



Oplegnotitie

Agendapunt	Onderwerp	Kenmerk	Portefeuillehouder
04.	Visie op informatievoorziening VRGZ		Mw. D.A. Bergman Mw. J.S. van Egmond
Dagelijks Bestuur	Algemeen Bestuur	Samensteller	
2 maart 2026 (schriftelijk)	12 maart 2026	Dhr. E. Slot-Rebel, dhr. P. van den Elzen	

Inhoud

1. Aanleiding, noodzaak en urgentie

De VRGZ heeft een wettelijke verplichting (met name gelegen in WvR artikel 10.i) om een informatievoorziening in te richten en in stand te houden voor de taken van de brandweer, GHOR, RAV, bedrijfsvoering en risico- en crisisbeheersing. Dat vraagt om een heldere IV-strategie. De Veiligheidsregio moet meebewegen in de huidige wereld, waarin de taakuitvoering steeds sterker leunt op digitale middelen, data en informatie. ICT en informatievoorziening (IV) zijn al lang niet meer slechts ondersteunende processen, maar een strategisch instrument voor het functioneren van onze primaire processen – en daarmee voor het verbeteren van de maatschappelijke veiligheid.

Tegelijkertijd moet de VRGZ ook gewapend zijn tegen de steeds geavanceerdere aanvalstechnieken die criminelen en statelijke actoren ontwikkelen. Dat stelt hoge eisen aan de (informatie)beveiliging. De dreiging is reëel: in 2025 hebben we bijvoorbeeld drie aanvallen gehad waarbij zelfs forensisch onderzoek nodig was om te achterhalen of er nadelige gevolgen waren. De verwachting vanuit samenleving en ketenpartners is dat de VRGZ onder alle omstandigheden digitaal paraat is. Een enkele verstoring kan leiden tot verlies van vertrouwen en directe maatschappelijke schade. Als brandweer, ambulance en crisispartners niet of vertraagd kunnen uitrukken of niet over de benodigde informatie beschikken, dan heeft dit directe impact op tijdigheid (responstijden), doeltreffendheid (juiste inzet/route/middelen) en veiligheid (patiënt én hulpverlener). En daarmee aan de zorg voor alle inwoners en bezoekers van Gelderland-Zuid.

Informatievoorziening is daarom ook een speerpunt in het Regionaal Beleidsplan VRGZ 2024-2027. De bestuurlijk vastgestelde ambities zijn voornamelijk gericht op verbeteren van informatiegestuurd werken:

- komen tot een continu actueel veiligheidsbeeld, gericht op het voorspellende vermogen in de 'koude' fase en een snellere beeldvorming en besluitvorming bij een incident of crisis ('warme' fase);
- komen tot een toekomstbestendige digitale infrastructuur, door het ontsluiten van informatie, zorgen voor een robuuste gegevensuitwisseling en een stabiel en veilig netwerk, en het verder versterken van de informatiebeveiliging;
- interregionale en landelijke samenwerking op het gebied van informatiegestuurde veiligheid;
- versterken van de informatiepositie van de GHOR/zorgketen;
- uitbreiden van de Baseline Informatiebeveiliging Overheid (BIO) van niveau 3 naar 4 en mogelijk 5 (mede vanwege de vitaalverklaring) – dit brengt investeringen in materiële en personele zin met zich mee.

Daarnaast zijn er ook recente ontwikkelingen die de noodzaak en urgentie van deze visie benadrukken:

- *Digitale dreiging:*
Het Cybersecuritybeeld Nederland 2025 (NCTV) laat zien dat het digitaal dreigingslandschap steeds complexer en onvoorspelbaarder wordt. Cyberaanvallen nemen in omvang en geavanceerdheid toe, terwijl digitale systemen onderling sterk afhankelijk zijn. Het is daarom van groot belang om de digitale weerbaarheid van de VRGZ op orde te brengen en te houden.

De volgende risico's voor de VRGZ zijn verbonden met de digitale dreiging die de NCTV schetst:

- Bedrijfscontinuïteit: verhoogd risico op datalekken, ransomware en verstoring van de primaire/operationele en bedrijfskritische processen van de VRGZ;
- Compliance: kans op sancties en reputatieschade door niet voldoen aan wet- en regelgeving (BIO2, NEN7510, NIS2, AVG, Wwk en andere normen);
- Incidentrespons: langzamere reactie door versnipperde verantwoordelijkheden en beperkte expertise;
- Menselijke factor: hogere kans op phishing en social engineering door gebrek aan awareness.

