity concerned has taken the necessary measures to remedy the deficiencies or comply with the requirements of the competent authority which initiated the application of these implementing measures.

Art. 61. Elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiale of een belangrijke entity op basis van de bevoegdheid om deze te vertegen-woordigen, de bevoegdheid om names deze entity beslissingen te nemen of de Bevoegdheid om controle uit te oefenen op deze entityit, heeft de bevoegdheid om ervoor te zorgen dat deze entity deze wet nakomt. Deze personen zijn aansprakelijk yor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze wet.

Art. 61. Any natural person responsible for a critical or important entity or acting as a legal representative of a critical or important entity based on the authority to represent it, make decisions on its behalf or exercise control over it has the authority to ensure that the entity complies with this Act. Such persons are liable for breaches of their duty to ensure compliance with this Act.

Said article does not include any of the following regulations that have been taken into account for overheids of instants, but also for ambtenaren en verkozen of benoemde overheidsfunctionarissen.

This Article is without prejudice to the rules on liability applicable to public institutions, as well as the liability of civil servants and elected or appointed officials.

TITLE 5. — *Specify the handling of overheidsectors*

TITLE 5. — *Provisions specific to the public administration sector*

Art. 62. De adminstratieve maatregelen en geldboetes bedoeld in de articles 59 en 60 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidsector.

Art. 62. The administrative measures and fines referred to in Articles 59 and 60 do not apply to entities within the public administration sector.

Art. 63. § 1. De Koning wordt gemachtigd een auriteit aan te wijzen als conformiteitsbeoordelingsinstantie voor alle de een deel van de overheidsinstanties.

Art. 63. § 1. The King is empowered to designate an authority as a conformity assessment body for all or part of the entities of the public administration. § 2. The authority referred to in paragraph 1 is

§ 2. De in paragraaf 1 bedoelde auriteit wordt erkend door de nationale cyberbeveiligingsautoriteit, volgens de door de Koning bepaalde modaliteiten, om de in article 39, eerste lid, 1o bedoelde regelmatige conformiteitsbeoordeling uit voeren.

approved by the national cybersecurity authority, in accordance with the procedures laid down by the King, in order to carry out the periodic conformity assessment referred to in Article 39, paragraph 1, 1o The approval referred to in paragraph 1 relates to one or more of the .

De in het eerste lid bedoelde erkenning heeft betrekking op een de mer van de in article 39 bedoelde referentiekaders.

frameworks of reference referred to in Article 39.

Art. 64. De inspectionienst van de nationale cyberbeveiligingsautori-teit de, in voorkomend geval, de sectorale inspectiedienst die Door de Koning est aangewezen voor de overheidssector, est bij de uitvoering van zijn toezichthoudende taken operationeel onafhankelijk van de over-heidsinstanties waarop hij toezicht houdt.

Art. 64. The inspection service of the national cybersecurity authority or, where applicable, the sectoral inspection service designated by the King for the public administration sector exercises its supervisory tasks while enjoying operational independence from the supervised public administration entities.

Art. 65. Article 47 is subject to inspection by article 64.

Art. 65. Article 47 is applicable to the inspection service referred to in Article 64.

TITLE 6. — *Verwerking van persoonsgegevens*

TITLE 6. — *Processing of personal data* CHAPTER 1. — *Principles*

HOOFDSTUK 1. — *Beginselen betreffende de verwerking* **Art. 66.**

relating to processing **Art. 66.** The definitions of Regulation

De definities van Verordening (EU) 2016/679 zijn van toepassing op deze titel.

(EU) 2016/679 apply to this Title.

Art. 67. De Verwerking van Persoonsgegevens vandt plaats voor de following documents:

Art. 67. The purposes for which personal data processing is carried out are as follows:

1o de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsinciden-ten en de bescherming tegen cyberdreigingen;

1o the improvement of cybersecurity through the search for an

increased level of protection of networks and information systems, the strengthening of prevention and security policies, the prevention of security incidents and defense against cyber threats;

2o de uitvoering van de uitvoering van de taken van de nationale cyberbeveiligings au-toriteit, met name het identificeren van de entiteiten, het informen en sensitien en van de gebruikers van informatie- en communicaties systems-temen, het toekennen van subsidies, de international samenwerking tussen de la nationale cyberbeveiligingsautoriteit, de bevoegde auritei-ten van andere lidstaten, international fora for cyberbeveiliging, Enisa en de Europese Commissie;

3o het beheer van cybercrises en cyberbeveiligingsincidenten;

4o of uitvoering taken by the national CSIRT bedoeld in de volgende articles: *a)* 19, § 1;

b) 21, §

2, tweede lid, 1o tot 3o ; *c)* 22,

§ § 2 to 6; *d)* 37,

§ § 1 to 3 in § 5; 5o de

samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overhe-den, het NCCN en de auriteiten die bevoegd zijn in het kader van de wet van 1 Juli 2011, alsook de auriteiten bedoeld in article 25, § 2, in het kader van de uitvoering van deze wet en de wet van 1 juli 2011;

6o of samenwerking which is essential in all its components and authoritative bedoeld in title 2, hoofdstuk 1;

7 % of the information provided by the authoritative authorities

Article 25, § 5;

8° of continuity of maintenance of essential entities; 9o het melden van incidents en bijna-

incidenten; 10% of control is essential in all aspects,

as well as in planning, organization, and administration.

Art. 68. De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:

1o voor het doeleinde bedoeld in article 67, 1o : de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in article 2, 91o van de wet van 13 June 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyber-dreigingen bedoeld in article 67, 1o ; 2o voor het doeleinde

bedoeld in article 67, 2o : de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in article 2, 91o van de wet van 13 June 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsauthorityit;

3o you can do it in article 67, 3o : de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in article 2, 91o van de wet van 13 juni 2005, van de personen die betrokken zijn bij cybercrises en cyberbeveilingsincidents;

4o voor het doeleinde bedoeld in article 67, 4o : de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in article 2, 91o van de wet van 13 June 2005, en elektronische-communicatiemetagegevens als bedoeld in article 2, 93o , from before-noemde wet van 13 June 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT; 5o

for the doeleinde bedoeld in article 67, 5o : de identificatiegege-vens van de personen die betrokken zijn bijn de samenwerking in het kader van de wet van 1 juli 2011;

6o voor het doeleinde bedoeld in article 67, 6o : de identificatiegege-Vens van de personen die betrokken zijn bij de samenwerking;

7o you can be found in article 67, 7o : de identificatiegege-vens van de personen die betrokken zijn bijn het delen van informatie; 8o you have the

right to read in article 67, 8o : de identificatiegege-vens van de personen die betrokken zijn bijn het waarborgen van de continuïteit van de servilening; 9o voor het doeleinde bedoeld in article

67, 9o : de identificatie-, verbindings-, locatie- en elektronische-communicatiegegevens als bedoeld in article 2, 91o van de wet van 13 June 2005, van de personen die betrokken zijn bij de melding;

10o voor het doeleinde bedoeld in article 67, 10o : de persoonsgege-vens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controls, dit toezicht of dese sancties.

2o the execution of the tasks of the national cybersecurity authority, in particular the identification of entities, information and awareness-raising of users of information and communication systems, the granting of subsidies, international cooperation between the national cybersecurity authority, competent authorities of other Member States, international cybersecurity forums, ENISA and the European Commission;

3o the management of cyber crises and cybersecurity incidents; 4o the execution

of the tasks of the national CSIRT referred to in the following articles:

a) 19, § 1;

b) 21, § 2, paragraph 2, 1o

to 3o ; *c)* 22, §

§ 2 to 6; *d)* 37, § § 1 to

3 and § 5; 5o cooperation, in particular the exchange of information between the national cybersecurity authority, any sectoral authorities, the NCCN and the competent authorities within the framework of the law of July 1 , 2011, as well as the authorities referred to in Article 25, § 2, within the framework of the execution of this law and the law of July 1 , 2011;

6o cooperation between essential and important entities and the authorities referred to in Title 2, Chapter 1; 7o sharing of information

between the authorities referred to in Article 25, § 5; 8o continuity of services provided by

important or essential entities; 9o notification of incidents and avoided incidents; 10o control and

supervision of essential and important entities, as well as the

preparation, organization, management and monitoring of administrative measures and fines.

Art. 68. The categories of personal data processed by the data controllers are as follows: 1o for the purpose referred to in Article

67, 1o : identification, connection, location and electronic communications data within the meaning of Article 2, 91o of the law of 13 June 2005, of persons concerned by the missions of improving cybersecurity, strengthening prevention and security policies, preventing security incidents and defending against cyber threats referred to in Article 67, 1o ;

2o for the purpose referred to in Article 67, 2o : identification, connection, location and electronic communications data within the meaning of Article 2, 91o of the law of June 13, 2005, of persons concerned by the execution of the tasks of the national cybersecurity authority;

3o for the purpose referred to in Article 67, 3o : identification, connection, location and electronic communications data within the meaning of Article 2, 91o of the law of June 13, 2005, of persons affected by cyber crises and cybersecurity incidents;

4o for the purpose referred to in Article 67, 4o : identification, connection, location, electronic communications data within the meaning of Article 2, 91o of the law of June 13, 2005 and electronic communications metadata within the meaning of Article 2, 93o of the aforementioned law of June 13, 2005, of the persons concerned by the execution of the tasks of the CSIRT;

5o for the purpose referred to in Article 67, 5o : the identification data of the persons concerned by the cooperation within the framework of the law of July 1 , 2011;

6o for the purpose referred to in Article 67, 6o : identification data persons concerned by the cooperation;

7o for the purpose referred to in Article 67, 7o : identification data persons concerned by the sharing of information;

8o for the purpose referred to in Article 67, 8o : the identification data of the persons concerned by the assurance of continuity of services;

9o for the purpose referred to in Article 67, 9o : identification, connection, location and electronic communications data within the meaning of Article 2, 91o of the law of 13 June 2005, of the persons concerned by the notification exercise; 10o for the purpose referred to in

Article 67, 10o : personal data necessary and relevant to the exercise of control, supervision and sanction missions, of the persons concerned by these controls, this supervision or these sanctions.

Art. 69. From people to different categories
Personen can be used to do so:

1o of personen die rechtstreeks deelnemen aan de opdrachten der krachtens titel 2 zijn toevertrouwd aan de nationale cyberbeveiliging-sautoriteit; 2o de personen bedoeld in het kader van de

verplichtingen voor
essential in the following categories: title 3;

3o de personen die betrokken zijn bij een incident; 4o de personen

die rechtstreeks betrokken zijn bij het toezicht, de control en de sancties bedoeld in titel 4.

Art. 70. De volgende entiteiten zijn verantwoordelijk voor de verwer-kingen die zij uitvoeren voor de verwezenlijking van de doeleinden bedoeld in article 67:

1o of national cyberbeveiligingsauthority; 2o het NCCN;

3o of possible

sectoral overheid; 4o of possible sectoral

inspection; 5 % of essential ingredients; 6o of entities

of the domeinnaamregistratiediensten verlenen;

7o of authoritative authority in article 23, § 1, 6o .

HOOFSTUK 2. — *Bewaarttermijn* **Art. 71.**

Verwerkingsverantwoordelijke bewaart de persoonsgege-vens die verwerktt worden en het kader van deze deze wet bedoelde

Verwerkingen om de doeleinden bedoeld in article 67 te realiseren, verminderd eventuale beroepsprocedures, gedurende vijf jaar na afloop van de laatste verwerking en maximaal gedurende tien jaar na de eerste verwerking.

HOOFDSTUK 3. — *Beperking van de rechten van de betrokkenen* **Art. 72.** § 1.

Met toepassing of article 23.1, point *a)* tot *e)* en *h),* van Verordening (EU) 2016/679 worden sommige verplichtingen en rechten van deze verordening beperkt de uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de fundamen-tele rechten en vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel. § 2. From articles 12 to 16, 18 to 19, you will not be able to read the wording before you enter the article 67. These articles are extensive and can

be used for your control, and you need to know how to use them.

