



# Collectiveringsvoorstel Digitale Veiligheid

Opdracht tot uitwerking

**Vereniging van Nederlandse Gemeenten**

Nassaulaan 12  
2514 JS Den Haag  
070 373 83 93

[info@vng.nl](mailto:info@vng.nl)

Auteurs: Kato Vierbergen (e.a.)  
Datum: 31 oktober 2025

# Opdracht tot Uitwerking (OtU) Digitale Veiligheid

## **Oproep: Gemeenten zetten nu collectief in op het versterken van de digitale weerbaarheid**

De geopolitieke ontwikkelingen leveren voor gemeenten toenemende complexe dreigingen. Gemeenten moeten zich voorbereiden op militaire en hybride dreigingen en hun digitale en maatschappelijke weerbaarheid versterken. Naast cyberdreigingen zoals ransomware aanvallen door criminelen en statelijke actoren, incidenten bij leveranciers, datalekken zien we moedwillige verstoring van vitale processen met maatschappelijke impact en essentiële gemeentelijke diensten die onder druk komen te staan. De digitale samenleving vraagt om bescherming van publieke waarden, privacy en het vertrouwen van inwoners en ondernemers in de overheid en de rechtstaat.

Naast deze groeiende digitale weerbaarheidsrisico's staan gemeenten ook onder druk door tekorten op de arbeidsmarkt, en een toenemende afhankelijkheid van grote (niet-Europese) technologieleveranciers. Versnipperde sourcing en de complexiteit van wet- en regelgeving vergroten deze kwetsbaarheden. Collectivering biedt mogelijkheden voor de gemeentelijke uitvoeringskracht, de digitale weerbaarheid en helpt bij het borgen van publieke waarden.

## **Doel van de opdracht tot uitwerking (otu)**

Met deze otu vragen we de ALV om steun en mandaat om de digitale veiligheid collectief te organiseren. Concreet vragen we om instemming met de voorgestelde visie, de scope en richting, en toestemming om deze verder uit te werken tot een volwaardig collectiviseringsvoorstel met deelvoorstellen (inclusief governance- en financieringsopties, sourcingstrategie en aansluiting op de thema's Cloud en AI).

Deze opdracht stelt gemeenten in staat om als één sterke bestuurslaag regie te nemen op de digitale veiligheid, door samen - collectief - de aanpak, uitvoering en dienstverlening te organiseren.

## **Visie**

Digitale Veiligheid is de norm!

De stip op de horizon is de [Agenda digitale veiligheid 2028](#). Als onderdeel van de [Digitale Agenda Gemeenten 2028](#) zien gemeenten de kans om gezamenlijk de digitale veiligheid van gemeentelijke dienstverlening, de voorbereiding op digitale ontwrichting en online aangejaagde ordeverstoringen én de digitale weerbaarheid van inwoners en ondernemers te verbeteren.

Doel is veilige, robuuste overheidsdienstverlening die privacy waarborgt en het vertrouwen in de overheid vergroot.

## **Scope**

Geopolitieke spanningen en een tekort aan expertise maken samenwerking noodzakelijk. Tegelijkertijd biedt dit ook mogelijkheden om voor die nieuwe taken een collectieve aanpak uit te

werken. Denk aan de taken in de voorbereiding op digitale ontzorging, gerichte cybercrisis-oefeningen zoals we al kennen voor de fysieke veiligheid (opleiding, training en oefening), het versterken van de weerbaarheid van inwoners en ondernemers tegen cybercriminaliteit én verantwoorde inzet van technologie, zoals AI in het veiligheidsdomein.

Aankomende wetgeving vraagt om versterking van de digitale weerbaarheid van de gemeentelijke dienstverlening, verscherpt leveranciersmanagement, strengere beveiliging van gevoelige informatie (persoonsgegevens, strafrechtelijke gegevens) en versterking van de informatieveiligheid van kritieke infrastructuur, zoals de aansturing van bruggen, sluisen, verwerking van afvalwater en verkeerbeheer (Operationele Technologie-systemen).