- *Aangescherpte normeringen*

De VRGZ moet voldoen aan diverse normen op het gebied van informatiebeveiliging, waaronder de Europese NIS2 (in Nederland vertaald naar de Cyberbeveiligingswet/BIO2, deze treedt naar verwachting tweede kwartaal van 2026 in werking), de NEN7510 (nieuwe versie vanaf 2025 verplicht) en de AVG. De Regionale Ambulancevoorziening (RAV) heeft eind 2025 – na een stevig verbetertraject – eind 2025 de NEN7510-audit succesvol doorlopen. De informatiebeveiliging van de overige organisatieonderdelen van de VRGZ voldoet nog niet aan de BIO2 en daarmee ook nog niet aan de in het Regionaal Beleidsplan neergelegde bestuurlijk vastgestelde ambitie.

- *Masterprogramma IV en strategische agenda van Veiligheidsberaad*

Het Veiligheidsberaad heeft op 6 oktober 2025 ingestemd met het Masterprogramma Informatievoorziening 2025-2030 voor de 25 veiligheidsregio's, dat aansluit op de Strategisch Agenda van het Veiligheidsberaad. Het masterprogramma rust op vijf programmalijnen:

1. informatiegestuurde veiligheid;
2. informatiegestuurde missiekritische communicatie;¹
3. data en infra;
4. informatieveiligheid;
5. digitaal fitte organisatie.

- *Vitaalverklaring VRGZ:*

Sinds juli 2025 is de VRGZ door het ministerie van JenV aangemerkt als vitale aanbieder voor de processen (a) inzet brandweer (verlenen van hulp in noodsituaties), (b) crisiscoördinatie en besluitvorming en (c) communicatie- en informatievoorziening hulpdiensten en crisispartners. Als vitale aanbieder heeft de VRGZ de verplichting om inzicht te hebben in de weerbaarheid van de processen en passende maatregelen te nemen om zich zoveel als mogelijk te beschermen tegen dreigingen.

- *Coalitieakkoord 'Aan de slag':*

In het coalitieakkoord van het beoogde kabinet-Jetten is het belang genoemd om te “zorgen voor een snelle implementatie van de NIS2-richtlijn gericht op digitale weerbaarheid, zodat onze vitale sectoren zijn voorbereid op cyberdreigingen en daar snel op kunnen acteren” evenals het belang om te “kiezen voor een actieve voorbereiding op grootschalige digitale aanvallen, door te oefenen met overheid, mkb en vitale sectoren, door ethische hackers te stimuleren en door snelle en gerichte uitwisseling van dreigingsinformatie tussen overheid en bedrijfsleven”.

- *Accountantsverklaring 2025:*

De accountant geeft aan dat van het management van de VRGZ een actieve rol wordt verwacht in het tijdig en volledig voldoen aan de eisen van de Cyberbeveiligingswet en neemt dit ook mee in de jaarlijkse IT-audit.

De Cyberbeveiligingswet (Cbw), gebaseerd op artikel 20 van de NIS2-richtlijn, bepaalt dat bestuurders altijd eindverantwoordelijk zijn voor de cyberveiligheid van hun organisatie, ook al zijn taken gedelegeerd. Dat betekent dat cybersecurity niet langer een IT-aangelegenheid is, maar een bestuurlijke kerntaak.

2. Bestuurlijke keuzes: van basis op orde naar strategische weerbaarheid

Om te kunnen voldoen aan de wettelijke taken – een informatievoorziening inrichten en in stand houden binnen veiligheidsregio en tussen de veiligheidsregio en (crisis)partners – moet eerst de basis op orde zijn. Dat is nu niet het geval. Daarom heeft de VRGZ een visie op informatievoorziening ontwikkeld.

¹ Missie kritische communicatie: applicaties die communicatie via spraak, data en beeld mogelijk maken. Niet alleen binnen iedere hulpverleningsdienst maar ook tussen de diensten onderling (o.a. C2000).