,

§ 3. De vrijstelling geldt voor de categorieën van persoonsgegevens bedoeld in article 68, 10o . Deze vrijstelling geldt ook ook voorberei-dende werkzaamheden de procedures met het oog op de eventuale passing van een administratieve sanctie.

§ 4. De vrijstelling geldt enkel voor de periode tijdens dewelke de betrokkene onderworpen est aan een controle, toezicht de voorberei-dende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit article bedoelde afwijking nadelig zou If your control is concerned, it should be noted that the controls you need are used. In this case, it is possible to take maximum control and control to avoid any possible damage.

De duur van de voorbereidende werkzaamheden bedoeld in het
In this case, you should be aware of the fact that in this paragraph 2 articles are not included in the article, it is necessary to maximize the maximum number of articles that are available.

§ 5. De verwerkingsverantwoordelijke die niet voldoet aan alle bepalingen van deze titel en met name van article 73, kan geen gebruik maken van de vrijstelling.

Art. 73. § 1. De betrokken verantwoordelijke verleent de betrokkene toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze mededeling de verwezenlij-king van de doelstellingen van deze wet niet in het gedrang brengt.
Hierbij moet het voor de betrokkene onmogelijk zijn om na te gaan de hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde If you die in the first place, it will stop.

Art. 69. The categories of persons whose personal data may be processed are as follows:

1o persons directly participating in the missions entrusted to
the National Cybersecurity Authority under Title 2;

2. persons covered by the obligations incumbent on entities
essential and important under Title 3;

3o persons involved in an incident; 4o persons directly

involved in the exercises of
supervision, control and sanction, referred to in Title 4.

Art. 70. The following entities are responsible for the processing they carry out to achieve the purposes referred to in Article 67:

1o the national cybersecurity authority; 2o
the NCCN;

3o any sectoral authority; 4o any

sectoral inspection service; 5o essential and

important entities; 6o entities providing

domain name registration services; 7o the authorities referred to in Article 23, § 1,

6o .

CHAPTER 2. — *Retention period*

Art. 71. Personal data processed within the framework of the processing referred to in this law in order to achieve the purposes provided for in Article 67, are kept, without prejudice to possible appeals, by the data controller for five years after the end of the last processing carried out and a maximum of ten years after the first processing carried out.

CHAPTER 3. — *Limitation of the rights of data subjects* **Art. 72.** § 1. Pursuant

to Article 23.1, points *(a)* to (e) and *(h),* of Regulation (EU) 2016/679, certain obligations and rights provided for by that Regulation are limited or excluded, in accordance with the provisions of this Chapter. These limitations or exclusions may not prejudice the essence of fundamental rights and freedoms and must be applied to the extent strictly necessary for the purpose pursued.

§ 2. Articles 12 to 16, 18 and 19 of the said regulation shall not apply to the processing of personal data carried out by an authority referred to in Article 15 for the purpose referred to in Article 67, 10o to the extent that the exercise of the rights enshrined in those articles would be detrimental to the needs of control, supervision or acts preparatory to it.

§ 3. The exemption applies to the categories of personal data referred to in Article 68, 10o . This exemption also applies to preparatory acts or to procedures aimed at the possible application of an administrative sanction.

§ 4. The exemption shall apply only during the period in which the person concerned is subject to control, supervision or acts preparatory thereto, to the extent that the exercise of the rights subject to the exemption referred to in this Article would harm the needs of the control, supervision or acts preparatory thereto and, in any case, shall apply only up to one year after the start of control, supervision or acts preparatory thereto.

The duration of the preparatory acts referred to in paragraph 1, during which the articles referred to in paragraph 2 are not applicable, may not exceed one year from the receipt of a request relating to the application of one of the rights enshrined in these articles.

§ 5. The data controller who does not comply with all the provisions of this Title and in particular Article 73, cannot benefit from the exemption.

Art. 73. § 1. The data controller concerned shall give the data subject access to limited information concerning the processing of his or her personal data, provided that such communication does not compromise the achievement of the objectives of this law and in such a way that the data subject is unable to know whether he or she is the subject of an investigation or not, and without being able under any circumstances to rectify, erase, limit, notify, transmit to a third party personal data, or cease any form of processing of said data which is necessary within the framework defined above.

§ 2. De maatregel betreffende de weigering de beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, moten opgeheven: 1o voor maatregelen die gerechtvaardigd zijn door de

verplichtingen inzake het melden van incidenten, bij het afsluiten van de verwerking van een incident door de authoriteiten bedoeld in de articles 34 en 38; 2. Before you leave the emergency door, check it out: 4, when it comes to control, you have to wait for the inspection

door, also during the period when it is possible to overload the sector after the inspection. zijn van de inspectioniedienst met het oog op vervolging; 3o uiterlijk één jaar na ontvangst van het verzoek dat is ingediend overeenkomstig de artikelen bedoeld in artikel 72, § 2, behalve indienne een controle de toezicht loopt.

§ 3. De betrokken verwerkingsverantwoordelijke heft de maatregel betreffende de weigering de beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in artikel 72, § 2, ook op zodra deze maatregel niet meer nodig is voor het nakomen van een van de doeleinden bedoeld in article 67.

§ 4. In all the passages of paragraphs 2 and 3, you will be informed of the functions you need to be aware of the possible operation of the equipment.

HOOFSTUK 4. — *Beperkingen inzake of verplichte melding van inbreuken in verband met persoonsgegevens* **Art. 74.** De betrokken

verwerkingsverantwoordelijke is vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een de meer welbepaalde betrokkenen, in de zin van artikel 34 van Verordening EU 2016/679, mits toestemming van de nationale cyber-beveiligingsautoriteit, You have two individual decisions to be taken into account in article 72, § 2, in which we refer you to the article 72, § 2.

TITLE 7. — *Slotbepalingen*

HOOFSTUK 1. — *Overgangsbepaling* **Art. 75.**

De Koning stelt de termijnen en vast waarbinnen en essentiële entiteiten un eerste regelmatige conformiteitsbeoordelingen bedoeld in article 39 uitvoeren.

HOOFSTUK 2. — *Wijzigingsbepalingen*

Afdeling 1. — Wijzigingen van de wet van April 15, 1994 betreffende de bescherming van de volking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle **Art. 76.** In article 1 of the wet on April 15, 1994, it will be tested by the

Federal Agency for Nuclear Control, which will be transferred to the wet on February 7. 2024, worden de woorden ÿ- ÿde wet van 7 april 2019ÿ: 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;ÿ vervangen door de woorden ÿ- de NIS2-wet: de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;ÿ.

Art. 77. In hoofdstuk III, afdeling 1, van dezelfde wet wordt arti-kel *15ter,* ingevoegd bij de wet van 7 April 2019, vervangen als volgt: ÿArt. *15ter.* Het Agentschap wordt

aangewezen als sectorale inspection-tiedienst, in de zin van de NIS2-wet, voor de sector energie, wat betreft de bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's die van toepassing zijn op de elementen van een nuclear installationatie bestemd voor de industriële productie van Electricity is due to your electrical transmission.

De Koning bepaalt de practische inspectione modaliteiten, na advies from the Agency.ÿ

Afdeling 2. — Wijzigingen van de wet van 22 February 1998 tot vaststelling van het organiek statutut van de Nationale Bank van België **Art. 78.** In article 36/1 on February

22, 1998, the vast majority of the articles of the National Bank of Belgium were published on December 20, 2023, and were announced on December 20, 2023. ÿ28o ÿ NIS2-wetÿ: from April 26, 2024 to the vast majority of information about cyber security and network intelligence;

§ 2. The measure of refusal or limitation of the rights enshrined in the articles referred to in Article 72, § 2, must be lifted:

1. for measures justified by incident notification obligations, upon closure of the processing of an incident by the authorities referred to in Articles 34 and 38;

2o for measures justified by the obligations under Title 4, upon closure of the control, supervision or preparatory acts for these carried out by the inspection service, as well as during the period during which the possible sectoral authority processes the documents coming from the inspection service with a view to carrying out proceedings; 3o at the latest one year from receipt of the request submitted pursuant to the articles referred to in Article 72, § 2, unless

a control or supervision is in progress.

§ 3. The data controller concerned shall also lift the measure of refusal or limitation of the rights enshrined in the articles referred to in Article 72, § 2, as soon as such a measure is no longer necessary to comply with one of the purposes referred to in Article 67.

§ 4. In all cases of application of paragraphs 2 and 3, the data protection officer shall inform the person(s) concerned in writing of the lifting of the refusal or limitation measure.

CHAPTER 4. — *Limitations to the obligations to notify personal data breaches* **Art. 74.** The data controller concerned is exempt

from notifying a personal data breach to a specific data subject or subjects, within the meaning of Article 34 of Regulation (EU) 2016/679, subject to the authorisation of the national cybersecurity authority, provided that and to the extent that such individual notification risks compromising the achievement of the purposes referred to in Article 72, § 2.

TITLE 7. — *Final provisions*

CHAPTER 1. — *Transitional provision* **Art. 75.** The

King sets the deadlines within which essential entities carry out their first periodic conformity assessments referred to in Article 39.

CHAPTER 2. — *Amending provisions*

Section 1. — Amendments to the law of 15 April 1994 relating to the protection of the population and the environment against the dangers resulting from ionizing radiation and relating to the Federal Agency for Nuclear Control

Art. 76. In Article 1 of the law of 15 April 1994 relating to the protection of the population and the environment against the dangers resulting from ionizing radiation and relating to the Federal Agency for Nuclear Control, last amended by the law of 7 February 2024, the words ÿ- ÿthe law of 7 April 2019ÿ: the law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security;ÿ are replaced by the words ÿ- the NIS2 law: the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security;ÿ.

Art. 77. In Chapter III, Section 1, of the same law, Article *15ter,* inserted by the law of April 7, 2019, is replaced by the following:

ÿArt. *15ter.* The Agency is designated as a sectoral inspection service, within the meaning of the NIS2 Act, for the energy sector, with regard to additional cybersecurity risk management measures applicable to the elements of a nuclear installation intended for the industrial production of electricity and which are used for the transmission of electricity.

The King shall determine the practical arrangements for inspections, after consulting the Agency.

Section 2. — Amendments to the law of 22 February 1998 establishing the organic status of the National Bank of Belgium **Art. 78.** In Article 36/1 of the Law of 22 February 1998 establishing the organic status of the National Bank of Belgium, last amended by the Law of 20 December 2023, 28o is replaced by the following:

ÿ28o ÿNIS2 Lawÿ: the law of April 26, 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security;ÿ.

Art. 79. In article 36/14 from wet to wet, it will be wet from December 20, 2023, the latest wording will be:

1o in paragraph 1, 20o, worden de woorden ÿaan de auriteit bedoeld in article 7, § 1, van de wet van 7 april 2019ÿ vervangen door de woorden ÿaan de nationale cyberbeveiligingsautoriteit bedoeld in article 8, 45o , from the NIS2-wetÿ;

2o in dezelfde paragraaf, 20o /1, worden de woorden ÿaan de authoriteit bedoeld in article 7, § 1, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid - NIS-wetÿ vervangen door de woorden ÿaan de nationale cyberbevei-ligingsautoriteit bedoeld in artikel 8, 45o van de NIS2-wet en aan het national CSIRT bedoeld in artikel 8, 46o van dezelfde wetÿ; 3o in dezelfde paragraaf, 24o ,ten bedoeld in article 7 van de wet van 7 april 2019 voor de , worden de woorden ÿaan de authoritei-uitvoering van de bepalingen van de wet van 7 April 2019ÿ vervangen door de woorden ÿaan de authoriteiten bedoeld in article 15 van de NIS2-wet

If you are using NIS2-wet products, please contact us.

