ONTWERP VAN DECREET TOT WIJZIGING VAN HET BESTUURSDECREET VAN 7 DECEMBER 2018, WAT BETREFT HET VLAAMSE DIGITALE VEILIGHEIDSBELEID EN DE OPRICHTING VAN EEN VLAAMS CENTRUM VOOR DIGITALE VEILIGHEID

Samenvatting

Het Regeerakkoord van de Vlaamse Regering 2024-2029 stelt dat Vlaanderen streeft naar een digitaal veilig Vlaanderen. In het Agentschap Digitaal Vlaanderen wordt daartoe een Vlaams Centrum voor Digitale Veiligheid gecreëerd dat een veiligheidsstrategie uitwerkt en coördineert in Vlaanderen. Het overkoepelende digitaal veiligheidsbeleid wordt uitgebreid naar de hele Vlaamse overheid en de lokale besturen.

Op 1 mei 2025 keurde de Vlaamse Regering de oprichting van het Vlaams Centrum Digitale Veiligheid (VCDV) binnen het agentschap Digitaal Vlaanderen (VR 2025 0404 DOC.0220/1BIS) goed.
Op 3 april 2026 stelde de Vlaamse Regering de Vlaamse beleidsstrategie digitale veiligheid vast.

Gelet op de centrale rol die het VCDV speelt in het digitale veiligheidsbeleid, en de opdrachten die aan haar zullen worden toebedeeld, is er nood aan een verdere decretale verankering.

Een van de opdrachten van het VCDV is om de beleidsstrategie digitale veiligheid op Vlaams en lokaal niveau verder uit te werken, te coördineren en op te volgen. Het VCDV werkt daartoe een Vlaams digitaal veiligheidsbeleid uit, met verplichtende richtlijnen en maatregelen. Het VCDV voert toezicht op dit beleid om de maturiteit van de betrokken instanties op te volgen en het veiligheidsbeleid te optimaliseren. Het VCDV voorziet in een aangepast begeleidings- en ondersteuningsaanbod. Het VCDV volgt actief bedreigingen en kwetsbaarheden op en informeert daarover. Het VCDV verzorgt de opvolging en afhandeling van incidenten inzake digitale veiligheid. Het VCDV neemt een verbindende regierol op en stemt de verschillende beleidsstrategieën op het gebied van digitale veiligheid binnen de Vlaamse beleidsdomeinen op elkaar af. Het VCDV is het aanspreekpunt voor Vlaamse en lokale overheidsinstanties en treedt op als gemandateerde gesprekspartner voor het Centrum voor Cybersecurity België (CCB) en andere regionale of internationale cyberveiligheidsinstanties en het Crisiscentrum Vlaamse overheid (CCVO) in geval van cyberincidenten. Het VCDV bouwt een netwerk uit van partners en deelt kennis met als gemeenschappelijk doel een digitaal weerbaar Vlaanderen.

Met de oprichting van het VCDV en de beleidsstrategie digitale veiligheid wordt invulling gegeven aan één van de ambities van het Vlaams regeerakkoord. Vlaanderen wil in 2030 een toonaangevende, veerkrachtige, digitaal weerbare en verantwoordelijke regio zijn die in staat is om de Vlaamse belangen in de online leef- en werkomgeving te beschermen en te bevorderen.

MEMORIE VAN TOELICHTING

I. ALGEMENE TOELICHTING

A. Situering

1. Het Vlaams Regeerakkoord 2024-2029 "Samen werken aan een warm en welvarend Vlaanderen, 30 september 2024", stelt:

> "Vlaanderen maakt werk van een versnelde digitalisering van de overheid en dat in nauwe samenwerking met de lokale besturen. We zetten de werking van het Cyber Response Team voort, zodat Vlaanderen lokale besturen kan bijstaan die te maken krijgen met een acuut cyberrisico."
>
> "We streven naar een digitaal veilig Vlaanderen. In het Agentschap Digitaal Vlaanderen creëren we een Vlaams Centrum voor Digitale Veiligheid, waarmee we een sterke veiligheidsstrategie kunnen uitwerken en coördineren in Vlaanderen. We breiden het overkoepelende veiligheidsbeleid uit naar de hele Vlaamse overheid en de (boven)lokale besturen. Bij die initiatieven erkennen we bestaande innovaties en waardevolle projecten op lokaal niveau en nemen we hun ervaringen mee."

2. Op 1 mei 2025 werd door de Vlaamse regering een belangrijke stap gezet met de oprichting van het Vlaams Centrum voor Digitale Veiligheid (VCDV) binnen het agentschap Digitaal Vlaanderen (VR 2025 0404 DOC.0220/1BIS). Een van de opdrachten van het VCDV is om de beleidsstrategie digitale veiligheid op Vlaams en lokaal niveau verder uit te werken. Het VCDV staat daarbij in voor de opmaak van de beleidsstrategie en de opvolging ervan.

3. Vlaanderen wil binnen Europa een vooruitstrevende regio zijn, die opportuniteiten uit digitale technologieën en data inzet om maatschappelijke uitdagingen beter aan te pakken en in te spelen op de noden van burgers, ondernemingen en verenigingen. Via één eenduidige en afgestemde digitale strategie voor de Vlaamse administratie en de andere overheden wordt meer dan ooit ingezet op een datagedreven overheid, op proactieve en slimme diensten, op onze digitale veiligheid en op een inclusieve dienstverlening. De Digitale Strategie voor Vlaanderen werd op 27 juni 2025 goedgekeurd (VR 2025 2706 DOC.0521).

Ook de geopolitieke uitdagingen hebben recent enorm aan belang gewonnen, waardoor Vlaanderen voor de uitdaging staat om haar eigen digitale autonomie en digitale veiligheid te waarborgen. De Digitale Strategie voor Vlaanderen, en de speerpunten en randvoorwaarden voor het garanderen van de digitale veiligheid moeten in een Vlaamse beleidsstrategie digitale veiligheid worden doorvertaald. Zo'n Vlaamse beleidsstrategie digitale veiligheid zorgt zoveel als mogelijk voor een alignatie van de bestaande beleidsstrategieën voor de overheden, de ondernemingen en de burgers. Ook wordt er gestreefd naar een zoveel als mogelijk op elkaar afstemmen van bewustmakingsinitiatieven en ondersteuningscampagnes, en om kennis en instrumenten ter beschikking te stellen van de Vlaamse en lokale entiteiten, alsook aan bedrijven.

4. Met de uitwerking van een Vlaamse beleidsstrategie digitale veiligheid en de inrichting van het Vlaams Centrum voor Digitale Veiligheid wordt invulling gegeven aan één van de ambities van het Vlaams regeerakkoord 2024-2029.

B. Inhoud

Probleemstelling en omgevingsanalyse

5. Digitalisering van diensten en technologische toepassingen zijn vandaag niet meer weg te denken uit onze samenleving, onze economie en onze overheidsdiensten. Deze digitale en technologische sprong heeft vele voordelen meegebracht, maar vereist ook waakzaamheid voor risico's en bedreigingen. Zo is cybercriminaliteit een gegeven geworden waar de samenleving constant mee geconfronteerd wordt: het aantal veiligheidsincidenten stijgt exponentieel, en de cybercriminelen gaan daarbij steeds innovatiever te werk. Zo blijk uit de cybersecurity barometer 2024[1] van het Departement WEWIS dat in 2024 één op twee Vlaamse bedrijven (45,8%) slachtoffer was van een cyberaanval, en dat deze cyberaanvallen in 1 op de 10 gevallen schade aan het bedrijf berokkenden. Het landschap van cyberdreigingen is in volle evolutie. Gegevens van besturen of ondernemingen worden gestolen of geblokkeerd, er wordt losgeld gevraagd om informatie of systemen terug vrij te geven. Online fraude neemt significant toe en manifesteert zich in verschillende vormen, zoals investerings- of cryptofraude, identiteits-, domicilie- en betaalfraude, nepwebshops en CEO- en factuurfraude. Ook desinformatie en fake news zijn in opmars, en vaak gericht op het schaden van het vertrouwen in de overheid.

De maatschappelijke en bestuurlijke impact bij dergelijke cyberincidenten is niet te onderschatten. Er is niet alleen de (tijdelijke) onbeschikbaarheid van noodzakelijke dienstverlening, maar ook de herstelkosten om de diensten terug operationeel te maken kunnen hoog oplopen. Daarnaast zijn er ook veel verborgen kosten: de impact op het imago, het heropbouwen van het vertrouwen en de mogelijke juridische consequenties. Het kunnen verzekeren van de continuïteit en beschikbaarheid van (al dan niet kritieke) (overheids)dienstverlening is een noodzaak. Het gaat bijvoorbeeld over de (zee)havens, het vervoer over de weg en de (binnen)wateren, ziekenhuizen en woonzorgcampussen, energie- en drinkwatervoorziening, maar ook de loketdiensten van de gemeenten en andere overheidsdienstverlening.

6. Overheidsdiensten blijken bovendien extra kwetsbaar voor cyberincidenten. Zo toont het ENISA Threat Landscape rapport van 2025[2], dat een overzicht van de getroffen sectoren waarbij de overheden met 38% de meest getroffen sector zijn en dat er een aanzienlijke stijging merkbaar is ten opzichte van 2024 (19%). Het meest recente specifieke sectorale dreigingsrapport van ENISA over de publieke sector (2024)[3] specifieert dat centrale overheden het vaakst het doelwit waren, goed voor 69% van de incidenten. Het merendeel van de incidenten was daarbij gericht op de websites van parlementen, ministeries en nationale autoriteiten of instanties. Lokale entiteiten volgen met 24%. Regionale entiteiten werden het minst getroffen met 6,8% van het totale aantal incidenten. De conclusie van het dreigingsrapport voorspelt weinig goeds: gezien de lage maturiteit van de publieke sector, en het feit dat deze als een potentieel doelwit wordt beschouwd, is het zeer waarschijnlijk dat de publieke sector in de EU op middellange tot lange termijn een

[1] CS-barometer 2024, http://www.vlaio.be/nl/begeleiding-advies/digitalisering/cybersecurity/waarom-inzetten-op-cybersecurity/cs-barometer.
[2] ENISA Threat Landscape 2025, http://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
[3] ENISA Sectorial Threat Landscape - Public Administration 2024, http://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape-public-administration

doelwit zal blijven. Dat wordt ook bevestigd door het sectoraal overzichtsrapport NIS360 (2024) uitgebracht door ENISA[4]. Het rapport meet de volwassenheid en kriticiteit van sectoren. Volgens dit rapport is de publieke sector bezig met het ontwikkelen van zijn digitale weerbaarheid, aangezien het zich nog in een vroeg stadium bevindt om te voldoen aan de NIS2-vereisten. Het openbaar bestuur werd daarom in het ENISA NIS360-rapport beoordeeld als zijnde in de "risicozone". Het vertrouwen van burgers in de (digitale) overheid staat of valt nochtans met een goede beveiliging. Burgers willen zekerheid wanneer hun persoonlijke gegevens gedeeld worden met de overheid, en willen zonder zorgen digitale overheidsdiensten gebruiken.

