vergadering **C71**
zittingsjaar 2021-2022

Woordelijk Verslag

# Commissievergadering

## Commissie voor Algemeen Beleid, Financiën, Begroting en Justitie

van 23 november 2021

*(Wegens de coronamaatregelen werd deze vergadering via videoconferentie georganiseerd.)*

Vlaams Parlement

INHOUD

VRAAG OM UITLEG van Peter Van Rompuy aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over de verkoop van drieduizend Belgische zendmasten door Telenet
– 339 (2021-2022) 3

VRAAG OM UITLEG van Jeremie Vaneeckhout aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over dataveiligheid bij het gebruik van de CovidSafeBE-app
– 563 (2021-2022) 4

VRAAG OM UITLEG van Stijn De Roo aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over de versterking van de digitale weerbaarheid van de Vlaamse overheid
– 569 (2021-2022) 8

**VRAAG OM UITLEG van Peter Van Rompuy aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over de verkoop van drieduizend Belgische zendmasten door Telenet**
**– 339 (2021-2022)**

**Voorzitter: de heer Steven Vandeput**

**De voorzitter**: De heer Van Rompuy heeft het woord.

**Peter Van Rompuy (CD&V)**: Minister-president, op 13 oktober heeft Liberty Global, de groep boven Telenet, bekendgemaakt dat het drieduizend zendmasten van Telenet te koop wil aanbieden op de markt, al dan niet aan de hoogste bieder. Het zou gaan over een pakket van 500 à 600 miljoen euro. Dat is ook in het buitenland al op een aantal plaatsen gebeurd. Mijn vragen aan u zijn eigenlijk relatief kort. Beschouwt u dit als kritische infrastructuur voor de Vlaamse economie? Hoe ziet u dat in relatie tot het screeningsmechanisme waarop we nog altijd wachten, om na te gaan of zendmasten zoals deze zouden worden verkocht aan bijvoorbeeld een Chinese staatsmaatschappij?

**De voorzitter**: Minister-president Jambon heeft het woord.

**Minister-president Jan Jambon**: Mijnheer Van Rompuy, een befaamd, u niet helemaal onbekend politicus zei dat we problemen pas moeten oplossen als ze rijzen. Bij mijn weten is er op dit ogenblik nog geen aanwijzing dat de infrastructuur in handen zou komen van landen of bedrijven die onze belangen zouden schaden. Telenet is gestart met een strategische oefening rond de telecommunicatiezendmastactiviteit. Het afstoten van zendmasten is een beweging die we in de bredere Europese telecommarkt zien, zoals u zelf in uw vraagstelling ook al aangaf. Op dit ogenblik werd er nog geen enkele beslissing genomen omtrent een eventuele transactie, in de vorm van een verkoop of iets anders, noch over de eventuele omvang daarvan.

Wat het delen van infrastructuur betreft, zijn er duidelijke federale regels waaraan eigenaars van zendmasten zich moeten houden, onder meer dat bepalingen voor gedeeld gebruik redelijk, proportioneel en niet-discriminerend moeten zijn. Ik wil er bovendien ook de aandacht op vestigen dat, zelfs als Telenet zou beslissen tot een verkoop, de mogelijkheid bestaat dat het enkel de masten verkoopt en niet de antennes, dus wat men in het jargon de passieve onderdelen noemt, veeleer dan de actieve onderdelen die de antennes zijn. Het potentieel strategisch risico is natuurlijk ook daarvan afhankelijk.

Over het screeningsmechanisme voor buitenlandse investeringen zijn de onderhandelingen nog bezig, dus dat laat ik even buiten beschouwing. Ik moet echter wel zeggen dat die de goede richting uitgaan, dat we aan een samenwerkingsakkoord tussen de deelstaten en de federale overheid aan het werken zijn. We hebben er tot nu toe vooral over gewaakt dat eventuele investeringen in een bepaald gewest niet door een ander gewest kunnen worden geblokkeerd, maar bij wijze van spreken enkel door de federale overheid indien er veiligheidsbedreigingen zijn. Maar goed, dat is eigenlijk buiten het perspectief van deze vraag. Ik ben het met u eens dat het screeningsmechanisme te lang op zich laat wachten. We hebben recent echter wel een aantal aanzienlijke stappen vooruit kunnen zetten.

