Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 08/2022 van 21 januari 2022

Betreft: Voorontwerp van wet inzake de certificering van cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (CO-A-2021-256)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig: De heren Yves-Alexandre de Montjoye, Bart Preneel en Frank Robben;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, en met name de artikelen 23 en 26 (hierna 'WOG');

Gelet op verordening (EU) nr. 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna 'AVG');

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna de 'WVP');

Gelet op de op 30 november 2021 ontvangen adviesaanvraag van de premier, Alexander De Croo;

Gelet op de aanvullende inlichtingen die op 14 december 2021 werden ontvangen;

Brengt het volgende advies uit op 21 januari 2022:

I. Onderwerp en achtergrond van het verzoek

1. Op 30 november 2021 heeft de premier de Autoriteit om advies gevraagd over het voorontwerp van wet inzake de certificering van cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (hierna 'het voorontwerp van wet').

2. Dit voorontwerp van wet strekt tot uitvoering van verordening (EU) 2019/881 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (ICT) (hierna de 'Cyberbeveiligingsverordening').

3. Deze Cyberbeveiligingsverordening heeft tot doel het vertrouwen in de ICT-sector te vergroten door een Europees kader voor cyberbeveiligingscertificering vast te stellen, waarin horizontale voorschriften worden vastgesteld voor de ontwikkeling van certificeringsregelingen op het vlak van cyberbeveiliging voor verschillende categorieën ICT-producten[1], -diensten[2] en -processen[3]. ENISA is verantwoordelijk voor het opstellen van certificeringsregelingen, die vervolgens door de Europese Commissie zullen worden aangenomen door middel van uitvoeringshandelingen. Een Europese cyberbeveiligingscertificeringsregeling is volgens de Cyberbeveiligingsverordening *"een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale overheidsinstantie zijn ontwikkeld en vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-producten, -diensten en -processen die onder het toepassingsgebied van de specifieke regeling vallen".* In elke certificeringsregeling wordt onder meer gespecificeerd op welke soort of categorieën ICT-producten, -diensten en -processen ze betrekking heeft, wat het doel is, welke normen er gelden en welke evaluatiemethoden er worden gebruikt. De Europese cyberbeveiligingscertificaten, afgegeven door de conformiteitsbeoordelingsinstanties die door nationale accreditatie-instanties zijn geaccrediteerd, bevestigen dat een ICT-product, -dienst of -proces is beoordeeld op het vlak van de naleving van de specifieke beveiligingseisen die in een Europese cyberbeveiligingscertificeringsregeling zijn vastgesteld. De Cyberbeveiligingsverordening definieert drie zekerheidsniveaus, die in verhouding staan tot verschillende risiconiveaus. Het gaat om de volgende niveaus: basis, substantieel en hoog.

---

[1] In de Cyberbeveiligingsverordening gedefinieerd als *"een element of groep elementen van een netwerk- of informatiesysteem".*

[2] In de Cyberbeveiligingsverordening gedefinieerd als *"een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen".*

[3] In de Cyberbeveiligingsverordening gedefinieerd als *"een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden".*

4. Tenzij in het recht van de Europese Unie of in de nationale wetgeving van een lidstaat anders is bepaald, vindt de certificering of de conformiteitsverklaring op vrijwillige basis plaats. De Europese Commissie zal op geregelde tijdstippen nagaan of het nodig is om certificaten verplicht te stellen. De Cyberbeveiligingsverordening voorziet in de mogelijkheid om zich te laten certificeren of over te gaan tot een conformiteitsverklaring. Een certificaat wordt afgegeven door een onafhankelijke en geaccrediteerde conformiteitsbeoordelingsinstantie. Een conformiteitsverklaring wordt afgegeven onder de verantwoordelijkheid van de ICT-fabrikant of -leverancier door middel van een zelfbeoordeling. In elke certificeringsregeling wordt aangegeven of een dergelijke conformiteitsverklaring al dan niet is toegestaan en de zelfbeoordeling is beperkt tot het 'basis'-zekerheidsniveau.

5. De lidstaten moeten, ter uitvoering van deze verordening, de nationale cyberbeveiligingscertificeringsautoriteit of -autoriteiten aanwijzen, die certificaten zullen afgeven, of zullen instaan voor het toezicht en de controle op de correcte toepassing van de regels door de verschillende actoren (fabrikanten, leveranciers en aanbieders van ICT-producten en -diensten die houder zijn van een certificaat of die een conformiteitsverklaring hebben afgegeven, en conformiteitsbeoordelingsinstanties). Bovendien moeten de lidstaten in hun nationale wetgeving specifieke regels vaststellen om de correcte toepassing van deze verordening te waarborgen, bijvoorbeeld met betrekking tot sancties of de intrekking van certificaten. Dat is het onderwerp van het voorontwerp van wet dat voor advies is voorgelegd.

II. Onderzoek

Algemene opmerkingen – Mededeling van gegevens door de autoriteiten die belast zijn met de controle op de naleving van de Cyberbeveiligingsverordening en de Europese regelingen voor de cyberbeveiligingscertificering en de bescherming van de klanten (natuurlijke personen) van de gecontroleerde aanbieders van ICT-diensten (of van de klanten-natuurlijke personen van dergelijke klanten van wie de gegevens zijn opgenomen in de gecontroleerde ICT-diensten)

6. Dit advies van de Autoriteit is slechts geldig voor zover gegevensverwerkingen met betrekking tot natuurlijke personen onder de bepalingen van het voorontwerp van wet vallen. De gegevensverwerkingen die moeten worden uitgevoerd in het kader van de door de Cyberbeveiligingsverordening vereiste controles, kunnen betrekking hebben op persoonsgegevens in de zin van de AVG wanneer de fabrikanten of leveranciers van ICT-producten, de aanbieders van ICT-diensten of van ICT-processen die houder of aanvrager zijn van een Europees conformiteitscertificaat inzake cyberbeveiliging, natuurlijke personen zijn, maar ook wanneer de controle van de naleving van de certificeringsregelingen door de leveranciers van deze

gecertificeerde ICT-diensten de verwerking van persoonsgegevens met zich meebrengt, zoals de gegevens van hun klanten-natuurlijke personen of de klanten-natuurlijke personen van hun klanten. Laten we de clouddiensten[4] als voorbeeld nemen: het is gebruikelijk dat de klanten van een aanbieder van clouddiensten deze diensten gebruiken voor hun eigen verwerkingen van persoonsgegevens, waarbij het kan gaan om bijzondere categorieën van gegevens in de zin van de AVG, afhankelijk van het werkterrein van die klanten (bv. een ziekenhuis, een advocatenkantoor of een overheidsinstantie die belast is met de preventie en opsporing van strafrechtelijke inbreuken).

7. Zoals de European Data Protection Supervisor heeft opgemerkt in een van zijn recente adviezen over de Europese strategie voor cyberbeveiliging en over de richtlijn NIS 2.1[5]: *"Article 5(1)(f) of Regulation (EU) 2016/679 (GDPR) has established security as one of the main principles relating to the processing of personal data. Article 32 GDPR further defines this obligation, applicable to both controllers and processors, to ensure an appropriate level of security. Both provisions make clear that security is essential for compliance with EU data protection law. This is why (...) improving cybersecurity is essential for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data (...). At the same time (...) the pursuance of the objectives of cybersecurity may lead to deploying measures that interfere with the rights to data protection and privacy of individuals. This means ensuring that any potential limitation of the right to the protection of personal data and privacy must fulfil the requirements of Article 52(1) of EU Charter of Fundamental Rights, in particular being achieved by way of a legislative measure, being both necessary and proportionate, and respecting the essence of the right."*

8. In het licht van deze overwegingen is het voorontwerp van wet problematisch omdat het voorziet in zeer ruime gegevensuitwisselingen tussen enerzijds de nationale cyberbeveiligingscertificeringsautoriteit en de andere autoriteiten die zullen worden aangewezen voor de uitvoering van de in de Cyberbeveiligingsverordening bedoelde controle-opdrachten, en anderzijds de volgende autoriteiten: de gerechtelijke overheden, de sectorale overheden of de inspectiediensten respectievelijk bedoeld in artikel 7, § 3 en § 5, 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, de markttoezichtautoriteiten, de nationale

[4] Cf. EUCS, a candidate cybersecurity certification scheme for cloud services, december 2020, beschikbaar op de ENISA-website: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@@download/fullReport. Er wordt bepaald dat "the EUCS scheme may cover any type of ICT service, provided that the ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface (ISO 17788) and that the ICT service aims at reaching the assurance level corresponding to one of the three levels "basic", "substantial" and "high" of the EUCSA as defined in the EUCS scheme".

[5] EDPS Opinion 05/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, beschikbaar op de website van de EDPS op https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en.

accreditatieautoriteit, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid.

9. Deze uitwisselingen doen vragen rijzen in verband met hun zeer ruime onderwerp, zoals thans in het voorontwerp van wet is bepaald. Meermaals wordt namelijk bepaald dat zij niet alleen plaatsvinden voor de uitoefening van openbaredienstopdrachten die bestaan in de controle op de naleving van de Cyberbeveiligingsverordening en de Europese cyberbeveiligingscertificeringsregelingen of de conformiteitsverklaringen die ter uitvoering van de genoemde verordening worden afgegeven, maar ook voor de toepassing van andere wettelijke bepalingen (zonder te specificeren om welke wettelijke bepaling het gaat; op die manier kan niet worden nagegaan of er een duidelijk verband bestaat met de bovengenoemde Cyberbeveiligingsverordening). Dit lijkt onevenredig, niet conform het toepassingsgebied van het voorontwerp van wet dat de Cyberbeveiligingsverordening ten uitvoer moet leggen, volgens de algemene overwegingen van de memorie van toelichting.

10. Bovendien dreigt dit gebrek aan een minimumkader voor dergelijke uitwisselingen de door de Europese cyberbeveiligingsverordening nagestreefde doelstelling van vertrouwen in gecertificeerde ICT-producten en -diensten te ondermijnen, aangezien de gegevens van de klanten (of hun klanten) van door de cyberbeveiligingscertificeringsautoriteit gecontroleerde ICT-dienstverleners volgens de formulering van het wetsontwerp kunnen worden verzameld en gebruikt door overheidsdiensten die geen specifieke cyberbeveiligingsopdracht hebben, zoals politie of inlichtingendiensten, voor hun eigen opdrachten van preventie en opsporing van strafbare feiten, onderzoek en vervolging, of zelfs voor opdrachten van de Staatsveiligheid en de Algemene Inlichtingen- en Veiligheidsdienst. Deze situatie kan een belemmering vormen voor de bevordering van ICT-diensten en -producten die gecertificeerd zijn in overeenstemming met de Cyberbeveiligingsverordening, en bijgevolg voor de verbetering van de informatiebeveiliging op deze gebieden.