7. Digitale veiligheid is een complexe maatschappelijke uitdaging. Gelet op het bovenstaande is investeren in digitale veiligheid essentieel, zowel voor de burger, de overheid als voor ondernemingen. De Vlaamse overheid en de lokale besturen blijven het eerste aanspreekpunt in het maatschappelijk veld. Een betrouwbare actor zijn is dus een noodzaak. De burger moet er immers op kunnen vertrouwen dat er op een correcte en veilige manier met zijn informatie en gegevens omgesprongen wordt. De overheid heeft daarbij ook een bewustmakingsopdracht, om haar burgers en personeelsleden te wapenen en digitaal weerbaar te maken. De voorbije jaren heeft de Vlaamse overheid dan ook volop ingezet op het versterken van de digitale veiligheid bij zowel haar administratie als op het lokale niveau. Dit vertaalde zich op Vlaams niveau onder meer in de Vlaamse Strategie Informatieveiligheid (2021), en op het lokale niveau in het aanbieden van preventieve en reactieve ondersteuning zoals de toolkit digitale veiligheid, de cofinanciering van ICT-veiligheidsaudits, de oprichting van het Vlaamse Cyber Response Team (Vo-CRT) en meer.

8. Niet alleen op Vlaams niveau werden maatregelen genomen om de digitale veiligheid te versterken. Sinds 18 oktober 2024 is immers ook de NIS2-wet van kracht. Deze wet geeft uitvoering aan Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 en legt een kader op voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Deze NIS2-wet en de uitvoeringsbesluiten ervan (de wet van 26 april 2024 en het koninklijk besluit van 9 juni 2024) beogen een versterking van de maatregelen op het gebied van cyberveiligheid, het incidentbeheer en het toezicht voor entiteiten die diensten leveren die essentieel zijn voor het in stand houden van kritieke maatschappelijke of economische activiteiten. Daarbij worden er bijkomende verplichtingen opgelegd zoals het nemen van minimale maatregelen in het kader van het risicobeheer, het melden van en rapporteren over de incidenten, het verhogen van het bewustzijn bij management en personeel en het periodiek evalueren van de systemen door het uitvoeren van risicoanalyses. Ook verschillende Vlaamse en lokale overheidsinstanties vallen onder de verplichtingen van deze nieuwe NIS2-wet.

De NIS2-wet en de uitvoeringsbesluiten ervan vereisen dat organisaties tijdig passende organisatorische, operationele en technische maatregelen nemen om risico's te beperken of, als cyberincidenten toch voorvallen, de impact zoveel als mogelijk beperkt of geminimaliseerd wordt. De genomen maatregelen moeten zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich (kunnen) voordoen. De NIS2-wet maakt daarbij het onderscheid tussen 'essentiële' en 'belangrijke' entiteiten, afhankelijk van de sectoren waarin het bestuur actief is. Daarbij moet rekening gehouden worden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen. De maatregelen worden bepaald op

[4] ENISA NIS360 2024, http://www.enisa.europa.eu/publications/enisa-nis360-2024

basis van een risicoanalyse. De vereiste maatregelen worden genomen op basis van CyFun® of ISO27001. CyFun®, het referentiekader van de nationale cyberbeveiligingsautoriteit, het Centrum voor Cybersecurity België (CCB), hanteert drie zekerheidsniveaus:

- Basis: Dit niveau bevat standaard informatiebeveiligingsmaatregelen die de organisatie beschermen tegen de meest voorkomende, bekende cyberrisico's. De maatregelen maken gebruik van technologie en processen die over het algemeen al beschikbaar zijn binnen ondernemingen;
- Belangrijk: Dit niveau is ontworpen om de risico's van gerichte cyberaanvallen door actoren met gangbare vaardigheden en middelen te minimaliseren, bovenop de risico's die onder 'Basis' vallen;
- Essentieel: Dit is het hoogste niveau en is bedoeld om het risico van geavanceerde cyberaanvallen door actoren met uitgebreide vaardigheden en middelen aan te pakken.

Met het overkoepelend Vlaams digitaal veiligheidsbeleid wil het VCDV een stap verder gaan. Los van de NIS2-verplichtingen is het implementeren van digitale veiligheidsmaatregelen, om incidenten te voorkomen of de gevolgen ervan zoveel mogelijk te beperken, een element van goed bestuur. Daarom moeten ook alle Vlaamse overheidsinstellingen en lokale besturen die momenteel niet door NIS2 gevat zijn tegen 1 januari 2030 het zekerheidsniveau 'basis' behalen. Alle administraties hebben er baat bij dat de digitale weerbaarheid zo optimaal mogelijk is gelet op de sterke verbondenheid van de verschillende overheidsdiensten. Er moet een risicobewustzijn bestaan waarbij elke betrokken overheidsinstantie zijn verantwoordelijkheid opneemt.

Met het Vlaams digitaal veiligheidsbeleid zorgen we voor een geïntegreerde visie en krachtlijnen, met een bijpassend instrumentarium, waaraan Vlaanderen moet en wil voldoen om een digitaal veilige overheid en samenleving na te streven. Het aangereikte instrumentarium van het Vlaams digitaal veiligheidsbeleid maakt het Vlaamse en lokale entiteiten makkelijker om de digitale veiligheidsdoelstellingen te behalen. Vanuit een strategie en implementatiebeleid met digitale veiligheidseisen, een centraal en vereenvoudigd ondersteuningsaanbod, waaronder de Vlaamse veiligheidsbouwstenen en gemeenschappelijke ICT- en raamcontracten waarin het wettelijke kader inzake cyberveiligheid standaard verwerkt zit, wordt de weerbaarheid tegen digitale risico's verhoogd én de gebruikerservaring verbeterd. Het toepassen van het digitaal veiligheidsbeleid zorgt niet alleen voor de nodige compliance met de NIS2-verplichtingen, maar resulteert in een verhoogde digitale weerbaarheid van het bredere overheidslandschap (en de toeleveringsketen) en werkt efficiëntiewinsten en schaalvoordelen in de hand. Door de centralisatie van beleidsvormende en ondersteunende activiteiten en door het voorzien van de nodige kennis en competenties - gelet op de beperkte beschikbaarheid van deze profielen op de arbeidsmarkt - zorgt het VCDV voor maximale hefbomen om de maturiteit inzake digitale veiligheid zowel op Vlaams als lokaal niveau te verhogen.

Met de jaarlijkse rapportage (zie infra), dat één van de essentiële pijlers en het sluitstuk vormt van het Vlaams digitaal veiligheidsbeleid, krijgt het VCDV bovendien een beeld waar het beleid nog aangescherpt kan worden, zodat de nodige ondersteuningstrajecten voorzien kunnen worden.

9. De geopolitieke situatie, de toenemende dreigingen en digitale veiligheidsincidenten, de bijzondere kwetsbaarheid van de publieke sector, en het NIS2 regelgevende kader, tonen aan dat digitale veiligheid een transversale beleidsthematiek is die meerdere beleidsdomeinen en de publieke en private sector impacteert. Het is duidelijk dat aandacht voor digitale veiligheid niet meer weg te denken is uit de dagelijkse bezigheden van alle Vlaamse en lokale administraties, en dat digitale veiligheid ingebakken zit in het risicobeheer van deze overheden.

De uitdagingen zijn dan ook enorm en complex, waardoor bijkomende acties nodig zijn om de cyberweerbaarheid te vergroten en het kader voor digitale veiligheid te versterken. Zo ontbreekt er tot op vandaag een helder, geïntegreerd beleid, alsook een coördinatie en globaal overzicht van de verschillende Vlaamse en (boven)lokale beleidslijnen en initiatieven. Eén overkoepelende coördinatie zowel beleidsmatig, met een Vlaamse beleidsstrategie digitale veiligheid, als operationeel, via een krachtenbundeling in een Vlaams Centrum voor Digitale Veiligheid, is noodzakelijk om de digitale weerbaarheid in Vlaanderen beter te waarborgen.

Beleidsmaatregelen en doelstelling

10. Vlaanderen wil in 2030 een toonaangevende, veerkrachtige, digitaal weerbare en verantwoordelijke regio zijn die in staat is om de Vlaamse belangen in de online leef- en werkomgeving te beschermen en te bevorderen. Gelet daarop versterkt dit ontwerp van decreet het kader voor digitale veiligheid binnen de Vlaamse en lokale besturen.

Het Vlaams Centrum voor Digitale Veiligheid zal de spil vormen van dit robuust Vlaams digitaal veiligheidsbeleid voor Vlaamse en lokale instanties. Hoewel het VCDV al op 1 mei 2025 werd opgericht binnen het agentschap Digitaal Vlaanderen (beslissing van de Vlaamse Regering VR 2025 0404 DOC.0220/1BIS) is er, gelet op de centrale rol die het VCDV zal spelen in het digitale veiligheidsbeleid, en de opdrachten die aan haar worden toebedeeld, nood aan een decretale verankering. Daartoe zal in Titel III, Hoofdstuk 3., van het Bestuursdecreet van 7 december 2018 een nieuwe afdeling 4/1 worden ingevoegd waarin de rol en opdrachten van het VCDV, en haar verhouding tot de Vlaamse overheidsinstellingen en lokale besturen, verduidelijkt worden. Het VCDV zal het Vlaams digitaal veiligheidsbeleid uitwerken en hierop toezicht houden. Het VCDV voorziet in een aangepast begeleidings- en ondersteuningsaanbod voor Vlaamse en lokale entiteiten en verzorgt de opvolging en afhandeling van digitale veiligheidsincidenten. Het VCDV treedt op als gemandateerde gesprekspartner voor het Centrum voor Cybersecurity België (CCB) en andere regionale of internationale cyberveiligheidsinstanties en het Crisiscentrum van de Vlaamse overheid (CCVO) in geval van cyberincidenten, en bouwt een netwerk uit van partners met als gemeenschappelijk doel een weerbaar Vlaanderen wat betreft de digitale veiligheid.

