

Antwoord van Gedeputeerde Staten op vragen van

E.W. Kegel | FVD

R. Westdijk | FVD

(d.d. 28-08-2026)

Nummer

4469

Onderwerp

Informatiehuishouding en veiligheid: wetten en
inlichtingen(plicht)

Aan de leden van Provinciale Staten

Toelichting vragensteller

Per 15 augustus jl. zijn de nieuwe Cyberbeveiligingswet (Cbw) en Wet weerbaarheid kritieke entiteiten (Wwke) formeel in werking getreden. Hiermee zet de wetgever een dwingende stap in het versterken van de digitale en fysieke weerbaarheid van Nederlandse organisaties tegen toenemende dreigingen. Bron: NCTV, 07-07-2026, [Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht](#) | Nationaal Coördinator [Terrorismebestrijding en Veiligheid](#)

Bijgevolg gelden nieuwe verplichtingen voor ruim 8.000 organisaties. De Provincie Zuid-Holland (PZH) behoort nadrukkelijk tot deze doelgroep. In het kader van de Cbw geldt de PZH als essentiële entiteit, wat betekent dat streng ex-ante en ex-post toezicht van toepassing is. In het kader van de Wwke wordt de PZH (potentieel) aangewezen als kritieke entiteit, voor zover zij door het Rijk specifieke taken aangewezen heeft gekregen in bijvoorbeeld het water- en vaarwegbeheer. In beide gevallen brengt dit een aanzienlijke aanscherping van verplichtingen met zich mee.

Op 11 maart jl. stonden het Programmaplan informatietransitie 2026, het Plan van aanpak Weerbaarheid en Informatieveiligheid 2025-2027 en de Zesde rapportage Autoriteit Persoonsgegevens geagendeerd in de Commissie BMM, voorafgegaan door een technische sessie. Uit de stukken, de sessie en de beraadslaging kwam het beeld naar voren van serieuze tekortkomingen in de provinciale informatie- en veiligheidsorganisatie. Dit beeld wordt bevestigd door intern en extern uitgevoerde periodieke metingen en evaluaties van volwassenheids- en competentieniveaus op een reeks deelgebieden.

In de voorbereiding op de commissiebehandeling heeft de fractie van FVD Zuid-Holland — op grond van artikel 167 van de Provinciewet en artikel 72a RvO — per e-mail via de griffie tijdig de volledige rapporten en verslagen (inclusief scorecards, bijlagen en toebehoren) van genoemde evaluaties opgevraagd bij Gedeputeerde Staten (hierna: GS). Reglementair had deze informatie voorafgaand aan de commissievergadering (uiterlijk 10 maart jl.) verstrekt moeten zijn. De daadwerkelijke beantwoording ontvingen wij pas op 17 april jl., na driemaal te hebben gerappelleerd via de griffie en ruim 5 weken na het verstrijken van de termijn. Deze overschrijding

levert een strijdigheid op met het reglement van orde en de wettelijke bepalingen die een deugdelijke commissievoorbereiding en de controlerende taak van de Provinciale Staten (hierna: PS) borgen.

Bovendien werden de opgevraagde documenten ook bij de vertraagde beantwoording niet overlegd. In plaats daarvan is onderstaande overzichtstabel verstrekt, waarin verreweg de meeste en belangrijkste inhoudelijke gegevens ontbreken:

Er worden diverse testen, audits en scans uitgevoerd (scorecards) op verschillende onderdelen binnen het IT-domein. Voor die scorecards waar de uitkomst bestaat uit een getal (score) is die toegevoegd.

