

Nota voor : vergadering algemeen bestuur

Datum : 10 september 2026

Onderwerp : Strategische visie op IV 2026 - 2031

Kenmerk : AB/2629

Portefeuillehouder: C. Blom

Bijlage: 1. Strategische visie Informatievoorziening (IV)

Inleiding

Er is een Strategische visie op de Informatievoorziening (IV) opgesteld. Informatievoorziening is van groot belang; zowel intern, als naar onze inwoners toe. Het is de derde primaire taak van VNOG, naast brandweer en risico- & crisisbeheersing/GHOR. Bovendien is dit één van de drie door het Rijk vitaal verklaarde processen.

Doel van dit document is om een visie neer te zetten waar de IV heengaat en hoe VNOG hier de komende jaren richting aan wil geven. Deze visie zal als kapstok dienen voor meer concrete uitvoeringsprogramma's de komende jaren, in lijn met de ingezette transitie op het gebied van IV binnen VNOG.

De Strategische visie IV geeft tenslotte ook invulling aan actiepunt 16 van het regionaal beleidsplan 2025 – 2028, te weten: “het opstellen van een strategische visie op de complete informatievoorziening (IV)”.

Advies-besluit

1. De Strategische visie op IV 2026 – 2031 vast te stellen.

Beoogd effect

Deze visie biedt kaders en doelstellingen die richting geven aan de ontwikkelingen en inrichting van de VNOG IV de komende vijf jaren.

Argumenten

1.1. De visie geeft een totaalbeeld van het complete onderwerp.

De visie geeft een kernambitie, overzicht van landelijke ontwikkelingen, beschrijving van strategische opgaven en dilemma's, strategische thema's en doelstellingen.

1.2. De visie geeft kaders en prioriteiten voor de activiteiten binnen informatievoorziening.

De visie bevat elf strategische doelen waar naartoe gewerkt wordt en waarlangs geprioriteerd kan worden.

1.3. De visie past in de 'Visie op bedrijfsvoering' en de opdracht zoals gegeven in het regionaal beleidsplan 2025-2028.

De 'Visie op bedrijfsvoering' is door het DB op 4 juni vastgesteld en op 25 juni in het AB mondeling toegelicht. De nu voorliggende “Strategische visie op IV” past hier naadloos in (en vice versa).

Kanttekeningen

1.1. De visie is ambitieus en vergt een grote verandering.

De Strategische visie IV met bijbehorende doelstellingen is ambitieus en is meer dan alleen een “technisch traject”. Deze visie beschrijft een veranderopgave voor de gehele organisatie, waar team Informatie hand in hand optrekt met de rest van de organisatie. Dit vraagt een meer gestructureerde manier van samenwerken, waarbij scherpe keuzes gemaakt moeten worden. Slimmer omgaan met capaciteit houdt ook in dat er op andere manieren gekeken moet worden naar samenwerkingsvormen met ketenpartners, Oost 5 of landelijk, die ook allemaal voor gelijksoortige uitdagingen staan. Om deze veranderopgave beheerst te realiseren, zijn enkele randvoorwaarden essentieel die reeds opgepakt worden binnen het transitieteam opgericht naar aanleiding van het onderzoek “Informatie als fundament” en binnen de “Visie op de totale Bedrijfsvoering”, zoals gepresenteerd in het AB van 25 juni.

Uitvoering/ communicatie/ inwerkingtreding

Uiteraard heeft VNOG de afgelopen jaren op dit thema niet stil gezeten en al vele zaken in gang gezet, uitgewerkt en doorontwikkeld. Mensen zijn getraind, samenwerkingen zijn aangegaan en verdiept, systemen zijn gebouwd/ingericht/aangeschaft, etc. etc. In de P&C-documenten in de afgelopen jaren is hier steeds over gerapporteerd. We hebben niet gewacht tot deze Strategische visie IV er was om aan dit belangrijke thema te werken. Maar nu de visie er wel is, heeft VNOG een duidelijke richting voor de verdere ontwikkelingen de komende jaren.

Deze visie zal binnen het transitieteam verder uitgewerkt worden in concretere uitvoeringsprogramma's. In deze uitvoeringsprogramma's worden de gemeenten aangehaakt.

Rapportage/ evaluatie

Via de reguliere P&C-cyclus wordt periodiek gerapporteerd over de voortgang.

Personele consequenties en Financiële consequenties

Voor nu niet. Voorstellen die volgen uit de concrete uitvoeringsprogramma's zullen via de reguliere weg van de P&C-documenten ter besluitvorming worden voorgelegd.

Het algemeen bestuur van de Veiligheidsregio Noord- en Oost-Gelderland;

Bijeen in de vergadering d.d. 10 september 2026;

Gelezen het voorstel van het dagelijks bestuur d.d. 3 september 2026;

Besluit:

1. De Strategische visie op IV 2026 – 2031 vast te stellen.

De secretaris

De voorzitter

dr. G. Bouwmeester

A.J.M. Heerts

Twello, 10 september 2026

STRATEGISCHE VISIE OP INFORMATIEVOORZIENING

2026-2031

Beschikbaar, betrouwbaar,
verbonden, betekenisvol



INHOUDSOPGAVE

Blik op de toekomst	3
Kernambitie	6
Landelijke ontwikkelingen	8
Strategisch opgaven	10
Strategische dilemma's	12
Strategische thema's en doelstellingen	14
Randvoorwaarden	18

Blik op de toekomst

In de nabije toekomst leggen burgers incidenten steeds vaker vast met hun smartphone en delen deze informatie met de hulpdiensten. De meldkamer ontwikkelt zich tot een operationeel centrum waarin digitale beelden, sensordata en telefonisch doorgegeven informatie worden verzameld, geanalyseerd en benut. Artificial Intelligence (AI) en spraak-naar-teksttechnologie spelen hierbij een belangrijke rol in de aanname, triage en het bieden van handelingsperspectief¹. Deze nieuwe werkwijzen zullen ook impact hebben op de samenwerking met VNOG.