Om de effectiviteit van het Vlaams digitaal veiligheidsbeleid te vergroten, en om versnippering tegen te gaan, voorziet dit ontwerp van decreet daarnaast dat er werk gemaakt wordt van één heldere, overkoepelende Vlaamse beleidsstrategie digitale veiligheid, die wordt goedgekeurd door de Vlaamse Regering. Deze beleidsstrategie digitale veiligheid zal de belangrijkste strategische beleidslijnen en prioriteiten op het vlak van digitale veiligheid beschrijven en bindende afspraken bevatten voor zowel de Vlaamse overheidsinstellingen als lokale besturen, met inbegrip van de minimale verplichtingen op het vlak van digitale veiligheid die moeten worden geïmplementeerd. Daarnaast zal deze beleidsstrategie ook richtlijnen en procedures voor toezicht, incidentmelding en afhandeling bevatten. De Vlaamse beleidsstrategie digitale veiligheid wordt voorbereid door het VCDV, dat ook zal instaan voor het omzetten ervan in concrete implementatierichtlijnen en het toezicht op de naleving ervan.

Door de bestendiging van het VCDV binnen het agentschap Digitaal Vlaanderen, en het (verder) ontwikkelen van een overkoepelende beleidsstrategie digitale veiligheid voor Vlaamse overheidsinstellingen en lokale besturen, wordt gezorgd voor een gecoördineerde aanpak voor digitale veiligheid in Vlaanderen. Samen met het bestaande regelgevende kader, in het bijzonder de NIS2-wet en de uitvoeringsbesluiten ervan, moet dit zorgen voor een digitaal veilig Vlaanderen.

VCDV als coördinator van het Vlaamse digitale veiligheidsbeleid.

11. Digitale veiligheid raakt menige beleidsuitdaging en vat verschillende beleidsdomeinen. De Europese en mondiale crisissen van de afgelopen jaren maakten duidelijk dat een crisisaanpak vanuit elke Vlaamse entiteit afzonderlijk of enkel vanuit de federale noodplanningsactoren niet volstaat om een solide garantie te kunnen bieden voor een continue economische en maatschappelijke dienstverlening. Om hieraan tegemoet te komen voorziet het ontworpen artikel III.78/4 dat het Vlaams Centrum voor Digitale Veiligheid een regierol zal opnemen om te komen tot een coherent en geïntegreerd Vlaams digitaal veiligheidsbeleid. Door afstemming te faciliteren tussen de Vlaamse entiteiten, die elk vanuit hun opdrachten rond digitale veiligheid werken voor Vlaams en lokaal niveau, creëert het VCDV een gealigneerd, coherent en geïntegreerd digitaal veiligheidsbeleid binnen Vlaanderen.

Het VCDV ontwikkelt daarbij een langetermijnvisie en een gecoördineerde aanpak voor digitale veiligheid in Vlaanderen, in samenwerking met alle betrokken beleidsdomeinen en over alle verschillende doelgroepen - burgers, verenigingen, ondernemingen en overheid - heen. Op deze manier worden bestaande regelgevingen en verplichtingen beter op elkaar gealigneerd, wordt kennis- en expertisedeling gefaciliteerd, en worden krachten gebundeld. Het biedt de mogelijkheid om uitdagingen en trends vanuit verschillende disciplinaire invalshoeken te bekijken, rekening houdend met bredere (geo)politieke, economische en maatschappelijke factoren. Elke entiteit behoudt weliswaar de eindverantwoordelijkheid voor digitale veiligheid binnen haar eigen bevoegdheidsdomeinen.

Om deze regierol te vervullen overlegt het VCDV periodiek met de betrokken Vlaamse entiteiten en relevante stakeholders om beleidsmatig de agenda's te aligneren, initiatieven beter op elkaar af te stemmen en gemeenschappelijke doelstellingen uit te werken.

Een Vlaamse beleidsstrategie digitale veiligheid

12. Met het oog op het opbouwen en versterken van de weerbaarheid tegen cyberdreigingen, keurt de Vlaamse Regering een overkoepelende Vlaamse beleidsstrategie digitale veiligheid goed waarin de strategie en prioriteiten op het vlak van digitale veiligheid wordt gecentraliseerd, en die bindende afspraken bevat voor de Vlaamse overheidsinstellingen en lokale besturen. Deze Vlaamse beleidsstrategie digitale veiligheid wil een belangrijke bijdrage leveren in het ontwikkelen van een digitale veiligheidscultuur en de digitale weerbaarheid op Vlaams en lokaal niveau. Ze heeft als doel het bewustzijn, het kennisniveau en de vaardigheden van de verschillende doelgroepen te verhogen om mogelijke risico's en dreigingen waar te kunnen nemen en adequaat te kunnen reageren. Een gecoördineerde aanpak is hierbij noodzakelijk. De Vlaamse beleidsstrategie digitale veiligheid stemt de verschillende strategieën rond digitale veiligheid voor overheden, ondernemingen, organisaties en burgers op elkaar af, aligneert initiatieven en ondersteuningscampagnes en beschrijft kennis en instrumenten die ter beschikking gesteld kunnen worden van Vlaamse en lokale overheidsinstanties alsook bedrijven.

Het is de opdracht van het Vlaams Centrum voor Digitale Veiligheid om deze Vlaamse beleidsstrategie digitale veiligheid voor te bereiden en te coördineren. Deze beleidsstrategie wordt, eens ze goedgekeurd is door de Vlaamse Regering, door het VCDV verder geoperationaliseerd via concrete implementatierichtlijnen. Deze richtlijnen kunnen wettelijke kaders, digitale veiligheidsdoelstellingen, en andere verplichte maatregelen of instrumenten omvatten (zoals een toolbox met templates om een ISMS te implementeren, sjablonen, webinars, trainingen en opleidingen etc.) die de toepassing van de beleidsstrategie door Vlaamse overheidsinstellingen en lokale besturen faciliteren. Doelstellingen, die specifiek zijn voor Vlaamse overheidsinstellingen, worden daarbij zoveel als mogelijk vertaald naar het lokale overheidslandschap.

De verplichtingen voor Vlaamse overheidsinstellingen en lokale besturen die voortvloeien uit de Vlaamse beleidsstrategie digitale veiligheid, en bijhorende implementatierichtlijnen, zijn complementair aan de verplichtingen uit de NIS2-wet. Door deze Vlaamse beleidsstrategie en bijhorende implementatierichtlijnen correct uit te voeren, en door gebruik te maken van de door het VCDV voorziene instrumenten, worden deze instanties en besturen maximaal ondersteund bij het behalen van het door de NIS2 wetgeving opgelegde zekerheidsniveau.

Toezicht op de implementatie en de naleving van de Vlaamse beleidsstrategie digitale veiligheid, en de NIS2 wetgeving door de Vlaamse overheidsinstellingen en lokale besturen.

13. Het Vlaams Centrum voor Digitale Veiligheid zal opvolgen hoe de Vlaamse overheidsinstellingen en de lokale besturen uitvoering geven aan de Vlaamse beleidsstrategie digitale veiligheid en de daaruit voortvloeiende implementatierichtlijnen. Daarnaast volgt het VCDV ook op hoe deze instanties de nodige minimale maatregelen nemen om in overeenstemming te zijn met de NIS2-wet en de uitvoeringsbesluiten ervan. De NIS2 wetgeving vereist immers dat organisaties tijdig passende organisatorische, operationele en technische maatregelen nemen om risico's te beperken of, als incidenten toch voorvallen, de impact daarvan zoveel als mogelijk te beperken of te minimaliseren.

Om deze opvolging te faciliteren zullen de Vlaamse overheidsinstellingen en lokale besturen jaarlijks aan het VCDV rapporteren over de implementatie van de beleidsstrategie digitale veiligheid en van de NIS2-verplichtingen. Deze jaarlijkse conformiteitstoets is noodzakelijk om te verzekeren dat het Vlaamse digitale veiligheidsbeleid succesvol doorvloeit naar alle betrokken instanties en om eventuele werkpunten tijdig te signaleren. De ketting is immers maar zo sterk als de zwakste schakel. Door het versterken van de digitale veiligheid wordt bovendien de weerbaarheid van Digitaal Vlaanderen gerealiseerd. Vlaamse en lokale besturen maken gebruik van de dienstverlening en Vlaamse bouwstenen die door Digitaal Vlaanderen aangeboden wordt. Als aanbieder van ICT-infrastructuur en -dienstverlening moet Digitaal Vlaanderen de hoogste zekerheidsgarantie aanbieden. Het is daarom ook belangrijk dat de overheden die gebruik maken van deze dienstverlening ook voldoende digitaal veilig zijn. Alle overheidsinstanties hebben er baat bij dat de digitale weerbaarheid zo optimaal mogelijk is gelet op de sterke verbondenheid van de verschillende overheidsdiensten. Verder geeft deze jaarlijkse meting een beeld waar het beleid nog aangescherpt kan (of moet) worden, zodat de nodige ondersteuningstrajecten voorzien kunnen worden. Op basis van de voortgang van de maturiteit van de entiteiten verkrijgt het VCDV ook aanwijzingen als er nog bijkomend nood is aan ondersteuning of implementatierichtlijnen. De rapporteringen worden door het VCDV geaggregeerd en geanonimiseerd, en bezorgd aan het stuurorgaan Vlaams Informatie- en ICT-beleid, vermeld in artikel III.74 van het Bestuursdecreet van 7 december 2018, het Auditcomité van de lokale besturen, het Auditcomité van de Vlaamse

administratie en Audit Vlaanderen. Ze geeft daarnaast zichtbaarheid aan de naleving via dashboards en de metrieken die gedeeld worden met beleidsverantwoordelijken. De rapportering wordt aldus gebruikt om het Vlaams digitaal veiligheidsbeleid en de beleidsondersteuning verder te optimaliseren en waar nodig bij te sturen. Naast de jaarlijkse rapportering voorziet het ontwerp van decreet ook in een driejaarlijkse conformiteitsbeoordeling waarbij alle Vlaamse overheidsinstellingen en lokale besturen minstens driejaarlijks hun stappen inzake digitale veiligheid extern laten verifiëren.