Voor de realisatie van deze visie zijn drie scenario's ontwikkeld (zie bijlage 4a en bijlage 4b, hoofdstuk 9). De eerste twee scenario's zijn gericht op het op orde komen en op orde houden van de basis. Scenario 3 zorgt er vervolgens voor dat de stap naar buiten en naar voren wordt gemaakt

Scenario 1: het op orde komen

Scenario 1 vormt een verplichte wettelijke ondergrens: het brengt de basis op orde, maar levert geen duurzame of structurele versterking van de IV-keten op. Bovendien blijft de IV-organisatie hiermee feitelijk functioneren als een 8-uursorganisatie, zoals we de afgelopen jaren gewend waren. Dat is tot op heden goed gegaan, maar past niet meer bij de realiteit van vandaag. Dreigingen, cyberincidenten en systeemuitval houden zich niet aan kantooruren. Door voor scenario 1 te kiezen accepteert het AB nadrukkelijk beperkingen in kwaliteit, wendbaarheid, betrouwbaarheid én paraatheid buiten kantooruren. Daarmee accepteert het AB ook dat we niet 24/7 in staat zijn snel en adequaat op te treden vanuit de IV-organisatie, met risico's op uitval in zowel de operationele organisatie, als de crisisorganisatie.

Scenario 2: het op orde houden van de basis

Scenario 2 is de eerste structurele volwassenheidsstap en maakt de overgang mogelijk naar een volwaardige 24/7 IV-organisatie, zoals deze past bij onze wettelijke vitale rol. Met scenario 2 kiest het AB voor structurele betrouwbaarheid, stabiliteit, continuïteit en een solide basis voor informatiegestuurd werken. Dit scenario vormt bovendien een noodzakelijke randvoorwaarde om bestuurlijke verantwoordelijkheid te kunnen dragen. Het verkleint de kans op incidenten en maakt dat we, wanneer zich toch iets voordoet, snel en adequaat kunnen handelen om uitval en maatschappelijke schade te beperken.

Scenario 3: naar buiten en naar voren

Scenario 3 zorgt er vervolgens voor dat de stap naar buiten en naar voren wordt gemaakt. Deze stap kan gefaseerd worden uitgevoerd. Het legt de lat hoger en maakt de VRGZ wendbaar en weerbaar en optimaal aangesloten op landelijke ontwikkelingen. Het AB kiest hiermee voor digitalisering als strategisch middel om veiligheid, informatievoorziening en crisisbeheersing te versterken. Dit sluit ook aan bij de ambities uit het Regionaal Beleidsplan 2024-2027. Daarbij creëert scenario 3 ook meer financiële voorspelbaarheid op de lange termijn en worden onverwachte kosten voor incidentherstel beperkt.

3. Consequenties niet kiezen voor scenario's

Indien gekozen wordt om geén van de voorgestelde scenario's te volgen en op de huidige werkwijze door te gaan, brengt dit aanzienlijke bestuurlijke risico's met zich mee. De VRGZ voldoet dan aantoonbaar niet aan wettelijke verplichtingen zoals BIO2, NIS2/Cyberbeveiligingswet, AVG en WvR art. 10i, terwijl bestuurders onder deze wetgeving altijd eindverantwoordelijk zijn. Dit vergroot de kans op bestuurlijke aansprakelijkheid en mogelijke sancties. Daarnaast ontstaat een reëel risico op uitval van missie kritische systemen, met directe impact op hulpverlening en veiligheid. De digitale weerbaarheid blijft onvoldoende, waardoor de kans op cyberaanvallen, datalekken en ontwrichting van bedrijfsvoering toeneemt. Financieel is 'niets doen' het duurste scenario: de structurele meerkosten bedragen €1,4 miljoen per jaar, zonder dat de IV-basis verbetert. Ook raakt de VRGZ verder achterop bij landelijke ontwikkelingen, neemt de afhankelijkheid van externe leveranciers toe. Niet kiezen betekent daarmee een bestuurlijk risico dat veiligheid, continuïteit, compliance én betrouwbaarheid van de VRGZ onder druk zet. In bovenstaande scenario's is dan ook gekozen voor een andere, minder afhankelijke koers en zetten we gemeenschapsgeld zo effectief en efficiënt mogelijk in.

4. Financiële consequenties

De realisatie van deze strategie om te komen tot een goede en betrouwbare informatievoorziening voor de uitvoering van de maatschappelijke opgave van de VRGZ, heeft de volgende financiële consequenties:

		2027	2028	2029	2030
Scenario 1	Totaal structureel benodigd	1.950	2.371	2.606	2.733
	Stijging per jaar	1.950	421	235	127
Scenario 2	Totaal structureel benodigd	2.562	3.390	3.818	4.088
	Stijging per jaar	2.562	828	428	270
Scenario 3	Totaal structureel benodigd	2.880	4.548	4.888	5.178
	Stijging per jaar	2.880	1.668	340	290

Bovengenoemde bedragen zijn na aftrek van de incidentele dekking uit de bestemde reserve BDuR ter versterking van crisisbeheersing en informatievoorziening. Daarnaast levert de AZGZ naar verwachting² een structurele bijdrage van € 300.000 per jaar. De bedragen op 'Totaal structureel benodigd' tonen het resterende te overbruggen bedrag. In de bijlagen is per scenario de kostenontwikkeling uitgewerkt, inclusief gedeeltelijke dekking.