VNOG maakt met het Veiligheidsinformatieknooppunt (VIK) een vergelijkbare ontwikkeling door. Risico- en crisisbeheersing en GHOR werken samen aan een dynamisch en actueel risicobeeld. Hierbij worden technologieën zoals AI en digital twins ingezet om risicoanalyses verder te verbeteren en te verdiepen. AI maakt het mogelijk om nieuwe verbanden te leggen tussen factoren die een crisis kunnen beïnvloeden. Daarnaast ondersteunen AI-toepassingen bij het efficiënter verzamelen en duiden van informatie uit de omgeving. Ervaringen tijdens onder andere de COVID19 pandemie en de vluchtelingen crisis laten zien dat VNOG zich ontwikkelt tot een informatieknooppunt richting ketenpartners. Voor het goed vervullen van deze rol zijn datakwaliteit en het gebruik van open standaarden randvoorwaarden.



Steeds meer gebouwen worden in 3D vastgelegd

Steeds meer gebouwen worden in 3D vastgelegd volgens het Bouwwerk Informatie Model (BIM). Dit maakt het mogelijk om virtueel door gebouwen en omgevingen te bewegen. Door het gebruik van virtuele, meestal geografische, kopieën van de werkelijkheid (digital twins) kunnen risico's beter in beeld worden gebracht en kunnen scenario's worden gesimuleerd en voorbereid.

Ook binnen de brandweer vindt verdere digitalisering plaats. VNOG past sensoren toe in voertuigen om de status continu te monitoren. Dit biedt operationele mogelijkheden, zoals het volgen van waterverbruik tijdens inzetten, maar ook voordelen voor de bedrijfsvoering, bijvoorbeeld door onderhoud uit te voeren op basis van actuele behoefte (predictive maintenance). Daarnaast wordt AI ingezet voor inzetvoorstellen en als beslisondersteuning voor bevelvoerders en officieren. Bij toepassingen waarbij AI invloed heeft op de inzet van hulpverlening, is het van belang om expliciet aandacht te besteden aan de ethische aspecten.



¹ 2030 Dichterbij dan je denkt, koersdocument RCDV 2030

Tijdens de hulpverlening neemt het gebruik van technologische middelen verder toe. Er wordt al gewerkt met een gedeeld situationeel beeld via mobiele data terminals en het Landelijk Crisismanagementsysteem (LCMS). Dit beeld wordt de komende jaren verder uitgebreid met sensordata, dronebeelden en uitkomsten van AI-modellen. De uitwisselbaarheid van data tussen eenheden, ook bovenregionaal, wordt steeds belangrijker. Daarnaast nemen de eisen toe rondom het delen van informatie en beelden met crisispartners en het opbouwen van een landelijk situatiebeeld, bijvoorbeeld via het Knooppunt Coördinatie Rijk-Regio (KCR2).

Binnen de bedrijfsvoering vindt eveneens een ontwikkeling plaats. Bedrijfsvoering ondersteunt niet alleen de interne organisatie, maar ook externe partners die gehuisvest zijn in het toekomstige Veiligheidscentrum. Hiermee ontwikkelt de rol zich van interne dienstverlener naar een bredere serviceorganisatie. Procesmatig werken wordt hierbij steeds belangrijker om een betrouwbare en consistente dienstverlening te waarborgen. Daarnaast wordt er gewerkt aan een centralere aansturing van de informatievoorziening, met een belangrijke rol voor een centraal CIO Office.

De toenemende afhankelijkheid van technologie kent ook risico's. Vraagstukken rondom continuïteit en betrouwbaarheid van systemen, weerbaarheid bij uitval en kwetsbaarheid voor cyberaanvallen krijgen een prominente plaats op de agenda. Deze ontwikkelingen moeten worden gezien in het licht van een verscherpt dreigingsbeeld en een instabiele internationale context. Nog scherper dan in de afgelopen jaren is sprake van een instabiele en onvoorspelbare wereldorde, waarbij de AIVD rapporteert dat Rusland zich voorbereidt op een langdurige confrontatie met het Westen. Hierbij spelen cyberaanvallen een prominente rol. Ook het Chinees cyberprogramma wordt benoemd als een belangrijke bedreiging².

Daarnaast neemt de aandacht voor digitale autonomie en soevereiniteit toe. Diverse adviesraden waarschuwen voor een groeiende afhankelijkheid van grote, niet-Europese technologiebedrijven.



Digitale autonomie: het vermogen van de overheid om autonoom te handelen en beslissingen te nemen over haar digitale technologie.

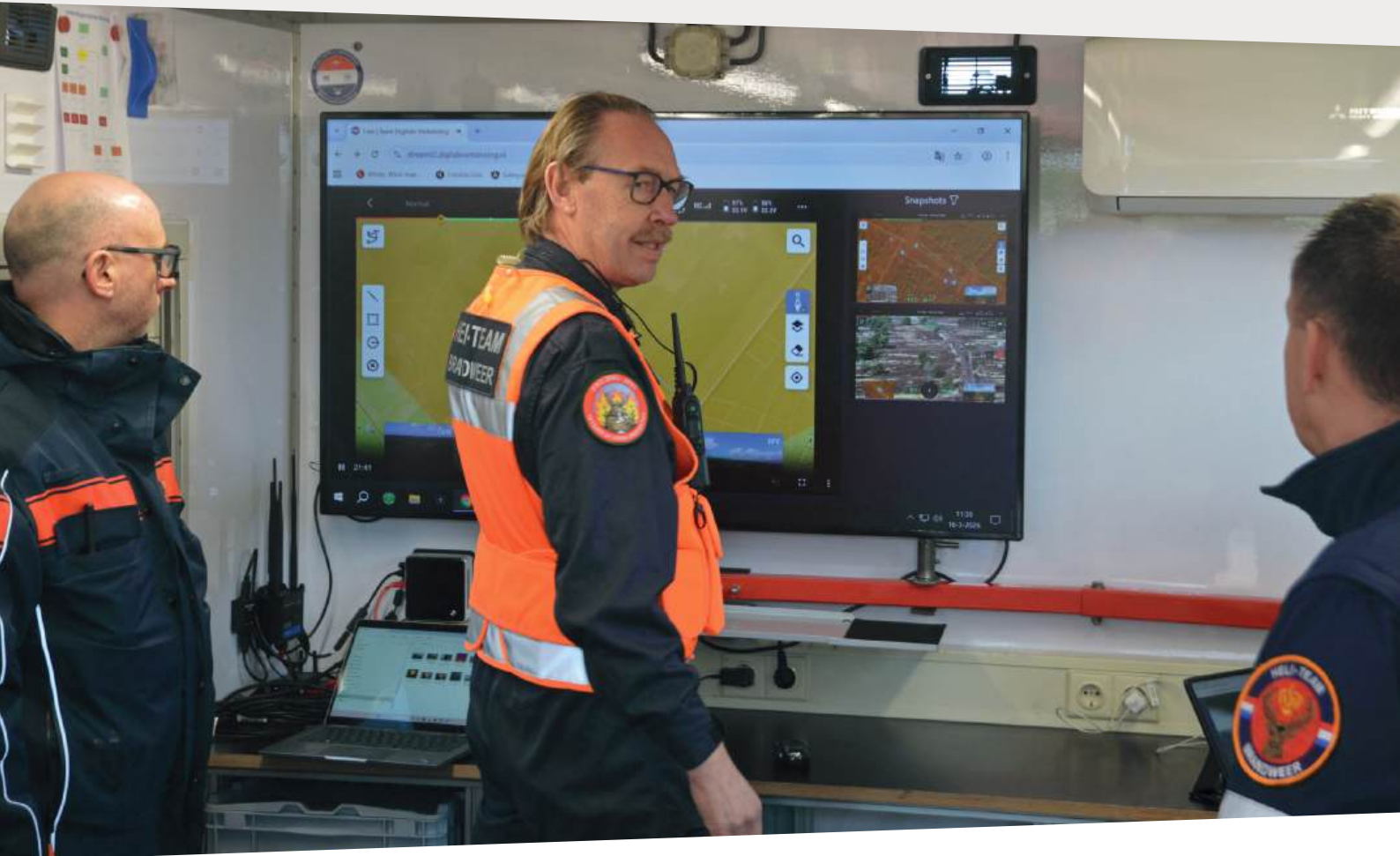
Soevereiniteit: juridische en bestuurlijke controle over digitale infrastructuur, data en systemen. Waar autonomie gaat over handelingsvrijheid, gaat soevereiniteit over zeggenschap.

