

bevolkingsonderzoek



nederland

Document marktconsultatie

Inrichting en beheer datawarehouse landing-zone en bijbehorende diensten

1. Inleiding

1.1 Algemene informatie aanbestedende dienst

Bevolkingsonderzoek Nederland (hierna BVO NL) is verantwoordelijk voor het uitvoeren van de onderzoeken naar borstkanker, baarmoederhalskanker en darmkanker. Deze Bevolkingsonderzoeken zijn onderdeel van het nationaal Programma Bevolkingsonderzoeken van het Ministerie van Volksgezondheid, Welzijn en sport. Bevolkingsonderzoek Nederland is een organisatie van circa 900 medewerkers. Bevolkingsonderzoek draagt door middel van kwalitatief hoogwaardige bevolkingsonderzoeken substantieel bij aan het vroegtijdig opsporen van kanker met als doel gezondheidswinst te realiseren en sterfte terug te dringen. Nadere informatie treft u ook aan op [Bevolkingsonderzoek Nederland](#).

1.2 Aanleiding voor marktconsultatie

De drie bevolkingsonderzoeken die worden uitgevoerd zijn:

1. darmkanker (DK)
2. baarmoederhalskanker (BMHK)
3. borstkanker (BK)

Deze onderzoeken kennen elk hun eigen proces met een aantal overeenkomsten en ook de nodige verschillen. Deze processen worden alle drie ondergebracht in hetzelfde bronsysteem. Daarnaast gebruikt BVO NL systemen voor de bedrijfsvoering die ook belangrijke stuurinformatie bevatten.

Bevolkingsonderzoek Nederland verwerkt bijzondere persoonsgegevens om de bevolkingsonderzoeken naar kanker te kunnen uitvoeren en te monitoren in een processysteem, om stuurinformatie te genereren en ook om over de effectiviteit van de programma's te kunnen rapporteren aan het RIVM en de tweede kamer. BVO NL heeft daarom een beveiligde integrale omgeving van waaruit zij kan rapporteren maar ook data kan analyseren en kan forecasten. Dit is een datawarehouse dat momenteel is gebouwd in een Microsoft omgeving. Op deze omgeving draait onder andere een Webfocus omgeving voor het maken van rapportages.

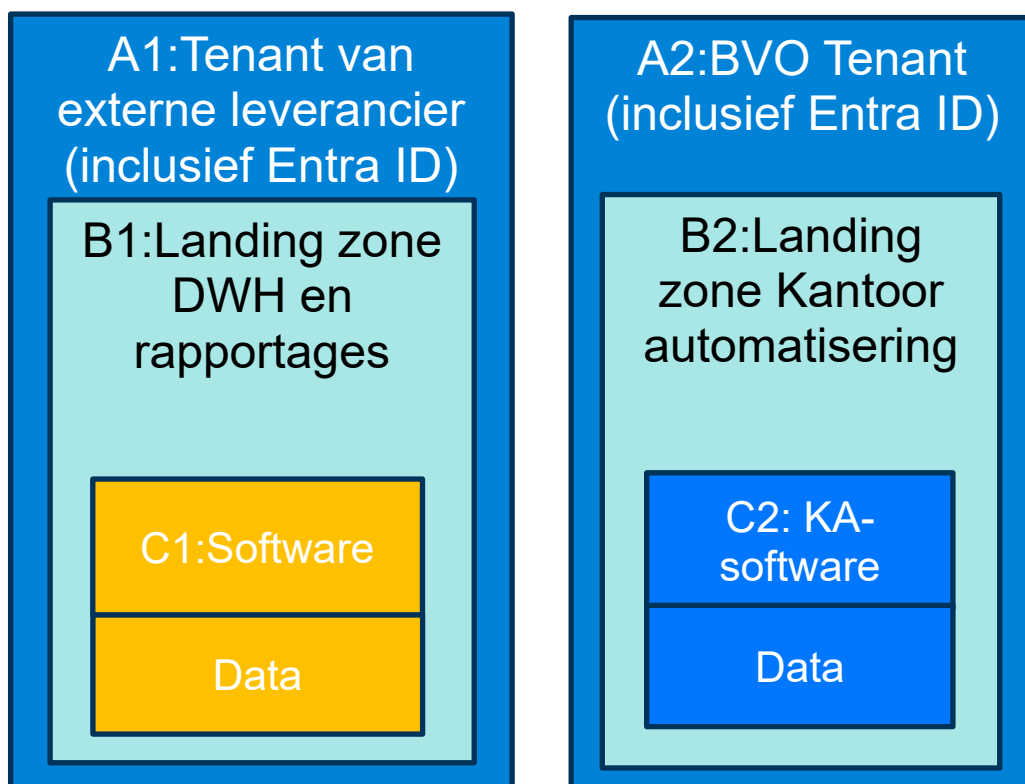
Dit alles stelt eisen aan de (rapportage)tools, technische inrichting, transparantie, hoogst mogelijke beveiliging, integriteit van data en goede ondersteuning, maar ook aan de organisatie en bemensing.