Vergeet ook niet dat er het aanbod is van de Vlaamse Regering om een tower company op te richten met de telecomoperatoren, iets wat ook relevant is in dit kader. Dat behoort dan echter weer tot de bevoegdheden van minister Crevits.

Samengevat: ik begrijp uw bezorgdheid, maar er zijn op dit ogenblik nog geen aanwijzingen dat de infrastructuur van Telenet in verkeerde handen dreigt te vallen. We blijven dat dossier echter natuurlijk van zeer nabij volgen.

**De voorzitter**: De heer Van Rompuy heeft het woord.

**Peter Van Rompuy (CD&V)**: Een bekend staatsman heeft ooit gezegd: "Gouverner, c'est prévoir." Ik denk trouwens dat u hem in het verleden ook al hebt geciteerd. Eigenlijk is mijn belangrijkste punt het laatste, namelijk dat ik denk dat het tijd is om te landen met heel dat systeem van het screeningsmechanisme. Dossiers zoals dit tonen immers aan dat het wel degelijk nodig kan zijn. Ik dank u voor uw antwoord.

**De voorzitter**: De heer Vande Reyde heeft het woord.

**Maurits Vande Reyde (Open Vld)**: Minister-president, u hebt terecht aangehaald dat de Vlaamse overheid ook werk maakt van de 5G tower company. Voor de collega's die daar misschien nog niet van gehoord hebben: de bedoeling daarvan zou zijn om een aantal infrastructuurelementen, zoals bijvoorbeeld de zendmast, maar misschien ook andere netwerkelementen gezamenlijk te beheren, zodat operatoren daar ook gezamenlijk gebruik van kunnen maken. Ik heb daarover een vraag lopende. Die zal volgende week beantwoord worden door minister Crevits in de commissie Economie. Collega's die interesse hebben mogen daar zeker bij aansluiten.

Ik heb een vraag, minister-president, maar als u daar niet meteen op kan antwoorden: geen probleem. Morgen zal de 5G-veiling hopelijk beslist zijn. Zal het bredere doel van de Vlaamse Regering op het vlak van telecommunicatie uiteindelijk zijn om een soort van openaccessmodel te maken, waarbij je de infrastructuur gemeenschappelijk maakt voor operatoren, waardoor dat ook qua ruimtelijke ordening meer kan gebundeld worden? Is dat het uiteindelijke doel waar we naartoe willen? Is het misschien nuttig om daarover een soort conceptnota of een strategische visienota te maken, waarin dat duidelijk wordt omschreven? Er zijn twee elementen: er is open access, zowel op de mobiele markt alsook op de markt van het vaste internet, waar Fluvius dat nu bijvoorbeeld in samenwerking met Telenet aan het ontwikkelen is. Mijn suggestie is om de visie daarover misschien te bundelen in een soort van bredere visienota.

**De voorzitter**: Minister-president Jambon heeft het woord.

**Minister-president Jan Jambon**: Dat is een goede suggestie, mijnheer Vande Reyde, maar ik denk dat er in het landschap natuurlijk al veel gebeurd is. Mocht je van een wit blad kunnen vertrekken, dan zou ik zeggen – en u weet dat ik geen grote believer in overheidsbedrijven ben –: laat ons het netwerk zelf door de overheid doen, zoals we dat ook met andere nutsvoorzieningen doen. Dan konden natuurlijk alle privéspelers, en ook de overheid, van dat netwerk gebruik maken. Mochten we van een wit blad vertrekken, dan zou dat inderdaad beter zijn. Maar we vertrekken niet van een wit blad. Er zijn al veel verdelingen gebeurd. Ik weet dat collega Muyters in zijn vorige functie ook veel geprobeerd heeft om daarin iets te bereiken, ook met dezelfde filosofie. Maar de suggestie die u doet, is een goede suggestie. We zullen daarop werken.