Art. 80. Article 36/47 by dezelfde wet, ingevoegd bij de wet van April 7, 2019, wordt vervangen als volgt: ÿArt. 36/47. To pass by the NIS2-wet bank word has changed to the sectoral overheid in sectoral inspections of the financial sector, with the exploitation of the operator of a handelsplatform in the zin of articles 3, 6o by the wet of November 21, 2017 over the infrastructure of the market for you , financial instruments in accordance with the Financial Regulations 2014/65/EU.

Wanneer zij dit nuttig acht, deelt de Bank zo snel mogelijk met de ECB relevante informatie over incidentmeldingen die zijtvangt rachtens de NIS2-Wet of Verordening (EU) 2022/2554 van het European Parliament in 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 in (EU) 2016/1011.ÿ

Afdeling 3. — Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële le sector et de financiële diensten **Art. 81.** In article 75, § 1, 15o van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, laatstelijk gewijzigd bij de wet van 20 Juli 2020, worden de woorden ÿartikel 7 van de wet van 7 April 2019 tot vaststelling van de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheidÿ vervangen door de woorden ÿartikel 15 van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesyste-men van algemeen belang voor de openbare veiligheidÿ.

Afdeling 4. — Wijzigingen van de wet van 17 Januari 2003 met betrekking tot het statutut van de regulator van de Belgische post- en telecommunicatiesector **Art. 82.** In article 1/1 from January 17, 2003, we will be trekking before the status of the regulator of the Belgische post- en telecommu-nicatiesector, we will see you on December 21, 2021, the word will be on the 1st vervangen als volgt: ÿ1o Richtlijn (EU) 2022/2555 of the European Parliament in the European Parliament on December 14, 2022, it should be noted that the level of cyber security in the United States, to which the Verordening (EU) nr. 910/2014 in Richtlijn (EU) 2018/1972 in tot trekking van Richtlijn (EU) 2016/1148;ÿ.

Art. 83. In article 14 of the wet, it is due to be wet on December 17, 2023, the wording of the previous month is: 1 o in paragraph 1, here is the bottom line, the wording of the wet on April 7, 2019 to the fullest extent of the story for you. beveiliging the netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheidÿ vervangen door de woorden ÿwet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesyste-men van algemeen belang voor de

2o in dezelfde paragraaf, eerste lid, 3o , openbare veiligheidÿ; the bepaling under *h)* vervangen als volgt:

ÿh) de wet van April 26, 2024 tot vaststelling van een kader de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid in de sectorale inspection of the digital sector infrastructure, met uitzondering van de verleners van vertrouwensdiensten in de zin van article 8, 24o dezelfde wetÿ; , van

Art. 79. In Article 36/14 of the same law, as last amended by the law of 20 December 2023, the following amendments are made:

1st paragraph 1, 20th , the words "to the authority referred to in Article 7, § 1, of the law of 7 April 2019" are replaced by the words "to the national cybersecurity authority referred to in Article 8, 45o of the NIS2 law";

2o in the same paragraph, 20o /1, the words ÿto the authority referred to in Article 7, § 1, of the law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security - NIS lawÿ are replaced by the words ÿto the national cybersecurity authority referred to in Article 8, 45o of the NIS2 law and to the national CSIRT referred to in Article 8, 46o of the same lawÿ; ,

3o in the same paragraph, 24o , the words "to the authorities referred to in Article 7 of the law of April 7, 2019 for the purposes of implementing the provisions of the law of April 7, 2019ÿ are replaced by the words ÿto the authorities referred to in Article 15 of the NIS2 law for the purposes of implementing the provisions of the NIS2 lawÿ.

Art. 80. Article 36/47 of the same law, inserted by the law of 7 April 2019, is replaced by the following: ÿArt. 36/47. For the application of the NIS2 law, the Bank is designated as the sectoral authority and sectoral inspection service for entities in the financial sector, with the exception of trading platform operators within the meaning of Article 3, 6o of the law of 21 November 2017 on financial market infrastructures. , financial statements and transposing Directive 2014/65/EU.

If it deems it useful, the Bank shall share with the ECB as soon as possible relevant information on incident notifications it receives under the NIS2 Act or Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.ÿ.

Section 3. — Amendment of the law of 2 August 2002 relating to the supervision of the financial sector and financial services **Art. 81.** In article 75, § 1, 15o , of the law of 2 August 2002 relating to the supervision of the financial sector and financial services, last amended by the law of 20 July 2020, the words ÿarticle 7 of the law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public securityÿ are replaced by the words ÿarticle 15 of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public securityÿ.

Section 4. — Amendments to the Law of 17 January 2003 on the status of the regulator of the Belgian postal and telecommunications sectors **Art. 82.** In Article 1/1 of the Law of 17 January 2003 on the status of the regulator of the Belgian postal and telecommunications sectors, replaced by the Law of 21 December 2021, paragraph 1 is replaced by the following:

ÿ1o Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a common high level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148;ÿ.

Art. 83. In Article 14 of the same law, as last amended by law from December 17, 2023, the following changes are made:

1o in paragraph 1, subparagraph 1, the words ÿlaw of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public securityÿ are replaced by the words ÿlaw of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public securityÿ;

2o in the same paragraph, paragraph 1, 3o follows: , the *h),* is replaced by what

ÿh) the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, with regard to the tasks assigned to the sectoral authority and the sectoral inspection service for the digital infrastructure sector, with the exception of service providers of the same lawÿ; trust within the meaning of Article 8, 24o ,

3o in dezelfde paragraaf wordt het tweede lid vervangen als volgt: ÿVoor

de toepassing van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesyste-men van algemeen belang voor de openbare veiligheid, wordt het Institute aangewezen als sectorale overheid in de zin van artikel 8, 54o van dezelfde wet en als , sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwens-diensten en de zin van artikel 8, 24o post- en korea services. , van dezelfde wet, in your sector

3o in the same paragraph, paragraph 2 is replaced by the following: ÿFor the

application of the law of April 26, 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, the Institute is designated as a sectoral authority within the meaning of Article 8, 54o of the same law and a sectoral inspection service within the meaning of Article 44, § 1, paragraph 2, of the same law for the digital infrastructure sector, with the exception of trusted service providers within the meaning of Article 8, 24o of the same law, and for the postal and shipping services sector.ÿ. ,

Afdeling 5. — Wijzigingen van de wet van 13 Juni 2005 betreffende de elektronische communicatie

Section 5. — Amendments to the law of 13 June 2005 on electronic communications

Art. 84. Article 1, tweede lid, van de wet van 13 June 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van December 21, 2021, wordt aangevuld met een paling onder 7o luidende: ,

Art. 84. Article 1, paragraph 2, of the law of 13 June 2005 on electronic communications, last amended by the law of 21 December 2021, is supplemented by the 7th paragraph, worded as follows:

ÿ7o Richtlijn (EU) 2022/2555 van het European Parliament in de Raad van 14 december 2022 betreffende maatregelen voor een hoog geza-menlijk level 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.ÿ

ÿ7o Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a common high level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.ÿ.

Art. 85. In article 2 when it is wet, it should be wet on July 20, 2022, the date of delivery is: 1o de paling onder 48/1o wordt vervangen als volgt: ÿ48/1o ÿregister voor topleveldomeinnamenÿ: een entity it waaraan een specifieke ke topleveldomeinnaam is gedelegeerd en die verantwoor-delijk is your beheer of the topleveldomeinnaam, and includes the registration of the domeinnamen on the topleveldomeinnaam and the technical exploitation of the topleveldomeinnaam, and the inclusion of the exploitation of the naamservers, the onderhoud of the databases and the verdeling of the zonebestanden of the topleveldomeinnaam over the naamservers, ongeacht of die activiteiten door de entiteit zelf en uitgevoerd de worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uittend voor eigen gebruik worden aangewend door een register;ÿ;

Art. 85. In Article 2 of the same law, as last amended by law of July 20, 2022, the following amendments are made: 1o 48/1o is replaced by the following: ÿ48/1o ÿtop-level domain registryÿ: an entity to which a specific top-level domain has been delegated and which is responsible for the administration of the top-level domain, including the registration of domain names under the top-level domain and the technical operation of the top-level domain, including the operation of its name servers, the maintenance of its databases and the distribution of the top-level domain's zone files on the name servers, whether these operations are carried out by the entity itself or are subcontracted, but excluding situations where top-level domain names are used by a registry solely for its own use;ÿ; 2o 48/3o is inserted as follows: ÿ48/3o ÿentity providing domain name registration servicesÿ: a registrar or an agent acting on behalf of registrars, such as a provider or reseller of anonymization or proxy registration services;ÿ;

2o de bepaling onder 48/3o wordt ingevoegd, luidende:

ÿ48/3o ÿentiteit die domeinnaamregistratiediensten aanbiedtÿ: een registrator of een agent die namesregistrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverko-per;ÿ; 3o de palingen onder

62/2o en 62/3o worden vervangen als volgt: ÿ62/2o ÿnetwerk- en informatiesysteemÿ: *a)* een elektronische-communicatienetwerk bedoeld in de bepaling onder3o ; *b)* . controle op afstand de la verkrijgen van werkingsgegevens en real time mogelijk maken; of *c)* digitale gegevens die worden opgeslagen, verwerkt, opgehaald de verzonden met behulp van de in de bepalingen onder *a)* en *b)* bedoelde elementen met het oog op de working, het gebruik, de bescherming en het onderhoud ervan;

3o 62/2o and 62/3o are replaced by the following:

ÿ62/2o ÿnetwork and information systemÿ:

a) an electronic communications network referred to in 3o ;

(b) any device or set of interconnected or related devices, one or more elements of which provide, in execution of a program, automated processing of digital data, including the digital, electronic or mechanical components of this device allowing in particular the automation of the operational process, remote control, or the obtaining of operating data in real time; or

(c) digital data stored, processed, retrieved or transmitted by the elements referred to in points *(a)* and *(b)* for the purpose of their operation, use, protection and maintenance;

62/3o ÿbeveiliging the netwerk- en informatiesystemenÿ: het vermo-gen van netwerk- en informatiesystemen om op een bepaald level van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticity, integrity of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens de van diensten die door de via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen; ÿ; 4o de bepalingen onder

62/4o tot 62/8o worden ingevoegd, luidende: ÿ62/4o ÿbeveiligingsincidentÿ: een gebeurtenis die de beschikbaar-heid, authenticity, integrity of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens de van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesyste-men, in gevaar brengt;

62/3o ÿsecurity of networks and information systemsÿ: the ability of networks and information systems to withstand, at a given level of confidence, any event likely to compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of the services that these networks and information systems offer or make accessible;ÿ; 4o 62/4o to 62/8o are inserted as follows: ÿ62/4o ÿsecurity incidentÿ: an event compromising the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or of the services that networks and information systems offer or make accessible; 62/5o ÿcybersecurityÿ: cybersecurity as referred to in Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European

62/5o ÿcyberbeveiligingÿ: cyberbeveiliging bedoeld in article 2, point 1), van Verordening (EU) 2019/881 van het European Parliament in de Raad van 17 April 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en zake de certificering van de cyberbe-veiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

Union Agency for Cybersecurity) and on cybersecurity certification of information and communications technologies, and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation);

62/6o ÿincidental handlingÿ: all actions in procedures that have taken place in the event of an incident;

62/7o ÿcyberdreigingÿ: een cyberdreiging als bedoeld in article 2, point 8), van Verordening (EU) 2019/881; 62/8o ÿsignificant cyber-

dreigingÿ: een cyber-dreiging waarvan op base van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit de gebruikers van de servicing van de entiteit door het veroorzaken van aanzienlijke materiële, lichamelijke of immateriële schadeÿ; 5o het article wordt aangevuld met een paling onder 94o ÿ94o ÿaanbieder de digitale infrastructuurÿ: een entity die

behoort tot de sector digitale infrastructuur, met uitzondering van de , liquid:

verleners van vertrouwensdiensten, in de zin van artikel 8, 24o van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.ÿ.