Afgelopen periode heeft BVO NL de huidige inrichting en opzet van het datawarehouse geëvalueerd. BVO wil het werk dat zij zelf doen en waar zij samenwerking zoeken met marktpartijen herijken. Als doelstelling heeft BVO NL dat zij medio juni 2027 beschikken over een rechtmatig gecontracteerd, geïmplementeerd en toekomstbestendig platform voor het BVO datawarehouse. De continuïteit, toepassing van open standaarden, hoogst mogelijke beveiliging, eigenaarschap van data, efficiëntie, kostenbesparing en interne regie zijn geborgd door een tijdige selectie, contractering en implementatie van een geschikte IT-partner.

1.3 Huidige en gewenste situatie

1.3.1 Huidige situatie

In de huidige situatie wordt voor de Datawarehouse en rapportage omgeving in de Tenant van een externe leverancier gebruikt. Daarnaast heeft BVO NL een eigen Tenant voor kortgezegd haar kantoorautomatisering. Dat ziet er als volgt uit:



Het datawarehouse o.a. bestaande uit de data-pipelines, koppelingen, ETL laag en de functionele inrichting wordt door BVO zelf ingericht en beheerd. De inrichting van de Azure omgeving, met oa: landing zone met cloud resources (t.b.v. het data warehouse), devops-omgeving (van ontwikkel naar productie inclusief release pipelines en code repositories), connectivity en security worden verwacht van de IT-partner.

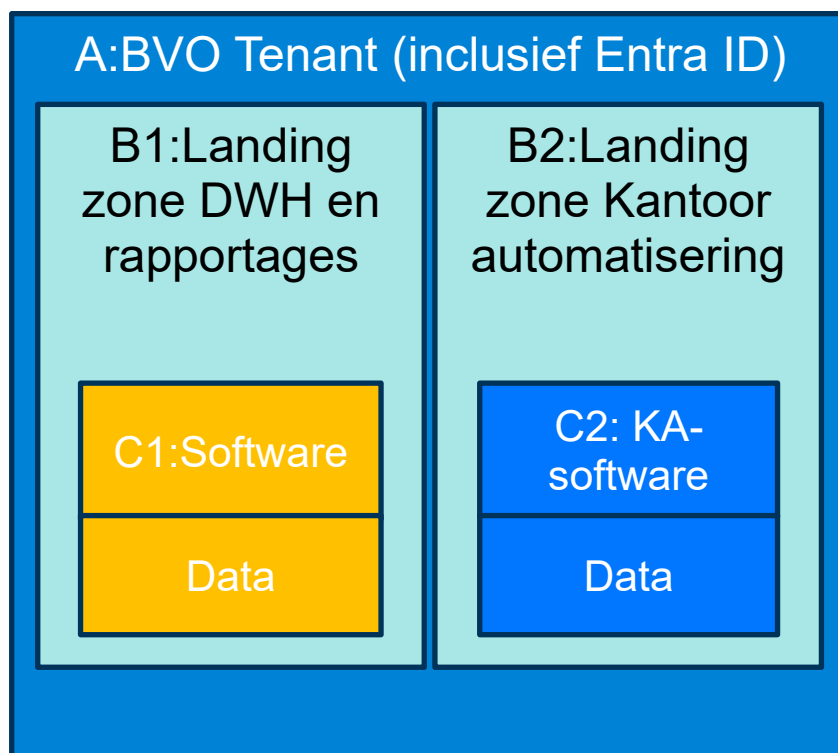
1.3.2 Gewenste situatie

Het doel is dat het datawarehouse in de IT-omgeving van BVO komt te staan, hierbij is er minder afhankelijkheid van een derde leverancier.