11. De auteur van het voorontwerp van wet moet daarom de uitwisselingen regelen in overeenstemming met wat strikt noodzakelijk en redelijk is in het licht van het toepassingsgebied en de doelstellingen van de Cyberbeveiligingsverordening. In artikel 58.7.a van de Cyberbeveiligingsverordening wordt trouwens bepaald dat de nationale cyberbeveiligingscertificeringsautoriteiten uitsluitend in samenwerking met *"andere betrokken markttoezichtautoriteiten* " moeten toezien op de naleving van de in de Europese cyberbeveiligingscertificeringsregelingen opgenomen regels en die regels moeten handhaven, en niet om het even welke overheidsinstantie. Artikel 58.7.h van die verordening bepaalt dan weer

het volgende: nationale cyberbeveiligingscertificeringsautoriteiten *"werken samen met andere nationale cyberbeveiligingscertificeringautoriteiten of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-conformiteit van ICT-producten, -diensten en -processen met de voorschriften van deze verordening of met de voorschriften van specifieke Europese cyberbeveiligingscertificeringsregelingen"*. In overweging 102 van deze verordening wordt in dat verband het volgende gespecificeerd: *"De Commissie moet die informatie-uitwisseling bevorderen door een algemeen elektronisch informatieondersteuningssysteem beschikbaar te stellen, bijvoorbeeld het informatie- en communicatiesysteem voor markttoezicht (ICSMS) en het systeem voor snelle waarschuwingen over gevaarlijke niet-levensmiddelen (Rapex), die overeenkomstig Verordening (EG) nr. 765/2008 al door markttoezichtautoriteiten worden gebruikt."* Dit voorbeeld van het melden van waarschuwingen over de aanwezigheid van producten of diensten die niet voldoen aan een certificeringsregeling, sluit goed aan bij het Europees kader voor cyberbeveiligingscertificering, zoals beschreven in artikel 46 van de Cyberbeveiligingsverordening. De Autoriteit is bijgevolg van oordeel dat de bedoelde uitwisselingen beperkt moeten blijven tot de verwezenlijking van deze doelstelling en geen ruimte mogen laten voor de toepassing van om het even welke wettelijke bepaling. Dit delen van informatie over de niet-naleving, door ICT-producten, -diensten en -processen, van de vereisten van de Cyberbeveiligingsverordening of van bepaalde specifieke Europese cyberbeveiligingscertificeringsregelingen vereist volgens de Autoriteit geen uitwisseling van de persoonsgegevens die de genoemde klanten in het kader van hun contractuele relatie aan de genoemde dienstverleners ter beschikking stellen.

12. Op de vraag wat de gegevensuitwisseling met de verschillende in artikel 6, § 3, van het voorontwerp bedoelde autoriteiten rechtvaardigt, antwoordde de afgevaardigde van de minister het volgende:
    a. Met betrekking tot de gerechtelijke autoriteiten: *"Il apparaît nécessaire que les autorités judiciaires puissent solliciter ou être notifiées des informations en cas d'infractions pénales (fraudes liées à la délivrance, aux contrôles, aux sanctions et aux réclamations des certifications de cybersécurité ou d'infractions pénales prévues par les différentes législations sectorielles - dont la loi NIS."* In dit verband merkt de Autoriteit in de eerste plaats op dat bij lezing van het voorontwerp van wet inbreuken op de Cyberbeveiligingsverordening en de Europese certificeringsregelingen enkel worden bestraft via de wijziging van het Wetboek van Economisch Recht en dat boek XV van dit wetboek reeds de gegevensmededeling regelt die de economische inspectie bij de uitoefening van haar opdrachten kan verrichten. Vervolgens wordt in artikel 29 van het Wetboek van Strafvordering (Sv.) reeds het volgende bepaald: *"Iedere gestelde overheid, ieder openbaar officier of ambtenaar (...) die in de uitoefening van zijn ambt kennis krijgt van een misdaad of van een wanbedrijf, is verplicht daarvan dadelijk bericht te geven aan*

de procureur des Konings bij de rechtbank binnen wier rechtsgebied die misdaad of dat wanbedrijf is gepleegd of de verdachte zou kunnen worden gevonden, en aan die magistraat alle desbetreffende inlichtingen, processen-verbaal en akten te doen toekomen." Het is niet nodig, en vanuit het oogpunt van de bescherming van persoonsgegevens zelfs contraproductief, om deze mededeling van gegevens in het voorontwerp van wet te herhalen zonder de modaliteiten ervan vast te leggen, temeer daar in artikel 29 Sv. de inachtneming van bepaalde formaliteiten in dit verband wordt opgelegd. De Autoriteit beveelt bijgevolg aan deze uitwisseling uit het voorontwerp van wet te schrappen.

b. Met betrekking tot de sectorale autoriteiten (NIS)[6]: *"Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle des mesures de sécurité des réseaux et systèmes d'informations (P.S.I., voir article 21 et suivants de la loi NIS), qui serait titulaire*

[6] Zoals uit de aanvullende informatie blijkt, gaat het om de volgende autoriteiten:

"Les autorités sectorielles visées à l'article 3, § 3 de l'avant-projet de loi sont les autorités visées à l'article 6, 2° de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après, "loi NIS").

Il s'agit concrètement des autorités suivantes :

- *Désignées par la loi NIS :*
  - *La BNB (art. 95. de la loi NIS qui a inséré un article 36/47 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique).*
  - *La FSMA (art. 90 et 91 de la loi NIS ayant modifiés les art. 71 et 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers).*
  - *L'IBPT (art. 88. de la loi NIS qui a modifié l'art. 14, § 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges).*
- *Désignées par l'annexe 1 de l'arrêté royal du 12 juillet 2019 (portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques) :*
  - *pour le secteur de l'énergie : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des transports :*
    - *En ce qui concerne le secteur du transport, à l'exception du transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
    - *En ce qui concerne le transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des fournisseurs de service numérique : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
- *Désignée par l'arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable :*
  - *le Comité national de sécurité pour la fourniture et la distribution d'eau potable."*

ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant."

In dit verband begrijpt de Autoriteit dat deze sectorale autoriteiten, die specifieke opdrachten hebben op het gebied van informatiebeveiliging, ervan in kennis moeten worden gesteld dat de organisaties waarvan zij de naleving van de bepalingen van de bovengenoemde wet van 7 april 2019 (bekend als de NIS-wet) controleren, gebruikmaken van gecertificeerde ICT-diensten of -producten waarvan de niet-naleving van de certificeringsregeling is vastgesteld door de nationale certificeringsautoriteit of door een autoriteit die is aangewezen ter uitvoering van artikel 5, § 2 van het voorontwerp van wet. In dit verband vraagt de Autoriteit zich af of de maatregelen tot intrekking van een certificering – die door hun aard aan publiciteitsmaatregelen zouden moeten worden onderworpen – hiervoor niet zouden moeten volstaan. Indien dit niet het geval zou zijn (wat in de memorie van toelichting zou moeten worden gemotiveerd), is de Autoriteit, gezien de met de cyberbeveiliging verband houdende aard van de opdrachten van de krachtens de NIS-wet opgerichte controle-autoriteiten, van oordeel dat deze uitwisselingen noodzakelijk lijken, maar dat het, naast het geven van een definitie van het in het voorontwerp van wet gebruikte begrip *"sectorale autoriteiten"* (uitdrukkelijke vermelding van de bedoelde autoriteiten), noodzakelijk is om in het voorontwerp van wet[7] duidelijk de omstandigheden en modaliteiten te bepalen van deze gegevensmededelingen door de nationale cyberbeveiligingscertificeringsautoriteit en de krachtens artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten, alsook het doel van de verwerking die door de bedoelde sectorale autoriteiten met deze informatie zal worden verricht. Bovendien moet dan ook worden voorzien in de beperking van de uitwisselingen over de vaststelling van een inbreuk op de informatiebeveiligingsnormen waarop deze autoriteiten controle uitoefenen, tot louter de entiteiten die onder het toezicht van de genoemde autoriteiten staan,

c. Met betrekking tot de markttoezichtautoriteiten: *"Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle portant sur les mesures de sécurité appliquées par les entités sur lesquelles elles ont une compétence de contrôle, qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant."*

Indien deze markttoezichtautoriteiten specifieke opdrachten hebben op het gebied van cyberbeveiliging, die de auteur van het voorontwerp van wet moet motiveren, en indien

[7] voor zover deze bijzonderheden niet reeds in de NIS-wet zijn opgenomen, wat de auteur van het voorontwerp van wet moet nagaan.

niet reeds elders is voorzien in dergelijke mededelingen betreffende de certificering van de betrokken entiteiten, lijken de bedoelde mededelingen relevant en noodzakelijk, maar voor de passende regeling ervan wordt verwezen naar de eerdere opmerkingen betreffende de sectorale autoriteiten (aanduiding van de toezichtautoriteiten die als enige over een dergelijke bevoegdheid beschikken, beperking van de uitwisselingen betreffende de vaststelling van een inbreuk op de informatiebeveiligingsnormen waarop deze markttoezichtautoriteiten controle uitoefenen tot louter de entiteiten die onder het toezicht van de genoemde autoriteiten staan, enz.). Zo niet, dan moet deze mededeling uit het voorontwerp van wet worden geschrapt.

d. Met betrekking tot de openbare veiligheidsdiensten: *"Dans le cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou dans le cas où ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services."*

Op de vraag welke autoriteiten onder dit begrip *"openbare veiligheidsdiensten"* vallen, preciseerde de afgevaardigde van de minister dat het om de volgende autoriteiten gaat: *"SPF Intérieur, Bruxelles Prévention et Sécurité, Service public de Wallonie, Vlaamse Overheid, Administrations publiques locales (provinces et communes), Gouverneurs, OCAM."*

Naast van het ontbreken van een definitie in het voorontwerp van wet van het begrip 'openbare veiligheidsdienst' (wat zou moeten worden rechtgezet door een uitdrukkelijke vermelding van de genoemde autoriteiten of eerder, in de meeste gevallen, van hun dienst die belast is met de openbare veiligheid), maakt het ontbreken van een minimumkader voor deze uitwisselingen deze onvoorspelbaar. Zoals uit de aanvullende informatie blijkt, moeten die worden beperkt tot de gevallen waarin een verplichte certificering door die autoriteiten is opgelegd om redenen van openbare veiligheid, en moet worden bepaald dat de maatregelen tot intrekking of schorsing van het certificaat van een entiteit (die aan deze verplichte certificering is onderworpen) alleen worden meegedeeld aan de autoriteit die is aangeduid in de norm die deze verplichte certificering oplegt. Dit is alleen het geval als er geen publiciteitsmaatregelen zijn voor de intrekking van een dergelijk certificaat wegens niet-naleving van de certificeringsregeling, wat in de memorie van toelichting moet worden gemotiveerd.