Art. 86. In article 6, 4o , van dezelfde wet, vervangen bij de mois van December 21, 2021, worden de woorden ÿnetwerken en dienstenÿ vervangen door de woorden ÿnetwerk- en informatiesystemenÿ.

Art. 87. In article 105, § 2, 2o van dezelfde wet, vervangen bij de wet van 17 Februari 2022, worden de woorden ÿof als aanbieder van essential diensten in de zin van de wet van April 7, 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheidÿ opgeheven.

Art. 88. In dezelfde wet wordt article 107/2, ingevoegd bij de wet on December 21, 2021, posted on this page:

"Art. 107/2. § 1. We will be aware of April 26, 2024, before the vast majority of information about cyber security of the network and the information systems of the open-source network. informatice-systemen. The Institute can be used to regulate vast amounts of risk analysis.

§ 2. Onverminderd Verordening (EU) 2016/679 of the European Parliament in the European Parliament on April 27, 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsge-gevens en betreffende het verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, last day of AVG, in the wet of July 30, 2018, be taken by natural persons and be trekking before being transported by people, last day of wet on July 30, 2018, of the operators and their date in ieder geval: 1o wordt gewaarborgd that all the people you have are the ones you are looking for; 2o opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of

onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; in 3o een beveiligingsbeleid wordt ingevoerd met betrekking

tot de verwerking van persoonsgegevens.

Het Institute can of door of ze operatoren genomen maatregelen controleren en aanbevelingen formularen over of beste praktijken betreffende het beveiligingspeil dat met deze maatregelen moet worden gehaald. § 3. De operatoren nemen all noodzakelijke matregelen,

inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiedien-sten en de internettoegangsdiensten zo volledig mogelijk te waarbor-gen in geval van uitzonderlijke netwerkuitval de in geval van over-macht.

Opportunity for the Institute of its own initiative, and advice from het Institute, kan de Koning deze maatregelen preciseren.

§ 4. De operators biéden abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste beveiligde diensten aan die de eindgebruikers en staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen.ÿ.

Art. 89. In dezelfde wet wordt artikel 107/3, ingevoegd bij de wet van December 21, 2021, vervangen als volgt: ÿArt. 107/3. § 1. In

geval van een significant cyberdreiging inform-meert de aanbieder van digitale infrastructuur het Instituut over de dreiging, over mogelijke beschermingsmaatregelen de oplossingen die de gebruikers kunnen toepassen, alsook over de maatregelen die hij heeft genomen de overweegt te nemen.

62/6o ÿincident handlingÿ: all actions and procedures aimed at preventing, detecting, analysing, containing, responding to and remediating an incident; 62/7o ÿcyber threatÿ: a cyber threat as defined in

Article 2(8) of Regulation (EU) 2019/881; 62/8o ÿsignificant cyber threatÿ: a cyber threat which, given its technical characteristics,

may be considered likely to have a serious impact on the networks and information systems of an entity or the users of the entity's services, causing significant material, bodily or moral damage;ÿ;

5o the article is supplemented by 94o , worded as follows: ÿ94o

ÿdigital infrastructure providerÿ: an entity which falls within the digital infrastructure sector, with the exception of trusted service providers, within the meaning of Article 8, 24o of the law of April 26, 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security.ÿ.

Art. 86. In Article 6, 4o , of the same law, replaced by the law of December 21, 2021, the words “networks and services” are replaced by the words “networks and information systems”.

Art. 87. In Article 105, § 2, 2o , of the same law, replaced by the law of February 17, 2022, the words "or as an operator of essential services within the meaning of the law of April 7, 2019 establishing a framework for the security of networks and information systems of general interest for public security" are repealed.

Art. 88. In the same law, article 107/2, inserted by the law of 21 December 2021, is replaced by the following:

ÿArt. 107/2. § 1. Without prejudice to the provisions of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, digital infrastructure providers analyze the risks to the security of their networks and information systems. The Institute may determine the terms and conditions for this risk analysis.

§ 2. Without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter referred to as the GDPR and the Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, hereinafter referred to as the Law of 30 July 2018, operators shall ensure at least:

1. ensure that only persons authorized to act for legally authorized purposes may have access to the personal data they process; 2. protect personal data stored or transmitted against accidental

or unlawful destruction, accidental loss or alteration and unauthorized or unlawful storage, processing, access and disclosure; and

3. ensure the implementation of a security policy relating to the processing of personal data.

The Institute is authorized to verify the measures taken by these operators and to issue recommendations on best practices regarding the level of security that these measures should achieve.

§ 3. Operators shall take all necessary measures, including preventive measures, to ensure the most complete availability possible of voice communications services and internet access services in the event of exceptional network failure or force majeure.

The King, on the proposal of the Institute or on the initiative of, on the advice of this one can specify these measures.

§ 4. Operators shall offer their subscribers, free of charge and taking into account technical possibilities, adequate secure services, in order to enable end users to avoid any form of unwanted electronic communication.ÿ.

Art. 89. In the same law, article 107/3, inserted by the law of 21 December 2021, is replaced by the following:

Art. 107/3. § 1. In the event of a significant cyber threat, the digital infrastructure provider shall inform the Institute of the cyber threat, of any protective or corrective measures that its users may take, as well as of the measures that it has taken or plans to take.

The Institute can provide detailed information about information technology worden verstrekt alsook de nadere regels voor die kennisgeving.

§ 2. In the meantime, the operator of the electronic communication system is responsible for the operation of the system and the operator.

Indian de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of persoon-lijke levenssfeer van een subscribee of een individueel persoon, stelt de operator van elektronische-communicatiediensten onverwijld ook de betrokken abonnee of individue persoon in kennis van de inbreuk.

De Gegevensbeschermingsautoriteit gaat na de deze operator deze verplichting nakomt en brengt het Instituut op de hoogte wanneer ze van oordeel est dat dit dit niet het geval is.

De kennisgeving van een inbreuk in verband met persoonsgegevens aan een betrokken subscriber of individue persoon is niet vereist wanneer de operator van elektronische-communicatiediensten tot voldoening van het Institute heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze Please note that the contents of the data are stored in the following data. Dergelijke technologische beschermingsmaat-regelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de operator van elektronische-communicatiediensten om de betrokken abonnees en individual

personen in kennis te stellen, indian deze operator of individual person niet reeds in kennis heeft gestureld van de inbreuk in verband met persoonsgegevens, kan het Institute op verzoek van de Gegevensbeschermingsautoriteit hem, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk If you want to know what to do, see what you do.

In order to keep a subscriber or an individual person's word ten minutes from the inbreuk in verband met people-gegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

De kennisgeving aan de Gegevensbeschermingsautoriteit bevat bovendien een omschrijving van de gevolgen van de inbreuk en verband met persoonsgegevens en van de door de operator van elektronische-communicatiediensten voorgestelde de regoffen maatre-gelen om die inbreuk te verhelpen.

§ 3. On the subject of technical guidance of the European Commission overeenkomstig article 4, point 5, van Richtlijn 2002/58/EG, en na advies van de Gegevensbeschermingsautoriteit, kan het Instituut richtsnoeren en, waar nodig, instructions uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door de operatoren van elektronische-communicatiediensten noodzakelijk is.

We refer to the technology used by the European Commission for article 4, point 5, of the Richtlijn 2002/58/EG, in accordance with the instructions of the Institute, in accordance with the instructions provided by the Commission. Please note that your two kennisgevings should be stored in the same format, but you must also handle the kennisgeving geschiedt.

From the operator of the electronic communications system you can find inventories in the verband with people in your possession, you will find more information in the verband with some inbreuken, you will be able to store the zijn genomen, you will be able to use it in your Institute. nagaan of de bepalingen van paragraaf 2 werden nageleefd. Deze inventories bevat uittend de voor dit doel noodzakelijke gegevens.ÿ.

Art. 90. In dezelfde wet wordt artikel 107/4, ingevoegd bij de wet van December 21, 2021, vervangen als volgt:

ÿArt. 107/4. § 1. Dit article is before passing, on verminderd of being palingen van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met name voor wat betreft de toezichtsbevoegdheden verleend aan de sectorale overheid of de sectorale inspectiedienst. § 2. The

Institute includes digital infrastructure and instructions that are included in the articles 107/2 and 107/3 in the articles 30 and 33 on April 26, 2024, on April 26, 2024, on April 26, 2024. Beveiligingsincident op te lossen de te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructions.

The Institute may specify the cases in which information must be notified as well as the terms of this communication.

§ 2. In the event of a personal data breach, the electronic communications services operator shall immediately notify the Data Protection Authority, which shall immediately notify the Institute.

Where the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the electronic communications services operator shall also promptly notify the subscriber or individual concerned of the breach.

The Data Protection Authority examines whether the operator complies with this obligation and informs the Institute when it considers that this is not the case.

Notification of a personal data breach to the subscriber or individual concerned is not required if the electronic communications services operator has proven, to the satisfaction of the Institute, that it has implemented appropriate technological protection measures and that these have been applied to the data concerned by the breach. Such technological protection measures render the data incomprehensible to any person who is not authorized to access it.

Without prejudice to the obligation of the electronic communications service operator to inform the subscribers and individuals concerned, if this operator has not already notified the subscriber or individual of the personal data breach, the Institute may, at the request of the Data Protection Authority, after having examined the potentially negative effects of this breach, require that it do so.

The notification to the subscriber or individual shall at a minimum describe the nature of the personal data breach and the points of contact from which additional information may be obtained and recommend measures to be taken to mitigate the possible adverse consequences of the personal data breach.

The notification made to the Data Protection Authority also describes the consequences of the personal data breach, and the measures proposed or taken by the electronic communications services operator to remedy it.

§ 3. Subject to technical implementing measures from the European Commission in accordance with Article 4, point 5, of Directive 2002/58/EC, and after consulting the Data Protection Authority, the Institute may adopt guidelines and, where appropriate, issue instructions specifying the circumstances in which operators of electronic communications services are required to notify the breach of personal data.

Subject to technical implementing measures from the European Commission in accordance with Article 4, point 5, of Directive 2002/58/EC, and after consulting the Institute, the Data Protection Authority may adopt guidelines and, where appropriate, issue instructions specifying the format applicable to this notification and its transmission procedure.

Operators of electronic communications services shall maintain an inventory of personal data breaches, including their context, effects and remedial measures, so that the Data Protection Authority and the Institute can verify compliance with the provisions of paragraph 2.

This inventory includes only the information necessary for this purpose.ÿ.

Art. 90. In the same law, article 107/4, inserted by the law of 21 December 2021, is replaced by the following:

ÿArt. 107/4. § 1. This article applies without prejudice to the provisions of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, in particular with regard to the supervisory powers granted to the sectoral authority or the sectoral inspection service.

§ 2. The Institute may give binding instructions within the framework of Articles 107/2, 107/3 as well as Articles 30 and 33 of the aforementioned Law of 26 April 2024 to a digital infrastructure provider, including the measures required to remedy a security incident or prevent such an incident from occurring when a significant cyber threat has been identified, as well as the deadlines for implementing these instructions.