Deze afhankelijkheid speelt zich op verschillende technologielagen af, van fysieke laag naar netwerken, cloud afwegingen tot aan applicaties zoals AI³. Daarnaast is aandacht nodig voor het soevereiniteitsrisico dat buitenlandse (veiligheids) diensten data opvragen wanneer de clouddienst door een buitenlands bedrijf wordt geleverd. Zo geeft de CLOUD Act de Amerikaanse overheid vergaande bevoegdheden om toegang te krijgen tot data van Europese burgers. Ook de Chinese overheid heeft wetgeving waarmee het toegang tot data bij bedrijven kan afdwingen⁴. Dit vraagt om gerichte beleidsontwikkeling, aanpassing van inkoop- en leveranciersbeleid en versterking van ICT kennis en vaardigheden binnen de organisatie.

² AIVD jaarverslag 2025

³ Position paper digitale autonomie, oktober 2025, VNG

⁴ Het rijk in de cloud, Algemene rekenkamer, 2025



Het is de verwachting dat AI impact gaat hebben op de werkzaamheden binnen VNOG. Voorheen werd bij automatisering vooral repetitief werk vervangen, met AI breidt dit zich uit naar kenniswerkers. Werkzaamheden zoals taalkundige taken, assisteren en administreren, dataverzameling, -productie en -analyse, visuele analyse en advies- en besluitvorming worden genoemd als taken die geheel of gedeeltelijk door AI kunnen worden overgenomen⁵. Hierdoor kan het werk in de toekomst ook veranderen, zoals de manier waarop desinformatie gevalideerd wordt, of hoe risicoanalyses uitgevoerd worden. VNOG zal de mogelijkheden van AI in de breedte onderzoeken, met aandacht voor de potentiële risico's en ethische consequenties van het gebruik van AI.

Tot slot vraagt de ontwikkeling van het personeelsbestand om aandacht. A&O onderzoek identificeert drie belangrijke ontwikkelingen voor 2035: vergrijzing, krapte op de arbeidsmarkt en een toenemende werkdruk voor de werknemers⁶. Dit rapport is opgesteld voor gemeenten, maar we kunnen als Veiligheidsregio dezelfde ontwikkelingen verwachten. Kennismanagement wordt daardoor belangrijker om specifieke kennis en ervaring te behouden. Tegelijkertijd treedt een nieuwe generatie medewerkers toe met andere verwachtingen ten aanzien van technologie. VNOG ondersteunt zowel huidige als toekomstige medewerkers met passende ICT-middelen en voorzieningen, zodat zij hun werk effectief en toekomstbestendig kunnen uitvoeren.

⁵ Op weg naar AI die werkt voor iedereen, UWV, 2025

⁶ Toekomst van de arbeidsmarkt, januari 2026, A&O

Kernambitie

De kernambitie van VNOG is: samen werken aan veiligheid. VNOG wil werken vanuit een sterke informatiepositie en heeft als doel: “het leveren van duidelijke informatie, die VNOG verzamelt, duidt en verspreidt waardoor zorg en hulp verbeteren⁷”. Dit doen we door op een (cyber) veilige manier informatie bij elkaar brengen, duiden en beschikbaar stellen aan medewerkers, partners en de omgeving, in de juiste vorm op het juiste moment. VNOG trekt daarbij op met strategische partners in de regio, interregionaal, nationaal en internationaal.

Dit doen we door de informatievoorziening betrouwbaar, beschikbaar, verbonden en betekenisvol in te richten.



AI-gegenereerde illustratie



Betrouwbaar: we kunnen handelen naar de verstrekte informatie.

We kunnen erop vertrouwen dat de informatie juist, actueel, consistent en uitlegbaar is, ook onder tijdsdruk en onzekerheid. Informatie is herleidbaar en verantwoordbaar richting bestuur, burger en partners. De inzet van data, dashboards en AI is transparant en de kwaliteit en context van informatie wordt bewaakt ondanks complexiteit, desinformatie en technologische versnelling. In bepaalde situaties kan het noodzakelijk zijn om met minder betrouwbare informatie te werken: de gebruiker moet dan inzicht hebben in de mate van onbetrouwbaarheid. Onze informatievoorziening is goed beveiligd, passend bij onze kritieke rol in de samenleving.



Verbonden: we kunnen ervan uitgaan dat alles logisch op elkaar aansluit.