Door collectivisering kunnen gemeenten ontzorgd worden. De [Informatiebeveiligingsdienst \(IBD\)](#) heeft zich als concrete collectieve dienst de afgelopen jaren al bewezen. Gemeenten gebruiken de [Eenduidige Normatiek Single Information Audit \(ENSIA\)](#) voor verantwoording over informatieveiligheid, worden ondersteund door het ENSIA-team en werken samen in één tool bij VNG. Het Gemeentelijk Gemeenschappelijk Infrastructuur inkoop-portfolio '[GGI-Veilig](#)' is een mantelcontract, waarmee gemeenten gemakkelijk informatiebeveiligingsdiensten en -producten kunnen afnemen, zoals een actieve monitoring en response-dienst voor het bewaken van gedrag en acties op het eigen bedrijfsnetwerk, beveiligingsproducten voor de gemeentelijke ICT-infrastructuur (zoals firewalls, anti-DDoS, end-point protection) of beveiligingsexpertise-diensten. Ook voor de versterking en uitbreiding van dit bestaande aanbod werken we aan collectieve oplossingen. Zo verhogen we met gemeenten en gemeentelijke samenwerkingsverbanden hun digitale weerbaarheid en maken zij hun ICT-infrastructuur veiliger.

Krapte op de arbeidsmarkt vraagt om het bundelen en slim inzetten van de beschikbare kennis en expertise. Denk aan poolvorming op specialistische kennis, zoals auditors, CISO's, FG's, adviseurs OOV, ENSIA-coördinatoren, pentesters. Dit kan door de verdere verbreding van het inkoop-portfolio GGI-veilig. Hierdoor worden gemeenten tevens ontzorgd op het aantrekken en selecteren van geschikte expertise. Andere vormen zijn: procesondersteuning voor de wettelijke vereisten zoals risicobeoordelingen, voor het borgen van bedrijfscontinuïteit of een gezamenlijk controle van geleverde diensten en versterking van het contract- en leveranciersmanagement.

Kortom: de breedte van de Agenda Digitale Veiligheid 2028 leent zich voor een collectieve aanpak, met oog voor lokale waardenkaders die bepalen wat in de nabijheid en in aansluiting op lokaal bestuur binnen de gemeenten zelf uitgevoerd moet worden.

### **Doorsnijdende thema's**

*Digitale autonomie en digitale veiligheid:* Onder de huidige geopolitieke spanningen opereren kwaadwillende statelijke actoren niet alleen via hacks en DDOS-aanvallen, maar mogelijk ook via het onder druk zetten van technologieleveranciers die onder hun rechtsgebied vallen. Het is daarmee niet langer ondenkbaar dat Nederlandse gemeenten plotseling toegang verliezen tot gegevens die essentieel zijn voor de continuïteit van hun publieke kerntaken. Dit collectiviseringsvoorstel moet daarom bijdragen aan een *integrale* versterking van de weerbaarheid van (het collectief van) gemeenten. Digitale autonomie is daar een onmisbaar onderdeel van.

*Digitaal vakmanschap en digitale veiligheid:* Zonder voldoende kennis en vaardigheden bij gemeenten blijft de digitale veiligheid een achterhoedegevecht tegen kwaadwillenden. De nieuwe Cyberbeveiligingswet is de nationale uitwerking van de NIS2 en verplicht bestuurders zich te scholen en risicogebaseerd aan de slag te kunnen met informatieveiligheid. Investeren in kennis - ook bij niet-technische functies - is cruciaal. Dit sluit aan bij de Nederlandse Digitaliseringsstrategie (NDS), waarin het verhogen van digitale weerbaarheid als prioriteit is benoemd.