**De voorzitter**: De vraag om uitleg is afgehandeld.

**VRAAG OM UITLEG van Jeremie Vaneeckhout aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over dataveiligheid bij het gebruik van de CovidSafeBE-app**
**– 563 (2021-2022)**

**Voorzitter: de heer Steven Vandeput**

**De voorzitter**: De heer Vaneeckhout heeft het woord.

**Jeremie Vaneeckhout (Groen)**: Minister, ik heb een vraag rond de app CovidSafeBE. Dat is een app, ondertussen bij velen van ons bekend, die door onder andere horeca-uitbaters en evenementorganisatoren wordt gebruikt om te controleren of bezoekers covidsafe zijn. De app kent twee gebruiksmodi: één voor horeca en events, die simpelweg resulteert in een groen of rood scherm, en één voor politie- en douanecontroles, die meer gegevens zichtbaar maakt. Switchen tussen de twee modi is gemakkelijk. Met één druk op de knop kan de cafébaas zo bijvoorbeeld het rijksregisternummer van zijn gasten zien en nagaan of ze gevaccineerd dan wel hersteld of negatief getest zijn. Dat is toch wel gevoelige informatie. Ik denk dat we het allemaal eens zijn dat het belangrijk is, zeker op dit ogenblik, dat er een absoluut vertrouwen is in de zaken die de overheid aanreikt om de covidcrisis te beheersen.

Digitaal Vlaanderen, dat de app ontwikkelde en beheert, erkent het probleem. Het beklemtoont dat het onrechtmatig overschakelen naar de politiefunctie strafbaar is. Ik denk dat het belangrijk is om dat te beklemtonen. Er wordt niet overwogen om de twee verschillende functies onder te brengen in twee afzonderlijke apps, of om daar een veiliger onderscheid tussen te voorzien. Wel zou er een update komen waarbij er een meldingsgeluidje zou gekoppeld worden aan de horeca- en evenementenversie. Zo zou de bezoeker kunnen horen dat de juiste versie wordt gebruikt.

Ik heb een paar vragen hierbij, minister-president.

Erkent u dat de app gevoelig is voor misbruik door de dubbele functie?

Acht u gevoelige informatie zoals het rijksregisternummer en dus de geboortedatum en medische gegevens voldoende beschermd bij gebruik van de CovidSafeapp?

Kan eventueel misbruik van de scanapp voldoende gemakkelijk vastgesteld worden? Hoe wordt hierop gecontroleerd?

Waarom wordt er toch niet geopteerd voor een aparte of strikter gescheiden politieversie van de app?

Hebt u weet van klachten over misbruik of van procedures bij de privacyinstanties?

**De voorzitter**: Minister-president Jambon heeft het woord.

**Minister-president Jan Jambon**: Dank u wel, mijnheer Vaneeckhout, voor deze vragen. Ik ga er redelijk uitgebreid op antwoorden, want ik denk wel dat het belangrijk is voor het vertrouwen in de systemen die wij aanreiken.

Erken ik dat de app gevoelig is voor misbruik? Overeenkomstig het samenwerkingsakkoord tussen de federale staat en de verschillende deelstaten van 14 juli 2021 heeft het agentschap Digitaal Vlaanderen de CovidScan-app ontwikkeld, overeenkomstig de instructies van het federale eHealthplatform, dit ter uitvoering van wat beslist werd in de EU-verordening en de verschillende samenwerkingsakkoorden. Dat is het kader.

Ik erken wel dat de CovidScanapp mogelijk verkeerdelijk gebruikt kan worden door de dubbele functie. Er zijn echter reeds bijkomende waarschuwingen aan de bestaande app toegevoegd om aan de aanbieder van een covidcertificaat meteen duidelijk te maken in welke modus de app gebruikt wordt, zodat hij, wanneer nodig, de controleur kan aanspreken over het verkeerde gebruik.