Dit toezicht door het VCDV is complementair aan het (op federaal niveau georganiseerde) toezicht dat plaatsvindt in het kader van de NIS2 wetgeving. Het toezicht uitgeoefend door het VCDV is dus geen formele inspectie als controleorgaan maar fungeert louter als een strategische facilitator (cfr supra). Het VCDV stemt wel af met formele controle-instanties, onder meer via de werkgroep single audit. Zo overlegt ze met de VTC als toezichthoudende autoriteit voor de toepassing van de Algemene Verordening Gegevensbescherming (AVG) door de Vlaamse en lokale instanties.

Het VCDV werkt ook samen met het Centrum voor Cybersecurity België (CCB). Het VCDV kan het CCB bij inspecties in het kader van de NIS2-conformiteitstoets ondersteunen of als expert bijstaan alsook door het uitwisselen van informatie. Het VCDV legt afspraken met betrekking tot het toezicht vast via samenwerkingsovereenkomsten met het CCB (cfr derde lid). In het kader van haar toezichtrol kan het VCDV ook andere bevoegde instanties bijstaan wanneer zij inspecties uitvoeren die betrekking hebben op de digitale veiligheid bij Vlaamse overheidsinstellingen of lokale besturen.

Aanbieden van advies, ondersteuning en nazorg bij digitale veiligheidsincidenten

14. Het Vlaams Centrum voor Digitale Veiligheid zet in op de ondersteuning en het ontzorgen van de Vlaamse overheidsinstellingen en lokale besturen bij cyberincidenten, zowel proactief (zie voorgesteld art III.78/2, tweede lid, 5°) als reactief (zie voorgesteld art III.78/2, tweede lid, 6°, en art. III. 78/8).

Vooreerst zal het VCDV een proactieve rol spelen door acute dreigingsinformatie te centraliseren vanuit Vlaamse overheidsinstellingen, lokale besturen, partners (CCB, sectorale overheden, ENISA, etc.) en toeleveranciers, en door proactief te communiceren over (het risico op) incidenten. Door in te zetten op sensibilisering en structurele kennisdeling wordt de weerbaarheid van zowel het VCDV als van de betrokken overheidsinstanties versterkt, wat een snellere en meer doeltreffende respons mogelijk maakt. Ter ondersteuning en ontzorging van de besturen worden centraal georganiseerde en op maat aangeboden veiligheidsdiensten ter beschikking gesteld zoals kwetsbaarhedenrapportering en penetratietesten, een security operations center (SOC) en securitymonitoringssystemen en ethische hackplatformen en phishingplatformen. Het gebruik van deze ondersteuning wordt aangemoedigd en opgevolgd via de jaarlijkse rapportering (cfr supra).

Voorkomen is beter dan genezen, maar wanneer incidenten zich voordoen is remediëring en ontzorging van essentieel belang. Het VCDV treedt daarom op als regionale Computer Security Incident Response Team (CSIRT) en fungeert als centraal aanspreek- en coördinatiepunt voor cyberincidenten bij Vlaamse overheidsinstellingen en lokale besturen.

Meldingen van onregelmatigheden of incidenten gebeuren centraal aan het CSIRT. Het CSIRT zal de evaluatie maken of een incident als een cyberincident gekwalificeerd wordt of niet. Niet enkel cybersecurityincidenten maar ook langdurige onderbrekingen moeten immers aan het CCB gemeld worden en bij

operationele onderbrekingen moet ook nagegaan worden of er bijkomend geen andere indicaties voorhanden zijn. De kwalificatie als (significant) incident zal door het CSIRT in afstemming met het geïmpacteerde bestuur gebeuren. Het regionaal CSIRT zal vervolgens samen met de entiteit de verplichte rapportering aan het CCB bezorgen.

Deze instanties en besturen zijn er bovendien toe gehouden om binnen de 24 uur alle significante incidenten waarvan ze slachtoffer zijn te melden aan het VCDV. Het VCDV zorgt samen met de betrokken entiteit voor de verdere rapportering en informering van het nationaal CSIRT (CCB) overeenkomstig de bepalingen van de NIS2-wetgeving (artikel 34 NIS-2 wet en e.v.). Op deze manier wordt vermeden dat digitale veiligheidsincidenten zich onopgemerkt kunnen uitbreiden over verschillende overheidsinstanties heen. Wanneer een incident zich dan voordoet staat het VCDV in voor de respons op de melding en biedt het adviesverlening en ondersteuning ter plaatse. In een eerste fase assisteert het VCDV als regionale CSIRT bij de opvolging van de wettelijke verplichtingen (zoals de initiële en tussentijdse rapporteringen bij het CCB in overeenstemming met de NIS2-wet, cfr. infra), in een tweede fase kan het ook ondersteuning bieden bij het onderzoeken van incidenten om de oorzaak te bepalen en adviseren over technische acties om risico op of impact van incidenten te vermijden.

Bij een incident is het belangrijk dat de geïmpacteerde entiteit makkelijk geïdentificeerd en gecontacteerd kan worden. Dit impliceert ook een centraal overzicht van de ICT-assets. Bij incidenten is de tijdsgevoeligheid en interconnectie tussen de verschillende gebeurtenissen belangrijk. Cyberaanvallen tegen overheidsinstanties zijn vaak geen alleenstaande gebeurtenissen. Een eerste aanval is dikwijls voorbode van de exploitatie van gelijkaardige zwakke punten in systemen bij andere overheden. Er wordt een log bijgehouden met een overzicht van de verschillende incidenten. Het VCDV coördineert de opmaak van het centraal overzicht én is daarbij het centraal contactpunt. Het VCDV biedt ook nazorg aan. Het VCDV kan met gerichte ondersteuning[5] helpen om de grondoorzaak bij incidenten te bepalen en zo (verdere) impact te vermijden.

De meldingsplicht aan en de respons door het VCDV doet geen afbreuk aan verplichtingen die uit andere regelgeving of beleidskaders zouden voortvloeien, zoals de AVG-regelgeving, de NIS2-wet, KSZ-regelgeving, of aan de verplichting van de getroffen entiteit om alle interne en externe belanghebbenden te informeren. Zo is op basis van de NIS2-wet iedere NIS2-entiteit verplicht om een significant cyberbeveiligingsincident te melden aan het nationale CSIRT (CCB). Het nationale CSIRT staat dan, als verantwoordelijke voor de NIS2-entiteiten, in voor de behandeling, classificatie en afhandeling van het incident. Het Nationaal Cybernoodplan biedt structuur om afspraken te maken over wie reageert op incidenten en/of cyberdreigingen binnen het complexe overheidslandschap. In overeenstemming met het Nationaal Cybernoodplan vereisen uiteenlopende soorten incidenten verschillende vormen van reactie, in samenwerking met het nationale CSIRT voor de classificatie van het incident en de afhandeling van NIS2-incidenten, afhankelijk van de urgentie of het belang ervan. De reactie van het VCDV zal variëren op basis van verschillende elementen en zich op verschillende onderdelen van de getroffen/aangevallen entiteit richten. Het VCDV en CCB wisselen informatie uit over de relevante (potentiële) cybermeldingen, in zoverre dit mogelijk is binnen de wettelijke bevoegdheden en de wettelijke en contractuele verplichtingen van de partijen.

Gelet op de dubbele meldingsplicht en het mogelijk gelijktijdig optreden van het VCDV en het CCB, hebben beide instanties afspraken gemaakt over de werking van

[5] De budgettaire impact is te bekijken op basis van de specifieke situatie en impact van het incident.

het VCDV als regionale CSIRT en de samenwerking met het CCB als nationale CSIRT (vastgelegd in een samenwerkingsovereenkomst van 23/12/2025).

De inzet van het VCDV als Cyber Response Team past in de EU-strategie om de mogelijkheid tot informatie-uitwisseling te voorzien rond cyberdreigingen door middel van informatie-uitwisselingsregelingen tussen gemeenschappen van gevatte organisaties, zoals de Vlaamse overheid en de lokale besturen, en het CCB als nationale CSIRT met als doel het niveau van cyberbeveiliging te verhogen.

Vlaamse overheidsinstellingen en lokale besturen kunnen beschikken over een eigen SOC en/of incident response team. In dat geval zullen er met deze entiteiten werkafspraken gemaakt worden om de informatiedoorstroming te stroomlijnen, zodat ook die informatie centraal opgevolgd en (waar wenselijk) verspreid kan worden. Het is daarbij essentieel dat deze eigen incident response teams en/of SOC's eenzelfde niveau van kwaliteit, prestaties en responstijden behaalt als het regionale CSIRT van het VCDV, en de door het VCDV aangeboden SOC.

Optreden als gemandateerde gesprekspartner voor institutioneel overleg met betrekking tot digitale veiligheid

15. Het Vlaams Centrum voor Digitale Veiligheid is de gemandateerde gesprekpartner voor institutioneel overleg inzake digitale veiligheid, zowel op lokaal, interfederaal, Europees als op internationaal niveau. Beleidsmatige afstemming en samenwerking met gefedereerde en internationale overheden is immers noodzakelijk. Zo is het VCDV de geprivilegieerde Vlaamse gesprekspartner voor onder meer het Centrum voor Cybersecurity voor België (CCB), Cyber Command en de Algemene Dienst Inlichting en Veiligheid (ADIV) en andere regionale, federale, Europese en internationale contactpunten en cyberveiligheidsinstanties.

Optreden als kenniscentrum rond digitale veiligheid

16. Het Vlaams Centrum voor Digitale Veiligheid is het centrale aanspreekpunt voor Vlaamse en lokale besturen en treedt op als kenniscentrum rond digitale veiligheid. Het VCDV zet in op beleidskaders, ondersteuning, opleiding en bewustwording, opdat Vlaamse en lokale besturen beschikken over voldoende kwalitatief geschoolde medewerkers en instrumenten om het Vlaams digitaal veiligheidsbeleid op hun werkterrein uit te kunnen rollen. Het VCDV ondersteunt met trainingen, webinars, bewustwordingscampagnes en faciliteert (mee) overheidsbrede crisisoefeningen. Alle Vlaamse overheidsinstellingen en lokale besturen kunnen deelnemen aan klankbordgroepen en opleidingssessies. Op deze wijze wordt de implementatie en draagvlakcreatie voor het beleid bestendigd en wordt er gewerkt aan de verdere kennisdeling.