We kunnen informatie samenhangend delen en combineren binnen de organisatie en met ketenpartners of op landelijk niveau, op een veilige en gestandaardiseerde manier. We vermijden eilandautomatisering en werken zoveel mogelijk met goed op elkaar aansluitende oplossingen. Dit doen we door architectuurkeuzes te maken die standaardisatie ondersteunen zonder flexibiliteit te verliezen. We zijn verbonden met onze medewerkers en zorgen ervoor dat informatie gebruiksvriendelijk aangeboden wordt. Als Veiligheidsregio zijn we onderdeel van een bredere maatschappelijke opgave, daarom werken we zoveel mogelijk samen met ketenpartners, Oost 5, landelijk en met internationale partners. De gemeenten zijn hier belangrijke samenwerkingspartners, die nauw verbonden moeten blijven bij onze IV.



Beschikbaar: we hebben toegang wanneer dit nodig is.

We kunnen informatie en systemen tijdig en continu toegankelijk houden wanneer dat nodig is, met name tijdens crises, verstoringen of personele uitval. Hierbij gebruiken we een risico-gerichte aanpak om te bepalen welke systemen en informatie kritisch zijn, en geven duidelijkheid over de beschikbaarheid die de organisatie kan verwachten voor de verschillende risico-categorieën. Kritische informatie blijft ook bij uitval van systemen of verbindingen beschikbaar doordat we een continuïteitsbeleid hebben dat voorziet in hybride, backup en analoge voorzieningen. We richten 24x7 support in voor de eigen organisatie en de te ondersteunen externe partners.



Betekenisvol: we begrijpen wat informatie betekent en gebruiken deze verantwoord.

Informatie is niet alleen beschikbaar en betrouwbaar, maar wordt ook begrepen, geduid en gebruikt voor handelen. Informatie krijgt pas waarde wanneer deze in de juiste context wordt geplaatst en leidt tot duidelijke, uitlegbare keuzes voor medewerkers, burgers, bestuur en partners. VNOG medewerkers gebruiken hierbij hun menselijk oordeel en kritisch denkvermogen om informatie te wegen, onzekerheden te erkennen en de juiste keuzes te maken, ook onder druk. Technologie kan dit proces ondersteunen, maar de mens blijft verantwoordelijk voor de interpretatie en het handelen. Dit vraagt dat VNOG actief investeert in ethisch bewustzijn, duiding, transparantie en het versterken van informatievaardigheden.

Landelijke ontwikkelingen

VNOG acteert binnen een landelijke context samen met 24 andere Veiligheidsregio's, het NIPV en vele ketenpartners. Op dit vlak zien we een aantal belangrijke ontwikkelingen:

Toenemende digitalisering van de overheid

Digitalisering is een structurele ontwikkeling die het functioneren van de overheid in toenemende mate beïnvloedt. De Nederlandse Digitaliseringsstrategie (NDS) beschrijft zes samenhangende prioriteiten. Daarbij wordt ingezet op cloud voorzieningen (online opslag- en/of werkomgeving) die voldoende controle en continuïteit bieden voor kritieke processen, het verantwoord delen en benutten van data via een federatief datastelsel en het verantwoord benutten van de mogelijkheden van AI. Daarnaast besteedt de strategie aandacht aan hoe burgers & ondernemers de digitale dienstverlening ervaren, het belang van digitale weerbaarheid & autonomie, en het digitaal vakmanschap van ambtenaren en een moderne werkomgeving.



De prioriteiten vanuit de NDS houden in dat VNOG expliciet moet sturen op controle over digitale afhankelijkheden, betrouwbare gegevensuitwisseling en verantwoorde inzet van AI, met blijvende aandacht voor weerbaarheid en (IV) vakmanschap.

Professionalisering van de Veiligheidsregio's

De evaluatie van de Wet Veiligheidsregio's heeft in 2023 geleid tot het voornemen om drie samenhangende opgaven in verbinding met elkaar uit te voeren, ook aangeduid als de drie grote werken. Zij richten zich op het versterken van de (boven)regionale crisisbeheersing en de daaraan gerelateerde informatievoorziening, het verbeteren van het brandweeronderwijsstelsel en het realiseren van een toekomst vaste brandweezorg. Binnen het grote werk gericht op crisisbeheersing wordt het belang van informatievoorziening expliciet benoemd, waarbij informatiegestuurd werken wordt gezien als randvoorwaarde voor effectieve coördinatie en besluitvorming. Ook het grote werk rond brandweezorg voorziet in een vernieuwing van de brandweerdoctrine, waarbij wordt verwacht dat informatie gestuurde brandweezorg een steeds prominentere rol zal innemen.

De informatievoorziening van de VNOG moet aansluiten op de landelijke grote werken en de daarin gekozen ontwikkelrichting.

Meer landelijke sturing

De Raad van Commandanten en Directeuren Veiligheidsregio (RCDV) stuurt steeds meer aan op scherpere gezamenlijke keuzes te maken, de bovenregionale samenwerking te versterken en te werken vanuit één verhaal en één koers. In 2026 zijn deze doelstellingen breed gecommuniceerd onder de noemer "kracht van het collectief". Deze sterkere landelijke sturing kan in gaan houden dat er meer landelijke standaardisatie op processen en informatiesystemen gaat komen. VNOG sluit zoveel mogelijk aan op deze ontwikkelingen, met als uitgangspunt: "regionaal wat moet, landelijk wat kan". Dit houdt in dat VNOG bij voorkeur landelijk oppakt wat mogelijk is en hier de regionale informatievoorzieningen op aan laat sluiten.

Meer strategische rol van informatievoorziening

In juni 2024 is door de RCDV besloten de strategische sturing op informatievoorziening (IV) te versterken. Ook de GHOR heeft als doelstelling om een excellente informatiepositie voor de Directeur Publieke Gezondheid (DPG) te creëren. Veiligheidsregio's hebben hierin een eigen opgave om IV op strategisch niveau te organiseren, terwijl gelijktijdig is verkend hoe landelijke samenhang en gezamenlijke slagkracht kunnen worden vergroot. Dit heeft geleid tot drie ontwikkelingen: de oprichting van een vakraad IV, de inrichting van een landelijke CIO Office, en de start van het Masterprogramma IV 2025-2030. Dit masterprogramma bundelt bestaande en nieuwe initiatieven op het gebied van informatievoorziening. De activiteiten zijn geordend langs vijf programmalijnen: Informatie Gestuurde veiligheid, Informatiegestuurde Missiekritische Communicatie, Data & Infrastructuur, Informatie-veiligheid en Digitaal Fitte Organisatie.