e. Wat de inlichtingendiensten betreft*: "Ils ont pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux menaces graves contre la sûreté de l'Etat. Lorsque cela s'avérerait nécessaire dans leurs recherches, par exemple lorsqu'une entité titulaire d'un certificat européen de cybersécurité aurait des liens avec des activités d'espionnage ou liées à une organisation criminelle, les services de renseignements devraient pouvoir avoir accès (en vertu de l'art. 14, al. 2 et art. 20, § 1er de la loi du 30 novembre 1998 sur les services de renseignement) aux informations collectées par le service d'inspection de l'autorité nationale de certification dans le cadre de ses missions de contrôle, au regard de l'importance de l'intérêt général protégé. En outre, dans la cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services. Faut encore qu'elles disposent de pouvoir d'investigation à ce sujet."*

In dit verband is de Autoriteit, naast de bovenstaande overwegingen met betrekking tot de publiciteitsmaatregelen voor de intrekking en schorsing van certificaten en naar het voorbeeld van de opmerking met betrekking tot de gerechtelijke autoriteiten, van mening dat het niet nodig is, of zelfs contraproductief vanuit het oogpunt van de bescherming van persoonsgegevens, om een mededeling van gegevens aan de inlichtingendiensten, die reeds in hun eigen organieke wetgeving is geregeld, te herhalen. Bovendien valt dit buiten het toepassingsgebied van dit voorontwerp van wet. Daarom moet deze uitwisseling ook worden geschrapt.

f. Met betrekking tot de politie: *"pour les mêmes motifs que ceux prévus pour les services de sécurité publique et les autorités judiciaires"*.

De Autoriteit verwijst naar haar bovengenoemde opmerkingen over dit onderwerp.

13. Bijgevolg dient de formulering van de bepalingen van het voorontwerp die voorzien in deze uitwisselingen (artt. 6, §§ 1 en 3, 7, 16, § 2, 17, §§ 1 en 3, 36, §§ 1 en 3, 4° en 38) te worden herzien om ze in overeenstemming te brengen met de bovenstaande overwegingen door ze te beperken tot wat vereist is voor de verwezenlijking van de doelstellingen van de Cyberbeveiligingsverordening of opdrachten van verwante openbare diensten die rechtstreeks betrekking hebben op de cyberbeveiliging, zoals de opdrachten die worden uitgeoefend door de toezichthoudende autoriteiten zoals bedoeld in de NIS-wet (sectorale autoriteiten). De auteur van

het voorontwerp van wet moet erover waken niet te voorzien in mededelingen van persoonsgegevens waarin reeds is voorzien door andere wettelijke bepalingen.

14. Teneinde de rechten en vrijheden te vrijwaren van de natuurlijke personen, die klant zijn van de onder toezicht staande dienstverleners en die de gevolgen kunnen ondervinden van deze uitwisselingen, is het bovendien absoluut noodzakelijk om in het wetsontwerp een bepaling op te nemen die stelt dat deze uitwisselingen geen betrekking mogen hebben op persoonsgegevens van klanten-natuurlijke personen (of klanten-natuurlijke personen van die laatsten) van de onder toezicht staande ICT-dienstverleners, gelet op de aanzienlijke risico's die dit inhoudt voor deze betrokkenen en gelet op het feit dat uit de door de afgevaardigde van de minister aangevoerde rechtvaardigingsgronden niet blijkt dat deze informatie in dit geval relevant en noodzakelijk is.

15. Tot slot is het, gelet op de doelstellingen van de Europese Cyberbeveiligingsverordening, van belang dat in het voorontwerp van wet expliciet een informatieplicht inzake de uitgevoerde intrekkingen van certificaten wordt opgelegd aan de nationale cyberbeveiligingscertificeringsautoriteit die belast zal zijn met de intrekking van de certificaten. Daartoe moet deze autoriteit worden verplicht om te beschikken over een openbare website en een informatiedienst (push) die alle betrokken actoren op de hoogte brengt van elke certificeringsintrekking. Dit vereist geen openbaarmaking van persoonsgegevens en is in overeenstemming met een van de doelstellingen van de Europese Cyberbeveiligingsverordening, namelijk het vertrouwen in gecertificeerde ICT-producten, -diensten en -processen te waarborgen. In voorkomend geval zou een uitzondering op deze openbaarmaking kunnen worden overwogen voor ICT-producten of -diensten die voor hun gebruik een veiligheidsmachtiging vereisen. In het algemeen moet elke uitzondering op de openbaarmaking van informatie over de herroeping of afgifte van certificaten uitdrukkelijk in het voorontwerp van wet worden opgenomen en naar behoren worden gemotiveerd en verantwoord in de memorie van toelichting.

<u>Bijzondere opmerkingen</u>

Toepassingsgebied van het wetsontwerp

16. Artikel 3 van het wetsontwerp bepaalt het toepassingsgebied ervan door te specificeren dat het wetsontwerp van toepassing zal zijn op vrijwillige Europese certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen zoals bedoeld in de Cyberbeveiligingsverordening en dat alleen de hoofdstukken 1 tot 4 en 7 en de artikelen 21 en 22 van dit wetsontwerp ook van toepassing zijn op de verplichte certificeringen.

17. Uit de aanvullende inlichtingen blijkt het volgende: *"Les mesures de contrôle et de sanctions liées aux certifications rendues obligatoires sont réglées ou devront être réglées par les différentes législations sectorielles applicables."* Op de vraag waarom hoofdstuk 8, dat handelt over de verwerking van persoonsgegevens ter uitvoering van het wetsontwerp, was uitgesloten van de verplichte Europese cyberbeveiligingscertificeringen, antwoordde de afgevaardigde van de minister dat dit een vergetelheid was en dat hoofdstuk 8 kon worden opgenomen in artikel 3, § 2 van het wetsontwerp. Hiervan is nota genomen.

Aanwijzing van de bevoegde toezichthoudende autoriteiten

18. Ter uitvoering van artikel 58 van de Cyberbeveiligingsverordening delegeert artikel 5 van het wetsontwerp aan de Koning de taak om de nationale cyberbeveiligingscertificeringsautoriteit aan te wijzen die zal worden belast met de controle- en toezichthoudende taken, bedoeld in artikel 58 van deze verordening. In de tweede paragraaf van deze bepaling wordt bepaald dat de Koning, *"naargelang het voorwerp van de betrokken certificeringsregeling en op verzoek van de betrokken overheid "*, de controle- en sanctietaken (met uitzondering van de intrekking en schorsing van certificaten) aan een andere overheid kan toevertrouwen. Hierover ondervraagd, specificeerde de afgevaardigde van de minister als volgt: *"Concrètement, il est envisagé d'utiliser éventuellement ce mécanisme au profit de l'IBPT, la FSMA, la BNB et l'inspection économique. Les dispositions modificatives ont été insérées dans le projet de loi à la demande de ces autorités car ces dernières considéraient les dispositions modificatives comme nécessaires pour que le Roi puisse éventuellement, dans les conditions imposées par la loi, les désigner."*[8] Hiervan is nota genomen.

Samenwerking op nationaal niveau (art. 6)

19. Artikel 6 van het voorontwerp van wet heeft betrekking op de samenwerking en gegevensuitwisseling op nationaal niveau die de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die zullen worden aangewezen ter uitvoering van artikel 5, § 2 van het ontwerp (voor de uitvoering van de opdrachten bedoeld in de hoofdstukken 5 en 6 van het voorontwerp van wet) alsook andere overheidsautoriteiten zullen uitvoeren voor de toepassing van de Cyberbeveiligingsverordening en elke andere wettelijke bepaling.

20. In dit verband wordt verwezen naar het commentaar in de algemene opmerkingen van dit advies.

[8] Gezien de aanwijzingen die reeds via de wijzigingsbepalingen zijn gedaan, vraagt de Autoriteit zich af of het artikel 5, § 2 van het ontwerp wel nodig is. Het verdient aanbeveling dat de auteur van het voorontwerp van wet dit in zijn voorontwerp verduidelijkt. In het vervolg van het ontwerpadvies zullen deze autoriteiten zonder onderscheid worden aangeduid als "ter uitvoering van artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten".

21. Indien de nationale cyberbeveiligingscertificeringsautoriteit en de in artikel 5, § 2 bedoelde autoriteiten structureel persoonsgegevens moeten verzamelen bij deze sectorale autoriteiten voor de uitoefening van de in de Cyberbeveiligingsverordening bedoelde openbaredienstopdrachten, moeten deze gegevensverzamelingen ook in het voorontwerp van wet worden opgenomen en aan dezelfde criteria inzake voorzienbaarheid voldoen; dit lijkt momenteel niet het geval te zijn.

22. Wat artikel 6, § 2, van het ontwerp betreft, dat houders van Europese cyberbeveiligingscertificaten en afgevers van conformiteitsverklaringen verplicht om de autoriteiten die belast zijn met het toezicht op de naleving van de Cyberbeveiligingsverordening en de Europese certificeringsregelingen alle informatie te verstrekken die zij nodig hebben voor de uitvoering van hun taken, lijkt deze ontwerpbepaling overtollig te zijn met de bepalingen van het voorontwerp die de inspectiebevoegdheden van de inspectiediensten van deze autoriteiten regelen en moet ze bijgevolg uit dit deel van het voorontwerp van wet te worden geschrapt.

Uitwisseling van gegevens die beschermd zijn door het beroepsgeheim of door een geheimhoudingsplicht (art. 6, § 4)

23. Artikel 6, § 4 van het ontwerp heeft betrekking op de kwestie van door het beroepsgeheim beschermde gegevens die zich zal voordoen in het kader van de uitwisseling van gegevens die de nationale cyberbeveilingscertificeringsautoriteit en de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten zullen hebben met derden, in deze bewoordingen:
"§ 4. Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, mogen deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, alsook eventueel aan andere overheden indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.
Het gaat met name om noodzakelijke informatie met betrekking tot de afgifte van certificaten, het toezicht, sancties en klachten. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing. De regelingen voor de uitwisseling van informatie dienen het vertrouwelijke karakter van de betrokken informatie te eerbiedigen."