ICT-sourcing, Cloud en digitale veiligheid: Gemeenten gebruiken veelal (cloud)diensten van derden, zoals softwareleveranciers. Met deze afhankelijkheid van een beperkt aantal aanbieders is het belangrijk om kritisch te blijven kijken naar onze groeiende afhankelijkheid van technologie. Gemeenten stellen grenzen aan wat ze acceptabel vinden en beperken zo de risico's van technologie vanuit landen met een offensief cyberspionageprogramma. Collectieve ICT-sourcing versterkt de weerbaarheid, verlaagt kosten en maakt gespecialiseerde kennis beter inzetbaar. Door krachtenbundeling kunnen gemeenten beter onderhandelen, risico's beperken en innovatie versnellen - essentieel om nationale en Europese digitaliseringsdoelen zoals de Digital Decade en de NDS te halen.

### **Richting en fasering**

De collectieve inzet op digitale veiligheid wordt in fasen uitgewerkt:

- *Bestuurlijke consensus en kaders.* We leggen per deelvoorstel de normen, rollen en verantwoordelijkheden samen vast, inclusief checks & balances;
- *Juridische, financiële en organisatorische afspraken.* We maken heldere afspraken over governance, aansprakelijkheid, kostenverdeling en collectieve inkoop die zorgt voor één uniforme manier van aanhaken voor leveranciers en gemeenten;
- *Institutionaliseren van het collectief.* We borgen beheer en doorontwikkeling.

Dit groeipad kent mijlpalen op 1, 2, 5 en 10 jaar. Niet alles hoeft overal tegelijk. Gemeenten sluiten stapsgewijs aan, afhankelijk van draagkracht, budget en politiek-bestuurlijk momentum. Dit zorgt voor voorspelbare kosten, duidelijke verantwoordelijkheden en meetbare resultaten.

Voor taken die niet binnen een collectief voorstel vallen, kunnen gemeenten gebruikmaken van bestaande voorzieningen, samenwerken via lokale Shared Service Centers en investeren in digitaal vakmanschap.

De aanpak is integraal en sluit aan op NDS-prioriteiten, bestaande beleidskaders (besparingsmotor, verenigingsstrategie etc.), en lopende programma's en projecten zoals GROEI en arbeidsmarktkrapte. De uitwerking van het bestuurlijk convenant rijk-gemeenten op digitale veiligheid bevat veel punten waarop 'groot helpt klein' en meer samenwerken mogelijk én gewenst zijn door gemeenten. Ook biedt het financieel addendum een handreiking voor kosten-baten analyses. De uitvoeringstoets cyberbeveiligingswet (NIS2) biedt een businesscase op de benodigde inzet, nieuwe taken en de mogelijke besparingen. Hiermee wordt inzichtelijk welke taken zich lenen om samen te organiseren.

Het collectiviseringsvoorstel Digitale Veiligheid is onlosmakelijk verbonden met de collectiviseringsvoorstellen op Cloud en AI, alsmede de doorsnijdende thema's: digitale autonomie, digitaal vakmanschap en sourcing.

### **Wat vragen we de ALV in deze opdracht tot uitwerking?**

- Steun voor de visie en ambitie: collectieve uitvoering van taken in collectieve diensten, waar het kan, inkoopondersteuning voor maatwerk, waar het moet;
- Bekrachtiging van de reikwijdte en scope: De Agenda Digitale Veiligheid, uitgewerkt in meerjarenplanning, aansluitend bij de NDS, het bestuurlijk convenant DV, nationale en Europese initiatieven;
- Mandaat om het complete collectiviseringsvoorstel uit te werken: inclusief financierings- en governance opties, collectieve ICT-sourcingstrategie en afspraken over cloud en digitale veiligheid;

- Bevestiging van de fasering en uitvoeringsprincipes: stapsgewijs met gedegen onderzoek wat wel/niet collectief kan. Met de focus op standaardisering en zoveel mogelijk werken via bestaande structuren.

Met dit besluit zet de ALV de gemeenten als één sterke bestuurslaag in positie om regie te nemen op digitale veiligheid.