Deze ontwikkeling betekent dat VNOG haar informatievoorziening moet positioneren op strategisch niveau en expliciet moet aansluiten op landelijke kaders en keuzes. De afhankelijkheid van gezamenlijke IV-ontwikkelingen neemt daarmee toe, terwijl ruimte nodig blijft voor regionale invulling en prioritering.



Strategische opgaven

VNOG staat de komende jaren voor een aantal samenhangende strategische opgaven die direct de IV raken. Maatschappelijke, technologische en geopolitieke ontwikkelingen vergroten de complexiteit van het werkveld. Deze opgaven versterken elkaar en vragen om een integrale aanpak.

De invloed van geopolitiek

Geopolitieke spanningen en toenemende cyberdreiging vergroten het belang van informatieveiligheid en continuïteit. Daarnaast stellen Europese wet- en regelgeving en internationale afhankelijkheden nieuwe eisen aan de informatievoorziening. VNOG moet binnen deze context de veiligheid, continuïteit en autonomie van haar informatievoorziening waarborgen. Dit vraagt om strategische keuzes ten aanzien van leveranciers, architectuurprincipes, aandacht voor cloudbeleid en open standaarden en het versterken van de weerbaarheid en compliance binnen IV.

Technologie als kans en risico

Technologische ontwikkelingen zoals data-analyse, sensoren, AI en digitale simulaties bieden kansen voor betere voorbereiding en hulpverlening. Tegelijkertijd nemen afhankelijkheden en risico's toe, met name op het gebied van informatieveiligheid en continuïteit. VNOG moet daarom technologische innovaties gericht gaan benutten, waarbij de risico's beheersbaar blijven. Dit vraagt om duidelijke kaders, bewuste architectuurkeuzes, balans tussen gebruiksgemak, veiligheid en continuïteit, en aandacht voor ethiek. Daarnaast vraagt dit om structurele aandacht voor weerbaarheid, zodat de organisatie bestand is tegen verstoringen en zich snel kan herstellen. Fallback-systemen worden ingericht, zodat de dienstverlening kan doorgaan wanneer digitale systemen uitvallen.

Crises en brandweerprocessen worden complexer en diverser

Crises en brandweerprocessen worden complexer en diverser. Extreem weer vergroot het risico's op bijvoorbeeld natuurbrand en wateroverlast, en nieuwe technologieën leiden tot nieuwe risico's zoals accubranden en continuïteitsvraagstukken. Tegelijkertijd beïnvloeden maatschappelijke ontwikkelingen, zoals polarisatie en desinformatie, het optreden van hulpdiensten. De informatiebehoefte neemt hierbij toe. Burgers, bestuur en ketenpartners verwachten snelle, betrouwbare en uitlegbare informatie. Dit versterkt de strategische rol van IV in zowel de voorbereiding als tijdens incidenten. IV is daarmee niet langer ondersteunend, maar een randvoorwaarde voor effectief en verantwoord optreden.

Groeiende strategische rol van IV

Een sterke informatiepositie is een van de leidende opgaven van VNOG. De hierboven genoemde landelijke ontwikkelingen onderstrepen verder het strategisch belang van IV. Dit stelt VNOG voor de opgave om IV structureel te positioneren als een strategisch domein dat sturing, besluitvorming en verantwoording mogelijk maakt. Dit vraagt om samenhangende sturing op IV, een nauwe verbinding met het primaire proces en versterking van informatiesturing binnen VNOG.

Professionaliseren van bedrijfsvoering

De ontwikkeling van het Veiligheidscentrum Apeldoorn betekent dat VNOG ook dienstverlening gaat leveren aan veiligheidspartners. Hierdoor ondersteunt VNOG niet alleen de eigen organisatie, maar ook (delen van) bedrijfsprocessen van andere organisaties. VNOG moet daarom de bedrijfsvoering professionaliseren en standaardiseren, zodat deze geschikt is voor dienstverlening aan meerdere organisaties met verschillende behoeften. Dit vraagt om een uniforme en procesmatige inrichting van bedrijfsvoering en een robuuste informatievoorziening. Daarnaast vraagt dit om duidelijke afspraken over rollen, verantwoordelijkheden en sturing tussen VNOG en betrokken partners.

De mens samen met technologie

Digitalisering vraagt om andere kennis en vaardigheden van medewerkers. Kennisverlies dreigt door vergrijzing, terwijl een nieuwe generatie andere, nieuwere digitale werkwijzen meebrengt. Daarnaast zien we de ontwikkeling dat de technologie versnelt, maar dat de mens moet blijven oordelen. Dit vraagt dat VNOG medewerkers goed om kunnen gaan met nieuwe technologieën en hier de bijpassende verantwoordelijkheden voor hebben. Dit stelt VNOG voor de opgave om structureel te investeren in vakbekwaamheid, digitale fitheid en bewust handelen binnen de informatievoorziening. Dat vraagt om aandacht voor opleiding, kennisdeling en bewustwording bij zowel IV-medewerkers als gebruikers, zodat technologie verantwoord, effectief en toekomstgericht kan worden ingezet.



6

Digitalisering vraagt om andere kennis en vaardigheden van medewerkers.

Toenemende druk op capaciteit en budget

Arbeidsmarktkrapte, stijgende kosten, andere licentiestructuren en onzekerheden in budgetten kunnen de beschikbare capaciteit en middelen onder druk gaan zetten. Dit kan de ruimte voor innovatie en ontwikkeling beperken en vraagt om scherpe en samenhangende keuzes. Het is belangrijk dat VNOG ook onder deze omstandigheden wendbaar en toekomstbestendig blijft. Dat vraagt om slim gebruik van technologie, om meer centrale sturing op standaardisatie, programma- en projectmanagement en in bepaalde gevallen bewust kiezen om bepaalde projecten niet te doen of uit te stellen, zodat capaciteit gericht ingezet wordt op activiteiten met de meeste toegevoegde waarde en / of urgentie voor VNOG.