Ik bespreek de reeds toegevoegde maatregelen. De CovidScan-app kan in twee verschillende modi gebruikt worden. De modus ‘evenement’ laat enkel toe na te gaan of de persoon die zijn of haar Covid Safe Ticket (CST) aanbiedt, een geldig vaccinatiebewijs heeft, hersteld is van een covidbesmetting of een recente negatieve covidtest heeft afgelegd en toont enkel de naam van de persoon. De modus ‘inkomende reiziger’

voert dezelfde controle uit, maar toont ook nog bijkomende informatie om te kunnen controleren of er aan de covidinreisverplichtingen voldaan wordt. Deze modus mag enkel door medewerkers op de luchthaven of door politiediensten gebruikt worden.

Deze twee modi worden nu in één en dezelfde scanapp ondersteund, maar zullen in de toekomst gescheiden worden en uitgevoerd worden in twee aparte scanapps. Om het verschil tussen beide modi duidelijk zichtbaar te maken, wordt er nu al een permanent zichtbaar kleurverschil getoond bij het scannen in deze verschillende modi: een blauwe balk bij de modus 'evenement', voor het CST, en een rode balk bij de modus 'inkomende reiziger'. Ik geef toe dat de echte oplossing de scheiding van die twee applicaties zal zijn. De CovidScanapp werd aangepast zodat bij het scannen een blauwe balk op het scherm de aanbieder van het covidcertificaat de zekerheid geeft dat de app in de modus 'evenement' staat. Is er een rode balk zichtbaar op het scherm, dan ziet de aanbieder meteen dat de CovidScanapp in de verkeerde modus 'Inkomende reiziger' staat, tenzij het wel degelijk om een scan op de luchthaven of door politiediensten gaat. Hij kan de persoon die de controle uitvoert, er dan meteen op wijzen dat deze de CovidScanapp op een illegale wijze gebruikt.

Enkel bij het scannen in de modus 'evenement' wordt een biepgeluid afgespeeld. Indien dit geluid niet hoorbaar is, kan de aanbieder ook hierdoor de persoon die de controle uitvoert, erop wijzen dat deze de CovidScanapp op een illegale wijze gebruikt. Bij de opstart van de CovidScanapp zal de app steeds in de modus 'evenement' starten zodat de persoon die de controle uitvoert niet per vergissing in de foutieve modus begint te scannen. De defaultinstelling is dus 'Evenement'.

Om alvast onmiddellijk te voorkomen dat een persoon die enkel het Covid Safe Ticket mag bekijken, nog opzettelijk of per ongeluk de verkeerde scanningsmodus zou gebruiken en daardoor onrechtmatig de volledige inhoud van het certificaat zou kunnen zien, is reeds in de nieuwe release in de modus 'inkomende reiziger' de mogelijkheid weggenomen om de details van het certificaat te bekijken. Zo is het niet langer mogelijk om het rijksregisternummer te bekijken. Ook zijn er andere beperkingen ingevoerd om te voorkomen dat de zichtbare gegevens van gescande covidcertificaten worden bewaard. Zo is het op Android niet mogelijk om screenshots van het scherm van de CovidScanapp te maken en zo gegevens bij te houden. Maar op iOS kun je dat als ontwikkelaar momenteel niet verbieden.

Er zijn nog maatregelen gepland. De bestaande CovidScanapp zal binnenkort volledig gesplitst worden. Met andere woorden, er komen twee verschillende scanapps ter beschikking: de huidige CovidScanBE-app, die dan enkel het Covid Safe Ticket zal scannen, de modus 'evenement', en een aparte app voor het scannen van de certificaten als een persoon vanuit het buitenland naar België komt, de modus 'inkomende reiziger'. Deze app mag enkel gebruikt worden door daartoe bevoegde personen. De ontwikkeling van deze twee apps is volop lopende.

Doordat er twee verschillende apps komen, zal binnen de bestaande CovidScanapp dus niet langer meer de mogelijkheid bestaan te switchen naar de modus 'inkomende reiziger'.

Dan vroeg u of ik gevoelige informatie zoals het rijksregisternummer, en dus de geboortedatum en medische gegevens, voldoende beschermd acht. Ik wil erop wijzen dat het rijksregisternummer nooit bekeken kan worden. Dat is immers niet opgenomen in het EU Digitaal Corona Certificaat (DCC) en kan dus ook onmogelijk getoond worden. In verband met uw vraag of de gegevens voldoende beschermd zijn bij gebruik van de CovidScanapp, verwijs ik u graag naar het antwoord op de eerste vraag.