24. Ten eerste ziet de Autoriteit niet in hoe voor de afgifte van beveiligingscertificaten informatie moet worden verzameld die onder het beroepsgeheim of onder een geheimhoudingsplicht valt. Volgens de memorie van toelichting wordt alleen de controle-opdracht genoemd als opdracht met mogelijke gevolgen voor het beroepsgeheim. Uit de aanvullende inlichtingen die zijn verkregen van de afgevaardigde van de minister, komt geen enkele rechtvaardiging naar voren voor de impact van de opdracht inzake de afgifte van beveiligingscertificaten op het beroepsgeheim. Bij gebrek aan een afdoende rechtvaardiging in de memorie van toelichting moeten de woorden *"afgifte van certificaten"* bijgevolg uit artikel 6, § 4, tweede lid, worden weggelaten.

25. Vervolgens merkt de Autoriteit op dat, wat de uitwisseling van gegevens betreft die beschermd zijn door het beroepsgeheim of door een geheimhoudingsplicht, er twee gevallen moeten worden onderscheiden:
    a. in de eerste plaats de situatie van een autoriteit die aan een geheimhoudingsplicht is onderworpen en die belet wordt om onder die geheimhoudingsplicht vallende informatie mee te delen, ook al is die mededeling legitiem, relevant en noodzakelijk (cf. supra);
    b. ten tweede, het verzamelen, door de inspectiediensten van de autoriteiten die belast zijn met de controle van de naleving van de Cyberbeveiligingsverordening, van persoonsgegevens die beschermd zijn door het beroepsgeheim (bijvoorbeeld tijdens audits van gecertificeerde ICT-systemen).

26. Deze twee situaties moeten in het voorontwerp van wet afzonderlijk worden behandeld en alleen de eerste moet aan de orde komen in artikel 6, gelet op de titel ervan (*"samenwerking op nationaal niveau"*).

27. De wettelijke bepaling betreffende de eerste situatie (23.a) moet zodanig worden geformuleerd dat de opheffing van de geheimhouding alleen kan gebeuren ten behoeve van autoriteiten waarvoor de uitwisseling van gegevens legitiem[9], relevant en noodzakelijk is (cf. supra) voor de uitoefening van de inspectietaken van de autoriteiten zoals bedoeld in artikel 5 van het voorontwerp van wet. Bovendien moeten het woord/de woorden *"notamment"/"met name"* in het tweede lid van § 4 van artikel 6 van het ontwerp worden geschrapt om het voorwerp van de bedoelde uitwisselingen correct te beperken.

28. De tweede situatie van gegevensuitwisseling met gevolgen voor het beroepsgeheim moet worden behandeld in het hoofdstuk over de inspectiebevoegdheden. Het voorontwerp van wet moet noodzakelijkerwijs duidelijk voorzien in specifieke waarborgen voor de rechten en vrijheden van de personen op wie de onder het beroepsgeheim vallende gegevens betrekking hebben, indien en slechts indien de toegang tot die gegevens onontbeerlijk is voor de uitvoering van onderzoeksmaatregelen door de inspectiedienst (voorafgaande toestemming van de onderzoeksrechter, tussenkomst van de beroepsorde waartoe de persoon behoort van wie de documenten met het oog op de uitvoering van de voornoemde controles moeten worden geraadpleegd op straffe van het in het gedrang brengen van voornoemde controles, verbod op bewaring van onder het beroepsgeheim vallende documenten door voornoemde autoriteiten, ..., cf. in die zin de artikelen 56*bis* en 90*octies* van het Wetboek van Strafvordering). Zo niet, dan moet uitdrukkelijk worden bepaald dat inlichtingen die onder het beroepsgeheim vallen in de zin van artikel 458 van het Strafwetboek, niet door de inspectiedienst mogen worden verzameld.

[9] Onder verwijzing naar de bepaling in het voorontwerp van wet die de modaliteiten van deze uitwisselingen zal beschrijven in overeenstemming met de opmerkingen van de Autoriteit (cf. supra).

Hoofdstuk 5 – Toezicht (artt. 13 t/m 18)

29. De artikelen 13 tot en met 18 van het wetsontwerp voorzien in een kader voor de controleprocedure van de nationale cyberbeveiligingscertificeringsautoriteit en in de bevoegdheden die haar inspectiedienst zal hebben.

30. In artikel 13, § 2 van het voorontwerp worden de verzoeken om informatie die de inspecteurs bij de uitoefening van hun taak kunnen doen, formeel vastgelegd in de volgende bewoordingen:
"Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt."

31. Om de gecontroleerde persoon in staat te stellen de relevantie en noodzaak te beoordelen van de gegevens (in voorkomend geval persoonsgegevens) die in dit verband nodig zullen zijn, moet in deze bepaling uitdrukkelijk worden vermeld dat de inspecteurs de wettelijke bepalingen of het deel (de delen) van de certificeringsregeling waarop een inbreuk wordt vermoed, moeten identificeren.

Controlebevoegdheden van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit – Invoering van waarborgen voor de bescherming van persoonsgegevens die zijn opgenomen in de geauditeerde IT-systemen

32. De ruime controlebevoegdheden van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit worden beschreven in artikel 15 van het voorontwerp van wet.

33. Naar het voorbeeld van wat is bepaald voor de huiszoekingen artikel 15, § 4 van het ontwerp, beveelt de Autoriteit aan om in het voorontwerp van wet waarborgen toe te voegen voor bevoegdheden die bijzonder intrusief zijn en waardoor de inspectiedienst toegang krijgt tot de persoonsgegevens van de klanten (of klanten van die klanten) van de ICT-dienstverleners of van leveranciers van ICT-producten die zullen worden geïnspecteerd. Daartoe moet, als waarborg voor de bescherming van de rechten en vrijheden van de betrokkenen, aan de inspectiedienst uitdrukkelijk worden verboden de gegevens van de klanten (of van de klanten van die klanten) van de gecontroleerde dienstverleners en leveranciers te verzamelen of mee te delen voor andere doeleinden dan het toezicht op de naleving van de verordening of van de betrokken certificeringsregeling. Evenzo is de Autoriteit van oordeel dat moet worden bepaald, naar het voorbeeld van wat is vastgelegd in artikel 66 van de voornoemde wet van 7 april 2019 (NIS-wet),

dat zodra andere persoonsgegevens dan die betreffende de houder van het Europees certificaat of zijn personeelsleden moeten worden geraadpleegd met het oog op de uitvoering van controles door de inspectiedienst, deze gegevens, indien mogelijk, eerst moeten worden gepseudonimiseerd in overeenstemming met de huidige regels van de kunst.[10].

34. De Autoriteit beveelt ook aan om de naleving van het evenredigheidsbeginsel bij de uitoefening van onderzoeksbevoegdheden uitdrukkelijk in het voorontwerp van wet op te nemen, zoals dat ook het geval is voor andere inspectiebevoegdheden, zoals die van de sociale inspectie (cf. Sociaal Strafwetboek). Zo moet in artikel 15 van het voorontwerp van wet uitdrukkelijk het volgende worden bepaald: "Bij de uitoefening van hun in dit artikel bedoelde controlebevoegdheden moeten de inspecteurs van de nationale cyberbeveiligingscertificeringsautoriteit en van de autoriteiten bedoeld in artikel 5, § 2 van het ontwerp ervoor zorgen dat de middelen die zij gebruiken, geschikt en noodzakelijk zijn voor het toezicht op de Cyberbeveiligingsverordening of op de bepalingen van het certificeringsschema waarvan zij de naleving controleren." Het verzamelen van persoonsgegevens bij de uitoefening van hun toezichthoudende taken moet beperkt blijven tot uitsluitend die gegevens die relevant zijn voor het aantonen van een inbreuk op de Cyberbeveiligingsverordening of de niet-naleving van een certificeringsregeling. In dit verband beschikken zij trouwens niet over andere bevoegdheden dan de hierboven genoemde.

35. Tot slot wijst de Autoriteit erop dat de wenselijkheid van het instellen van onderzoeken *in concreto* moet worden beoordeeld door de inspecteurs op basis van de feiten waarover zij beschikken. Zij beschikken over een beoordelingsbevoegdheid in dit verband. De inspecteurs zullen de elektronische verzameling van de noodzakelijke gegevens oordeelkundig en met mate uitvoeren en alleen persoonsgegevens raadplegen indien ze, gelet op de feiten, beschikken over een samenhangende en ernstige reeks aanwijzingen dat de gewenste persoonsgegevens de preventie en opsporing van inbreuken op de Cyberbeveiligingsverordening of de certificeringsregeling waarvan de naleving wordt gecontroleerd, mogelijk zouden maken of zouden versnellen.

Mededeling door de inspectiedienst van zijn inspectieverslagen en pv's van controle aan derden

36. Artikel 16, § 2, van het voorontwerp van wet bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, van het voorontwerp van wet, een afschrift van haar inspectieverslag meedeelt aan de *"markttoezichtautoriteiten, de nationale accreditatieautoriteit, de openbare*

[10] Zie hierover ENISA: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases en https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation.

veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid, op hun verzoek en voor zover dit nodig is voor het vervullen van hun wettelijke opdrachten."

37. Om de in de algemene opmerkingen van dit advies uiteengezette redenen ziet de Autoriteit niet in waarom een dergelijke openbaarmaking op eenvoudig verzoek gepast is voor de inlichtingendiensten, de openbare veiligheidsdiensten en de politiediensten voor de goede uitvoering van de Cyberbeveiligingsverordening. Ondervraagd over dit onderwerp, verklaarde de afgevaardigde van de minister het volgende: *"La transmission d'une copie d'un rapport d'inspection ou d'un procès-verbal relatif au contrôle d'un certificat de cybersécurité par l'une des autorités précitées peut s'avérer nécessaire à l'exécution des missions légales de ces autorités ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique."* Hij haalde de bestaande wettelijke bepalingen aan op grond waarvan bepaalde autoriteiten, zoals het Nationaal Crisiscentrum of het OCAD, over dit soort informatie kunnen beschikken. In dit verband merkt de Autoriteit in de eerste plaats op dat de auteur van het voorontwerp van wet ervoor moet zorgen dat niet in vage bewoordingen wordt voorzien in gegevensstromen die reeds door andere wettelijke bepalingen worden geregeld. Bovendien valt het niet binnen de doelstellingen of het toepassingsgebied van het voorontwerp van wet om de inspectiebevoegdheden te regelen van andere overheidsautoriteiten dan die welke belast zijn met het toezicht op de naleving van de Europese verordening en de op grond van die verordening vastgestelde certificeringsregelingen. Om de evenredigheid van deze ontwerpbepaling te waarborgen, moeten vervolgens de voor de uitvoering van de Europese Cyberbeveiligingsverordening legitieme en relevante omstandigheden en doeleinden waarin de bedoelde verslagen mogen worden meegedeeld aan uitsluitend de autoriteiten met specifieke openbaredienstopdrachten op het gebied van cyberbeveiliging, duidelijk worden bepaald in het voorontwerp van wet, in plaats van te voorzien in mededelingen op eenvoudig verzoek, zonder enige andere precisering en onverminderd andere wettelijke bepalingen op grond waarvan overheidsautoriteiten toegang kunnen krijgen tot bepaalde verslagen of bepaalde daarin vervatte inlichtingen.