Strategische dilemma's

Het werken aan de strategische opgaven binnen de eerder beschreven toekomstvisie en landelijke ontwikkelingen maakt dat VNOG met bepaalde waardenspanningen werkt, die strategische dilemma's opleveren. Momenteel wordt hier nog versnipperd naar gekeken binnen VNOG, vaak zal er ook niet altijd één beste keuze zijn. VNOG moet hier transparante en weloverwogen besluiten nemen.

Digitale autonomie versus totale gebruikers-ervaring

Bij de keuze voor applicaties weegt VNOG steeds vaker af of deze passen binnen de strategie voor digitale autonomie. Op dit moment werkt VNOG, net als andere Veiligheidsregio's, bijvoorbeeld veel met Microsoft-producten. Deze zijn vertrouwd voor gebruikers en beheerders. Stoppen met deze producten heeft daarom grote gevolgen. Gebruikers moeten anders gaan werken en ICT-medewerkers hebben nieuwe kennis en vaardigheden nodig. In het verleden is bewust gekozen voor een Microsoft-strategie. Bij nieuwe keuzes kijken we breder. We nemen ook de impact op digitale autonomie en soevereiniteit mee. Dit kan betekenen dat we vaker kiezen voor alternatieven, bijvoorbeeld van Europese aanbieders. Dit kan leiden tot een minder uniform applicatielandschap. Ook kan dit meer vragen van gebruikers en beheerders, bijvoorbeeld extra training en ondersteuning. Dit vraagt dus extra inspanningen op het gebied van digitale fitheid van de VNOG medewerkers.

Kopen versus ontwikkelen

Bij de inrichting van de informatievoorziening volgt VNOG in principe de lijn van de Veiligheidsregio Referentie Architectuur (VeRA): kopen gaat voor zelf ontwikkelen. Dit betekent dat waar mogelijk wordt gekozen voor bestaande, bewezen oplossingen. De snelle ontwikkeling van AI zorgt echter voor nieuwe mogelijkheden waarvoor nog niet altijd kant-en-klare producten beschikbaar zijn. Dit vraagt om zorgvuldige afwegingen. VNOG heeft innovatie hoog in het vaandel staan en kiest daarbij soms bewust voor zelf ontwikkelen of co-creatie met leveranciers, in plaats van af te wachten tot de markt passende oplossingen biedt. Wanneer VNOG kiest voor (mee) ontwikkelen, is het van belang dat het beheer van deze toepassingen goed wordt ingericht. Dit voorkomt afhankelijkheden en zorgt ervoor dat oplossingen duurzaam en veilig gebruikt kunnen worden.

Landelijk versus regionale initiatieven

Bij de ontwikkeling van oplossingen hanteert VNOG het uitgangspunt: "regionaal wat moet, landelijk wat kan". Dit sluit aan bij de landelijke ambitie van de Kracht van het Collectief van de RCDV en de inzet van de vakraad IV om de gezamenlijke slagkracht te vergroten. De keuze voor landelijk kan in bepaalde gevallen leiden tot een (tijdelijke) terugval in functionaliteit, met name in situaties waar een Veiligheidsregio een koploper is. Tegelijkertijd geldt dat innovatieve toepassingen, zoals AI, vaak beter tot stand komen in een kleinschalige en afgebakende omgeving. Zolang dit niet mogelijk is in een landelijke omgeving, zal dit regionaal plaats vinden. Per toepassing maakt VNOG een bewuste afweging tussen landelijke en regionale ontwikkeling. Hierbij wordt gekeken naar snelheid, schaalbaarheid en samenwerking. Wanneer gekozen wordt voor regionale ontwikkeling, worden de mogelijkheden voor opschaling vanaf het begin meegenomen. Dit zorgt ervoor dat succesvolle toepassingen later breder ingezet kunnen worden.



Regionaal wat moet,
landelijk wat kan.

Beveiliging versus gebruikersgemak

VNOG streeft naar een hoge mate van beveiliging van informatiesystemen, passend bij de rol als vitale organisatie. De toenemende geopolitieke spanningen en cyberdreigingen maken dit noodzakelijk. Beveiliging is daarom een randvoorwaarde voor de continuïteit en betrouwbaarheid van de organisatie. Tegelijkertijd moet de beveiliging in balans zijn met het gebruiksgemak. Medewerkers van VNOG werken vaak onder druk en in bijzondere omstandigheden, waarbij snelle en eenvoudige toegang tot informatie essentieel is. Daarom wordt bij beveiligingsmaatregelen nadrukkelijk gekeken naar de impact op de eindgebruiker. VNOG zoekt hierin actief de balans tussen veiligheid en werkbaarheid, zodat medewerkers hun werk effectief en veilig kunnen uitvoeren.

Vooruitstrevende of behoudende digitale fitheid

Bij de inrichting van de informatievoorziening staat VNOG voor de keuze tussen het vooruitstrevend of behoudend invullen van digitale fitheid. Vertrouwde, algemeen gebruikte applicaties bieden gebruiksgemak en zorgen ervoor dat medewerkers snel en effectief kunnen werken, zeker in operationele situaties. Deze oplossingen sluiten goed aan bij de bestaande kennis en ervaring binnen de organisatie. Tegelijkertijd vraagt de verdere digitalisering, met name bij de inzet van data en AI, om het gebruik van meer gespecialiseerde en soms complexere toepassingen. Deze bieden vaak meer mogelijkheden, maar vragen ook andere vaardigheden van medewerkers zoals kritisch denken en het duiden van de uitkomsten. VNOG zoekt hierin een balans waarbij ingezet wordt op gebruiksvriendelijke oplossingen, maar ook gericht geïnvesteerd wordt in het vergroten van de digitale fitheid van medewerkers, zodat zij ook met meer geavanceerde toepassingen kunnen werken.



Strategische thema's en doelstellingen

VNOG wil invulling gaan geven aan deze strategische visie middels drie strategische thema's, namelijk:

- **De wendbare organisatie:** VNOG ondersteunt snel en passend bij voorbereiding en inzet. Dit vraagt om goede informatievoorziening en effectieve samenwerking
- **Een stevig digitaal fundament:** informatie en systemen zijn betrouwbaar, veilig en beschikbaar, ook in situaties van verstoring.
- **Menselijke maat:** informatievoorziening is begrijpelijk, werkbaar en verantwoord. Medewerkers kunnen hiermee werken en blijven eindverantwoordelijk voor het handelen.