Zowel in de modus 'evenement' als in de modus 'inkomende reiziger' worden er bij het scannen nooit gescande gegevens bewaard. Die worden enkel op het moment van scannen geïnterpreteerd en zodra het scanproces is afgerond, uit het geheugen van het scantoestel – dus de smartphone – gewist.

In de modus 'evenement' worden enkel als resultaat getoond: naam en voornaam en de duurtijd van de geldigheid van het Covid Safe Ticket. Geen enkel ander gegeven wordt getoond als resultaat. Met andere woorden: de persoon die scant, kan nooit afleiden om welke reden iemand rood scant. En enkel de noodzakelijke gegevens die nodig zijn om een persoonsidentificatie te kunnen verrichten, worden getoond.

Bij een scan in de modus 'inkomende reiziger' worden ondertussen enkel nog als resultaat getoond: naam en voornaam en de geboortedatum, indien die beschikbaar is op het certificaat. Die aanpassing is dus al gebeurd.

Vervolgens vroeg u of misbruik voldoende gemakkelijk kan worden vastgesteld en of daarop wordt gecontroleerd. In het eerste deel van mijn antwoord heb ik al gezegd hoe het kan worden vastgesteld. Ook wordt de burger ervan op de hoogte gesteld hoe dit te controleren, op basis van berichtgeving in verschillende nieuwsmedia, alsook via een FAQ op de site www.covidsafe.be.

Overeenkomstig onder andere artikel 222 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens kan men in het geval van misbruik strafrechtelijk worden gesanctioneerd.

U vroeg ook waarom er niet wordt geopteerd voor een aparte politieversie. Ik heb u al gezegd dat we dat ondertussen dus wel doen. De ontwikkeling daarvan is met hoge prioriteit lopende.

Ik heb momenteel, bij datum van 15 november, geen weet van klachten over misbruik of lopende procedures met betrekking tot de dubbele functie van de CovidScanapp bij de Vlaamse Toezichtcommissie of de federale Gegevensbeschermingsautoriteit. De Belgische stichting Ministry of Privacy, die zich opwerpt als onafhankelijke privacywaakhond, vecht de uitbreiding van het CST naar onder meer de horeca en het mogelijk verkeerde gebruik van de CovidScanapp momenteel wel aan bij het Grondwettelijk Hof. Maar ik denk dat u daarvan op de hoogte bent.

Excuseer voor het wat uitgebreide antwoord, maar ik denk dat het wel belangrijk was in dezen.

**De voorzitter**: De heer Vaneeckhout heeft het woord.

**Jeremie Vaneeckhout (Groen)**: Geen enkel probleem dat het een uitgebreid antwoord was, het toont dat u de problematiek en de uitdaging ernstig neemt. We moeten ons er ook van bewust zijn, collega's, dat het gebruik van die app intussen niet enkel meer plaatsvindt in een veeleer anonieme context, bijvoorbeeld bij reizen, maar dat het ook gaat over de cafébaas van het café in eigen dorp die over die informatie beschikt en daar dus mee aan de slag kan gaan. Dat komt dus toch iets dichter in de levenswereld van mensen, vandaar dat onze fractie het ook belangrijk vindt om daar voldoende antwoord op te formuleren.

Uw antwoord is in die zin bevredigend, minister-president, dat u ook bezig bent met een structurele oplossing op dat gebied. De huidige oplossing verwacht natuurlijk wel nog relatief veel kennis van de gecontroleerde. Die moet ook wel op zoek gaan. Ik heb net zelf de oefening gedaan in mijn eigen app. Je moet op zoek naar de 'frequently asked questions', om daar terug te vinden hoe je kunt controleren dat er een correct gebruik is. Misschien moeten we tussentijds eens bekijken hoe dat nog iets zichtbaarder in de app kan worden opgenomen.