Het VCDV functioneert op die manier ook als een katalysator voor het lokale ecosysteem. Door actieve betrokkenheid en ondersteuning aan partnerorganisaties met ICT-dienstverlening bij lokale besturen gebeurt de doorvertaling naar het lokaal overheidslandschap. De partners worden nauw betrokken, via onder andere een regulier stakeholderoverleg, bij de totstandkoming en de implementatie van het digitaal veiligheidsbeleid. De kennis die daar wordt gegenereerd wordt in de mate van het mogelijk ook verder ontsloten.

Impactanalyse

Maatschappelijke impact

17. De voorgestelde wijzigingen zullen bijdragen aan een robuuster juridisch kader dat het digitale veiligheidsbeleid van de Vlaamse overheid en lokale besturen uitbouwt en versterkt.

Voor dit ontwerp van decreet werd geen JoKER gemaakt omdat de inhoud ervan geen specifieke impact heeft op kinderen- en jongeren.

Voor dit ontwerp van decreet werd geen armoedetoets gemaakt omdat de inhoud ervan geen specifieke impact heeft op mensen die in armoede leven.

Impact op de grondrechten en het gelijkheidsbeginsel

18. Het voorliggend ontwerp van decreet heeft geen impact op de grondrechten en het gelijkheidsbeginsel.

Budgettaire impact

19. Het voorliggende voorontwerp van decreet vormt de decretale basis voor het Vlaams Centrum voor Digitale Veiligheid en de Vlaamse beleidsstrategie digitale veiligheid (zie beslissingen Vlaamse Regering: VR 2025 0404 DOC.0220/1BIS Opstart van het Vlaams Centrum voor Digitale Veiligheid; VR 2026 0304 DOC XXX Digitaal Veilig Vlaanderen: Vlaams Centrum voor Digitale Veiligheid en VR 2026 0304 DOC XXX Digitaal Veilig Vlaanderen: Vlaamse beleidsstrategie digitale veiligheid). Er is daarom geen nieuwe budgettaire impact.

Bestuurlijke impact op de lokale en provinciale besturen en op Brussel

20. Vanuit de Vlaamse beleidsstrategie digitale veiligheid is er in een eerste fase geen rechtstreekse impact op de lokale en provinciale besturen. Vlaamse overheidsinstellingen en lokale besturen die momenteel niet door NIS2 gevat zijn zullen het zekerheidsniveau basis tegen 1 januari 2030 moeten halen en de minimale maatregelen hieraan gekoppeld genomen hebben. Dit wordt opgevolgd door het Vlaams Centrum voor Digitale Veiligheid in het kader van haar toezichtsfunctie. Los van de NIS2-verplichtingen beschouwen we het implementeren van de nodige maatregelen om incidenten inzake digitale veiligheid te voorkomen of de gevolgen ervan zoveel mogelijk te beperken als een element van goed bestuur.

De bestaande afsprakennota organisatiebeheersing van Audit Vlaanderen - opgesteld in samenwerking met ABB, VVSG, Audio en VVP - wordt aangepast.

Verder wordt verwezen naar de beslissing van 4 april 2025 betreffende de opstart van het Vlaams Centrum voor Digitale Veiligheid (cfr VR 2025 0404 DOC.0220/1BIS).

Implementatie

Dit ontwerp van decreet vereist geen bijkomende uitvoeringshandelingen en treedt in werking op 1 januari 2027.

C. Totstandkomingsprocedure

24. De Inspectie Financiën verleende advies op 05/03/2026.

25. Het begrotingsakkoord werd aangevraagd op 12/03/2026

26. Het ontwerp van decreet werd aangepast aan het wetgevingsadvies nummer 2026/50 van 4 maart 2026, bezorgd op 04/03/2026.

27. Het ontwerp van decreet werd een eerste keer principieel goedgekeurd door de Vlaamse Regering op dd/mm/2026.

Advies Vlaamse Toezichtscommissie voor de verwerking van persoonsgegevens

28. De Vlaamse toezichtcommissie (VTC) gaf advies nr. … van …, bezorgd op dd/mm/2026.

Advies Raad van State

29. De Raad van State gaf advies nr. … van …, bezorgd op dd/mm/2026.

D. Bevoegdheid van de Vlaamse Gemeenschap en het Vlaamse Gewest

30. Het voorliggend ontwerp van decreet regelt een aangelegenheid die zowel behoort tot de bevoegdheid van het Vlaamse Gewest als van de Vlaamse Gemeenschap.

II. Toelichting bij de artikelen

Artikel 1

Het voorliggend ontwerp van decreet regelt een aangelegenheid die zowel behoort tot de bevoegdheid van het Vlaamse Gewest als van de Vlaamse Gemeenschap aangezien het decreet dat via voorliggend decreet wordt gewijzigd, ook zowel gemeenschaps- als gewestaangelegenheden betreffen.

Artikel 2

Aan Titel III, Hoofdstuk 3, van het Bestuursdecreet van 7 december 2018 wordt een nieuwe afdeling 4/1 ingevoegd met als opschrift "Vlaamse digitale veiligheidsbeleid en het Vlaams Centrum voor Digitale Veiligheid".

Artikel 3

Via artikel 3 wordt een nieuw artikel III.78/1 ingevoegd, dat de omschrijving van een aantal definities omvat.

Essentieel daarbij zijn de definities van "Vlaamse overheidsinstelling" (punt 1°) en "lokaal bestuur" (punt 2°), aangezien ze het toepassingsgebied van het Vlaamse digitale veiligheidsbeleid en het werkingsgebied van het Vlaams Centrum voor Digitale Veiligheid bepalen. Deze begrippen zijn beperkter dan de bestaande begrippen "Vlaamse overheid" of "Vlaamse administratie" en "lokale overheid", aangezien niet alle entiteiten die onder deze bestaande begrippen vallen geviseerd worden. Voor een aantal van de niet-gevatte instanties staan de implicaties op het vlak van het opgelegde veiligheidsbeleid en maatregelen niet in verhouding tot de beperkte grootte en werking. Daarnaast vallen bepaalde instanties en hun operationele werking reeds onder de verantwoordelijkheid van andere entiteiten.

De definitie van digitale veiligheid (punt 3°) is gebaseerd op de definitie "cyberbeveiliging" uit de Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening). Digitale veiligheid gaat echter breder dan cyberbeveiliging. Digitale veiligheid slaat op alle activiteiten die nodig zijn om digitale en fysieke infrastructuur en activiteiten, netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, alsook de organisatie, te beschermen.

Punt 5° voorziet het begrip "NIS2-wet" zodat op een eenvoudige en eenduidige manier verwezen kan worden naar het belangrijkste, bestaande kader inzake cyberbeveiliging dat bestaat uit, de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid en bijhorende uitvoeringsbesluiten, die voor België Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 omzetten.

De definities van cyberdreiging (punt 4°) en incident (punt 6°) zijn gebaseerd op de definities uit de NIS-2 wet. Voor de definitie van cyberdreiging werd daarbij de definitie uit de cyberbeveiligingsverordening (Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013) overgenomen.

Artikel 4

Het Vlaams Centrum voor Digitale Veiligheid, dat werd opgericht bij het agentschap Digitaal Vlaanderen, krijgt een decretale verankering in artikel III.78/2 van het Bestuursdecreet. Dat artikel zet ook de opdrachten van dit centrum uiteen:

- voorbereiden, coördineren, en operationaliseren van de Vlaamse beleidsstrategie digitale veiligheid, vermeld in artikel III.78/5;
- opnemen van een regierol binnen het Vlaamse beleid over digitale veiligheid;
- toezicht houden op de implementatie en naleving van de Vlaamse beleidsstrategie digitale veiligheid, vermeld in artikel III.78/5, door de Vlaamse overheidsinstellingen en lokale besturen;
- opvolgen van de naleving van de NIS2-wet en de uitvoeringsbesluiten ervan door de Vlaamse overheidsinstellingen en lokale besturen;
- het actief opvolgen, detecteren, analyseren en registreren van bedreigingen en kwetsbaarheden voor de digitale veiligheid van Vlaamse overheidsinstellingen en lokale besturen en ook het permanent informeren en ondersteunen van Vlaamse overheidsinstellingen en lokale besturen over deze bedreigingen en kwetsbaarheden, en hen daarbij ondersteunen;
- aanbieden van advies, ondersteuning en nazorg in geval van incidenten bij Vlaamse overheidsinstellingen en lokale besturen;
- optreden als gemandateerde gesprekspartner voor institutioneel overleg over digitale veiligheid, op lokaal, interfederaal, Europees en internationaal niveau;
- optreden als kenniscentrum rond digitale veiligheid, door kennis op te bouwen, wetenschappelijk onderzoek te ontsluiten, en opleidingen te organiseren.

Bij de uitoefening van deze opdrachten zal het VCDV op regelmatige tijdstippen overleggen met het stuurorgaan Vlaams Informatie en ICT-beleid, vermeld in artikel III.74 van het Bestuursdecreet. Dit stuurorgaan is de aangewezen partner om op

regelmatige tijdstippen met de verschillende belanghebbenden (de Vlaamse administratie, lokale overheden en externe overheden) de strategische lijnen op het vlak van de digitale veiligheid te bespreken zodat het flankerend beleid op een eenvormige en gecoördineerde manier vertaald wordt en de samenwerking en co-creatie verdergezet en bestendigd wordt.

Rekening houdend met de transversale aard van het digitale veiligheidsbeleid zal het in veel gevallen nodig zijn om praktische afspraken te maken met overheidsinstanties van alle niveaus. Gelet hierop voorziet artikel III.78/2, derde lid, 2° in een delegatie aan het VCDV om samenwerkingsovereenkomsten af te sluiten met lokale overheden, Vlaamse overheden, en instanties van externe overheden over de manier waarop het VCDV haar opdrachten uitvoert.

Artikel 5

Omdat het Vlaams Centrum voor Digitale Veiligheid zich in haar werking ook zal richten op lokale besturen wordt voorzien dat de strategische en beleidsmatige beslissingen voorafgaand besproken worden in een stuurgroep waarin ook het agentschap Binnenlands Bestuur vertegenwoordigd wordt vanuit haar taak om ondersteuning te bieden aan lokale en provinciale besturen.