De volgende strategische doelen zijn gesteld binnen deze thema's voor 2031. Deze zijn geordend naar strategisch thema, zonder onderlinge prioritering. De doelen binnen de thema's “stevig digitaal fundament” en “menselijke maat” zijn in veel gevallen randvoorwaardelijk voor het realiseren van de doelen binnen “wendbare organisatie”.



Gedeeltelijk AI-gegenereerde illustratie

De wendbare organisatie

1. Verdere uitbouw van gedeeld digitaal operationeel beeld

Nieuwe technologieën zoals AI, sensordata en digital twins maken het mogelijk om het gedeeld operationeel beeld verder uit te bouwen.

Real-time data verwerking speelt hierbij een steeds grotere rol. Een goede verbinding met de meldkamer blijft hierbij essentieel. VNOG onderzoekt in 2026 de mogelijkheid om een Team Digitale Verkenningen in te richten, met focus op de inzet van drones en sensoren. Hiermee wordt de informatiepositie voor het gedeeld operationeel beeld verder versterkt. Ook werken we verder aan het uitwisselen van bovenregionale en internationale beelden, onder andere door het gebruik van open standaarden. Landelijke initiatieven, zoals de Landelijke Voorziening Crisisbeheersing (LVCb) zijn hierbij leidend. VNOG zet in op nauwe samenwerking met Oost5partners en Duitsland om te komen tot een samenhangend en grensoverstijgend informatiebeeld.

2. VNOG als informatiemakelaar

De toenemende informatiebehoefte van burgers, bestuur en ketenpartners aan snelle, betrouwbare en uitlegbare informatie vraagt om een sterke rol van VNOG als informatiemakelaar, in de koude en warme situatie. VNOG BI- en geo-omgeving vormt de basis, daarnaast is de mogelijkheid tot vastlegging van contactgegevens van ketenpartners belangrijk. Het Veiligheidsinformatie knooppunt (VIK) ontwikkelt zich door, waarbij steeds meer gebruik wordt gemaakt van AI-toepassingen voor actuele, dynamische risicoanalyses, zowel regionaal als in Oost5 en landelijk verband. Tijdens de warme fase wordt de opgebouwde informatiepositie ook gebruikt in het gedeeld operationeel beeld. Er kan snel een passende informatieomgeving worden ingericht die direct inzetbaar is bij een nieuwe crisis. Goede digitale geoefendheid en beschikbaarheid en toegankelijkheid van systemen zijn hierbij belangrijk. Hierbij sluiten wij aan bij de Nederlandse Digitaliseringsstrategie, waarin het verantwoord delen en benutten van data een belangrijk uitgangspunt vormt. Wij verzamelen en gebruiken alleen data die noodzakelijk zijn

voor de uitvoering van onze wettelijke taken en maken steeds een bewuste afweging of dit past binnen onze ethische, juridische, privacy- en informatieveiligheidskaders.

3. Accurate stuurinformatie

Betere stuurinformatie stelt VNOG in staat om gericht keuzes te maken in de aansturing en prioritering van de organisatie. De Key Performance Indicatoren (KPI's) worden bepaald in de vakafdelingen en vormen de basis voor dashboards en analyses. De centralisatie van de informatieorganisatie leidt tot een meer uniforme werkwijze, met vaste processen en heldere kwaliteitsstandaarden. Hierbij willen we flexibiliteit behouden, maar wildgroei voorkomen.

4. Goede ondersteuning van het Veiligheidscentrum voor heel VNOG

Het nieuw te bouwen Veiligheidscentrum wordt naar verwachting eind 2028, begin 2029 opgeleverd. Vanaf dat moment ondersteunt Bedrijfsvoering naast de interne organisatie ook externe partners. Deze ontwikkeling vraagt om een verdere professionalisering van de bedrijfsvoering. Procesmatig werken wordt daarbij leidend en er kunnen aanvullende verplichtingen ontstaan op het gebied van certificering en auditing. De bedrijfsvoering-processen en -systemen worden ingericht zodat meerdere organisaties effectief en integraal kunnen worden ondersteund.



Een stevig digitaal fundament

5. Goed beheerde centrale datavoorziening

De vier doelstellingen van de wendbare organisatie steunen op een goed beheerde, centrale datavoorziening. Deze datavoorziening kan zowel landelijk, op Oost5 en op regionaal niveau ingericht worden. De datasets die beheerd worden in de centrale datavoorziening zijn geclassificeerd en worden beheerd conform de BIV (beschikbaarheid, integriteit en vertrouwelijkheid) standaard.

De dataclassificatie is zodanig ingericht dat de zogenoemde “kroonjuwelen” inzichtelijk zijn. Voor deze gegevens gelden aangescherpte eisen op het gebied van integriteit, beschikbaarheid en informatiebeveiliging. Hiermee borgt VNOG dat kritieke informatie betrouwbaar, veilig en continu beschikbaar is.

6. Werken met architectuur

VNOG gaat Enterprise Architectuur als centrale kapstok gebruiken ter ondersteuning van de strategische rol van IV en het verder professionaliseren van de bedrijfsvoering. Architectuur zorgt ervoor dat keuzes niet op zichzelf staan, maar aansluiten op de visie van VNOG en bijdragen aan een consistent en toekomstbestendig geheel. Hiermee wordt voorkomen dat losse oplossingen en dubbelingen ontstaan en wordt gestuurd op standaardisatie, hergebruik en interoperabiliteit. Dit ondersteunt VNOG in haar rol als informatie-makelaar, doordat informatie zo makkelijker gedeeld kan worden.

7. Beveiliging & continuïteit passend bij de rol van vitale aanbieder

Op 10 juli 2025 heeft de minister van Justitie en Veiligheid de veiligheidsregio's aangewezen als vitale aanbieder voor verschillende processen, waaronder de communicatie- en informatievoorziening voor hulpdiensten en crisispartners. Dit betekent dat VNOG haar digitale weerbaarheid en continuïteit aantoonbaar op orde moet hebben. VNOG werkt toe naar het behalen van volwassenheidsniveau 3 van de Baseline Informatiebeveiliging Overheid (BIO) eind 2027 en niveau 4 eind 2029. VNOG richt eind 2028 een ISMS (information security management system) kwaliteitsproces in voor

de continue bewaking van de beveiligingsnorm. Dit proces identificeert, analyseert en mitigeert structureel de risico's op het gebied van informatiebeveiliging, passend bij de rol van vitale aanbieder. Daarnaast zal VNOG zich eind 2028 ISO 27001 certificeren, mede ter voorbereiding voor de rol als externe service provider. Hierbij blijft het belangrijk om de beveiligingsmaatregelen goed af te wegen tegen gebruiksgemak, rekening houdende met de operationele taken van VNOG.