Ik heb maar één afsluitende vraag. Wat is de timing voor die afzonderlijke app voor politiegebruik? Ik zal u daar niet op vastpinnen, maar een of andere richtdatum zou natuurlijk wel een beetje helpen.

**De voorzitter**: Minister-president Jambon heeft het woord.

**Minister-president Jan Jambon**: Dat heeft de allerhoogste prioriteit. Men is daar echt met man en macht aan bezig. Ik kan er niet echt een richtdatum op kleven, maar het heeft de hoogste prioriteit.

**De voorzitter**: De heer Vaneeckhout heeft het woord.

**Jeremie Vaneeckhout (Groen)**: Ik denk dat dat de juiste classificatie is. We zullen in de komende weken wel eens polsen hoe het daar verder mee staat. Dank u wel.

**De voorzitter**: De vraag om uitleg is afgehandeld.

**VRAAG OM UITLEG van Stijn De Roo aan Jan Jambon, minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management, over de versterking van de digitale weerbaarheid van de Vlaamse overheid**
**– 569 (2021-2022)**

**Voorzitter: de heer Steven Vandeput**

**De voorzitter**: De heer De Roo heeft het woord.

**Stijn De Roo (CD&V)**: Minister-president, op 15 oktober heeft de Vlaamse Regering de strategie goedgekeurd om de digitale overheid weerbaarder te maken tegen dreigingen en aanvallen. In de afgelopen periode zijn de cyberaanvallen en -dreigingen toegenomen, onder meer door een verschuiving naar cybercriminaliteit ten aanzien van digitale gegevens en digitale infrastructuur van personen, bedrijven en overheden. Vlaanderen beschikt over gevoelige digitale informatie van burgers, bedrijven en organisaties en moet die te allen tijde beschermen. De regering maakt 5 miljoen euro vrij voor het aanscherpen van de beveiligingstechnologie, voor het versterken van de veiligheidscultuur en voor het uitbouwen van een goed crisismanagement. Het Stuurorgaan Vlaams Informatie- en ICT-Beleid is de eindverantwoordelijke voor het beleid inzake informatieveiligheid. Daarin krijgt het ondersteuning van een werkgroep met experts inzake informatieveiligheid en van de centrale diensten van Digitaal Vlaanderen.

Minister-president, ik heb een aantal vragen over die goedkeuring en die budgettoezegging. Kunt u het traject kaderen waarin deze middelen in de digitale weerbaarheid worden geïnvesteerd? Hoe worden die verdeeld over de doelstellingen? Wanneer wenst u welke mijlpalen te bereiken voor de veiligheidsstrategie? Wat is de rol van het stuurorgaan daarin? Op welke manier zult u de samenwerking tussen de diverse administraties verbeteren en de uitbouw van een algemene veiligheidscultuur faciliteren? Op welke manier zult u monitoren dat de gevoelige informatie van onze Vlaamse burgers, bedrijven en organisaties beschermd blijft?

**De voorzitter**: Minister-president Jambon heeft het woord.

**Minister-president Jan Jambon**: Mijnheer De Roo, ik geef een uitgebreid antwoord op deze belangrijke vraag. De middelen voor digitale weerbaarheid worden geïnvesteerd in drie domeinen: de aanpak van de informatieveiligheid; het verhogen van de digitale competenties; weerbare digitale processen en een robuuste infrastructuur. Ik zal daar wat meer details over geven.

Wat de aanpak van de informatieveiligheid betreft, versterken we het leiderschap op het vlak van informatieveiligheid, met inbegrip van de bescherming van de persoonsgegevens, door een duidelijk kader en een duidelijke governance en verantwoordelijkheden vast te leggen om naar een door de hele Vlaamse overheid gedragen aanpak voor informatieveiligheid te evolueren. Op basis van een periodieke

rapportering van hoge kwaliteit moet het voor beslissingsnemers en beleidsvoerders mogelijk zijn om de juiste investeringsbeslissingen te nemen. Met deze prioriteit willen we een Vlaamseoverheidbreed overzicht en focus op informatieveiligheid leggen, met een duidelijk beleidskader binnen de Vlaamse overheid inzake het beheersen van risico's op het vlak van informatieveiligheid, met inbegrip van de bescherming van de persoonsgegevens, en met betere en geïnformeerde beslissingen zowel wat de hele Vlaamse overheid als de entiteiten ervan betreft, door een duidelijk begrip van de risicoblootstelling van de Vlaamse overheid op het vlak van informatieveiligheid en de veiligheid van de persoonsgegevens.