De stuurgroep bestaat uit de hoofden van de agentschappen Digitaal Vlaanderen en Binnenlands Bestuur, de personen die binnen deze agentschappen belast zijn met de ICT-werking, het hoofd van het Vlaams Centrum voor Digitale Veiligheid en de persoon die binnen het agentschap Digitaal Vlaanderen instaat voor de NIS2-coördinatie. Op deze manier wordt gegarandeerd dat de juiste expertise aanwezig is om de strategische en beleidsmatige beslissingen voor te bereiden.

Wanneer de stuurgroep van het VCDV bijeenkomt over beslissingen die een rechtstreekse impact kunnen hebben op lokale besturen, kan deze stuurgroep in functie van de te bespreken agendapunten aangevuld worden met vertegenwoordigers van de lokale overheden. Deze vertegenwoordiging is analoog aan de vertegenwoordiging van lokale overheden in het stuurorgaan Vlaams Informatie- en ICT-beleid, vermeld in artikel III.74 van het Bestuursdecreet. Indien gewenst kan de Vlaamse Regering daarnaast in de toekomst de samenstelling van de stuurgroep verder uitbreiden, door extra leden toe te voegen, zonder daarbij de bestaande leden aan te tasten.

Om haar bij te staan bij de uitvoering van haar opdrachten kan het VCDV interne werkgroepen oprichten.

Artikel 6

Digitale veiligheid is een transversaal thema dat tal van maatschappelijke uitdagingen, sectoren en beleidsdomeinen raakt. Recente Europese en mondiale crisissen tonen aan dat een gefragmenteerde aanpak onvoldoende is om een duurzaam en weerbaar digitaal veiligheidsbeleid te voeren. Daarom voorziet het in te voegen artikel III.78/4 in een centrale coördinatierol voor het Vlaams Centrum voor Digitale Veiligheid, dat een geïntegreerd en coherent digitaal veiligheidsbeleid uitwerkt en afstemt tussen de verschillende beleidsdomeinen van de Vlaamse administratie. Het VCDV ontwikkelt daarbij een langetermijnvisie en faciliteert samenwerking over beleidsdomeinen en doelgroepen heen, waardoor regelgeving, kennisdeling en initiatieven beter op elkaar worden afgestemd. Zo wordt vanuit een coördinerende rol ingespeeld op uitdagingen rond onder meer cybersecurity, digitale vaardigheden, inclusiviteit, economische veiligheid en de weerbaarheid van

kritieke infrastructuur, met behoud van de eindverantwoordelijkheid bij elke entiteit.

Artikel 7

Om het Vlaamse digitale veiligheidsbeleid te concretiseren en te structureren voorziet het in te voegen artikel III.78/5 dat de Vlaamse Regering een beleidsstrategie digitale veiligheid goedkeurt, waarin de strategie en prioriteiten op het vlak van digitale veiligheid worden opgenomen. Deze beleidsstrategie zal de spil vormen waarrond het digitale veiligheidsbeleid binnen de Vlaamse overheidsinstellingen en lokale besturen georganiseerd wordt, en bevat:

- het strategische kader inzake digitale veiligheid, met inbegrip van de nagestreefde doelstellingen;
- de minimale verplichtingen op het vlak van digitale veiligheid die moeten worden geïmplementeerd door de Vlaamse overheidsinstellingen en lokale besturen;
- de richtlijnen en procedures voor toezicht, incidentmelding en afhandeling.

De Vlaamse beleidsstrategie digitale veiligheid wordt voorbereid door het Vlaams Centrum voor Digitale Veiligheid, en afgestemd met het stuurorgaan Vlaams Informatie en ICT-beleid. Op deze manier wordt terugkoppeling met de verschillende betrokken belanghebbenden (Vlaamse administratie, lokale overheden, etc.) verzekerd. Na goedkeuring door de Vlaamse Regering worden de afspraken uit de beleidsstrategie bindend voor de Vlaamse overheidsinstellingen en/of lokale besturen. Daarbij worden doelstellingen of minimale verplichtingen die specifiek zijn voor Vlaamse overheidsinstellingen zoveel als mogelijk vertaald naar het lokale overheidslandschap.

Binnen de krijtlijnen van de Vlaamse beleidsstrategie digitale veiligheid worden door het VCDV 'implementatierichtlijnen' opgesteld, die concrete instructies of maatregelen bevatten die de toepassing van de beleidsstrategie door Vlaamse overheidsinstellingen en lokale besturen verder uitwerken en faciliteren. Het gaat over expliciete, technische richtlijnen die deze instanties en besturen moeten toepassen binnen het digitale veiligheidsbeleid van hun organisatie. Ook deze implementatierichtlijnen worden immers bindend voor de Vlaamse overheidsinstellingen en/of lokale besturen (naar gelang het geval). Gelet op het technische karakter van deze implementatierichtlijnen, is het VCDV het best geplaatst om deze, op basis van hun expertise en kennis, uit te werken. Het gaat dan bijvoorbeeld over een verplichting om enkel ICT-producten en -diensten aan te kopen of te ontwikkelen die voldoen aan (door het VCDV te bepalen) veiligheidsvereisten, het gebruik van sterke wachtwoorden of een paswoord manager. Daarnaast kan het ook gaan over de verplichting voor overheidsinstellingen en/of lokale besturen om bepaalde veiligheidsbouwstenen te gebruiken, dan wel om uit te leggen waarom ze dit niet doen (zogenaamde 'comply or explain' verplichtingen). Tot slot is het ook mogelijk dat bepaalde implementatierichtlijnen zich beperken tot suggesties of aanbevelingen. Deze implementatierichtlijnen worden steeds afgestemd op het betrokken niveau. Daarbij worden de richtlijnen die van toepassing zijn op Vlaamse overheidsinstellingen zoveel als mogelijk vertaald naar de lokale besturen.

Artikel 8

Om te verzekeren dat de Vlaamse beleidsstrategie digitale veiligheid succesvol wordt geïmplementeerd binnen de betrokken Vlaamse overheidsinstellingen en lokale besturen voorziet het in te voegen artikel III.78/6 in een verplichte rapportering. Jaarlijks, uiterlijk voor 30 juni, moeten deze instanties en besturen aan het Vlaams Centrum voor Digitale Veiligheid een rapport bezorgen over hoe ze uitvoering geven aan de Vlaamse beleidsstrategie digitale veiligheid, met inbegrip van de goedgekeurde implementatierichtlijnen. Deze rapportering beperkt zich echter niet tot de Vlaamse beleidsstrategie, maar strekt zich ook uit tot de uitvoering die de instanties en besturen geven aan de NIS2-regelgeving. Door het opvolgen van de NIS-2 implementatie bij de Vlaamse overheidsinstellingen en lokale besturen krijgt het VCDV een zicht op de voortgang en digitale maturiteit van de gevatte entiteiten. Op deze manier beschikt het VCDV over de nodige informatie om de nood aan bijkomende ondersteuning te capteren, en om ook haar eigen beleid verder te ontwikkelen en te optimaliseren.

Deze rapportering bevat minstens:

- een beoordeling van bedreigingen in het kader van de digitale veiligheid, en de huidige stand van zaken;
- een beoordeling over het zekerheidsniveau dat behaald moet worden volgens de Vlaamse beleidsstrategie digitale veiligheid, of NIS2-wet en de uitvoeringsbesluiten ervan;
- een overzicht van geïmplementeerde beveiligingsmaatregelen en investeringen in digitale veiligheid;
- een overzicht en beknopte samenvatting van de incidenten en bijna-incidenten, van het voorbije jaar.

De definitie van bijna-incident (§1, derde lid) is daarbij gebaseerd op de definitie uit de NIS-2 wet. Het gaat om gebeurtenissen die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of die toegankelijk zijn via netwerk- en informatiesystemen, in gevaar hadden kunnen brengen, maar die met succes zijn voorkomen of zich niet hebben voorgedaan.

De rapportering moet in digitale vorm worden ingediend op basis van richtlijnen die het VCDV opstelt. Vandaag de dag is deze rapportage over het gevoerde digitale veiligheidsbeleid voor de Vlaamse overheidsinstellingen al gedeeltelijk opgelegd via de strategie Informatieveiligheid (VR 2021 1510 DOC.1151/1) met een mandaat aan het stuurorgaan en het agentschap Digitaal Vlaanderen om deze op te volgen. Voor de Vlaamse overheidsinstellingen vormt dit dus geen nieuwe verplichting, al zal een deel van de rapportage nu ook informatie omhelzen over verplichtingen die voortvloeien uit de NIS2-wet en bijhorende uitvoeringsbesluiten. Voor de lokale besturen sluit deze rapportering aan bij de jaarlijkse rapportering over het organisatie-beheersingssysteem, zoals deze voortvloeit uit het artikel 219 van het decreet Lokaal Bestuur (DLB) en artikel 96bis van het Provinciedecreet (DPB), en waarin digitale veiligheid ook een plaats heeft. Ook deze rapportering dient (uiterlijk) op 30 juni van het daaropvolgende jaar te gebeuren. Door aan te sluiten bij bestaande rapporteringen, en door te voorzien in eenvoudige sjablonen of semiautomatische rapportering via digitale vormen, wordt de rapporteringslast zoveel als mogelijk beperkt. De documenten die entiteiten in het kader van de regelmatige conformiteitsbeoordeling in het kader van de NIS2-regelgeving bezorgen aan het CCB zullen ook kunnen gebruikt worden in het kader van het toezicht door het VCDV. Hierover zal een samenwerkingsovereenkomst gesloten worden met het CCB. Het VCDV zal er daarnaast maximaal op toezien dat de rapportering geen bijkomende planlast veroorzaakt.