8. Meer centrale aansturing op de IV organisatie

Het in begin 2026 opgestelde rapport “Informatie als fundament” adviseert een sterkere centrale regie op IV. Hierbij wordt ingezet op het centraliseren van functioneel beheer en de Business Intelligence (BI), goede data governance en het inrichten van een CIO office. Er wordt aandacht gevraagd voor het gebruik van een enterprise architectuur als kapstok voor de IV, meer eenduidig opstellen en naleven van beleid en kaders, centrale monitoring van nieuwe en bestaande digitale wetgeving en het inrichten van project- en portfolio management. Belangrijke beleidsmatige aandachtsgebieden voor de komende jaren zijn onder andere AI, digitale autonomie en soevereiniteit, schaalbaarheidseisen en cloud ontwikkelingen.

9. Digitale autonomie en soevereiniteit

VNOG versterkt haar digitale autonomie en soevereiniteit om onafhankelijk en weerbaar te kunnen opereren in een steeds digitaler en geopolitiek complexer landschap. VNOG kan dit niet alleen en zal hierbij met name leunen op “de kracht van het collectief”, dus op landelijke initiatieven. Daarnaast maakt VNOG bewuste keuzes in het gebruik van technologie, leveranciers en cloud voorzieningen, met aandacht voor Europese alternatieven en open standaarden. VNOG bereid hierop voor door te investeren in kennis en vaardigheden om deze nieuwe technologieën te kunnen voeren en gebruiken, en om verantwoorde keuzes te maken binnen de kaders van wet- en regelgeving. Hierbij wordt een balans gezocht tussen digitale autonomie en gebruiksgemak passend bij de operationele functie van de organisatie, waarbij we accepteren dat we af en toe terug gaan in gebruiksgemak.

Menselijke maat

10. Digitale fitheid.

De snelle digitale ontwikkelingen vragen om voortdurende aanpassing van kennis en vaardigheden. Met name AI kan grote invloed hebben op de manier van werken en brengt nieuwe vraagstukken met zich mee, zoals het goed omgaan met desinformatie. VNOG ondersteunt medewerkers bij het versterken van hun digitale vaardigheden. Tegelijkertijd vraagt de instroom van een nieuwe generatie medewerkers, die digitaal is opgegroeid, om passende ondersteuning. VNOG bouwt voort op deelname aan de “Maand van de Digitale Fitheid” en ontwikkelt dit door naar een structurele aanpak. Daarbij is ook aandacht voor het versterken van digitaal leiderschap binnen het managementteam en bij teamleiders.



De snelle digitale ontwikkelingen vragen om voortdurende aanpassing van kennis en vaardigheden.

11. IV is van iedereen

Informatievoorziening is een gezamenlijke verantwoordelijkheid van de hele organisatie en niet uitsluitend van de afdeling Informatievoorziening. Met de ambitie van VNOG om informatie gestuurd te werken en de vitaal verklaring van communicatie- en informatievoorzieningsprocessen, zijn alle afdelingen medeverantwoordelijk voor de kwaliteit en goede vastlegging van informatie, zodat er bij besluiten vertrouwd kan worden op de juistheid hiervan. De toepassing van nieuwe technologieën zoals AI vraagt dat VNOG komende jaren meer aandacht besteedt aan het ethisch bewustzijn en data-geletterdheid van haar medewerkers, passend bij het gebruik van dit soort toepassingen. Steeds meer aandacht is nodig om invulling te geven aan het werkconcept van “mens met technologie”, waarbij ook vanuit de vak inhoud gekeken wordt hoe nieuwe technologieën kunnen ondersteunen bij de werkzaamheden. Dit vereist om een meer strategische positionering van IV binnen VNOG, waarbij IV een integrale verantwoordelijkheid wordt binnen de organisatie.



De blusrobot van Veiligheidsregio Zuid-Limburg.

Randvoorwaarden

De hierboven beschreven strategische visie met bijbehorende doelstellingen voor de komende vijf jaren is ambitieus en is meer dan alleen een “technisch traject”. Deze visie beschrijft een veranderopgave voor de gehele organisatie, waar de afdeling informatievoorziening hand in hand optrekt met de rest van de organisatie. Deze verandering wordt ingezet in een omgeving van meer en complexere crises en brandweerinzetten, en schaarste in capaciteit en budget. Dit vraagt een meer gestructureerde manier van samenwerken, waarbij scherpe keuzes gemaakt moeten worden. Slimmer omgaan met capaciteit houdt ook in dat er op andere manieren gekeken moet worden naar samenwerkingsvormen met ketenpartners, Oost 5 of landelijk, die ook allemaal voor gelijksoortige uitdagingen staan.

Om deze veranderopgave beheerst te realiseren, zijn enkele randvoorwaarden essentieel. Dit vraagt om duidelijke sturing en governance op de informatievoorziening, een samenhangende architectuur die richting geeft aan keuzes en standaardisatie, en het structureel borgen van informatiebeveiliging en continuïteit passend bij de rol van vitale aanbieder. Daarnaast zijn goed ingericht datamanagement, heldere afspraken over rollen en verantwoordelijkheden en blijvende investering in digitale vaardigheden noodzakelijk om de ambities duurzaam te kunnen realiseren. Dit alles moet bereikt worden terwijl de huidige dienstverlening door blijft lopen. Tegelijkertijd blijft ruimte voor innovatie essentieel, om zo ook de kansen van nieuwe technologieën te kunnen gebruiken. Op deze manier werkt VNOG naar een informatievoorziening die beschikbaar, betrouwbaar, verbonden en betekenisvol is.



AI-gegenereerde illustratie

Verantwoording

AI is gebruikt om deze tekst leesbaarder te maken.

De verantwoordelijkheid voor de tekst ligt volledig bij de auteur.

Publicatiedatum: September 2026