Dan is er het verhogen van de digitale competenties. Een gebrek aan kennis en expertise met betrekking tot informatieveiligheid leidt tot een situatie waarin we niet in staat zijn om in te schatten wat de risico's van onze informatieverwerking zijn en ons niet adequaat kunnen beschermen. Op die manier is het onmogelijk om onze beoogde doelstellingen te halen. Met deze prioriteit willen we de volgende resultaten bereiken: een versterkte slagkracht met betrekking tot het garanderen van informatieveiligheid door een sterke coördinatie onder toezicht van het stuurorgaan; een breed draagvlak creëren door de participatie van diverse stakeholders, zoals een werkgroep, de private sector, onderzoek; capaciteiten verhogen door een beroep te doen op strategische partners gespecialiseerd in cybersecurity; minder blootstelling aan risico's met betrekking tot informatieveiligheid door het opleiden en bewustmaken van de werknemers van de Vlaamse overheid; interne competentie- en kennisopbouw verhogen door een pool aan specialisten met brede inzetbaarheid.

Dan is er het element van de weerbare digitale processen en een robuuste infrastructuur. Deze prioriteit heeft als doelstelling om het veiligheidsniveau van de informatieverwerking op operationeel niveau te verhogen door in de juiste organisatie en veiligheidsbouwstenen te voorzien. Elke entiteit staat binnen de eigen organisatie in voor het correct implementeren van maatregelen en controles zoals gedefinieerd in het informatieclassificatieraamwerk van de Vlaamse overheid. Het is echter logischer en efficiënter om een aantal diensten op een Vlaamseoverheidsbreed basisaanbod te baseren. Die omvatten onder meer het overkoepelend monitoren en opvolgen van informatieveiligheidsincidenten – dat is eerder operationeel – en het optimaal inrichten van veiligheidsgerelateerde dienstverlening, wat eerder organisatorisch en technologisch is.

Deze aanpak combineert proactieve en reactieve maatregelen om een zo volledig mogelijke omgeving te verkrijgen. Met deze prioriteit willen we een aantal resultaten bereiken: het verhogen van de maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening en tools, de geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen, het verhogen van het operationele veiligheidsniveau door Vlaamseoverheidbrede veiligheidsbouwstenen verder uit te bouwen, de tijdige detectie van informatieveiligheidsincidenten en versterkte slagkracht met betrekking tot ernstige informatieveiligheidsincidenten.

Om deze resultaten te bereiken werd na de goedkeuring van de veiligheidsstrategie op 15 oktober 2021 door de Vlaamse Regering een bijbehorend veiligheidsprogramma opgestart. De verdeling van de voorziene middelen over de verschillende domeinen zal pas in de verdere opzet van dit programma gedetailleerd worden. Er werd een programmamanager aangeduid, die is gestart met het opzetten van de communicatiekanalen en de programmastructuur naast de opsplitsing in concrete projecten. Een eerste rapporteringsmoment aan het Stuurorgaan Vlaams Informatie- en ICT-beleid is voorzien voor 2 december, volgende week dus.

De veiligheidsstrategie goedgekeurd door de Vlaamse Regering wordt operationeel gemaakt door middel van een strategisch plan met bijhorend veiligheidsprogramma. Dit strategisch plan 2020-2024 focust op een aantal prioriteiten: een integrale aanpak van de informatieveiligheid door middel van een duidelijk beleidskader binnen

de Vlaamse overheid en een verhoogde digitale slagkracht. Dat kan door een verhoging van de digitale competenties van de werknemers door middel van opleiding, bewustmaking, strategische partners, competentie en kennisopbouw, en door weerbare processen, geautomatiseerd in robuuste applicaties en infrastructuur, door middel van een adequaat dienstverleningsmodel met de juiste veiligheidsbouwstenen.