De rapportering vormt een belangrijke manier voor het VCDV om toezicht uit te oefenen op de naleving door de Vlaamse overheidsinstellingen en de lokale besturen van de vereisten inzake digitale veiligheid zoals deze voortvloeien uit de Vlaamse beleidsstrategie digitale veiligheid en de NIS-2 regelgeving, en de effectiviteit van de ingerichte maatregelen. Op deze manier kan het VCDV het Vlaams digitaal veiligheidsbeleid en de beleidsondersteuning verder optimaliseren en waar nodig bijsturen. Wanneer het VCDV zou vaststellen dat bijkomende informatie nodig is om haar toezicht uit te oefenen, dan voorziet paragraaf 2, tweede lid, in de mogelijkheid om bijkomende informatie op te vragen bij de betrokken Vlaamse overheidsinstelling of lokale bestuur. Het kan daarbij gaan van een eenvoudig verzoek tot het bezorgen van aanvullende documentatie, het vragen van een nadere toelichting van al eerder overgemaakte informatie, tot een plaatsbezoek bij de betrokken Vlaamse overheidsinstelling of het lokale bestuur. In deze gevallen krijgt het VCDV toegang tot alle informatie en documenten die noodzakelijk zijn om tot een volledige rapportering te komen.

De rapporteringen worden door het VCDV geaggregeerd en geanonimiseerd, en bezorgd aan het Stuurorgaan Vlaams Informatie- en ICT-beleid, het Auditcomité van de lokale besturen, het Auditcomité van de Vlaamse administratie en Audit Vlaanderen.

Paragraaf vier van het in te voegen artikel III.78/6 voorziet tot slot dat als het VCDV vaststelt dat een Vlaamse overheidsinstelling of lokaal bestuur ernstige tekortkomingen vertoont met betrekking tot de naleving van de Vlaamse beleidsstrategie digitale veiligheid, of de NIS2-wet en de uitvoeringsbesluiten ervan, het daarvan melding kan maken bij Audit Vlaanderen. Op basis van deze melding kan Audit Vlaanderen nagaan of het nodig is om een bijkomende audit uit te voeren. Dit artikel doet geen afbreuk aan meldingsverplichtingen, of -mogelijkheden die bestaan op grond van andere regelgeving.

Belangrijk bij deze rapportering is dat de overgemaakte informatie en documentatie vertrouwelijk wordt behandeld. Met toepassing van de uitzonderingsgronden in titel 2, hoofdstuk 3 van het Bestuursdecreet kunnen de bestuursdocumenten die worden uitgewisseld in het kader van dit artikel, met uitzondering van het rapport vermeld in paragraaf 3, dan ook niet openbaar gemaakt worden, gelet op de impact op de openbare orde en de veiligheid.

De Vlaamse regering kan de regeling rond de rapportering, de vraag tot bijkomende informatie, en de melding bij Audit Vlaanderen, nader bepalen. Zij kan daarbij zowel de procedure als de inhoud verder uitwerken, zonder daarbij nieuwe elementen toe te voegen of nieuwe kernvoorwaarden te creëren.

Artikel 9

Naast de jaarlijkse rapportering aan het Vlaams Centrum voor Digitale Veiligheid, ingevoegd bij artikel 8, voorziet het nieuwe artikel III. 78/7 in een driejaarlijkse externe conformiteitsbeoordeling. Het doel van deze conformiteitsbeoordeling is om vast te stellen of de betrokken Vlaamse overheidsinstelling, of lokale bestuur het vereiste zekerheidsniveau (opgelegd door de NIS2-wet en de uitvoeringsbesluiten ervan, dan wel door de Vlaamse beleidsstrategie digitale veiligheid) behaalt. De beveiligingsketen is namelijk slechts zo sterk als haar zwakste schakel. Entiteiten die gedeeltelijk, afwijkend of niet geïntegreerd zijn met de centrale dienstverlening inzake digitale veiligheid vanuit Digitaal Vlaanderen staan zelf in voor het realiseren van een veilige digitale en fysieke werkomgeving. Om erop toe te zien dat deze entiteiten een gelijkwaardig veiligheidsniveau als de dienstverlening van Digitaal Vlaanderen bereiken, is een onafhankelijke, externe beoordeling noodzakelijk. Op die manier wordt ervoor gezorgd dat de beveiliging op het niveau van de Vlaamse overheid consistent is. Digitaal Vlaanderen is als

aanbieder van ICT-infrastructuur en – dienstverlener gehouden om het hoogste zekerheidsniveau te voorzien. Om deze garantie waar te maken moeten ook de dienstenafnemers en toeleveranciers in de keten ervoor zorgen dat de nodige maatregelen geïmplementeerd worden. Deze externe conformiteitsbeoordeling garandeert dat de schakels voldoende stevig zijn om de digitale veiligheid in het specifiek ecosysteem te garanderen. In de NIS2-wet en de uitvoeringsbesluiten ervan wordt ook verwezen naar het belang van maatregelen rond weerbaarheid en de afhankelijkheden tussen geconnecteerde systemen.

Deze conformiteitsbeoordeling is gelijkaardig aan de conformiteitsbeoordeling die voorzien is op grond van artikel 39 en 41 van de NIS2-wet. Artikel 39 van deze wet voorziet dat 'essentiële' entiteiten zich moeten onderwerpen aan een regelmatige conformiteitsbeoordeling van de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's. Artikel 41 van dezelfde wet voorziet dat 'belangrijke' entiteiten zich vrijwillig kunnen onderwerpen aan eenzelfde regelmatige conformiteitsbeoordeling. Om te vermijden dat Vlaamse overheidsinstellingen, of lokale besturen, die onder de NIS2-wet vallen verplicht zouden worden om meerdere conformiteitsbeoordelingen te laten uitvoeren bepaalt het tweede lid dat artikel III.78/7, §1., eerste lid niet van toepassing is op Vlaamse overheidsinstellingen en lokale besturen die al onderworpen zijn aan een – verplichte dan wel vrijwillige - regelmatige conformiteitsbeoordeling op grond van artikel 39 of 41 van de NIS2-wet. Voor deze instanties is het voldoende dat zij de resultaten van deze regelmatige conformiteitsbeoordeling toevoegen aan de jaarlijkse rapportering vermeld in artikel III.78/6.

Artikel III.78/7 moet op die manier gezien worden als een noodzakelijke aanvulling op de NIS2-wet en de uitvoeringsbesluiten ervan, die garandeert dat alle Vlaamse overheidsinstellingen en lokale besturen minstens driejaarlijks hun stappen inzake digitale veiligheid extern laten verifiëren. Deze conformiteitsbeoordeling dient te gebeuren door een erkende conformiteitsbeoordelingsinstantie. Dit zijn in de eerste plaats de conformiteitsbeoordelingsinstanties die zijn aangeduid op basis van een door het VCDV voorgestelde raamovereenkomst. Gelet op de overeenstemming tussen de uit dit artikel voortvloeiende conformiteitsbeoordeling en de regelmatige conformiteitsbeoordeling op grond van de NIS2-wet en de uitvoeringsbesluiten ervan voorziet dit ontwerp van decreet dat de beoordeling ook kan gebeuren door een conformiteitsbeoordelingsinstantie die erkend is overeenkomstig artikel 40 van de NIS2-wet.

Gelet op de inwerkingtreding van dit decreet op 1 januari 2027 zal een eerste conformiteitsbeoordeling moeten worden uitgevoerd tegen uiterlijk 31 december 2029.

Artikel 10

Het Vlaams Centrum voor Digitale Veiligheid zal ook een belangrijke rol spelen in de ondersteuning van Vlaamse overheidsinstellingen en lokale besturen wanneer digitale veiligheidsincidenten zich voordoen.

Paragraaf 1 van het in te voegen artikel III.78/8 voorziet daarbij een gelaagde ondersteuning vanuit het VCDV. De ondersteuning door het VCDV is breed, van adviesverlening via de telefoon tot assistentie ter plaatse. Het doel is om de organisaties te helpen de situatie snel en efficiënt onder controle te krijgen. Bijkomend deelt VCDV verkregen nuttige informatie rond incidenten en kwetsbaarheden gericht met andere cyberveiligheidsautoriteiten.
In het kader van deze ondersteuning voorziet het VCDV minstens in:
1° coördinatie bij significante incidenten. De coördinatie door het VCDV omvat zowel begeleiding en assistentie met het sporenonderzoek en technische adviezen

als strategische opvolging. Het VCDV werkt nauw samen met het CCB, VTC en het CCVO en helpt de organisatie met de wettelijke verplichtingen.
2° ondersteuning bij het onderzoeken van significante incidenten om de oorzaak te bepalen. Het VCDV biedt daarbij hulp aan zoals bijstand bij de analyse van logs of (mogelijke) malware.
3° advisering over technische acties om risico op of impact van incidenten te mitigeren;
4° communicatie en samenwerking met de belangrijkste partners en belanghebbenden bij grotere significante incidenten of crisissituaties zoals het CCB en het CCVO. Deze uitwisseling van informatie en samenwerking past binnen een nationaal kader, zoals het nationale cybernoodplan. Afspraken hieromtrent worden vastgelegd in samenwerkingsovereenkomsten zoals bepaald in artikel III.78/2.;
5° ondersteuning bij het maken van verplichte meldingen over het significante incident;
6° gericht delen van urgente dreigingsinformatie en kwetsbaarheden naar de relevante Vlaamse overheidsinstellingen en lokale besturen. Dit past eveneens in de radarfunctie die het VCDV vervult om informatie te centraliseren en gericht er rond te informeren om incidenten zoveel als mogelijk te voorkomen (cfr infra).

Om te zorgen dat het VCDV steeds op de hoogte is van de meest recente digitale veiligheidsincidenten en om te vermijden dat een incident zich uitbreidt wanneer het zich voordoet, voorziet paragraaf 2 van hetzelfde artikel een meldingsplicht voor Vlaamse overheidsinstellingen en lokale besturen om binnen de 24 uur alle significante incidenten te melden waarvan zij het slachtoffer zijn. Cyberaanvallen op overheden staan immers zelden op zichzelf. Vaak wijst een eerste aanval erop dat vergelijkbare kwetsbaarheden in de systemen van andere overheden eveneens zullen worden uitgebuit. Deze meldingsplicht bestaat parallel aan, en onafhankelijk van, andere meldingsplichten zoals deze voortvloeien uit andere regelgeving (vb. de NIS2-wet). Zo zijn entiteiten die onder de NIS2 vallen verplicht om ook melding van een incident te doen via https://notif.safeonweb.be. Het VCDV zal de entiteiten ondersteunen bij het bezorgen van deze verplichte melding. Om te zorgen voor een gestroomlijnde aanpak bij grootschalige digitale veiligheidsincidenten worden er door het VCDV afspraken gemaakt met andere entiteiten die ondersteuning en nazorg bieden bij grootschalige incidenten, zoals het CCB, het CCVO en het Nationaal Crisiscentrum. Deze afspraken hebben betrekking op o.a. taak- en rollenverdeling en de doorstroom van informatie tussen entiteiten.