Scorecard	Reikwijdte	periode	score
PEN-testen	Websites en diensten die in verbinding staan met het internet	Jaarlijks	
DigiD audit	Inrichting en veiligheid DigiD diensten, conform baseline informatieveiligheid overheid (BIO)	Jaarlijks	
Security assesment Microsoft 365	Configuratie M365 conform best practices	2-jaarlijks	
Vulnerability scan netwerk	Kwetsbaarheden in netwerkcomponenten	maandelijks	
Vulnerability scan IT-infrastructuur	Kwetsbaarheden in IT-hardware	maandelijks	
Digital workplace maturity	Volwassenheid digitale werkplek, product en supportorganisatie	3-jaarlijks	
Reliability assessment	Robuustheid IT-infrastructuur	Na mature wijzigingen	
Interne audits (EAA)	Diverse audits op gebied van techniek, organisatie en weerbaarheid	Meerdere per jaar, diverse onderwerpen	
Privacy Volwassenheidsmodel	Standaard scorecard van Centrum Informatiebeveiliging en Privacybescherming	Self assessment	2,2 uit 5
Data gedreven werken	Standaard scorecard van Interbestuurlijk Datastrategie IBDS	Self assessment	1,5 uit 4

Slechts op 2 van de 10 geëvalueerde onderdelen is een getalsmatige score verstrekt, waarbij bovendien de historische en vergelijkende cijfers van eerdere meetmomenten ontbreken. Van belang is dat het nut van scorecards erin bestaat om de actuele toestand en de voortgang inzichtelijk te maken; dit inzicht is PS onthouden. Op de overige 8 onderdelen is geen enkele

kwantitatieve of kwalitatieve uitslag overlegd. Er is daarbij geen wettelijke grond gegeven voor het onthouden van deze inlichtingen, zoals een expliciet beroep op het openbaar belang (art. 167 lid 3).

VRAGEN

Weergave aanleiding

1. *a. Kunnen GS bevestigen dat de hiervoor beschreven aanleiding en feitelijke gang van zaken correct zijn weergegeven?*

Antwoord

Gedeputeerde Staten kunnen bevestigen dat de beschreven technische sessie, commissiebehandeling en het informatieverzoek hebben plaatsgevonden. Ook kunnen GS bevestigen dat de beantwoording van het verzoek later heeft plaatsgevonden dan gewenst. GS betreuren de vertraging. Voor een aantal conclusies en kwalificaties in de aanleiding verwijzen GS naar het antwoord op vraag 1b.

b. Zo niet, op welke onderdelen is de weergave volgens GS onjuist, en wat is volgens GS op die onderdelen wel de correcte weergave?

Antwoord

De weergave is onjuist voor zover daaruit wordt geconcludeerd dat uit de beschikbare onderzoeken, audits en evaluaties sprake zou zijn van serieuze tekortkomingen in de informatie- en veiligheidsorganisatie. De verschillende onderzoeken hebben een eigen doel en rapportagevorm. Niet alle onderzoeken leiden tot een score, volwassenheidsmeting of overkoepelend oordeel. Daarom kunnen de uitkomsten niet als één integraal beeld worden gepresenteerd en kan de genoemde conclusie niet uit de beschikbare stukken worden getrokken.

Cbw en Wwke

2. *a. Zijn GS volledig en gedetailleerd op de hoogte van de per 15 augustus jl. van kracht geworden Cbw en Wwke en de dwingende verplichtingen die hieruit voor de PZH voortvloeien?*

Antwoord

Ja. GS zijn op de hoogte van de inwerkingtreding van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten en de verplichtingen die hieruit voor de provincie voortvloeien. De provincie werkt actief aan de verdere implementatie van deze verplichtingen binnen de bestaande programma's voor weerbaarheid en informatieveiligheid.

b. Hebben alle GS-leden een Cbw/Wwke-bestuurstraining gevolgd en, zo niet, welke GS-leden wel en welke niet, en welk oordeel hebben GS over het nut en de noodzaak hiervan?

Antwoord

Nee. De bestuurstraining is ingepland en vindt plaats in Q4 van dit jaar. GS onderschrijven het belang van deze training.

c. Zijn GS zich ervan bewust dat de Cbw en Wwke geen wettelijke overgangsperiode of begunstigingstermijn kennen, waardoor alle wettelijke plichten (registratie-, zorg- en meldplicht en de bestuurlijke aansprakelijkheid van GS) per direct en onverkort gelden?