Grofweg is de IT-omgeving van BVO in de cloud opgebouwd uit drie delen:

- A. Een basis laag waarin ieder medewerker toegang krijgt. In deze laag worden basis beveiligingsinstellingen neergezet en worden de toegangsrechten voor diverse specifieke omgevingen per medewerker vastgelegd. Dit wordt de BVO Tenant genoemd en het onderdeel wat de toegangsrechten per medewerker vastlegt wordt Entra ID genoemd.
- B. Vervolgens is er een laag per toepassingsgebied waarin wederom beveiligingsinstellingen worden vastgelegd, maar op dit niveau specifiek voor dat toepassingsgebied. Daarnaast wordt server en opslagcapaciteit toegewezen. Deze laag wordt de "landing zone" genoemd. Er zullen in ieder geval twee landing zones zijn:
 1. één voor de basis IT-voorzieningen op de werkplek, de kantoorautomatisering (KA) landing zone
 2. één voor de software en data voor het datawarehouse en rapportages
- C. In de derde laag zitten dan de daadwerkelijke toepassingen en zoals de software voor het datawarehouse en rapportages.

Omdat je op één centrale plaats je basisbeveiliging en je toegangsrechten wil beheren zien de lagen er schematisch in een ideaalsituatie er als volgt uit (de letters corresponderen met bovenstaande opsomming):



De inrichting van de Tennant en de basisbeveiliging (onderdeel A) wordt door een derde leverancier gedaan. Van de beoogde IT-partner worden grofweg de volgende werkzaamheden verwacht in onderdeel B:

Technisch beheer

- Continu waarborgen van de beschikbaarheid en werking van de omgeving (bv. certificaatbeheer, het signaleren van end-of-life componenten, etc.).
- Beheer van gebruikers en groepen voor VM's, databases en Azure DevOps repositories met een acceptabele reactietijd (vastleggen in SLA).
- Actieve monitoring (inclusief inzage in monitoringsgegevens) van security, storage, systeempowerformance (CPU, geheugen), gebruikers/ groepen en kosten
- Periodieke en proactieve communicatie over monitoringresultaten (bv. direct bij problemen en wekelijks algemene updates).
- Beheer van Azure DevOps build- en release pipelines, inclusief wijzigingen en het opzetten van nieuwe pipelines.
- Actief updaten van de omgeving (patches, service releases, etc.).
- Beschikbaar stellen en actueel houden van technische documentatie voor BVO.

Configuratie

- Configureren in de landing zone van nieuwe resources. Zoveel als mogelijk Infrastructure as a Code
- Inrichten van eventueel toekomstige Azure resources Azure-resources zoals Databricks, Fabric, VM's, etc.

Documentatie en architectuurinzicht

- Aanleveren van actuele documentatie en visuele weergaven van o.a. de architectuur.

Back-up en strategie

- Vormgeven in inrichten door leverancier in afstemming met BVO.

Disaster recovery beleid

- Ontwerp en inrichting van een disaster recovery beleid, inclusief periodieke tests, afgestemd met BVO
- Ontwerp en inrichting van een exit strategie

Contact

- Beheerhelpdesk inclusief incident afhandeling en problem management
- Servicemanagement
- Vast aanspreekpunt op engineersniveau (inclusief reactietijden in SLA).
- Vast aanspreekpunt op managementniveau (inclusief reactietijden in SLA).

Consultancy

- Voor toekomstige vragen heeft BVO (onderwerpfafhankelijk) behoefte aan een gespreks-partner met verstand van zaken.
- Mogelijkheid tot inhuur van gekwalificeerde mensen via leverancier.