38. Bovendien moet, naar het voorbeeld van wat reeds is aanbevolen, duidelijk worden gemaakt dat deze verslagen geen persoonsgegevens over klanten (of klanten van die klanten) van de gecontroleerde ICT-dienstverleners mogen bevatten vanwege de risico's die dit voor deze betrokkenen inhoudt. Voor het overige verwijst de Autoriteit naar haar algemene overwegingen hierboven. De formulering van het artikel 16, § 2 van het ontwerp moet dienovereenkomstig worden herzien.

39. Artikel 16, § 3, van het voorontwerp bepaalt de geadresseerden aan wie deze inspectieverslagen systematisch moeten worden toegezonden in geval van een *"controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, 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 of het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer".*

40. Daarmee voert het voorontwerp van wet een wettelijke verplichting in om persoonsgegevens te verwerken (ervan uitgaande dat deze rapporten persoonsgegevens zullen bevatten of betrekking zullen hebben op een dienstverlener/leverancier van ICT-diensten/-producten die als natuurlijk persoon opereert) in de zin van artikel 6.1.c van de AVG. Aangezien de specifieke wetgevingen bedoeld in artikel 16, § 3 van het ontwerp een gelijkaardig doel nastreven als de Cyberbeveiligingsverordening, heeft de Autoriteit geen bezwaar tegen de mededeling van verslagen in het geval dat een inspectie door de in artikel 5 van het voorontwerp van wet bedoelde autoriteiten betrekking heeft op entiteiten die gebruik maken van de genoemde ICT-diensten of -producten bedoeld in de wetgevingen zoals vermeld in artikel 16, § 3. In een streven naar rechtszekerheid en voorzienbaarheid en om te voldoen aan artikel 6.3 van de AVG moet het begrip *"bevoegde sectorale autoriteit en inspectiedienst"* echter adequaat worden gedefinieerd, moet in artikel 16, § 3, het precieze doel worden vastgesteld waarvoor deze ontvangende autoriteiten deze verslagen zullen gebruiken (namelijk de uitoefening van hun bij de genoemde specifieke reglementeringen opgelegde openbaredienstopdrachten) en moet worden gespecificeerd dat de verslagen uitsluitend mogen worden gericht aan de bevoegde sectorale autoriteit op basis van de dienstverlener of leverancier van de ICT-dienst waarop het verslag betrekking heeft.

41. Artikel 17, §§ 1 tot 4, van het voorontwerp bepaalt op zeer ruime wijze de mededeling aan derden van gegevens en processen-verbaal van controle door de inspectiedienst van de nationale certificeringsautoriteit.

42. De formulering *"die ervan op de hoogte moeten zijn (...) voor de uitoefening van hun functie of opdracht die verband houdt met deze wet of andere wettelijke bepalingen"* artikel 17, § 1 van het ontwerp is een vaag en te ruim criterium om de verstrekking van door de inspectiedienst verzamelde persoonsgegevens aan andere autoriteiten te regelen, temeer daar § 2 van artikel 17 van het ontwerp de inspectiedienst onderwerpt aan het beroepsgeheim. Bijgevolg moet dit artikel 17, § 1 worden geschrapt.

43. Met betrekking tot artikel 17, § 3 van het ontwerp, dat voorziet in de mededeling door de inspectiedienst van pv's of aanvullende informatie aan de verschillende bedoelde autoriteiten, verwijst de Autoriteit naar het commentaar in de algemene opmerkingen in dit advies en naar het commentaar bij artikel 16, § 2 van het ontwerp, die *mutatis mutandis* van toepassing zijn. Evenzo wordt voor artikel 17, § 4 verwezen naar het commentaar bij artikel 16, § 3.

Afwijking van het beginsel van vertrouwelijkheid van elektronische communicatie ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit

44. Artikel 17, § 5 van het ontwerp voorziet als volgt in een afwijking van het beginsel van vertrouwelijkheid van communicatie via een openbaar netwerk en een openbare elektronisch-communicatiedienst[11] ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit:

"§ 5. Bij de uitoefening van hun functie mogen de personeelsleden van de inspectiedienst:

1° met opzet kennisnemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hen bestemd is;

2° met opzet de personen identificeren die bij de overdracht van de informatie en de inhoud ervan betrokken zijn;

3° met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon."

45. Binnen de grenzen van artikel 15 van de richtlijn betreffende privacy en elektronische communicatie kan in dergelijke afwijkingen worden voorzien. Artikel 15.1 van de richtlijn betreffende privacy en elektronische communicatie bepaalt: *"De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, [...] en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de*

[11] vastgelegd in artikel 5, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), in Belgisch recht omgezet in artikel 124 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Europese Unie."[12] Met de inwerkingtreding van de AVG moet artikel 15 van de richtlijn betreffende privacy en elektronische communicatie worden gelezen als een verwijzing naar artikel 23 van de AVG. Deze bepaling van de AVG voorziet onder meer als een grond voor beperking van de rechten van betrokkenen in *"een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen"*; met name de veiligheid en de landsverdediging, de openbare veiligheid, de voorkoming en de opsporing van strafbare feiten, andere belangrijke doelstellingen van algemeen openbaar belang, met name een belangrijk economisch of financieel belang, en de voorkoming en de opsporing van schendingen van de beroepscodes voor gereglementeerde beroepen.

46. Allereerst is het aan de auteur van het voorontwerp van wet om in de memorie van toelichting uit te leggen hoe de voorgestelde afwijking ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit aansluit bij een of meer van de gronden van artikel 23.1 van de AVG.

47. Vervolgens vraagt de Autoriteit zich af, gelet op de gronden waarop de lidstaten van dit vertrouwelijkheidsbeginsel kunnen afwijken, of het in dit geval niet passend zou zijn deze afwijkingen te beperken tot de controles die moeten worden uitgevoerd bij conformiteitsbeoordelingsinstanties en houders van verplichte certificaten, aangezien er op gebieden van groot openbaar belang wetgevende maatregelen zouden moeten worden genomen om dergelijke certificaten verplicht te stellen. Het is aangewezen dat de auteur van het voorontwerp van wet de keuze die hij zal maken voor het toepassingsgebied van de afwijking, vanuit deze invalshoek motiveert en zijn motivering in de memorie van toelichting opneemt.

48. Gevraagd naar de behoeften van de inspectiedienst die een dergelijke afwijking van het beginsel van vertrouwelijkheid van elektronische communicatie vereisen, heeft de afgevaardigde van de minister het volgende verklaard: *"Ne sont pas visées les écoutes téléphoniques mais la* (prise de connaissance) *des e-mails émanant et reçus des organismes d'évaluation de la conformité, des émetteurs de déclaration de conformité, des titulaires de certificat de cybersécurité européen et ce uniquement lorsque les données en question sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification dont le respect est contrôlé."*

[12] Artikel 6, §§ 1 en 2, van het Verdrag betreffende de Europese Unie luidt als volgt: "1. De Unie erkent de rechten, vrijheden en beginselen die zijn vastgesteld in het Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg, dat dezelfde juridische waarde als de Verdragen heeft [...]." Uit de rechtspraak van het HvJEU volgt dat alle in artikel 23 (oud artikel 13 van richtlijn 95/46) van de AVG genoemde rechtvaardigingsgronden een afwijking van dit beginsel van vertrouwelijkheid van elektronische communicatie kunnen rechtvaardigen.

49. Om het proportionele karakter van de afwijking te waarborgen, is het dus aan de auteur van het wetsontwerp om in artikel 17, § 3 van het ontwerp te specificeren dat de inspecteurs enkel kennis kunnen nemen van elektronische communicatie die uitgaat van en ontvangen wordt door conformiteitsbeoordelingsinstanties (verstrekkers van conformiteitsverklaringen)[13], houders van het (verplichte) Europese cyberbeveiligingscertificaat[14], en enkel indien deze informatie waarschijnlijk zal bijdragen tot het ophelderen van een ernstige inbreuk op een gecontroleerde (verplichte) certificeringsregeling of op de Europese Cyberbeveiligingsverordening. In een streven naar rechtszekerheid en voorzienbaarheid moet ook uitdrukkelijk worden vermeld dat artikel 17, § 3 afwijkt van artikel 124 van de voornoemde wet van 13 juni 2005.

50. Tot heeft de afgevaardigde van de minister op de vraag of het wenselijk was te voorzien in waarborgen voor de gecontroleerde personen, zoals hun voorafgaande instemming met de raadpleging van hun elektronische communicatie of, bij gebreke daarvan, de instemming van de onderzoeksrechter, het volgende gepreciseerd: *"En l'absence du consentement expresse de l'entité contrôlée, les membres assermentés du service d'inspection de l'autorité nationale de certification de cybersécurité ne pourront pas prendre connaissance de ces informations (ceux-ci n'ayant pas la qualité d'officier de police judiciaire)."* Daarom is het aangewezen om in artikel 17, § 3 van het ontwerp te bepalen dat de bedoelde raadplegingen plaatsvinden na het verkrijgen van de toestemming van de gecontroleerde persoon.

Hoofdstuk 8 – Verwerking van persoonsgegevens

51. De auteur van het wetsontwerp heeft ervoor gekozen in zijn voorontwerp van wet een specifiek hoofdstuk op te nemen waarin de verschillende elementen van de onder het voorontwerp van wet vallende verwerking van persoonsgegevens worden vastgesteld.

Categorieën van verwerking van persoonsgegevens en doeleinden van die verwerking

52. In artikel 36, §§ 1 en 3, worden de categorieën van verwerking van persoonsgegevens in het kader van de uitvoering van het voorontwerp als volgt omschreven:

"Art. 36, § 1. In het kader van de uitvoering van deze wet vinden de volgende verwerkingen van persoonsgegevens plaats:

1° informatie-uitwisseling tussen de autoriteit bedoeld in artikel 5, § 1, de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, de gerechtelijke overheden, de sectorale overheden of de inspectiediensten respectievelijk bedoeld in artikel 7, § 3 en § 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen

[13] Afhankelijk van de keuze die in het licht van de vorige overweging moet worden gemaakt.

[14] *Ibidem.*

belang voor de openbare veiligheid, de markttoezichtautoriteiten, de nationale accreditatieautoriteit, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid;

(…)

2° informatie-uitwisseling tussen conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen, enerzijds, en de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, anderzijds;

(…)

3° de verwerking van gegevens door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie, voor het vervullen van de in hoofdstuk 7 bedoelde taken rond klachten.