Antwoord

Ja. GS zijn zich bewust van de verplichtingen die sinds de inwerkingtreding van beide wetten gelden, waaronder de zorg-, registratie- en meldplicht en de daarbij behorende bestuurlijke verantwoordelijkheden.

d. Kunnen GS een integraal overzicht verstrekken van alle concrete verplichtingen die voor de PZH voortvloeien uit de Cbw en Wwke, hetzij rechtstreeks in de beantwoording van deze vragen, hetzij via een toezegging van een afzonderlijke GS-brief op korte termijn?

Antwoord

De Cbw bevat onder meer verplichtingen op het gebied van zorgplicht, registratieplicht, meldplicht, governance en training. De uitwerking hiervan is omvangrijk en technisch van aard. GS zijn bereid hierover een technische toelichting te verzorgen.

e. Voldoet de PZH op dit moment aantoonbaar aan alle aangescherpte verplichtingen uit beide wetten?

Antwoord

Nee. De provincie voldoet op veel onderdelen aan bestaande normen en verplichtingen, maar werkt nog aan de verdere implementatie van de aanvullende eisen uit de Cbw en Wwke. Hiervoor wordt uitvoering gegeven aan het Plan van Aanpak Weerbaarheid en Informatieveiligheid 2025-2027 en het verbeterprogramma voor Operationele Technologie.

f. Zo niet, op welke onderdelen voldoet de PZH nog niet, voldoet de PZH tenminste wel aan de Baseline Informatiebeveiliging Overheden (BIO 1.0) en op welke termijn reikt de realistische planning voor de overgang naar BIO 2.0 en volledige Cbw/Wwke-compliance?

Antwoord

De provincie voldoet reeds op veel onderdelen aan de BIO en werkt aan de verdere implementatie van de aanvullende eisen uit de Cbw, Wwke en BIO 2.0. De hiervoor benodigde verbetermaatregelen zijn opgenomen in het Plan van Aanpak Weerbaarheid en Informatieveiligheid 2025-2027 en het verbeterprogramma voor het OT-domein. De uitvoering daarvan loopt gefaseerd tot en met 2027, waarbij voor onderdelen van het OT-domein een langere doorlooptijd geldt.

g. Is de PZH reeds formeel aangewezen als essentiële entiteit voor de Cbw en aangewezen als kritieke entiteit voor de Wwke, en zijn GS bereid toe te lichten hoe deze aanwijzingen betrekking hebben op de PZH als geheel en/of op onderdelen van de organisatie?

Antwoord

De provincie wordt onder de Cbw aangemerkt als essentiële entiteit. Voor de Wwke is nog geen formeel aanwijzingsbesluit ontvangen. De provincie houdt in haar voorbereidingen wel rekening met de verplichtingen die hieruit kunnen voortvloeien.

h. Heeft de PZH de verplichte registraties via MijnNCSC en/of SSONRijk reeds afgerond en, zo niet, waarom niet en wanneer wel?

Antwoord

Ja. De provincie heeft zich in een eerder stadium aangemeld bij het NCSC en maakt gebruik van de beschikbare voorzieningen voor informatie-uitwisseling en samenwerking.

i. Beschikken GS over een (goedgekeurde) GAP-analyse en uitgewerkte visie op de scheiding én gecontroleerde koppeling tussen operationele technologie (OT, m.n. beheer- en bedieningssystemen van infrastructurele werken) en informatietechnologie (IT) en is geborgd waar de verantwoordelijkheden voor de beveiliging van beide domeinen in de organisatie zijn belegd?

Antwoord

Ja. Voor zowel IT als OT zijn analyses uitgevoerd om de weerbaarheid verder te versterken. De uitkomsten zijn verwerkt in het Plan van Aanpak Weerbaarheid en Informatieveiligheid 2025-2027. De verantwoordelijkheden voor beide domeinen zijn binnen de organisatie belegd.

j. Wat is de actuele stand van zaken in de contacten tussen de PZH en de toezichthouder, de Rijksinspectie Digitale Infrastructuur (RDI), waaronder (doch niet uitsluitend) recente of geplande bestuurlijke monitoringsgesprekken, systeemininspecties, audits, opgevraagde risicoanalyses en incidentmeldingen, en wat is de actuele positie van de PZH binnen de interventiestrategie (interventieladder) van de RDI?