§ 3. In this article you will find articles 107/2 and 107/3 in articles 30 and 33 on April 26, 2024, to be widely spoken about cyber-beveiliging of netwerk- and information systems that are open to the public, kan het Institute of digital infrastructure development is:

a) inspected by your elders, including the control of steelwork, by the wording of professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door het Institute of door een onafhankelijke instantie; *c)* ad hoc audits;

d) beveiligingsscans on the basis of objectivity, non-discrimination, eerlijke en transparent risicobeoordelingscriteria, indian nodig in samenwerking met de betrokken aanbieder van digitale infrastructuur;

e) Verzoeken om informatie die nodig est om de door de betrokken aanbieder van digitale infrastructuur genomen maatregelen voor het beheer van cyberbeveiligingsrisico's; *f)* Verzoeken van tot alle gegevens, documenten

en informa-tie die het Institute nodig acht voor de uitoefening van zijn toezicht-houdende taken;

g) Verzoeken om bewijs van de uitvoering van het cyberbeveiligings-beleid, zoals de resultaten van beveiligingsaudits die door een gekwa-lificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in het eerste lid, *b),* bedoelde gerichte beveiligingsaudits zijn gebaseerd opdoor het Institute of gecontroleerde entity verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde infor-matie.

Wanneer de in het eerste lid, *b),* bedoelde beveiligingsaudit wordt uitgevoerd door een onafhankelijke instantie, dan stelt de aanbieder van digitale infrastructuur een de meer instanties ter goedkeuring aan het Instituut voor. The Institute needs to be informed of the instantaneous development of the audit that you are looking for in the digital infrastructure. Once the system has been activated, it will be installed immediately. Deze laatste bezorgt aan het Institute volledige verslag en de resultaten van deze audit en de kosten van de audit zijn ten laste van de anbieder van digitale infrastructuur, behalve in naar behoren met redenen omklede gevallen waarin het Instituut anders besluit.

Bij de uitoefening van zijn bevoegdheden uit hoofde van lid 1, *e),* f) d) *de g),* vermeldt het Instituut het doel van het verzoek en de gevraagde informatie.

The Institute can be used when it comes to digital technology IT infrastructure over risk analysis to move forward.

Opt for the Institute that does not need to be implemented by the digital infrastructure of the network and the organization of the network.

Opt for the Institute in which it is located when there are warning incidents, the digital infrastructure of the Institute and the contact person mee die steeds bereikbaar is.

§ 4. Opinion of the Institute in which it is published in which it is written without conformity with articles 30 and 33 in April 26, 2024, tot vaststelling of the cyberbelieving of netwerk- in information systems with the use of open space Veiligheid, of met een uitvoeringsmaatregel, alsook naar de gevolgen ervan voor de beveiliging van netwerk- en informatiesystemen, geeft de ananbieder van digitale infrastructuur het Institute toegang alle elementen van zijn netwerk.

§ 5. We shall be aware of the national cyberbevei-ligingsautoriteit coördineert het Instituut de initiatiatieven round de beveiliging van openbare elektronische-communicatienetwerken en openbare elektronische-communicatiediensten.

Het ziet toe op het opsporen, Observe and analyzen van beveiligingsproblemen, en kan de gebruikers hierover informatie verstrekken.

§ 6. Indian een aanbieder van digitale infrastructuur dit artikel de een op grond van dit artikel genomen beslissing van het Institute niet naleeft, kunnen de in titel 4, hoofdstuk 2, van de wet van 26 April 2024

§ 3. Within the framework of the supervision of Articles 107/2 and 107/3 as well as Articles 30 and 33 of the Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, the Institute may subject the digital infrastructure provider to:

(a) on-site inspections and remote monitoring, including random checks carried out by trained professionals;

(b) regular and targeted security audits carried out by an organization independent or by the Institute; *c)* ad

hoc audits;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the digital infrastructure provider;

(e) requests for information necessary for the assessment of the cybersecurity risk management measures adopted by the relevant digital infrastructure provider;

(f) requests for access to data, documents and any information that the Institute considers necessary for the performance of its supervisory tasks; (g) requests for evidence of the implementation of cybersecurity

policies, such as the results of security audits carried out by a qualified auditor and the corresponding underlying evidence.

The targeted security audits referred to in paragraph 1(b) are based on risk assessments carried out by the Institute or the audited entity, or on other available risk-related information.

When the security audit referred to in paragraph 1, *b),* is carried out by an independent body, the digital infrastructure provider shall propose one or more bodies to the Institute for approval. The Institute shall give its approval when the independent body is qualified to carry out the audit and is independent of the digital infrastructure provider. If the Institute fails to agree within the time limit it set at the time of the request, the Institute shall appoint the independent body itself. The latter shall provide the Institute with the full report and the results of this audit. The costs of the audit shall be borne by the digital infrastructure provider, unless the Institute decides otherwise in duly justified cases.

When exercising its powers under paragraph 1(e), (f) or *(g),* the Institute shall specify the purpose of the request and the information required.

The Institute may determine the terms and conditions for the provision by the digital infrastructure provider of information concerning the risk analysis. At the request of the Institute,

a digital infrastructure provider shall participate in an exercise relating to the security of networks and information systems or organize such an exercise.

At the request of the Institute and as part of security incident management, a digital infrastructure provider provides the Institute with a permanently available point of contact.

§ 4. At the request of the Institute and to investigate a case of non-compliance with Articles 30 and 33 of the Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security or an enforcement measure as well as its effect on the security of networks and information systems, the digital infrastructure provider gives it access to any element of its network.

§ 5. Without prejudice to the powers of the national cybersecurity authority, the Institute coordinates initiatives relating to the security of public electronic communications networks and publicly available electronic communications services.

It oversees the detection, observation and analysis of security issues, and can provide users with information on these issues.

§ 6. Failure by a digital infrastructure provider to comply with this article or with a decision of the Institute taken on the basis of

tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatregelen de geldboetes worden opge-legd.ÿ.

Art. 91. In article 126/3, § 3, *l),* for wet weather, it is due to wet weather on July 20, 2022, wording “essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op base van de wet van 7 April 2019 tot vaststelling van We have the opportunity to be aware of the netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheidÿ vervangen door de woorden ÿdiensten van essentiële entiteiten en de zin van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen You can also use the open-air veilig-heidÿ.

Art. 92. In article 164/1 van dezelfde wet, ingevoegd bij de wet van July 10, 2012, the following words were posted:

1o de woorden ÿInternetdomeinnaamregistreerbureau van het topni-veaudomeinÿ worden vervangen door de woorden ÿregister voor topleveldomeinnamen van het topleveldomeinÿ;

2o in de bepaling onder 4o wordt het woord ÿdomeinnaamregistreer-bureauÿ vervangen door de woorden ÿregister for topleveldomeinna-menÿ; 3o in

de bepaling onder 4o wordt het woord ÿInternet-domeinnaamregistreerbureauÿ vervagen door de woorden ÿregister for topleveldomeinnamenÿ;

4o in de bepaling onder 5o wordt het woord ÿtopleveldomeinÿ vervangen door het woord ÿtopleveldomeinÿ.

Art. 93. In article 164/2 we have the following wording: 1o de woorden

ÿInternetdomeinnaamregistreerbureauÿ worden ver-vangen door de woorden ÿregister your topleveldomeinnamenÿ;

2o in the Dutch text wordt het woord ÿtopleveldomeinÿ vervangen door het woord ÿtopleveldomeinÿ.

Art. 94. In title VI, hoofdstuk III, van dezelfde wet, wordt een article 164/3 ingevoegd, title:

"Art. 164/3. § 1. Registers for top-level registrations in the national registers are verified, but they are not yet registered in the national registers and are held in a special database overeenkomstig het Unierecht inzake de bescherming van persoonsgegevens.

§ 2. From the registered offices you will be able to contact the top level of the domain, you will be identified by contacting you. Die informatie omvat ten minste:

1o of domeinnaam;

2o of registratiedatum;

3o de naam van de houder van de domeinnaam, zijn e-mailadres en his phone number;

4o het e-mail addresses en het telefoonnummer van het contactpuntpunt dat dat de domeinnaam beheert, indien desze verschillen van die van de houder van de domeinnaam.

From now on, at the advice of the Institute, the privacy of proxy registrars will be transferred to you in terms of the registration of your respective domains.

De naleving van de dit article bedoelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal worden ver-zameld bij de betrokkene. If you register your top level-domestic registers and register them, you will find the same ones.

De Koning kan, na advies van het Institute, de modaliteiten van deze samenwerking preciseren.

§ 2. De registers voor topleveldomeinnamen en de entiteiten de domeinnaamregistratiediensten verlenen, beschikken over beleidslij-nen en procedures, waaronder verificatieprocedures, om te garanderen dat de in paragraaf 1, eerste lid, bedoelde databases juiste en volledige informatie bevatten. Deze beleidslijnen en procedures worden open-baar gemaakt.

This article may be subject to the administrative measures or fines referred to in Title 4, Chapter 2, of the law of April 26, 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security.ÿ.

Art. 91. In Article 126/3, § 3, *l),* of the same law, inserted by the law of 20 July 2022, the words ÿessential essential service providers designated on the basis of the law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public securityÿ are replaced by the words ÿessential entities within the meaning of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public securityÿ.

Art. 92. In Article 164/1 of the same law, inserted by the law of July 10, 2012, the following changes are made:

1o the words “Internet domain name registrar of the top-level domain” are replaced by the words “top-level domain name registry of the top-level domain”;

2nd to 4th, the words “domain name registrar” are replaced by the words “top-level domain name registry”.

3rd to 4th , the words ÿdomain name registrar Internet” are replaced by the words “top-level domain name registry”; 4o to 5o in the Dutch text, the word

“topniveaudomein” is replaced by the word ÿtopleveldomeinÿ.

Art. 93. In Article 164/2 of the same Act, the following amendments are made: 1o the

words ÿInternet domain name registrarÿ are replaced each time by the words ÿtop-level domain name registryÿ; 2o in the Dutch text, the word ÿtopniveaudomeinÿ

is replaced each time by the word ÿtopleveldomeinÿ.

Art. 94. In Title VI, Chapter III, of the same law, a Article 164/3, worded as follows:

ÿArt. 164/3. § 1. Top-level domain name registries and entities providing domain name registration services shall collect, with all due diligence, domain name registration data and maintain them accurate and complete in a dedicated database in accordance with Union law on the protection of personal data. § 2. The domain name registration data referred to in paragraph 1 shall contain the information necessary to identify and contact the domain

name holders and the contact points that manage the domain names under the top-level domains.

This information includes at least the following:

1o the domain name; 2o the

registration date; 3o the name of

the domain name holder, their email address and telephone number; 4o the email address and telephone number for contacting the

point of contact that manages the domain name, if these contact details are different from those of the holder.

After consulting the Institute, the King may order providers and resellers of anonymization or proxy registration services to share domain name registration data with registrars and define the terms and conditions.

Compliance with the obligations referred to in this Article shall not result in unnecessary duplication of the collection of domain name registration data from the data subject. To this end, top-level domain name registries and entities providing domain name registration services shall cooperate

rent between them.

After consulting the Institute, the King may specify the terms of this cooperation.

§ 2. Top-level domain name registries and entities providing domain name registration services shall have policies and procedures, including verification procedures, aimed at ensuring that the databases referred to in paragraph 1, subparagraph 1, contain accurate and complete information. These policies and procedures shall be made available to the public.

Wanneer de domeinnaamregistratiegegevens opgesomd en paragraaf 1, tweede lid, van een domeinnaam onjuist, onnauwkeurig de onvolle-dig zijn, blokkeren de registers voor topleveldomeinnamen en de entiteiten domeinnaamregistratiediensten verlenen onmiddellijk het functioneren van deze Domeinnaam tot de houder van demeinnaam de registratiegegevens correctert zodat deze juist, auw-keurig en volledig worden.

If the domain name registration data listed in paragraph 1, subparagraph 2, of a domain name is incorrect, inaccurate or incomplete, top-level domain name registries and entities providing domain name registration services shall immediately block the operation of that domain name until the domain name holder corrects the registration data to become correct, accurate and complete.

Indian de houder van de domeinnaam nalaat om dit te doen binnen de termijn zoals bepaald door het register voor topleveldomeinnamen of door de entityit die domeinnaamregistratiediensten verleent, wordt de domeinnaam geannuleerd.