Ter indicatie (onderstaande kengetallen zin indicatief) geven we de volgende achtergrond informatie mee:

Kenmerken	Nu
Aantal eindgebruikers	340
Aantal ontwikkelaars Webfocus/ BI specialisten	6
Aantal data engineers	6
Aantal rapporten	200
Data	2,5 TB 300 tables in Transaction Repository 400 fact tables
Data verwerking	50 dagelijkse data pipelines 1 bronsysteem 200 ETL scripts
Azure resources	~300 resources

1.4 Doelstellingen

1.4.1 Scope beoogde aanbesteding

BVO NL overweegt een IT partner in te zetten voor de technische datawarehouse en rapportage omgeving. Deze partner zou de volgende zaken moeten gaan doen:

- Een landingzone, bestaande uit ontwikkelomgeving, een beoogde test acceptatie en productie omgeving (inclusief code repositories en release mechanismes) inrichten met:
 - De hoogst mogelijke beveiligingseisen, zie bijlage C voor de eisen op hoog niveau
 - Adequate performance, zodat bijvoorbeeld tijdig ETL processen afgerond zijn en rapportages binnen acceptabele wachttijd beschikbaar zijn
 - Deze landingzone dient maximaal overdraagbaar te zijn na afloop of beëindiging contract (geen lock-in bij de IT partner) naar een andere IT-partner en zal op de omgeving van BVO NL zelf draaien. Dit vraagt eisen aan documentatie, infrastructuur als a code en duidelijke exit strategie
- Deze landingszone adequaat beheren (zie voorgaande paragraaf voor een eerste opsomming van wat hieronder wordt verstaan)
- Kosten controle en kosten beheersing uitvoeren op de resources uit de cloud (momenteel Azure) en advies geven over een koste efficiënte inrichting en abonnementsvorm. De abonnementen zullen buiten deze aanbesteding worden verworven.
- Toekomstige uitbreidingen/wijzigingen projectmatig uitvoeren bij innovaties, nieuwe behoeftes en groei
- Adviseren bij inrichting van pipelines, ETL, database tot en met rapportage/analyse en op afroep kan ondersteunen.

1.4.2 Doelen marktconsultatie

Het doel van deze marktconsultatie is vast te stellen of:

1. Of de opdracht realistisch is
2. Op welke wijze de verdeling van de verantwoordelijkheid tussen de IT-partner, BVO NL en andere IT-leverancier kan plaatsvinden;
3. Een indicatie krijgen van de aandachtspunten en risico's van de transitie;
4. Een indicatie krijgen van de aandachtspunten en risico's van het beheer;
5. Hoe de aanbesteding eruit kan zien.

2. Verloop en voorwaarden marktconsultatie

2.1 De spelregels

Ten aanzien van de marktconsultatie gelden naast de elders in dit document genoemde voorschriften, de hiernavolgende bepalingen. Door deelname aan de marktconsultatie verklaart de deelnemende marktpartij zonder voorbehoud akkoord te zijn met alle genoemde bepalingen.

Nadrukkelijk wordt vermeld dat deze marktconsultatie geen onderdeel uitmaakt van een aanbestedingsprocedure.