(...);

4° de verwerking van gegevens door de autoriteit bedoeld in artikel 5, § 1, of door de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, met betrekking tot haar taken op het vlak van toezicht en sancties.

(…)

§ 3. 2. De in paragraaf 1 bedoelde verwerkingen vinden plaats voor de volgende doeleinden:

1° de afgifte van Europese cyberbeveiligingscertificaten;

2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of conformiteitsbeoordelingsinstanties;

3° de verwerking van klachten ingediend op basis van artikel 63, lid 1, van de Cyberbeveiligingsverordening;

4° nationale en internationale samenwerking, met inbegrip van informatie-uitwisseling;

5° het opleggen van de sancties bedoeld in hoofdstuk 6."

53. Ten eerste merkt de Autoriteit op dat het begrip *"verwerking van persoonsgegevens in het kader van de uitvoering van deze wet"* niet voldoet aan de eisen van voorzienbaarheid. Gelet op het toepassingsgebied van het voorontwerp van wet is het aangewezen om alleen de verwerking van persoonsgegevens te regelen die door de nationale cyberbeveiligingscertificeringsautoriteit en, in voorkomend geval, de ter uitvoering van artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten (voor zover deze laatste verwerkingen niet reeds door de organieke wetten van deze autoriteiten worden geregeld) zal worden verricht bij de uitvoering van de in de Europese Cyberbeveiligingsverordening beschreven openbaredienstopdrachten die het voorontwerp van wet hun toekent. Het voorontwerp van wet mag geen gegevensverwerkingen regelen die buiten dit toepassingsgebied vallen of die bovendien reeds zijn geregeld door de organieke wetten van andere autoriteiten; het is aan de auteur van het voorontwerp van wet om dit na te gaan.

54. Een uitputtende beschrijving van de gegevensverwerkingscategorieën die ter uitvoering van het wetsontwerp worden verricht, zoals artikel 36, § 1 van het ontwerp poogt te doen, zou afbreuk kunnen doen aan de uitoefening van de openbaredienstopdrachten van de nationale certificeringsautoriteit in het geval er sprake zou zijn van een vergetelheid. Een duidelijke en

concrete vaststelling van de doeleinden van de verwerkingen van deze autoriteit (naast de vaststelling van de andere essentiële elementen ervan) moet volstaan om de noodzakelijke voorzienbaarheid van deze verwerkingen van persoonsgegevens te waarborgen. De Autoriteit beveelt de schrapping van artikel 36, § 1 aan.

55. Wat de bepaling van de doeleinden van de verwerkingen in artikel 36, § 3 van het ontwerp betreft, moet worden verwezen naar de doeleinden waarvoor de nationale certificeringsautoriteit en/of de autoriteiten die ter uitvoering van artikel 5, § 2 van het voorontwerp van wet zullen worden aangewezen, persoonsgegevens zullen verwerken in het kader van de openbaredienstopdrachten die hun worden toegekend door het voorontwerp van wet en de Europese Cyberbeveiligingsverordening[15]. De volgende opmerkingen zijn in dit verband op hun plaats:
    a. De in artikel 36, § 3, 1° en 3°, genoemde doeleinden moeten op nuttige wijze worden samengevoegd: de afgifte van Europese cyberbeveiligingscertificaten en het beheer van de daarmee verband houdende klachten;
    b. De doeleinden bedoeld in artikel 36, §3, 2° en 5° moeten eveneens worden samengevoegd en er moet worden verwezen naar de relevante bepalingen van het voorontwerp van wet in de volgende bewoordingen: toezicht op houders van een Europese cyberbeveiligingscertificaat, verstrekkers van conformiteitsverklaringen van de Europese Unie en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties in overeenstemming met de hoofdstukken 5 en 6 van deze wet;
    c. Wat de "samenwerking, met inbegrip van de uitwisseling van informatie op nationaal en internationaal niveau" betreft, dit is geen verwerkingsdoel in de zin van de AVG, maar een gegevensverwerking op zich die reeds moet worden gedekt door de bovengenoemde controle- en sanctiedoeleinden en, indien nodig en overeenkomstig de Cyberbeveiligingsverordening, door het doel van *"afgifte van certificaten"*. Artikel 36, § 3, 4° moet bijgevolg worden geschrapt en, in voorkomend geval, indien de bestaande wettelijke bepalingen (NIS-wet) niet reeds op voorzienbare wijze voorzien in deze stromen, moet deze bepaling van het ontwerp worden vervangen door het concrete doel waarvoor een mededeling van informatie door de nationale certificeringsautoriteit en de ter uitvoering van artikel 5, § 2 van het ontwerp aangewezen autoriteiten alleen zal worden gedaan aan de bevoegde sectorale autoriteiten (NIS), in overeenstemming met de artikelen 16 en 17 van het voorontwerp van wet (aangepast in overeenstemming met de bovenvermelde aanbevelingen van de Autoriteit). Indien de auteur van het voorontwerp van wet de nationale cyberbeveiligingscertificeringsautoriteit wil laten deelnemen aan de internationale samenwerking om de kwaliteit van de certificeringen te

[15] Artikel 36 van het ontwerp is momenteel gericht op het reguleren van *"gegevensverwerking in het kader van de uitvoering van de wet"*. Niet alle gegevensverwerkingen die worden uitgevoerd als doel *"de afgifte van Europese cyberbeveiligingscertificaten"* vallen echter, terecht, onder het voorontwerp van wet. De formulering van artikel 36 van het ontwerp moet bijgevolg in dit opzicht worden herzien.

verbeteren en de benaderingen op dit gebied te harmoniseren, en indien voor een dergelijke samenwerking een uitwisseling van persoonsgegevens tussen de nationale cyberbeveiligingscertificeringsautoriteiten vereist is, is het aangewezen dat een dergelijk doel concreet en nauwkeurig wordt vermeld.

Kwalificatie van de verwerkingsverantwoordelijke

56. Om elke dubbelzinnigheid over de identiteit van de entiteit die moet worden beschouwd als verwerkingsverantwoordelijke te vermijden, en aldus de uitoefening van de rechten van de betrokkene waarin de artikelen 12 tot en met 22 van de AVG voorzien, te vergemakkelijken, verzoekt de Autoriteit de auteur van het voorontwerp van wet om de verwerkingsverantwoordelijke(n) explicieter te identificeren dan in artikel 36, § 1 van het ontwerp het geval is.

57. Daartoe volstaat de precisering dat de nationale cyberbeveiligingscertificeringsautoriteit de verantwoordelijke is voor de verwerkingen die zij uitvoert voor de in artikel 36, § 3 genoemde doeleinden. Hetzelfde geldt voor de in artikel 5, § 2 van het voorontwerp bedoelde autoriteiten met betrekking tot de verwerkingen die worden verricht voor in de hoofdstukken 5 en 6 van het voorontwerp van wet bedoelde toezicht- en sanctiedoeleinden.

Rechtsgrondslag

58. In artikel 36, § 2 van het ontwerp wordt de rechtsgrondslag van de bedoelde verwerkingen als volgt omschreven:
"§ 2. De in paragraaf 1 bedoelde verwerkingen zijn noodzakelijk om te voldoen aan wettelijke verplichtingen van de Cyberbeveiligingsverordening of van deze wet, of om een taak van algemeen belang te vervullen die is opgedragen aan een van de in deze wet bedoelde overheden."

59. De Autoriteit merkt op dat de meeste verwerkingen van persoonsgegevens waarop het voorontwerp van wet betrekking heeft, verwerkingen zullen zijn die door de nationale cyberbeveiligingscertificeringsautoriteit (en de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten) worden uitgevoerd bij de uitvoering van hun openbaredienstopdrachten; de rechtsgrondslag, in de zin van de AVG, is artikel 6.1.e van de AVG (met uitzondering van de verplichte systematische verstrekking van inspectieverslagen en processen-verbaal waarin is voorzien in artikel 16, § 3 en artikel 17, § 4 van het voorontwerp van wet, waarvan de rechtsgrondslag artikel 6.1.c van de AVG is).

60. Artikel 36, § 2 van het ontwerp voegt geen meerwaarde toe wat de voorzienbaarheid van de bedoelde gegevensverwerkingen betreft. Om de rechtmatigheid en voorzienbaarheid van

verwerkingen op grond van artikel 6.1.e van de AVG te waarborgen, moet een rechtstreeks toepasselijke nationale of supranationale rechtsnorm op voldoende duidelijke en nauwkeurige wijze de openbaredienstopdrachten die aan de verwerkingsverantwoordelijke zijn toevertrouwd, vaststellen (wat het geval is in het voorontwerp van wet en de Europese Cyberbeveiligingsverordening), maar het is niet vereist dat deze norm of de nationale norm ter uitvoering van een Europese verordening specificeert dat de gegevensverwerkingen die voor dit doel worden uitgevoerd, plaatsvinden *"ter uitvoering van een openbaredienstopdracht die aan de verwerkingsverantwoordelijke is toevertrouwd".* Bijgevolg moet dit artikel 36, § 2 van het ontwerp worden geschrapt.

Categorieën van verwerkte persoonsgegevens

61. In artikel 36, § 4 worden de categorieën van verwerkte persoonsgegevens als volgt omschreven:
"§ 4. De verwerkte persoonsgegevens zijn identificatie- of authenticatiegegevens en elektronischecommunicatiegegevens.
Na advies van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, kan de Koning het vorige lid aanvullen met andere persoonsgegevens."

62. Afgezien van het feit dat in het voorontwerp van wet niet wordt gespecificeerd door welke entiteit deze gegevenscategorieën worden verwerkt, biedt deze vaststelling geen meerwaarde wat de voorzienbaarheid van de gegevensverwerkingen in kwestie betreft. Bovendien is de Autoriteit, in toepassing van het legaliteitsbeginsel, van oordeel dat het in dit geval niet aan de Koning kan worden gedelegeerd om de lijst aan te vullen van de categorieën van persoonsgegevens die zullen moeten worden verwerkt door de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die ter uitvoering van artikel 5, § 2 van het voorontwerp van wet zijn aangewezen voor de uitvoering van de openbaredienstopdrachten die het voorontwerp van wet hun toevertrouwt. Aangezien de huidige lijst duidelijk onvolledig is (quid met de gegevens over de deskundigheid of de opleiding van het personeel van de dienstverlener die gecertificeerd is of bezig is met de certificeringsprocedure?), moet ze worden aangevuld in het licht van de gemeenschappelijke criteria (common criteria)[16] op dit gebied en moet de inhoud ervan naar behoren worden verantwoord en gemotiveerd in de memorie van toelichting.