If the domain name holder fails to do so within the time period set by the top-level domain name registry or the entity providing domain name registration services, the domain name is cancelled.

De transfer van deblokkeerde domeinnaam naar een andere Entiteit die domeinnaamregistratiediensten verleent, est verboden.

Transferring a blocked domain name to another entity providing domain name registration services is prohibited.

§ 3. From the registers of your top level domeinnamen and from the entities of the domeinnaamregistratiediensten verlenen, maken de domeinnaamregis-tratiegegevens die geen persoonsgegevens zijn, onverwijld openbaar na de registratie van een domeinnaam.

§ 3. Top-level domain name registries and entities providing domain name registration services shall make publicly available, without undue delay after registration of a domain name, domain name registration data that is not personal data.

§ 4. Op een naar behoren met redenen omkleed verzoek, verschaffen de registers voor topleveldomeinnamen en de entiteiten domein-naamregistratiediensten verlenen, kosteloos, aan de legitieme toegang-vragende partijen, de gegevens opgesomd in paragraaf 1, tweede lid, onverwijld en in elk geval binnen tweeënzeventig uur na ontvangst van het verzoek, de vierentwintig uur na ontvangst van het verzoek ingeval van hoogdringendheid.

§ 4. Upon duly motivated request, top-level domain name registries and entities providing domain name registration services shall provide the data listed in paragraph 1, subparagraph 2, free of charge to legitimate access requesters, without undue delay and in any event within seventy-two hours of receipt of any access request, or twenty-four hours of receipt of any access request in an emergency.

Legitimized party participation is based on the nature of right-wing parties who are verzoek indienst voor het onderzoeken, vaststel-len, uitoefenen de verdedigen van strafrechtelijke, burgerrechtelijke of andere bepalingen in the Unierecht of Belgisch recht.

Legitimate applicants for access include any natural or legal person who makes a request for the examination, establishment, exercise or defence of criminal, civil or other provisions of Union or Belgian law.

Als legitieme toegangvragende partij worden beschouwd: 1o elke

persona in het kader van inbreuken op intellectuale eigen-domsrechten of naburige rechten; 2o

het Institute; 3o

het CCB;

4th national CSIRT;

5o of politiediensten;

6o of gerechtelijke overheden; 7o

de inlichtingen- en veiligheidsdiensten; 8o of

FOD Economy;

9th of FOD Financiën.

The following are considered legitimate access applicants: 1.

any person in the context of violations of intellectual property rights or related rights; 2. the Institute; 3. the CCB;

4th the national CSIRT;

5o the police services; 6o

the judicial authorities; 7o the

intelligence and security services; 8o the FPS

Economy;

9th the FPS Finance.

From now on, at the advice of the Institute, we have legitimate rights to participate in a number of cases.

After consulting the Institute, the King may add additional legitimate access applicants to this list.

From the registers of your top level domeinnamen and from the entities of the domestic registers, you will be able to check them in the state where they are stored.

Top-level domain name registries and entities providing domain name registration services provide the applicant with the opportunity to easily submit their application.

Er is sprake van hoogdringendheid indiana het gebruik van een domeinnaam kan leiden tot levensbedreigende situaties en/of onher-stelbare schade.

It is a matter of urgency if the use of a domain name may lead to life-threatening situations and/or irreparable damage.

Elke weigering van een behoren met redenen omkleed verzoek wordt with redenen omkleed.

Any refusal of a duly justified request shall be justified.

Het beleid en de procedures met betrekking early of bekendmaking van deze gegevens worden openbaar gemaakt.

The policies and procedures for disclosing this data are made public.

From the registers of your top level dome innamen and from the entities of the domein-naamregistratiediensten verlenen, mogen de houder van een domein-naam niet op de hoogte brengen wanneer een verzoek zoals bedoeld in het eerste lid werd ingediend.

Top-level domain name registries and entities providing domain name registration services may not inform the holder of a domain name when a request referred to in paragraph 1 has been made.

§ 5. The Institute can register your top level domestic entity of the national register for the instructions given in this article.

§ 5. The Institute may give binding instructions to a top-level domain name registry or an entity providing domain name registration services, with a view to compliance with this article.

§ 6. Indian een register voor topleveldomeinnamen of een entity die domeinnaamregistratiediensten verleent dit artikel, een in uitvoering van dit artikel aangenomen koninklijk besluit of een bindende instruc-tie van het Instituut niet naleeft, kan het Instituut de in hoofdstuk 2 van de wet van April 26, 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk-en informatiesystemen van algemeen belang voor de openbare veiligheid bedoelde administratieve maatre-gelen de geldboetes opleggen.ÿ.

§ 6. If a top-level domain name registry or an entity providing domain name registration services fails to comply with this Article, a Royal Decree adopted pursuant to this Article or a binding instruction issued by the Institute, the Institute may impose the administrative measures or fines referred to in Chapter 2 of the Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security.ÿ.

Afdeling 6. — Wijzigingen van de wet van November 21, 2017 over the infrastructure of your financial markets and instruments in accordance with which Richtlijn 2014/65/EU

Art. 95. In article 71 from November 21, 2017 on the infrastructure of your financial markets

houdende omzetting van Richtlijn 2014/65/EU, gewijzigd bij de wet van 7 April 2019, worden de woorden ÿen van titel 2 van de wet van 7 April 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de open-bare monitoring. Your customer service will be wet before April 7, 2019, FSMA will not be able to provide specialized external services and will be able to provide you with the appropriate service.

Art. 96. Artikel 79, § 4, van dezelfde wet, ingevoegd bij de wet van April 7, 2019, wordt opgeheven.

HOOFSTUK 3. — *Opheffingsbepaling* **Art. 97.**

From April 7, 2019 to the vast majority of people who understand the network and informatics systems that are open to the public.

HOOFSTUK 4. — *Inwerkingtreding* **Art. 98.**

Deze wet treedt in working op 18 October 2024.

If it is wet, it should be noted that it is the Lands Zegel zal worden Please note that the *Belgisch Staatsblad* has the right word to read.

Gegeven te Brussel, April 26, 2024.

FILIP

Van Koningswege: De

Eerste Minister, A. DE CROO

By Minister Binnenlandse Zaken, A. VERLINDEN

Met's Lands zegel gezegled:

The Minister of Justice,

P. VAN TIGCHELT

Note

(1) Kamer van volksvertegenwoodigers (www.dekamer.be): *Stukken :* 55 3862

Full version : April 18, 2024.

Section 6. — Amendments to the Law of 21 November 2017 on financial instrument market infrastructures and transposing Directive 2014/65/EU **Art. 95.** In Article 71 of the Law of 21 November 2017 on financial instrument market infrastructures and transposing Directive 2014/65/EU, amended by the Law of 7 April 2019, the words ÿand Title 2 of the Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security. For the performance of the aforementioned tasks concerning the Law of 7 April 2019, the FSMA may nevertheless instruct a specialized external service provider to carry out specific control tasks or obtain the assistance of such a service provideršy are repealed.

Art. 96. Article 79, § 4, of the same law, inserted by the law of April 7, 2019, is repealed.

CHAPTER 3. — *Repealing provision* **Art. 97.**

The law of April 7, 2019 establishing a framework for the security of networks and information systems of general interest for public security is repealed.

CHAPTER 4. — *Entry into force* **Art. 98.**

This law enters into force on October 18, 2024.

We promulgate this law, order that it be affixed with the Seal of the State and published in the *Belgian Monitor.*

Given in Brussels, April 26, 2024.

PHILIPPE

By the King:

The Prime Minister, A. DE CROO

The Minister of the Interior, A. VERLINDEN

Sealed with the seal of the State:

The Minister of Justice,

P. VAN TIGCHELT

Note

(1) Chamber of Representatives (www.lachambre.be): *Documents :* 55 3862

Full report : April 18, 2024.

Bijlage I bij de wet van April 26, 2024 tot vaststelling van een kader de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Bijlage I - Zeer kritieke sectors		
Sector	Deelsector	Soort entity
1. Energy	a) Electricity	- Elektriciteitsbedrijven zoals definieerd in article 2, point 57, van Richtlijn (EU) 2019/944 of the European Parliament in the European Parliament on June 5, 2019 shall be subject to internal regulations relating to electricity in accordance with the law of the European Parliament 2012/27/EU, the operation of which shall be verified by the ÿleveringÿ of the zoals shall be defined. in article 2, point 12, van die richtlijn
		- Distribution systems listed in article 2, point 29, of Richtlijn (EU) 2019/944 of June 5, 2019 shall be subject to current regulations for your internal electricity market in accordance with Richtlijn 2012/27/EU
		- Transmissiesysteembeheerders zoals definieerd in article 2, point 35, van Richtlijn (EU) 2019/944 van 5 Juni 2019 betreffende gemeenschappelijke regels voor de internelle markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU
		- Produced by zoos defined in article 2, point 38, by Richtlijn (EU) 2019/944 on June 5, 2019, the regulations governing your internal electricity market must be taken into account. Regulation 2012/27/EU

Bijlage I - Zeer kritieke sectors		
Sector	Deelsector	Soort entity
		- Benoemde elektriciteitsmarktbeheerders zoals gedefinieerd in article 2, point 8, from Verordening (EU) 2019/943 from Europe Parliament and the House
		- Marktdeelnemers zoals defined in article 2, point 25, van Verordening (EU) 2019/943 of the European Parliament in de Raad on June 5, 2019, the internal market of your electricity, die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken zoals definieerd in article 2, points 18, 20 en 59, van Richtlijn (EU) 2019/944 on June 5, 2019 will be subject to current regulations for your internal electricity market. wijziging van Richtlijn 2012/27/EU
		- Exploiting the power to be transferred to you beheer in exploitation van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namesens en voor rekening van een aanbieder van mobiliteitsdiensten
	b) Stadsverwarming en -koeling	- Exploiting the stadsverwarming of stadskoeling zoals gedefini-eerd in article 2, point 19, van Richtlijn (EU) 2018/2001 van het European Parliament on December 11, 2018 is the subject of energy consumption and energy consumption.
	c) Aardolie	- Exploiters of oliepijpleidingen
		- Operator of your products, refining in behandeling van olie, opslag in transport
		- Centrale entity for your control of zoos defined in article 2, point *f),* van Richtlijn 2009/119/EG van de Raad van September 14, 2009 you will be informed of your lidstaten om minimum voorraden ruwe aardolie en/of aardolieproducten in hold you
	d) Aardgas	- Leveringsbedrijven zooals defined in article 2, point 8, van Richtlijn 2009/73/EG of the European Parliament and of Raad van July 13, 2009 will be subject to internal regulations markt for aardgas en tot trekking van Richtlijn 2003/55/EG
		- Distributiessystemeembeheerders zoals defined in article 2, point 6, van Richtlijn 2009/73/EG on July 13, 2009, there will be some regulations for your internal markt for your aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Transmissiesysteembeheerders zoals defined in article 2, point 4, van Richtlijn 2009/73/EG on July 13, 2009, there are some regulations for your internal markt for your aardgas en tot intrekking van Richtlijn 2003/55/EG
		- Opslagsysteembeheerders zoals defined in article 2, point 10, van Richtlijn 2009/73/EG on July 13, 2009 will be subject to regulations for your internal market during your trek van Richtlijn 2003/55/EG
		- LNG-systeembeheerders zooals defined in article 2, point 12, van Richtlijn 2009/73/EG on July 13, 2009 will be subject to regulations for your internal market during your trek van Richtlijn 2003/55/EG
		- Aardgasbedrijven zoals gedefinieerd in article 2, point 1, van Richtlijn 2009/73/EG on July 13, 2009 will be subject to the regulations for your internal markt for your aardgas during your trek. Richtlijn 2003/55/EG
		- Operators of refining in production van aardgas
	e) Waterstof	- Operator of your product, opslag en water transmission
2. Transport	a) Air	- Please note that zoo conditions are defined in article 3, point 4, Verordening (EG) nr. 300/2008 of the European Parliament in de Date of March 11, 2008, the legal regulations are subject to change. be prepared for benevolence of burgers during your trek van Verordening (EG) nr. 2320/2002, your commercial documents are subject to written terms