Antwoord

De provincie heeft regelmatig contact met de RDI in het kader van de voorbereiding op het toezicht onder de Cyberbeveiligingswet. Er lopen geen handhavingstrajecten en er zijn geen inspecties of audits aangekondigd. De contacten staan in het teken van voorbereiding en kennisuitwisseling.

k. Is de personele bezetting binnen de PZH-domeinen IT, OT en cybersecurity op orde, en wat is in het bijzonder de actuele status van de werving, selectie en indiensttreding of inhuur van de Chief Information Officer (CIO)?

Antwoord

De afgelopen periode is geïnvesteerd in de versterking van de capaciteit voor informatiebeveiliging en cyberweerbaarheid. Voor zowel IT als OT zijn gespecialiseerde teams ingericht. De invulling van de CIO-functie maakt onderdeel uit van de verdere ontwikkeling van de informatievoorziening en volgt de reguliere procedure.

I. Kunnen GS een volledig inzicht geven in de financiële consequenties van de inwerkingtreding van de Cbw en Wwke voor de PZH, en hoe worden de kosten in het lopende begrotingsjaar opgevangen, en op welke wijze worden de structurele middelen verwerkt in de Kadernota en de Begroting 2027?

Antwoord

De kosten van de Cbw en Wwke zijn niet volledig los te zien van de bredere investeringen die de provincie al doet op het gebied van informatieveiligheid en weerbaarheid. Waar aanvullende investeringen nodig zijn, worden deze afgewogen binnen de reguliere planning- en controlcyclus.

Inlichtingenplicht

a. In hoeverre hebben de in maart jl. gevraagde en tot op heden niet of nauwelijks verstekte inlichtingen over evaluaties en metingen in de IT-, OT- en cybersecurity-domeinen direct betrekking op de nu geldende wettelijke verplichtingen vanuit de Cbw en Wwke?

Antwoord

De gevraagde evaluaties, audits en metingen geven inzicht in de informatieveiligheid en digitale weerbaarheid van de provincie. Deze onderwerpen raken ook aan de verplichtingen uit de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. Niet alle gevraagde onderzoeken zijn echter uitgevoerd in het kader van deze wetten of leiden tot een beoordeling van naleving daarvan.

b. Waarom was de beantwoording van de technische vraag destijds zodanig vertraagd dat een deugdelijke voorbereiding van de commissiebehandeling belemmerd is geworden, en waarom zijn de gevraagde inlichtingen bij de vertraagde beantwoording en tot op heden niet of nauwelijks verstrekt?

Antwoord

GS erkennen dat de beantwoording van het verzoek langer heeft geduurd dan gewenst en betreuren deze vertraging. Sindsdien is de informatiepositie verder ontwikkeld. Waar mogelijk verstrekken GS in de beantwoording van deze schriftelijke vragen aanvullende geaggregeerde informatie over de ontwikkeling van de provinciale weerbaarheid en informatieveiligheid. GS zijn niet bekend met een nog lopend informatieverzoek over dit onderwerp, anders dan de onderhavige schriftelijke vragen.

c. Zijn GS bereid alsnog volledig te voldoen aan hun wettelijke inlichtingenplicht (ex art. 167 Provinciewet) door alle namens Statenlid Ewald Kegel opgevraagde technische documenten (scorecards, evaluatierapporten, audits en verslagen inclusief bijlagen op alle IT/OT-onderdelen, tot 5 jaar terug dan wel vanaf de aanvang van de metingen) uiterlijk

binnen de reglementaire beantwoordingstermijn van deze vragen integraal aan PS te verstrekken en op Notubiz te publiceren?