- De voertaal tijdens deze marktconsultatie is Nederlands.
- Aan de consultatie kunnen geen rechten worden ontleend, noch zal deelname aan de consultatie leiden tot enig voordeel of nadeel in de aanbestedingsprocedure die eventueel daarna volgt.
- Afzien van deelname aan de consultatie zal niet leiden tot uitsluiting van de aanbestedingsprocedure die eventueel daarna volgt.
- De marktconsultatie is geen uitnodiging om in te schrijven op de voorgenomen aanbesteding waarvoor deze marktconsultatie als voorbereiding dient.
- Deelnemende partijen kunnen geen aanspraak maken op vergoeding van eventueel gemaakte kosten in het kader van de marktconsultatie.
- Deze marktconsultatie is geen aanbesteding of pre-selectie. Dit houdt in Bevolkingsonderzoek Nederland zich in een oriënterende fase bevindt en dat de uitwerkingen nog in ontwikkeling zijn en uitwerking behoeven. Bevolkingsonderzoek Nederland behoudt zich het recht voor om de verkregen inzichten en informatie te gebruiken bij het opstellen van de aanbestedingsdocumenten (of om te besluiten dit niet te doen).
- Marktpartijen zijn niet verplicht mee te werken aan deze marktconsultatie;
- Bevolkingsonderzoek Nederland neemt bij deze marktconsultatie altijd in acht dat er een gelijk speelveld is voor alle marktpartijen. Dit betekent onder meer dat:
 - participatie aan deze marktconsultatie en de kwaliteit van de antwoorden van deelnemende organisatie op geen enkele wijze de positie van de betreffende organisatie beïnvloeden tijdens de aanbesteding;
 - De informatie die door Bevolkingsonderzoek Nederland wordt verstrekt gedurende de marktconsultatie kan afwijken van de informatie die in een later stadium wordt verstrekt ten behoeve van de aanbesteding.
- Door deelnemende partijen verstrekte informatie wordt na afloop van de marktconsultatie niet geretourneerd.
- BVO NL behoudt zich het recht voor deze marktconsultatie tijdelijk of definitief te staken.

- Door uw deelname aan deze marktconsultatie stemt u er mee in dat de door u verstrekte informatie zonder enig voorbehoud door Bevolkingsonderzoek Nederland mag worden gebruikt in (de voorbereiding van) een eventuele aanbesteding(en). Eventuele door u verstrekte bedrijfsvertrouwelijke informatie wordt vertrouwelijk behandeld. Bevolkingsonderzoek Nederland verwacht dat u zelf aangeeft wanneer informatie bedrijfsvertrouwelijk is.

2.2 Eventuele gesprekken tijdens de marktconsultatie

Bevolkingsonderzoek Nederland houdt de optie open om naar aanleiding van de ingediende reacties marktpartijen uit te nodigen om mondeling een aanvullende toelichting te geven op hun antwoorden. Voor ieder gesprek is ca. 2 uur beschikbaar. Indien er meer dan 4 reacties uit de markt zijn binnengekomen, kan BVO NL ervoor kiezen een selectie te maken in uit te nodigen partijen. Selectie vindt plaats passend binnen de beschreven doelstellingen, gewenste situatie en gegeven antwoorden.

Per aanbieder mogen maximaal twee personen aanwezig zijn bij een eventueel gesprek. Tijdens het gesprek wordt er verder ingegaan op de gegeven antwoorden en kan de aanbieder een uitleg/demonstratie geven van de mogelijke oplossing. BVO NL zal er in het kader van de marktconsultatie tijdens het gesprek bepaalde informatie niet geven of vragen vanuit de aanbieder niet beantwoorden. Dit om, indien de vraag van BVO NL in de markt wordt gezet, deze aanbieder geen voordeel te geven ten opzichte van de partijen die niet voor een gesprek zijn uitgenodigd.

De informatie uit de marktconsultatie wordt mogelijk gebruikt als input voor eventuele vervolgtrajecten. Bij een publicatie van een eventueel vervolgtraject, waarin de gegevens van de marktconsultatie worden gebruikt, hebben alle bedrijven die hierop inschrijven evenveel kans om voor gunning in aanmerking te komen. Dit is onafhankelijk van het wel of niet meedoen met deze marktconsultatie c.q. uitgenodigd worden voor een toelichtingsgesprek. In het kader van transparantie zal alle door BVO NL gegeven informatie uit de marktconsultatie met de markt worden gedeeld, en openbaar gemaakt op www.tenderned.nl.

2.3 Planning

De voorziene planning van de marktconsultatie is in onderstaande tabel aangegeven. Deze planning is nog indicatief, er kunnen geen rechten aan worden ontleend. Het staat Bevolkingsonderzoek Nederland vrij om op een later tijdstip te besluiten de marktconsultatie en/of mogelijke aanbesteding tijdelijk of definitief te staken.