[16] De gemeenschappelijke criteria voor de evaluatie van de beveiliging van IT-technologieën (bekend als de Common Criteria of CC) zijn een internationale norm (ISO/IEC 15408) voor de certificering van IT-beveiliging.

63. Wat de gegevenscategorieën betreft die worden verwerkt ter uitvoering van de hoofdstukken 5 en 6 van het voorontwerp van wet (toezicht en sanctie), erkent de Autoriteit dat het niet mogelijk is deze anders dan op functionele wijze vast te stellen, door te specificeren dat het gaat om gegevens die noodzakelijk zijn voor de uitoefening van de in de hoofdstukken 5 en 6 van het voorontwerp bedoelde toezicht- en sanctietaken.

64. Bijgevolg moet artikel 36, § 4 uit het voorontwerp van wet dienovereenkomstig worden herzien.

Categorieën van natuurlijke personen ten aanzien van wie gegevens worden verwerkt

65. Artikel 36, § 5 bepaalt in deze bewoordingen de categorieën van personen ten aanzien van wie gegevens worden verwerkt voor de hierboven genoemde doeleinden:
"§ 5. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van de in paragraaf 1 bedoelde verwerkingen:
1° iedere persoon die optreedt voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of voor een overheid;
2° iedere persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten bedoeld in hoofdstuk 5;
3° iedere persoon die een klacht indient."

66. In de eerste plaats moet worden verwezen naar natuurlijke personen, en niet gewoon naar personen.

67. Ten tweede vraagt de Autoriteit zich af of deze opsomming misschien onvolledig is in het licht van haar algemene opmerkingen aan het begin van het advies. Als dit het geval is, moet dit worden verholpen en, als waarborg voor de bescherming van de rechten en vrijheden van de klanten (of de klanten van die laatsten) van de dienstverleners/leveranciers van ICT-producten en in overeenstemming met de algemene overwegingen van de Autoriteit zoals uiteengezet aan het begin van het advies, is het van belang te specificeren dat de nationale cyberbeveiligingscertificeringsautoriteit en de krachtens artikel 5, § 2 van het ontwerp aangewezen autoriteiten geen gegevens mogen verwerken met betrekking tot natuurlijke personen-klanten (of klanten van die laatsten) van de onder toezicht staande dienstverleners/leveranciers van ICT-producten voor andere doeleinden dan het toezicht op de naleving door deze dienstverleners/leveranciers van de Europese Cyberbeveiligingsverordening en de Europese certificeringsregelingen waarop het toezicht betrekking heeft.

Bewaartermijn

68. Artikel 39 bepaalt de bewaartermijn van de krachtens het voorontwerp van wet verzamelde gegevens in de volgende bewoordingen:
"Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening EU 2016/679, bewaart de verwerkingsverantwoordelijke de in uitvoering van de wet verwerkte persoonsgegevens, onverminderd eventuele beroepsprocedures, gedurende 10 jaar na afloop van de verwerking die is uitgevoerd om een van de doeleinden bedoeld in artikel 36, § 3, te realiseren."

69. Zoals hierboven reeds is uiteengezet, moet de bewaartermijn van de persoonsgegevens die worden verzameld door de nationale cyberbeveiligingscertificeringsautoriteit en de ter uitvoering van artikel 5, § 2 van het project aan te wijzen autoriteiten voor de verwezenlijking van de in artikel 36, § 3 beoogde doeleinden, worden vastgesteld. De formulering van artikel 39 van het ontwerp moet nuttig worden aangepast in die zin.

70. Wat de beoogde bewaartermijn betreft, heeft de Autoriteit geen opmerkingen.

Afwijking van de rechten van de betrokkenen

71. Artikel 37 van het voorontwerp van wet wijkt in zeer ruime mate af van alle rechten van de betrokkenen krachtens de AVG.

72. Elke beperking van de rechten van betrokkenen krachtens de AVG moet niet alleen een van de in artikel 23.1 van de AVG genoemde doeleinden nastreven, maar ook voldoen aan de in artikel 23.2 van de AVG voorgeschreven vormen. Bovendien moet elke beperking van de rechten van de betrokkenen ook beperkt blijven tot wat strikt noodzakelijk is, zowel wat de reikwijdte als wat de duur betreft[17].

73. In de eerste plaats moeten de verwerkingsverantwoordelijke(n) die deze afwijkingen genieten, uitdrukkelijk worden vermeld, namelijk, zoals blijkt uit de aanvullende informatie, de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die ter uitvoering van het artikel 5, § 2 van het ontwerp zullen worden aangewezen.

[17] Advies nr. 34/2018 van 11 april 2018 *over een voorontwerp van wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG*, meer bepaald de overwegingen 36 tot 38; Advies nr. 41/2018 van 23 mei 2018 *over een voorontwerp van wet houdende diverse financiële bepalingen*; Advies nr. 88/2018 van 26 september 2018 *over het ontwerp van besluit van de Vlaamse Regering houdende aanpassing van de besluiten van de Vlaamse Regering aan de verordening (EU).*

74. Volgens artikel 37 van het ontwerp komen de verwerkingen van de genoemde verantwoordelijken waarvoor de beoogde afwijking zal gelden, overeen met de verwerkingen die worden verricht met als doel het beheer van klachten in verband met de toekenning van een cyberbeveiligingscertificaat of de weigering om een dergelijk certificaat af te geven.

75. Hoewel de Autoriteit begrijpt dat er voor controleverwerkingen moet worden voorzien in afwijkingen van bepaalde door de AVG gewaarborgde rechten (om deze controleverrichtingen niet in het gedrang te brengen), vraagt zij zich af of het nodig is in dit soort afwijkingen te voorzien voor het beheer van klachten in verband met de toekenning of de weigering van certificaten. Wat de laatstgenoemde verwerkingen betreft, kan de Autoriteit anderzijds begrijpen dat het nodig is in het voorontwerp van wet te voorzien in de mogelijkheid voor klagers om te verzoeken dat hun klacht zodanig wordt behandeld dat hun anonimiteit wordt bewaard (voor zover de behandeling van de klacht dit toelaat), maar afgezien van dit geval, dat in het voorontwerp van wet kan worden opgenomen, lijkt het in het licht van de verkregen aanvullende inlichtingen niet nodig te voorzien in een afwijking van de in de artikelen 12 tot 22 van de AVG bedoelde rechten om te garanderen dat klachten naar behoren worden verwerkt. Bij gebrek aan een relevante rechtvaardiging in de memorie van toelichting moet het toepassingsgebied van de afwijking dienovereenkomstig worden beperkt.

76. Vervolgens, met betrekking tot de afwijking ten behoeve van de gegevensverwerkingen door de inspectiediensten met als doel de uitoefening van hun controle-opdrachten zoals bedoeld in artikel 13 van het voorontwerp van wet, merkt de Autoriteit op dat het ter toepassing van artikel 23.2 van de AVG aan de auteur van het voorontwerp van wet is om in artikel 37 van het ontwerp de reikwijdte van de beperkingen te specificeren, niet alleen op het vlak van rechten waarvan wordt afgeweken, maar ook op het vlak van limieten van de beoogde afwijking, in plaats van te bepalen: *"De uitzondering geldt enkel indien en voor zover deze verwerkingen noodzakelijk zijn voor de hierboven bepaalde doeleinden, met name voor zover de toepassing van de rechten waarin deze verordening voorziet nadelig zou zijn voor een controle, onderzoek of klacht"*; wat de vereiste rechtszekerheid op dit vlak niet ten goede komt.

77. In dit verband beveelt de Autoriteit aan, zonder exhaustief te willen zijn, te specificeren dat de afwijkingen van de rechten van de betrokkenen alleen gelden gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of een onderzoek (met inbegrip van voorbereidende handelingen tot één jaar na ontvangst van het verzoek om uitoefening van het recht[18]) en gedurende de periode die nodig is voor de vervolging ter zake, voor zover de

[18] Teneinde te zorgen voor een redelijke beperking in de tijd voor de afwijking.

uitoefening van de rechten afbreuk zou doen aan de behoeften van de controle, het onderzoek of de voorbereidende handelingen.

78. Wat de keuze betreft van de artikelen van de AVG waarvan in het voorontwerp van wet voor de uitoefening van de inspectie-opdracht wordt besloten af te wijken, dienen de volgende opmerkingen te worden gemaakt:
    a. Artikel 12 van de AVG vermeldt uitdrukkelijk de transparantie van informatie en communicatie en de modaliteiten voor de uitoefening van de rechten van de betrokkenen en vormt op zich geen recht van de betrokkenen. Er is geen reden om hiervan af te wijken.
    b. Het is niet nodig om voor het beoogde doel af te wijken van het recht op gegevenswissing (art. 17 AVG). Hierover ondervraagd specificeerde de afgevaardigde van de minister het volgende: *"Il est prévu que les données à caractère personnel soient conservées sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. Cette durée se justifie par la nécessité de s'assurer de conserver plus longtemps les données à caractère personnel pouvant être liées à un faux ou usage de faux relatif à une certification de cybersécurité. Le service d'inspection doit également pouvoir d'identifier les cas de récidive pour les mêmes faits dans un délai de trois ans (qui peuvent donner lieu au doublement de l'amende administrative en vertu de l'article 24, § 4 de l'avant-projet). Or, sur base du droit à l'effacement, la personne concernée pourrait obtenir l'effacement prématuré de ses données. Il apparaît donc nécessaire de limiter ce droit."* In dit verband merkt de Autoriteit op dat betrokkenen op grond van het recht op gegevenswissing niet kunnen verkrijgen dat hun gegevens voortijdig worden gewist, maar uitsluitend wanneer een van de in artikel 17 genoemde gronden van toepassing is, wat in casu geen belemmering lijkt voor de controleprocedure van de inspectiedienst. We wijzen er ook op dat de diensten van de sociale inspectie en de fiscale inspectie evenmin van dit recht mogen afwijken, hoewel de redenen voor hun afwijkingen van de rechten van de betrokkenen in de AVG dezelfde zijn. Daarom moet de afwijking van dit recht uit artikel 37 van het ontwerp worden geschrapt.
    c. In dezelfde geest als het bovenstaande moet ook de afwijking van het recht van verzet om dezelfde redenen uit artikel 37 van het ontwerp worden geschrapt. In artikel 21 van de AVG wordt bepaald dat wanneer een betrokkene bezwaar maakt tegen verwerking van zijn gegevens ten behoeve van de uitoefening van een openbaredienstopdracht, *"de verwerkingsverantwoordelijke [...] de verwerking van de persoonsgegevens [staakt] tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering"*; wat voor de certificeringsautoriteit moeilijk te bewijzen zal zijn in het geval dat een dergelijk recht

wordt uitgeoefend door een gecontroleerde persoon; wat trouwens erg onwaarschijnlijk is aangezien een betrokkene dit recht pas kan uitoefenen wanneer hij er kennis van heeft dat hij wordt gecontroleerd; wat niet het geval zal zijn aangezien afgeweken wordt van de rechten op informatie en toegang.