Bijlage I - Zeer kritieke sectors		
Sector	Deelsector	Soort entity
		- Luchthavenbeheerders zoals gedefinieerd in article 2, point 2, van Richtlijn 2009/12/EG of the European Parliament in the Raad van 11 March 2009 inzake luchthavengelden, luchthavens als bedoeld in article 2, point 1, in the rich text, and in the book of Kernlucht-Havens in Bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 of the European Parliament in December 11, 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot trekking van Besluit nr. 661/2010/EU for this purpose, it is also possible to set up the two facilities for which we are responsible.
		- Operator and control operator Luchtverkeersleidingsdiensten zoals defined in article 2, point 1, van Verordening (EG) nr. 549/2004 of the European Parliament in by Raad on 10 March 2004 tot vaststelling van het kader voor de totstandbrenging of the gemeenschappel (ke Europese luchtruim give up
	b) Spoor	- Infrastructuurbeheerders zoals defined in article 3, point 2, van Richtlijn 2012/34/EU of the European Parliament in de Raad from November 21, 2012 to start with European information
		- Spoorwegondernemingen zoals gedefinieerd in article 3, point 1, van Richtlijn 2012/34/EU on November 21, 2012 to start with Europe is a spoorwegruimte, inclusive of the operator of the services provided by the zoals defined in article 3, point 12, at the end richtlijn
	c) Water	- Bedrijven voor voer voer over water (binnenvaart, kust- en zeever-voer) van passengers en bulkht, die in bijlage I bij Verordening (EG) nr. 725/2004 of the European Parliament in the Raad van 31 March 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten als bedrijven en maritiem vervoer worden definieerd, met uitzondering van deze ze bedrijven individual exploitation is carried out
		- Beheerders van havens zoals gedefinieerd in article 3, point 1, van Richtlijn 2005/65/EG of the European Parliament and of Raad van October 26, 2005 will be released before the end of October 26, 2005 havens, inclusive of havenfaciliteiten zoals gedefinieerd in article 2, point 11, van Verordening (EG) nr. 725/2004 from Europe Parliament of Raad on March 31, 2004 shall be subject to verbatim van deveiliging van schepen en havenfaciliteiten; alsook entities-ten die uitrusting in havens beheren
		- Exploiters of verkeersbegeleidingssystemen (VBS) zooals gede-finieerd in article 3, point *o),* van Richtlijn 2002/59/EG van het European Parliament in Raad on June 27, 2002 will be published invoering community monitoring in information systems for your first trip to Richtlijn 93/75/EEG van de Raad
	d) Weg	- We have authorized zoo data in article 2, point 12, at gedelegeerde Verordening (EU) 2015/962 van de Commissie van December 18, 2014 was published by Richtlijn 2010/40/EU by het European Parliament in Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft die verantwoordelijk zijn you will see what you have said, and you will find the overheard instants the use of intelligent operating systems means that they are not essential for any purpose activity is
		- Operator of intelligent control systems for controlled animals in article 4, point 1, van Richtlijn 2010/40/EU van het Europees Parliament in de Raad on July 7, 2010 will be released by your party Invoeren van intelligent vervoerssystemen op het gebied van wegvervoer en voor interfaces met etere vervoerswijzen

Bijlage I - Zeer kritieke sectors		
Sector	Deelsector	Soort entity
3. Banking		- Kredietinstellingen zoals gedefinieerd in article 4, point 1, Veror-dening (EU) nr. 575/2013 of the European Parliament in de Raad on June 26, 2013, you should be careful to check your credit reports and be informed to the fullest extent of Veror-dening (EU) nr. 648/2012
4. Financial market infrastructure		- Operators of handelsplatforms zoals defined in article 4, point 24, van Richtlijn 2014/65/EU van het Europees Parliament in de Raad on May 15, 2014 will be marked for you financial instruments in accordance with the Financial Regulations 2002/92/EG and Regulation 2011/61/EU
		- Centrale tegenpartijen zooals defined in article 2, point 1, Verordening (EU) nr. 648/2012 of the European Parliament in Posted on July 4, 2012, OTC derivatives will be transferred, centrally tegenpar-tijen en transactieregisters
5. Health care organization		- Zorgaanbieders zoals defined in article 3, point *g),* van Richtlijn 2011/24/EU of the European Parliament and of Raad van March 9, 2011 there will be a delay in passing by the patient. bij grensoverschrijdende gezondheidszorg
		- EU-referentielaboratoria als bedoeld in article 15 van Verordening (EU) 2022/2371 of the European Parliament in the European Parliament November 23, 2022 inzake ernstige grensoverschrijdende gezond-heidsbedreigingen en tot trekking van Besluit nr. 1082/2013/EU inzake ernstige grensoverschrijdende bedreigingen van de gezond-heid
		- Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zooals defined in article 1, point 2, van Richtlijn 2001/83/EG of the European Parliament in de Raad van 6 november 2001 tot vaststelling van een communautair Wetboek betreffende geneesmiddelen voor menselijk gebruik
		- Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in bijlage I, sectie C, afdeling 21, van Verordening (EG) nr. 1893/2006 of the European Parliament in Posted on December 20, 2006, the vast story of statistics classification of economic activities NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 in enkele EG-verordeningen op specifieke statistische gebieden vervaardigen
		- Entiteiten die dische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (ÿde lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelenÿ) in de zin van article 22 van Verordening (EU) 2022/123 van het Europees Parliament in December 25, 2022 will be open to the public van het Europees Geneesmiddelenbureau inzake crisisparatheid in -beheersing op het gebied van geneesmiddelen en medische helpers
6. Drinkwater		- Leveragers in distributors for low consumption bestemd water zoals defined in article 2, point 1, *a),* van Richtlijn (EU) 2020/2184 of the European Parliament in de Raad on December 16, 2020, the content of your comments will be confirmed consumption bestemd water, met uitzondering van distributors how to distribute water to your monthly consumption niet-essentieel deel est van hun algemene activiteit van distributie Van Andere Waren en Goederen die niet worden beschouwd als essential of belangrijke diensten
7. Afvalwater		- Ondernemingen d'estelijk afvalwater, huishoudelijk afvalwater of industrial afvalwater zoals defined in article 2, points 1, 2 in 3, van Richtlijn 91/271/EEG van de Raad van 21 May 1991 inzake de behandeling van stedelijk afvalwater opvangen, lozen de behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrial afvalwater is not essential onderdeel van hun algemene activity is

Bijlage I - Zeer kritieke sectors		
Sector	Deelsector	Soort entity
8. Digital infrastructure		- Aanbieders van internetknooppunten
		- DNS service providers, who operate the van root-nameservers
		- Registers for top level domains
		- Aanbieders van cloudcomputing services
		- Information about data centers
		- Aanbieders van netwerken voor de levering van inhoud
		- Verleners van vertrouwensdiensten
		- Aanbieders van openbare elektronische-communicatienetwerken
		- Aanbieders van openbare elektronische-communicatiediensten
9. Support for ICT services (business-to-business)		- Notes on previous services
		- Aanbieders van beheerde beveiligingsdiensten
10. Oversight		- Overheids instanties of the Federal State after they have changed
		- Overheids instanties die van deelgebieden afhangen, geïdenti-ficeerd overeenkomstig artikel 11, § 2, van de wet
		- De hulpverleningszones in de zin van article 14 van de wet van May 15, 2007 betreffende de civiele veiligheid de Bruxelles Hoofdstedelijke Services for Brandweer and Dringende Medische Hulp opgericht door de orderantie van 19 Juli 1990 houdende Oprichting van de Brussels Hoofdstedelijke Dienst voor Brandweer and medical help
11. Ruimtevaart		- Operator of the ground facilities die in het bezit zijn van de beheerd of geëëxploiteerd worden door de lidstaten of door particu-liere partijen en die de verlening van vanuit de ruimte operarende diensten ondersteunen, met uitzondering van aanbieders van openbare electronic communication service

Please note that your words will be written on April 26, 2024, to the fullest extent of your cyber awareness.
the netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP

Van Koningswege:

The First Minister,
A. DE CROO

From Minister van Binnenlandse Zaken,
A. VERLINDEN

Bijlage II is due on April 26, 2024 to broad-speak for our cyberbelieving
the netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Bijlage II - Andere kritieke sectors		
Sector	Deelsector	Soort entity
1. Post and courier services		- Aanbieders van postdiensten zoals definieerd in article 2, point *1bis,* van Richtlijn 97/67/EG of the European Parliament in de Posted on December 15, 1997, the current regulations are valid. for access to internal marketing services Gemeenschap en de verbetering van de kwaliteit van de services, met inbegrip van aanbieders van koeriersdiensten
2. Fuel supplier		- Ondernemingen die handelingen en het kader van afvalstoffenbe-heer uitvoeren zoals definieerd in article 3, point 9, van Richtlijn 2008/98/EG of the European Parliament on November 19, 2008 will be made by the European Parliament on November 19, 2008. Richtlijnen, met uitzondering van ondernemingen waarvoor afval-stoffenbeheer niet de voornaamste economics activiteit is

Bijlage II - Andere kritieke sectors		
Sector	Deelsector	Soort entity
3. Vervaardiging, productie in distribution of chemical fabrics		- Ondernemingen die fabrics vervaardigen en fabric de mengsels distributed en als bedoeld in article 3, point 9 en 14, van Verorde-ning (EG) nr. 1907/2006 of the European Parliament on December 18, 2006, registration and authorization of chemical materials (REACH) are authorized by European Agents for chemical materials, which are authorized by the Richtlijn 1999/45/EG en houdende intrekking van Verordening (EEG) nr. 793/93 van de Raad en Verordening (EG) nr. 1488/94 van de Commissie alsmede Richtlijn 76/769/EEG van de Raad en de Richtlijnen 91/155/EEG, 93/67/EEG, 93/105/EG en 2000/21/EG van de Commissie en ondernemingen die voorwerpen zoals definieerd en artikel 3, point 3, van die verordening produceren uit stoffen de mengsels
4. Product, delivery and distribution of products and services		- Levensmiddelenbedrijven zoals defined in article 3, point 2, Verordening (EG) nr. 178/2002 of the European Parliament of January 28, 2002 to the vaststelling of algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tutttelling van procedures voor Voedselveiligheidsaangelegen-heden die zich bezighouden met grothandel en industriële produc-tie en verwerking
5. Management	a) Vervaardiging of hulpmiddelen medische hulp-middelen voor in-vitrodiagnostiek	- Entiteiten die dische hulpmiddelen zoals definieerd in article 2, point 1, van Verordening (EU) 2017/745 van het European Parliament in de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 in Verordening (EG) nr. 1223/2009, in total intrekking van Richtlijnen 90/385/EEG en 93/42/ EEG van de Raad vervaardigen entiteiten die dische hulpmiddelen voor in-vitrodiagnostiek zoals definieerd in article 2, point 2, van Verordening (EU) 2017/746 of the European Parliament in the European Parliament on April 5, 2017 should be taken into account by the medical authorities for in-vitrodiagnostics in the early days of Richtlijn 98/79/EG in Besluit 2010/227/EU by the Commission vervaardigen, met uitzon-dering van entiteiten die hospital medicine Vervaardigen als bedoeld in bijlage I, point 5, vijfde streepje, van deze richtlijn
	b) Verification of computer products in electronic and optical products	- Ondernemingen economic activities uitvoeren als bedoeld in bijlage I, sectie C, afdeling 26, van Verordening (EG) nr. 1893/2006 of the European Parliament in December 20, 2006, tot vaststelling of statistical classification of economic activities by NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 in EG-verordeningen op specifieke statistische gebieden
	c) Control of electrical devices	- Ondernemingen die economic activiteiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 27, van Verordening (EG) nr. 1893/2006 of the European Parliament in December 20, 2006, tot vaststelling of statistical classification of economic activities by NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 in EG-verordeningen op specifieke statistische gebieden
	d) Vervaardiging van machines, apparaten en werktuigen, neg	- Ondernemingen economic activities uitvoeren als bedoeld in bijlage I, sectie C, afdeling 28, van Verordening (EG) nr. 1893/2006 of the European Parliament in December 20, 2006, tot vaststelling of statistical classification of economic activities by NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 in EG-verordeningen op specifieke statistische gebieden
	e) Vervaardiging de motorvoer-tuigen, aanhangers en opleggers	- Ondernemingen die economic activitesiten uitvoeren als bedoeld in bijlage I, sectie C, afdeling 29, van Verordening (EG) nr. 1893/2006 of the European Parliament in December 20, 2006, tot vaststelling of statistical classification of economic activities by NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 in EG-verordeningen op specifieke statistische gebieden