Mijlpaal	Datum
Publiceren van marktconsultatie	4 februari 2026
Gelegenheid tot het stellen van vragen over de marktconsultatieprocedure	20 februari 2026 17:00 uur
Beantwoording gestelde vragen	24 februari 2026
Sluitingsdatum voor het indienen van de gevraagde schriftelijke informatie	2 maart 2026 17:00 uur
Bekend maken welke leverancier worden uitgenodigd voor een toelichtend gesprek	6 maart 2026
Start van eventuele verdiepende gesprekken	11, 12 maart 2026
Afronden marktconsultatie en verslaglegging	1 april 2026

2.4 Communicatie tijdens de marktconsultatie

Communicatie verloopt via de berichtenmodule van TenderNed. U kunt de berichtenmodule raadplegen voor (proces) vragen en/of opmerkingen over de marktconsultatie. Aan de marktpartijen wordt gevraagd om in eerste instantie schriftelijk antwoord te geven op de vragen in dit document. Bevolkingsonderzoek

Nederland verzoekt u de antwoorden op de vragen 2 maart 2026 om 17:00 uur in te dienen via de berichtenmodule van TenderNed.

In het kader van de marktconsultatie heeft u de mogelijkheid om via TenderNed vragen te stellen aan BVO NL conform het gestelde in deze paragraaf en met gebruikmaking van het formulier dat is opgenomen in Bijlage A. De beantwoording van de vragen wordt gedeeld via TenderNed. Alle volgens dit document op tijd en correct ingediende vragen zullen geanonimiseerd beantwoord worden, en gepubliceerd op TenderNed.

2.5 Afronden marktconsultatie en verslag

Afsluitend stelt Bevolkingsonderzoek Nederland een geanonimiseerd verslag op, waarin op hoofdlijnen de bevindingen van de marktconsultatie zijn samengevat. Dit verslag wordt aan alle deelnemende partijen beschikbaar gesteld.

3. Vraagstelling

3.1 Inleiding

Dit marktconsultatiedocument dient als leidraad voor een schriftelijke consultatie. U wordt vriendelijk verzocht om onderstaande vragen schriftelijk te beantwoorden.

3.2 Vragen aan de markt

In deze paragraaf staan de vragen die aan partijen worden gesteld (deze zijn ook herhaald in bijlage B).

Nr.	Vraag
Visie	
1.	Kunt u uw oplossing voor een toekomstige landing zone schetsen voor de BVO NL? Wat maakt uw oplossing anders dan andere oplossingen in de markt?
Antwoord	
2.	Is de gevraagde dienstverlening passend voor u als potentiële inschrijver: - Inrichten landing zone (zie eerdere beschrijving) - Beheer van de landing zone (zie eerdere beschrijving) - Kosten management voor Azure kosten en Microsoft licenties - Advies voor verbetering en innovatie van de omgeving, oa: DWH inrichting, beveiliging, capaciteitsmanagement - Op afroep ondersteuning bij inrichting, ETL logica en BI Welke onderdelen zou u niet adviseren, welke aanscherpingen heeft u en welke onderdelen zou aanvullend binnen scope adviseren?
Antwoord	
3.	Is de beschreven scheiding in verantwoordelijkheden tussen Tenant, Landing zone en toepassingen helder en logisch? - Welke afstemming op grensvlakken voorziet u met de beheerder van de Tenant en wat is de beste wijze om dit vorm te geven? - Welke afstemming op grensvlakken ziet u met de leveranciers van bronsystemen en brondata? - Welke afstemming ziet u met BVO NL?
Antwoord	