d. Wat de afwijking van artikel 22 van de AVG door artikel 37 van het ontwerp betreft, betoogde de afgevaardigde van de minister in dit verband het volgende: *"Des décisions individuelles automatisées (fondées sur l'utilisation d'algorithmes) en matière de contrôle et de sanctions ne sont pas prévues à ce stade mais leur utilisation pourrait s'avérer dans le futur utile ou nécessaire."* In overeenstemming met artikel 22.2 van de AVG moeten, opdat de in artikel 5 van het voorontwerp van wet bedoelde autoriteiten, uitsluitend op basis van geautomatiseerde verwerking besluiten zouden kunnen nemen die rechtsgevolgen hebben voor de betrokkenen of hen ingrijpend treffen, deze besluiten worden genomen op grond van een specifieke wettelijke bepaling die de geautomatiseerde besluiten regelt en voorziet in passende maatregelen om de rechten en vrijheden van de betrokkenen te beschermen; dit is niet het geval in het voorontwerp van wet dat ter advies is voorgelegd. De afwijking van artikel 22 van de AVG lijkt bijgevolg niet nodig en moet eveneens worden weggelaten.

e. Artikel 20 van de AVG moet ook worden geschrapt van de lijst van artikelen waarvan wordt afgeweken, aangezien het in casu toch niet van toepassing is, zoals de afgevaardigde van de minister heeft bevestigd.

79. Teneinde artikel 37 van het ontwerp verenigbaar te maken met artikel 23.2 van de AVG moet bovendien worden voorzien in soortgelijke garanties als die waarin hoofdstuk 5/1 van het Sociaal Strafwetboek voorziet, aangezien de genoemde afwijkingen en garanties voor de rechten en vrijheden van de betrokkenen reeds zijn goedgekeurd door de gegevensbeschermingsautoriteit[19] (opname van de functionaris voor gegevensbescherming bij de autoriteiten zoals bedoeld in artikel 5 van het ontwerp voor de vastlegging van de feitelijke of juridische gronden waarop het besluit tot weigering van het recht van de betrokkene is gebaseerd en terbeschikkingstelling van deze gronden aan de Gegevensbeschermingsautoriteit op haar eerste verzoek, het in kennis stellen van de betrokkenen van de afwijzing van hun verzoek en de redenen daarvoor, tenzij dit het doel van de controle in gevaar zou brengen, en het in kennis stellen van de betrokkenen die hun rechten hebben willen uitoefenen van de opheffing van de afwijking na de afronding van de controle, het in kennis stellen van de betrokkenen van de rechtsmiddelen waarover ze in dat verband beschikken, ...).

[19] Ibidem.

80. De Autoriteit ziet de relevantie van het artikel 37, § 4 van het ontwerp niet in. Bovendien biedt het niet de rechtszekerheid die voor een afwijking van een grondrecht vereist is. De schrapping ervan wordt aanbevolen.

81. Artikel 37, § 5 moet eveneens worden geschrapt aangezien het overbodig is ten opzichte van andere bepalingen van het voorontwerp van wet en geen verband houdt met de vereisten van artikel 23.2 van de AVG.

Afwijking van artikel 20 van de WVP

82. Artikel 38 voorziet in een afwijking van de verplichting om de doorgifte van persoonsgegevens door middel van een protocol te formaliseren, zowel voor de autoriteiten die gegevens zullen meedelen aan de cyberbeveiligingscertificeringsautoriteit en aan de in artikel 5, § 2 van het voorontwerp van wet bedoelde autoriteiten, als voor laatstgenoemden.

83. De Autoriteit herinnert eraan dat de verplichting om een gegevensuitwisseling te formaliseren zoals bedoeld in artikel 20 van de WVP niet geldt voor een punctuele mededeling van gegevens[20]; dit zou het geval zijn bij de toepassing van artikel 29 van de Sv. (gerechtelijke autoriteiten).

84. De norm, om te kunnen afwijken van artikel 20 van de WVP, moet een kader bieden voor de bedoelde structurele stroom van persoonsgegevens, op voorzienbare wijze en in overeenstemming met de beginselen van noodzakelijkheid en evenredigheid; dit vereist dat *"uitdrukkelijk wordt bepaald aan wie (ontvanger(s)) wat (categorieën van meegedeelde gegevens), wanneer en waarom (doeleinden en modaliteiten van de mededeling) wordt verstrekt* "[21], in overeenstemming met de beginselen van noodzakelijkheid en evenredigheid; dit moet gebeuren op het niveau van de bepalingen van het wetsontwerp die een kader bieden voor deze mededelingen van gegevens door de nationale autoriteit voor de certificering van cyberbeveiliging. In dit verband wordt verwezen naar de bovengenoemde opmerkingen van de Autoriteit over de artikelen 16 en 17 van het voorontwerp van wet, die een kader bieden voor deze structurele mededeling van gegevens.

85. De structurele verzamelingen van persoonsgegevens die de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten bedoeld in artikel 5, § 2, zouden verrichten bij de sectorale autoriteiten (cf. supra) voor de uitvoering van de openbaredienstopdrachten waarin de Cyberbeveiligingsverordening voorziet, moeten aan dezelfde

[20] Aanbeveling 02/2020 van de Autoriteit van 31 januari 2020 betreffende draagwijdte van de verplichting om een protocol te sluiten om de mededelingen van persoonsgegevens door de federale publieke sector te formaliseren, p. 17.

[21] Ibidem, p. 16.

voorzienbaarheidscriteria voldoen opdat deze sectorale autoriteiten zouden worden vrijgesteld van de formalisering ervan door middel van een protocol in de zin van artikel 20 van de WVP. Voor zover de normen die deze sectorale autoriteiten regelen, hier niet in voorzien (wat de auteur van het voorontwerp van wet moet nagaan), moeten de bovengenoemde modaliteiten van deze mededelingen in het onderhavige voorontwerp van wet worden opgenomen voor zover zij betrekking hebben op persoonsgegevens.

Om deze redenen
is de Autoriteit
van oordeel dat het voorontwerp van wet dat voor advies is voorgelegd, in de volgende zin moet worden aangepast:

1. Herziening van artikel 6 §§ 1 en 3, 7, 16 §§ 2 en 3, 17 § 1 en 3, 36 §§ 1 en 3, 4° en 38, die voorzien in de uitwisseling van gegevens, teneinde deze adequaat te beperken tot hetgeen strikt noodzakelijk en evenredig is in het licht van de doelstellingen van de Cyberbeveiligingsverordening of aanverwante openbaredienstopdrachten die rechtstreeks van invloed zijn op de cyberbeveiliging, in overeenstemming met de algemene overwegingen van het advies en de specifieke overwegingen met betrekking tot deze bepalingen van het ontwerp (overw. 6 tot 14 en 19, 20, 37, 40 , 43 , 55, 85);

2. Oplegging van een specifieke informatieplicht aan de nationale certificeringsautoriteit in overeenstemming met overweging 15;

3. Schrapping van de taak van de afgifte van certificaten uit het toepassingsgebied van de afwijking van de geheimhoudingsplicht en het beroepsgeheim (overw. 23);

4. Omkadering van de afwijkingen van de geheimhoudingsplicht die nodig zijn voor de uitvoering van inspectietaken door de nationale certificeringsinstantie en de in artikel 5, § 2 bedoelde autoriteiten, in overeenstemming met overweging 26;

5. Instelling van passende waarborgen voor de eventuele verzamelingen van gegevens die nodig zijn voor de uitoefening van deze inspectietaken en die onder het beroepsgeheim vallen, in overeenstemming met overweging 27;

6. Verduidelijking van artikel 13, § 2 betreffende het verzamelen van informatie door de inspectiedienst, in overeenstemming met overweging 31;

7. Toevoeging van waarborgen voor de vrijwaring van de rechten en vrijheden van de klanten (natuurlijke personen) van de onder toezicht staande ICT-dienstverleners (of de natuurlijke personen die klanten zijn van die klanten) met betrekking tot de rechtmatige inzamelingen en mededelingen van de inspectiedienst (overw. 33, 38, 67);

8. Oplegging van de naleving van het evenredigheidsbeginsel bij de uitoefening van inspectietaken (overw. 34);

9. Motivering van het noodzakelijke karakter van de afwijking van het vertrouwelijkheidsbeginsel van elektronische communicatie en beperking van de afwijking tot strikt noodzakelijke gevallen, omkadering van deze afwijking, in overeenstemming met de overwegingen 49 en 50 (overw. 45 tot 50);

10. Schrapping van de beschrijving van de categorieën van verwerking van persoonsgegevens (overw. 53 en 54);

11. Rectificatie van de beschrijving van de doeleinden van de gegevensverwerking van de nationale cyberbeveiligingscertificeringsautoriteit en van de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten, in overeenstemming met overweging 55;

12. Verduidelijking van de kwalificatie van de verwerkingsverantwoordelijke, in overeenstemming met de overwegingen 56 en 57;

13. Schrapping van artikel 36, § 2 van het ontwerp (overw. 58 tot 64);

14. Exhaustieve precisering van de categorieën gegevens die de nationale cyberbeveiligingscertificeringsautoriteit en de in overeenstemming met artikel 5, § 2 aangewezen autoriteiten zullen verwerken bij de uitoefening van de opdrachten die hun door het voorontwerp van wet worden toevertrouwd in overeenstemming met de overwegingen 61 e.v.;

15. Aanpassing van de categorieën van betrokkenen ten aanzien van wie de in artikel 5 bedoelde autoriteiten gegevens zullen verwerken, in overeenstemming met de overwegingen 66 en 67;

16. Verduidelijking van artikel 39 van het ontwerp over de duur van de gegevensbewaring, in overeenstemming met overweging 69;

17. Beperking van de rechten van de betrokkenen uit hoofde van de AVG waarvan wordt afgeweken tot louter de rechten waarvan de uitoefening de inspectietaken in het gedrang brengt, en het bieden van een passend kader voor dergelijke afwijkingen van deze rechten en van de verplichting uit hoofde van artikel 20 van de WVP om een protocol voor gegevensuitwisseling te sluiten, in overeenstemming met de overwegingen 73 tot 81.

Voor het Kenniscentrum,
(get.) Rita Van Nuffelen - Verantwoordelijke a.i. van het Kenniscentrum