Bijlage II - Andere kritieke sectors		
Sector	Deelsector	Soort entity
	f) Vervaardiging van andere transportmiddelen	- Ondernemingen economic activities uitvoeren als bedoeld in bijlage I, sectie C, afdeling 30, van Verordening (EG) nr. 1893/2006 of the European Parliament in December 20, 2006, tot vaststelling of statistical classification of economic activities by NACE Rev. 2 in total wijziging van Verordening (EEG) nr. 3037/90 enkele EG-verordeningen op specifieke statistische gebieden - Aanbieders van online marktplaatsen - Aanbieders van onlinezoekmachines
6. Digital additions		
		- Aanbieders van platforms voor socialenetwerkdiensten
7. Undersearch		- Search organizations

Gezien om te worden gevoegd bij de wet van April 26, 2024 tot vaststelling van een kader de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP

Van Koningswege: De

Eerste Minister, A. DE CROO

By Minister van Binnenlandse Zaken, A. VERLINDEN

Annex I to the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security

Annex I - Highly critical sectors		
Sector	Subsector	Entity type
1. Energy	a) Electricity	- Electricity undertakings within the meaning of Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU, which perform the function of ÿsupplyÿ within the meaning of Article 2(12) of that Directive
		- Distribution system operators within the meaning of Article 2(29) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU
		- Transmission system operators within the meaning of Article 2(35) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU
		- Producers within the meaning of Article 2(38) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU
		- Designated electricity market operators within the meaning of Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market in electricity
		- Market participants within the meaning of Article 2, point 25), of the Regulation (EU) 2019/943 providing energy aggregation, demand response or storage services within the meaning of Article 2(18), (20) and (59) of Directive (EU) 2019/944 of European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU

Annex I - Highly critical sectors		
Sector	Subsector	Entity type
		- Charging point operators who are responsible for the management and operation of a charging point, which provides a charging service to end users, including in the name and on behalf of a mobility service provider
	b) Heating and cooling network	- Heat network or cooling network operators within the meaning of Article 2, point 19, of Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources
	c) Oil	- Oil pipeline operators
		- Operators of oil production, refining, processing, storage and transportation facilities
		- Central storage entities within the meaning of Article 2(f) of Council Directive 2009/119/EC of 14 September 2009 requiring Member States to maintain a minimum level of stocks of crude oil and/or petroleum products
	d) Gas	- Supply companies within the meaning of Article 2, point 8, of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- Distribution system operators within the meaning of Article 2, point 6, of Directive 2009/73/EC of the European Parliament and of the Council Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- Transmission system operators within the meaning of Article 2, point 4, of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- Storage facility managers within the meaning of Article 2, point 10, of Directive 2009/73/EC of the European Parliament and of the Council Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- LNG installation operators within the meaning of Article 2, point 12, of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- Natural gas undertakings within the meaning of Article 2, point 1, of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC
		- Operators of natural gas refining and processing facilities
	e) Hydrogen	- Operators of hydrogen production, storage and transport systems
2. Transport	a) Air transport	- Air carriers within the meaning of Article 3, point 4, of the Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, used for commercial purposes
		- Airport managing bodies within the meaning of Article 2(2) of Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges, airports within the meaning of Article 2(1) of that Directive, including core network airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU, and entities operating ancillary facilities located at airports
		- Air traffic control services within the meaning of Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the Single European Sky

Annex I - Highly critical sectors		
Sector	Subsector	Entity type
	b) Rail transport	- Infrastructure managers within the meaning of Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area
		- Railway undertakings within the meaning of Article 3(1) of Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area, including service facility operators within the meaning of Article 3(12) of that Directive
	(c) Water transport	- Inland waterway, sea and coastal passenger and freight transport companies, as defined for the maritime transport sector in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, excluding ships operated individually by these companies
		- Port managing bodies within the meaning of Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, including port facilities within the meaning of Article 2(11) of Regulation (EC) No 725/2004 of the European Parliament and of the Council Council of 31 March 2004 on improving the safety of ships and port facilities, as well as entities operating infrastructure and equipment within ports
		- Vessel traffic service (VTS) operators within the meaning of Article 3(o) of Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC
	d) Road transport	- Road authorities within the meaning of Article 2(12) of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Cou Council on the provision throughout the Union of real-time traffic information services responsible for the control of traffic management, excluding public entities for which traffic management or the operation of intelligent transport systems constitutes a non-core part of their general business
		- Operators of intelligent transport systems within the meaning of Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of intelligent transport systems in the field of road transport and interfaces with other modes of transport
3. Banking sector		- Credit institutions within the meaning of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
4. Financial market infrastructures		- Operators of trading venues within the meaning of Article 4(24) of Directive 2014/65/EU of the European Parliament and of the Council Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
		- Central counterparties within the meaning of Article 2, point 1), of the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories
5. Health		- Healthcare providers within the meaning of Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare
		- European Union reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 concerning serious cross-border threats to health and repealing Decision No 1082/2013/EU

Annex I - Highly critical sectors		
Sector	Subsector	Entity type
		- Entities carrying out research and development activities in the field of medicinal products within the meaning of Article 1, point 2, of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 establishing a Community code relating to medicines for human use
		- Entities manufacturing basic pharmaceutical products and pharmaceutical preparations within the meaning of Annex I, Section C, Division 21 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical classification of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 and certain EC Regulations relating to specific statistical domains
		- Entities manufacturing medical devices considered critical in the event of a public health emergency (list of critical medical devices in the event of a public health emergency) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a strengthened role of the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices
6. Drinking water		- Suppliers and distributors of water intended for human consumption within the meaning of Article 2(1) *(a)* of Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption, excluding distributors for whom the distribution of water intended for human consumption constitutes a non-essential part of their general activity of distribution of other products and goods
7. Wastewater		- Undertakings collecting, discharging or treating urban waste water, domestic waste water or industrial waste water within the meaning of Article 2(1), (2) and (3) of Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment, excluding undertakings for which the collection, discharge or treatment of urban waste water, domestic waste water or industrial waste water constitutes a non-essential part of their general business
8. Digital infrastructure		- Internet exchange point providers
		- DNS service providers, excluding domain name root server operators
		- Top-level domain name registries
		- Cloud computing service providers
		- Data center service providers
		- Content delivery network providers
		- Trusted service providers
		- Providers of public electronic communications networks
		- Providers of publicly available electronic communications services
9. ICT service management (inter-company)		- Managed Service Providers
		- Managed Security Service Providers
10. Public administration		- Public administration entities that depend on the federal state
		- Public administration entities that depend on federated entities, identified in accordance with Article 11, § 2 of the law

Annex I - Highly critical sectors		
Sector	Subsector	Entity type
		- Emergency zones within the meaning of Article 14 of the law of 15 May 2007 relating to civil security or the Fire and Rescue Service urgent medical service of the Brussels-Capital Region created by the order of July 19, 1990 establishing a Service fire and emergency medical aid of the Brussels Region-Capital
11. Space		- Operators of land-based infrastructure, owned, managed and operated by Member States or by private parties, which support the provision of space services, excluding providers of public electronic communications networks

Seen to be annexed to the law of April 26, 2024 establishing a framework for the cybersecurity of networks and systems information of general interest for public safety

PHILIPPE

By the King:

The Prime Minister,
A. DE CROO

The Minister of the Interior,
A. VERLINDEN

Annex II to the law of April 26, 2024 establishing a framework for cybersecurity networks and information systems of general interest for public safety

Annex II - Other critical sectors		
Sector	Subsector	Entity type
1. Postal and shipping services		- Postal service providers within the meaning of Article 2, point 1a), of Directive 97/67/EC of the European Parliament and of the Council of December 15, 1997 concerning common rules for the development of the internal market for postal services Community and improving the quality of service, including shipping service providers
2. Waste management		- Companies carrying out waste management operations in meaning of Article 3(9) of Directive 2008/98/EC of the European Parliament European Parliament and of the Council of 19 November 2008 on waste and repealing certain directives, excluding companies for in which waste management is not the main activity economic
3. Manufacture, production and distribution of chemical products		- Companies engaged in the manufacture of substances and distribution of substances or mixtures within the meaning of Article 3, points 9 and 14 of Regulation (EC) No 1907/2006 of the European Parliament European and Council of 18 December 2006 concerning the registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Regulation (EEC) No 793/93 of the Council and Regulation (EC) No 1488/94 of the Commission as well as Council Directive 76/769/EEC and the directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC the Commission and companies producing articles in meaning of Article 3(3) of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		- Food sector companies within the meaning of Article 3, point 2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 establishing the general principles and general requirements of food legislation, establishing the European Food Safety Authority and setting food safety procedures that carry out wholesale distribution activities as well as industrial production and processing

Annex II - Other critical sectors		
Sector	Subsector	Entity type
5. Manufacturing	(a) Manufacture of medical devices and medical devices in vitro diagnostic	- Entities manufacturing medical devices within the meaning of Article 2, point 1), of Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 relating to medical devices, amending the Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC and entities manufacturing medical devices of in vitro diagnostic within the meaning of Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 relating to in vitro diagnostic medical devices and repealing the Directive 98/79/EC and Commission Decision 2010/227/EU, except for entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this directive
	(b) Manufacture of computer, electronic and optical products	- Companies carrying out one of the economic activities referred to in Annex I, Section C, Division 26 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical nomenclature of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 as well as certain regulations (EC) relating to specific statistical areas
	(c) Manufacture of electrical equipment	- Companies carrying out one of the economic activities referred to in Annex I, Section C, Division 27 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical nomenclature of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 as well as certain regulations (EC) relating to specific statistical areas
	(d) Manufacture of machinery and nec equipment	- Companies carrying out one of the economic activities referred to in Annex I, Section C, Division 28 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical nomenclature of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 as well as certain regulations (EC) relating to specific statistical areas
	e) Construction of motor vehicles, trailers and semi-trailers	- Companies carrying out one of the economic activities referred to in Annex I, Section C, Division 29 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical nomenclature of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 as well as certain regulations (EC) relating to specific statistical areas
	(f) Manufacture of other equipment transport	- Companies carrying out one of the economic activities referred to in Annex I, Section C, Division 30 of Regulation (EC) No 1893/2006 of the European Parliament and of the Council of 20 December 2006 establishing the statistical nomenclature of economic activities NACE Rev. 2 and amending Council Regulation (EEC) No 3037/90 as well as certain regulations (EC) relating to specific statistical areas
6. Digital Suppliers		- Online marketplace providers
		- Online search engine providers
		- Providers of social networking service platforms
7. Research		- Research organizations

Seen to be annexed to the law of April 26, 2024 establishing a framework for the cybersecurity of networks and systems information of general interest for public safety

PHILIPPE

By the King:

The Prime Minister,
A. DE CROO

The Minister of the Interior,
A. VERLINDEN