5. Themabijeenkomst AB VRGZ 26 februari 2026

Tijdens de themabijeenkomst is gesproken over de landelijke ontwikkelingen in informatievoorziening (IV) en de voorgestelde IV-strategie 2026–2030 voor de VRGZ. De noodzaak van versterking van de IV-organisatie werd door uw bestuur onderkend. Er zijn nog wel vragen over hoe snel en in welke vorm. Uw bestuur heeft daarbij gevraagd om de risico's en bestuurlijke keuzes expliciet te maken per scenario.

Andere thema's in de discussie waren:

1. Waarom nu: tijdspad voor zorgvuldige weging en besluitvorming
2. Afweging tussen in- of uitbesteden;
3. Mate van noodzakelijke robuustheid en schaalgrootte van de IV-organisatie;

Risico's en bestuurlijke keuzes zijn nader uitgewerkt bijlage 4a en bijlage 4b, hoofdstuk 9 en samengevat weergegeven onder kopje 2 van de oplegnotitie

De IV-strategie wordt nu voorgelegd omdat wettelijke verplichtingen, toenemende digitale dreiging, aanbestedingstermijnen aflopende contracten per 1-12-2026, de bestuurlijke ambities uit het Regionaal Beleidsplan 2024-2027 en operationele noodzaak samenkomen — en verder uitstel leidt tot onrechtmatigheidsrisico, hogere kosten en groeiende kwetsbaarheid.

Inbesteden biedt VRGZ duidelijke voordelen: lagere structurele kosten (minder meerkosten), meer eigen regie, hogere betrouwbaarheid en wendbaarheid en betere aansluiting op landelijke IV-ontwikkelingen. Uitbesteden is voor de VRGZ financieel duurder, operationeel risicovoller, minder flexibel en minder passend bij onze vitale status en het zijn van 24-uursorganisatie.

Voor een uitgebreide toelichting wordt verwezen naar bijlage 4a Beantwoording vragen algemeen bestuur

Doel van de bespreking

Het AB wordt gevraagd te bepalen welk scenario uitgangspunt vormt voor de realisatie van de visie op informatievoorziening, inclusief ambities, investeringen en fasering. Waarbij er mogelijkheden zijn om het ingroeipad voor scenario 3 met 1 of 2 jaar op te schuiven, waardoor de kosten meer verspreid worden over de komende jaren en dit scenario doorloopt tot 2031/2032

Afhankelijk van de bestuurlijke discussie op 12 maart 2025 worden de incidentele en structurele kosten meegenomen in de ontwerpbegroting 2027.

Beslispunten

Het AB VRGZ wordt voorgesteld om:

1. De visie op Informatievoorziening VRGZ 2026-2029 vast te stellen.
2. Scenario 2 te kiezen voor uitvoering als wettelijke verplichte ondergrens en noodzakelijke basis.
3. Scenario 3 richtinggevend te verklaren als het beoogde eindbeeld voor 2030, 2031 of 2032, waarbij het AB instemt met een gefaseerd ingroeipad.
4. De financiële gevolgen te verwerken in de ontwerpbegroting 2027 en meerjarenraming 2028-2030

Bijlagen

- a. Beantwoording vragen algemeen bestuur 26 februari 2026
- b. IV-strategie 2026-2030

² Bekostiging en financiering van de ambulance bedrijfsvoering (waaronder IV) is jaarlijks onderwerp van gesprek tussen zorgverzekeraars en de regionale ambulancevoorziening

Besluitvormingsproces

Historie

Gremium	Datum	Inhoud besluit
DB VRGZ	05-02-2026	Vaststellen agendapunt visie informatievoorziening voor AB
Ambtelijk overleg	12-02-2026	Bespreken visie met adviseurs crisisbeheersing en gemeentelijke adviseurs IV
AB VRGZ (thema)	26-02-2026	Bespreken kaders en scenario's visie informatievoorziening.

Vervolg

Gremium	Datum	Inhoud besluit
AB VRGZ	12-03-2026	Vaststellen visie informatievoorziening
DB VRGZ	19-03-2026	Vaststellen begroting VRGZ 2027