Antwoord

Nee. GS achten het niet verantwoord om alle gevraagde documenten integraal openbaar te maken. Een deel van deze documenten bevat informatie over kwetsbaarheden, beveiligingsmaatregelen en risicoanalyses. Openbaarmaking daarvan kan de informatiebeveiliging en digitale weerbaarheid van de provincie schaden. De rapportages geven bovendien op zichzelf geen volledig beeld van de feitelijke veiligheidsstatus. GS zullen steeds beoordelen welke informatie openbaar, vertrouwelijk of geaggregeerd kan worden verstrekt.

d. Zijn GS bereid in aanvulling op de gevraagde technische inlichtingen (vraag 3.c.) de volgende vragen technisch te (laten) beantwoorden?

I. Hoeveel cyberincidenten, datalekken, ransomware-aanvallen en ernstige IT- of OT-verstoringen hebben zich de afgelopen vijf jaar binnen de PZH voorgedaan?

II. Hoeveel van deze incidenten zijn gemeld bij de Autoriteit Persoonsgegevens, het NCSC, een CSIRT of een andere toezichthouder?

III. Beschikt de PZH over een actueel en getest incidentresponsplan dat specifiek rekening houdt met aanvallen op OT-systemen en infrastructurele werken?

Antwoord

Ja.

I. Voor datalekken zijn registraties beschikbaar. In de jaren 2021 tot en met 2025 zijn respectievelijk 7, 25, 34, 59 en 51 datalekken geregistreerd. Tot en met het tweede kwartaal van 2026 zijn 21 bevestigde datalekken geregistreerd. Voor ransomware-aanvallen en ernstige IT- of OT-verstoringen zijn geen afzonderlijke aantallen beschikbaar die op een vergelijkbare wijze zijn geregistreerd. Er zijn geen ernstige verstoringen geregistreerd.

II. Van de geregistreerde datalekken zijn in de jaren 2021 tot en met 2025 respectievelijk 1, 1, 12, 21 en 18 meldingen gedaan bij de Autoriteit Persoonsgegevens. Tot en met het tweede kwartaal van 2026 zijn 2 meldingen gedaan bij de Autoriteit Persoonsgegevens. Er zijn geen meldingen gedaan bij het NCSC.

III. Ja. De provincie beschikt over vastgestelde processen voor de afhandeling van beveiligingsincidenten en calamiteiten. Daarnaast wordt de crisisorganisatie periodiek geoefend. In 2025 en 2026 zijn oefeningen uitgevoerd waarbij scenario's rond operationele technologie en infrastructurele werken onderdeel waren van de oefening.

e. Indien GS besluiten gevraagde inlichtingen geheel of gedeeltelijk te weigeren, zijn GS dan bereid dit niet stilzwijgend te doen, maar per document en vraag expliciet te motiveren waarom verstrekking in strijd is met het openbaar belang (ex art. 169 lid 3 Provinciewet), en daarbij alle mogelijkheden te benutten om de informatie vertrouwelijk aan PS ter beschikking te stellen (bijv. via een besloten notatie of beveiligde terinzagelegging)?

Antwoord

Ja. Indien GS besluiten informatie niet te verstrekken, zullen zij dit motiveren binnen de geldende wettelijke kaders. Daarbij wordt steeds gezien welke informatie wel kan worden gedeeld. Waar mogelijk verstrekken GS aanvullende informatie in geaggregeerde vorm, zonder afbreuk te doen aan de veiligheid en weerbaarheid van de provincie.

f. Hebben alle GS-leden en het ambtelijk topkader (waaronder de bestuursadviseurs) een bestuurstraining gevolgd op het gebied van het staats- en bestuursrecht, in het bijzonder de werking van de inlichtingenplicht in Provinciewet? Zo niet, welke GS-leden en functionarissen wel/niet, en hoe beoordelen GS het nut en de noodzaak hiervan?