De definitie van 'significant incident' is daarbij gebaseerd op de definitie uit de NIS2-wet en omvat elk incident dat significante gevolgen heeft voor de verlening van een van de diensten van een entiteit, en een ernstige operationele verstoring van de diensten van een entiteit of financiële verliezen voor een entiteit heeft veroorzaakt, of kan veroorzaken, of andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Ook informatie die in het kader van deze ondersteuning uitgewisseld wordt tussen de betrokken entiteiten en het VCDV moet als vertrouwelijk beschouwd worden, en kan met toepassing titel 2, hoofdstuk 3 van het niet openbaar gemaakt worden wanneer dit een impact zou hebben op de openbare orde en de veiligheid.

Artikel 11

Via het in te voegen artikel III.78/9 worden de Vlaamse overheidsinstellingen en lokale besturen verplicht om een functionaris voor digitale veiligheid aan te stellen. In de praktijk gaat het over het aanstellen van een ISO (Information Security Officer) of een CISO (Chief Information Security Officer). De aanstelling van een ISO/CISO binnen de entiteiten van de Vlaamse overheid werd reeds in 2024 verplicht gesteld door het stuurorgaan (zitting van 17 april 2024). Via dit decreet wordt deze verplichting decretaal verankerd en uitgebreid naar alle

overheidsinstanties die binnen het toepassingsgebied van de Vlaamse beleidsstrategie digitale veiligheid en het Vlaamse Centrum Digitale Veiligheid vallen.

De uitdagingen waarmee de Vlaamse overheid en lokale besturen geconfronteerd worden op het gebied van digitale veiligheid worden steeds groter. Gelet op de conformering van overheidsinstanties aan hun toepasselijk NIS-2 zekerheidsniveau en het Vlaams digitaal veiligheidsbeleid is een aanwijzing van een ISO/CISO om de organisatie op het vlak van digitale veiligheid te ondersteunen onontbeerlijk. De referentiekaders ISO27001 en CyFun® belangrijk en essentieel impliceren de rol van (C)ISO.

De term (C)ISO staat voor '(Chief) Information Security Officer' en is een gebruikelijke en goed gekende rol in de wereld van de digitale veiligheid. De (C)ISO beweegt zich op strategisch en tactisch niveau. Dit veronderstelt een door het management gedocumenteerd en goedgekeurd informatieveiligheidsbeleid, inclusief de beschrijving van de rollen en verantwoordelijkheden en het nodige mandaat om de (C)ISO-rol te kunnen invullen. Naast een adviserende rol is de (C)ISO verantwoordelijk voor beleidsvorming en beleidstoezicht in het kader van informatieveiligheid. De (C)ISO geeft advies en helpt bij de vertaling en implementatie van NIS2, ISO 27001, CyFun® en andere raamwerken en normen. De aanduiding van een ISO/CISO gebeurt steeds door de desbetreffende overheidsinstantie en kan door het aanduiden van een personeelslid dat reeds in dienst is, een aanwerving of door een externe medewerker. Eén persoon kan ook voor meerdere overheidsinstanties de rol van ISO/CISO uitvoeren voor zover er geen belangenconflicten optreden. (Chief) Information Security Officer is de referentie die gehanteerd wordt naar het in te vullen takenpakket, maar de overheidsinstanties hebben de vrijheid om zelf de titelvoering te kiezen. (C)ISO moet minimaal als rol ingevuld worden, maar een instantie kan de rol als functie definiëren. Dat geeft de instanties meer mogelijkheden om het bijhorende takenpakket in te vullen volgens de noden en mogelijkheden van hun organisatie.

Conform de algemene verordening gegevensbescherming en het e-govdecreet zijn Vlaamse overheden en lokale besturen verplicht om een functionaris voor gegevensbescherming aan te stellen. Net zoals gegevensbescherming vormt digitale veiligheid een cruciaal thema binnen de Vlaamse overheid en de lokale besturen. Via de decretale verplichting van een (C)ISO leggen we de lat voor digitale veiligheid op dit vlak gelijk met de functionarisvereiste voor gegevensbescherming.

In het kader van haar toezichtrol zal het VCDV opvolgen of een ISO/CISO is aangesteld.

Artikel 12

Het in te voegen artikel III.78/10 voorziet in een aantal maatregelen die het Vlaams Centrum voor Digitale Veiligheid kan nemen wanneer een Vlaamse overheidsinstelling of lokaal bestuur niet voldoet aan de rapporteringsverplichting, vermeld in artikel III.78/6, of de verplichting tot het uitvoeren van een driejaarlijkse conformiteitsbeoordeling, vermeld in artikel III.78/7, of wanneer een Vlaamse overheidsinstelling of een lokaal bestuur tekortkomingen vertoont bij de naleving van de Vlaamse beleidsstrategie digitale veiligheid of de implementatierichtlijnen vermeld in artikel III.78/5, §1 en 3, of de NIS2-wet en de uitvoeringsbesluiten ervan.

In eerste instantie zal het VCDV in dergelijke gevallen in dialoog treden met de Vlaamse overheidsinstelling of het lokale bestuur in kwestie. Het doel van deze dialoog is om, in samenspraak en met ondersteuning van het VCDV, te komen tot

een gedegen oplossing van de tekortkoming. Indien de Vlaamse overheidsinstelling of het lokale bestuur, ondanks de vraag tot dialoog, nalaat om de tekortkoming te remediëren kan het VCDV een formele ingebrekestelling versturen.

Als ook na deze formele ingebrekestelling de tekortkoming blijft voortbestaan zal het VCDV aan de Vlaamse overheidsinstelling of het lokale bestuur in kwestie een administratieve sanctie kunnen opleggen. Deze administratieve sanctie beoogt een preventief effect te hebben, met name de Vlaamse overheidsinstellingen en lokale besturen er maximaal toe aan te zetten om de verplichtingen die op haar rusten tijdig en correct uit te voeren. Vanuit dit perspectief meent de decreetgever dat deze administratieve sanctie dan ook geen strafrechtelijk karakter heeft.

Het vierde lid van het in te voegen artikel III.78/10, §1., bepaalt dat tegen de beslissing tot het opleggen van een administratieve sanctie beroep kan worden ingesteld bij de Vlaamse regering. Gelet op de rol die deze reeds opneemt als toezichthoudende overheid t.a.v. de lokale besturen, zal dit beroep in de praktijk behandeld worden door de Vlaamse minister, bevoegd voor het binnenlands bestuur. Voor de Vlaamse overheidsinstellingen zal het beroep worden behandeld door de Vlaamse minister, bevoegd voor bestuurszaken.

Via het vijfde lid van deze eerste paragraaf wordt de Vlaamse Regering gemachtigd om het kader voor deze sanctie verder uit te werken, met inbegrip van de aard van de sanctie, de manier waarop de overtreding wordt vastgesteld, en de procedure voor het opleggen en uitvoeren ervan.

Paragraaf 2 voorziet daarnaast in een bijkomende maatregel om de digitale veiligheid van het centrale netwerk van de Vlaamse overheid te beschermen. Zoals hierboven aangehaald is de beveiligingsketen namelijk slechts zo sterk als haar zwakste schakel. Wanneer entiteiten (Vlaamse overheidsinstellingen of lokale besturen) die geheel of gedeeltelijk geïntegreerd zijn met de centrale ICT-dienstverlening van Digitaal Vlaanderen, nalaten om de nodige maatregelen te nemen om hun digitale veiligheid te verzekeren dan brengen zij niet enkel zichzelf, maar het hele netwerk en de andere daarop aangesloten entiteiten in gevaar.

Om te verzekeren dat de tekortkomingen bij één entiteit de digitale veiligheid van andere entiteiten niet in gevaar brengt, voorziet artikel III.78/10, §2, dat het agentschap Digitaal Vlaanderen op voorstel van het Vlaams Centrum voor Digitale Veiligheid in gevallen van ernstige tekortkomingen in het digitale veiligheidsbeleid van een Vlaamse overheidsinstellingen of lokale bestuur, de betrokken entiteit geheel of gedeeltelijk kan laten afsluiten van de centrale ICT-dienstverlening vanuit Digitaal Vlaanderen. Het gaat dan bijvoorbeeld over het niet of onvoldoende nemen van acties om onveiligheden in systemen te voorkomen, kwetsbaarheden te detecteren en om de gevolgen daarvan te beperken, op een behoorlijke en afdoende wijze gevolg geven aan incidenten, etc. Het betreft een uitzonderlijke maatregel die uitsluitend wordt toegepast als ultieme beschermingsmiddel, en steeds wordt toegepast in relatie tot de grootte van de potentiële bedreiging voor andere entiteiten binnen het netwerk. Deze mogelijkheid doet geen afbreuk aan de dialoog die moet plaatsvinden conform paragraaf 1.

Ook hier geldt dat informatie die in het kader van deze procedure tussen de betrokken entiteiten en het VCDV uitgewisseld wordt, als vertrouwelijk moet worden beschouwd, en met toepassing van titel 2, hoofdstuk 3 van het Bestuursdecreet niet openbaar gemaakt kan worden wanneer dit een impact zou hebben op de openbare orde en de veiligheid.

Artikel 13

De inwerkingtreding van het nieuwe kader inzake digitale veiligheid bij de Vlaamse overheidsinstellingen en lokale besturen is vastgesteld op 1 januari 2027. Er wordt gekozen voor een heldere datum vanaf wanneer de verplichtingen uit de nieuwe afdeling 4/1 verplichtend worden. Het betreft regels van interne werking waarbij de overheid zelf de voornaamste belanghebbende is, waardoor er geen nood is om te wachten op een eventuele publicatie in het Belgisch staatsblad.

De minister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie en Industrie, Buitenlandse Zaken, Digitalisering en Facilitair Management,

Matthias DIEPENDAELE

De Vlaamse minister van Binnenland, Steden- en Plattelandsbeleid, Samenleven, Integratie en Inburgering, Bestuurszaken, Sociale Economie en Zeevisserij,

Hilde CREVITS