Het is niet mogelijk en zelfs niet zinvol om alle beschikbare technologische en/of organisatorische veiligheidsmaatregelen toe te passen op alle digitale toepassingen. Daartoe hebben we het informatieclassificatieraamwerk ontwikkeld. Dit raamwerk zorgt ervoor dat informatie naar juiste waarde wordt geschat en navenant wordt beveiligd. Het vormt aldus de basis voor het informatieveiligheidsbeleid en de daaraan gekoppelde veiligheidsmaatregelen voor de Vlaamse administratie en is een belangrijke pijler van onze strategie informatieveiligheid.

Een belangrijke rol is weggelegd voor het Stuurorgaan Vlaams Informatie- en ICT-beleid als verantwoordelijke voor de validatie van het informatieveiligheidsbeleid van de Vlaamse administratie en voor de overkoepelende aansturing en coördinatie van de implementatie van dit beleid. Het stuurorgaan wordt hierin ondersteund door de speciaal daartoe opgerichte Werkgroep Informatieveiligheid.

We voeren het 'lines of defence'-model in. Dit lijnenmodel is een governancemodel om aan optimaal risicobeheer te kunnen doen. De eerste lijn is elke entiteit van de Vlaamse overheid. Een entiteit beslist autonoom hoe zij haar eigen omgeving beveiligt, binnen de grenzen van haar onafhankelijkheid en bevoegdheden. De tweede lijn is het Digital Security Office van het agentschap Digitaal Vlaanderen. Dit office bewaakt voor de gehele Vlaamse administratie de kwaliteit van het beheer van de informatieveiligheid. De derde lijn is een onafhankelijke partij die verifieert welke controles en maatregelen werken en of de geïdentificeerde risico's reëel en volledig zijn. Hierbij gaat het om een entiteit zoals Audit Vlaanderen of een externe auditeur.

Onze strategie informatieveiligheid voorziet in de nodige technologie en in de nodige governance om een veilige en vlotte digitale transformatie mogelijk te maken. Maar om na te gaan of de strategie werkt, moet er gemeten worden. Dit doen we door een periodieke kwaliteitsvolle rapportering over informatieveiligheid aan beslissingsnemers en beleidsvoerders, door het inrichten van selfassessments en een conformiteitstoetsing.

Daarnaast voeren we het 'lines of defence'-governancemodel in, zoals ik al heb gezegd in het antwoord op de vorige vraag. Het monitoringaspect zit hierbij in de derde lijn: er wordt een beroep gedaan op een onafhankelijke partij, die verifieert welke controles/maatregelen werken en of de geïdentificeerde risico's reëel en volledig zijn. Hierbij gaat het om een entiteit zoals Audit Vlaanderen of een externe auditeur.

**De voorzitter**: De heer De Roo heeft het woord.

**Stijn De Roo (CD&V)**: Dank u, minister-president, voor uw antwoord. Het was een uitgebreid antwoord, en dat is ook goed, want het toont aan dat u en de hele Vlaamse Regering de digitale veiligheid en digitale weerbaarheid bijzonder belangrijk vinden en daar ook de nodige middelen voor voorzien. Ik heb in uw antwoord een op-maataanpak gehoord, ik heb in uw antwoord een gelaagd systeem gehoord, ik heb in uw antwoord ook competentieopbouw gehoord, zowel intern als extern, naast een aantal zeer technische zaken. Ik zal het verslag van uw antwoord nog eens heel rustig opnieuw lezen. Ik heb geen bijkomende vragen.

Ik denk dat het belangrijk is om te herhalen dat er tot op vandaag geen grote incidenten zijn geweest bij de Vlaamse overheid – hout vasthouden – en ik hoop dat we dat zo kunnen houden. Als overheid hebben we de taak om informatie goed te beschermen en moeten we er alles aan doen om de burgers en hun informatie

zo goed mogelijk te beschermen via investeringen. Die investeringen zijn nu gebeurd, en we zullen dat de komende periode opvolgen.

**De voorzitter**: De vraag om uitleg is afgehandeld.