Antwoord

Er wordt geen afzonderlijke bestuurstraining gegeven die specifiek is gericht op de inlichtingenplicht uit de Provinciewet. Nieuwe medewerkers en bestuurders worden wel geïnformeerd over de bestuurlijke verhoudingen en hun rollen binnen het provinciaal bestuur. GS vinden kennis van staats- en bestuursrecht van belang en ondersteunen initiatieven die bijdragen aan het versterken van deze kennis binnen de organisatie.

g. Erkennen GS dat het onthouden van door PS opgevraagde inlichtingen het wettelijk recht op feitelijke controle door de gekozen volksvertegenwoordiging rechtstreeks belemmert, en zijn GS bereid op het eigen handelen te reflecteren in het licht van, respectievelijk, de rechtsstatelijke en democratische beginselen?

Antwoord

GS erkennen het belang van adequate informatievoorziening aan Provinciale Staten voor de uitoefening van hun controlerende taak. Tegelijkertijd biedt de Provinciewet ruimte om informatie niet te verstrekken indien dit in strijd is met het openbaar belang. In dergelijke gevallen maken GS steeds een zorgvuldige afweging tussen het belang van informatieverstrekking aan PS en andere wettelijke belangen. GS zijn bereid hierover met Provinciale Staten het gesprek te voeren en te zoeken naar passende vormen van informatievoorziening.

h. Welke maatregelen achten GS passend om het eigen bestuurlijk handelen en dat van de ambtelijke top (Provinciesecretaris, Algemene Directie, Opgave-/Afdelingshoofden en Bestuursadviseurs) te toetsen aan naleving van de wettelijke inlichtingenplicht, teneinde te borgen dat ondergeschikte ambtelijke of strategische belangen nooit prefereren boven de wettelijke rechten van PS?

Antwoord

GS en ambtenaren zijn gehouden aan de wet en leggen daarvoor een eed of gelofte af. Bij verzoeken om informatie is het uitgangspunt dat informatie wordt verstrekt, tenzij sprake is van een wettelijke uitzondering. Indien informatie mogelijk niet verstrekt kan worden, vindt daarop een juridische toets plaats. GS achten deze waarborgen passend om de rechten van Provinciale Staten zorgvuldig te borgen.

i. Hoe reflecteren GS specifiek op de verhouding tussen de eigen ambtelijke organisatie onder leiding van de Provinciesecretaris en de ambtelijke ondersteuning van PS onder leiding van de Griffier, mede in het licht van het dualisme en de noodzaak dat de Griffie haar ondersteunende taak aan PS, in het bijzonder ten aanzien van het proces van het verstrekken van inlichtingen, onafhankelijk en onbelemmerd moet kunnen uitvoeren?

Antwoord

GS hechten aan een zorgvuldige invulling van het duale stelsel. De griffie heeft een zelfstandige rol in de ondersteuning van Provinciale Staten en moet die rol onafhankelijk kunnen vervullen. GS

respecteren die positie en vinden een goede samenwerking tussen de ambtelijke organisatie, de griffie en Provinciale Staten van groot belang.

j. Realiseren GS zich dat de democratische verhoudingen vereisen dat zij hun eigen controleur actief faciliteren, juist omdat PS als deeltijds lekenbestuur met beperkte ambtelijke ondersteuning niet alleen afhankelijk zijn van de bereidwilligheid en openheid van GS, maar ook van de strikte wettelijke naleving van de inlichtingenplicht door GS om hun grondwettelijke en statutaire controletaak überhaupt te kunnen uitoefenen?

Antwoord

Ja. GS hechten aan een zorgvuldige invulling van het duale stelsel. De griffie heeft een zelfstandige en onafhankelijke rol in de ondersteuning van Provinciale Staten en moet die rol onbelemmerd kunnen vervullen. GS respecteren deze positie en vinden een goede samenwerking tussen de ambtelijke organisatie, de griffie en Provinciale Staten van groot belang. Daarbij staat steeds voorop dat Provinciale Staten hun kaderstellende en controlerende taak goed kunnen uitoefenen.

Beantwoording

Kunnen GS alle bovenstaande vragen en subvragen volledig, nauwkeurig en afzonderlijk beantwoorden?

Antwoord

Ja.

Den Haag, 6 oktober 2026

Gedeputeerde Staten van Zuid-Holland,
secretaris,

voorzitter,

drs. M.J.A. van Bijnen MBA

mr. A.W. Kolff