4.	Hoe ziet u de evolutie van een traditioneel datawarehouse naar een toekomstbestendige data-architectuur, inclusief nieuwe architectuurprincipes en inzet van AI?
Antwoord	
Implementatie	
5.	Als BVO NL maatregelen zou willen nemen ten aanzien van portabiliteit wat dient zij dan op te nemen in de aanbesteding (bijvoorbeeld overdracht naar een private cloud op termijn, open standaarden, back-up en recovery en exit-clausules)? Hoe voorkomen we een vendor lock-in danwel lock-in bij de IT-partner?
Antwoord	
6.	Welke risico's verwacht u tijdens de migratie/ implementatie? Hoe kan BVO NL deze mitigeren? Acht een live gang in de nieuwe landing zone medio juni 2027 reëel indien de migratie 1 september 2026 van start gaat?
Antwoord	
7.	Ziet u alternatieve mogelijkheden om meer digitaal soeverein te zijn wat betreft IT voor een datawarehouse binnen BVO NL? Op welke termijn acht u dit realistisch? Welke extra aandachtspunten brengt uw eventuele voorstel met zich mee?
Antwoord	
Governance, beheer en onderhoud	
8.	Welke SLA eisen acht u realistisch? Ga hier in het bijzonder in op meetbare service levels.
Antwoord	
9.	Wat zijn uw verwachtingen aan regie en welke randvoorwaarden zou u stellen aan BVO NL om tot een goede samenwerkingsrelatie te komen?
Antwoord	
10.	Welke risico's verwacht u tijdens de beheerfase? Hoe kan BVO NL deze mitigeren?
Antwoord	
11.	Welke maatregelen ten aanzien van beveiliging acht u nodig en realistisch? In bijlage C is een overzicht opgenomen van beveiligingseisen die BVO NL reeds beoogd mee te geven.
Antwoord	
Selectie en gunning	
12.	Welke geschiktheidseisen en selectiecriteria acht u logisch, proportioneel en haalbaar. Vooral nog denkt BVO NL bijvoorbeeld aan: - ISO 27001/ NEN7510 en eventueel aanvullende beveiligingsmaatregelen zoals ISO 27017 (aanvullende maatregelen voor clouddiensten) en ISO 27018 (privacy/persoonsgegevens in de cloud) en ISAE 3000 - Eisen vanuit Maatschappelijk Verantwoord Opdrachtgeven en Inkopen - Microsoft Azure kennis en hoe deze op peil te houden - Referenties met vergelijkbare opdrachten: - o Zoals technisch beheer Datawarehouse omgeving binnen een overheidsinstellingen en zorginstelling - o Samenwerking in keten van leveranciers (koppelingen/ pipelines) andere systemen - o Soevereiniteit/ overdraagbaarheid - o Ervaring met kosten management voor Azure kosten en Microsoft licenties - o Adviesfunctie voor verbetering en innovatie van de Azure omgeving - ...

Antwoord	
13.	Welke subgunningscriteria zijn voor u logisch. Vooralsnog denkt BVO NL bijvoorbeeld aan: ○ Prijs ○ Plan van aanpak, incl. wijze van documenteren en het opbouwen van infrastructure as a code ○ Beheer en SLA afspraken, en zo ja welke? ○ Security maatregelen ○ Kwaliteit en beschikbaarheid adequaat personeel ○ ...
Antwoord	
Overig	
14.	Welke informatie heeft u nodig om een goede inschrijving te kunnen doen en een goede prijs te bepalen?
Antwoord	
15.	Wat wilt u overigens nog kwijt ten behoeve van deze marktconsultatie?
Antwoord	

Bijlage A – Indienen vragen en opmerkingen

Deze Bijlage is als separaat Word document toegevoegd.

Bijlage B – Invulformulier reactie marktconsultatie

Deze Bijlage is als separaat Word document toegevoegd.

Bijlage C: Overzicht van essentiële beveiligingsvoorschriften

Dit zijn de fundamentele hygiëne-eisen

Domein	Eis (De leverancier dient...)	Referentie waar dit in de NEN 7510 norm staat
1. Governance & Beleid	Een gedocumenteerd informatiebeveiligingsbeleid te hebben en een persoon of functie te hebben aangewezen die verantwoordelijk is voor informatiebeveiliging.	5.19
2. Personele Beveiliging	Medewerkers met toegang tot BVO NL data te screenen. Dit omvat minimaal het overleggen van een Verklaring Omtrent het Gedrag (VOG) met een relevant screeningsprofiel (bv. voor omgang met vertrouwelijke gegevens), voor zover wettelijk toegestaan, en het laten ondertekenen van een geheimhoudingsverklaring.	5.20n
	Te zorgen dat medewerkers met toegang tot BVO NL data periodiek bewustwordingstraining ontvangen op het gebied van informatiebeveiliging en privacy.	5.20k
3. Toegangsbeheer	Te zorgen voor unieke, persoonlijke accounts voor alle gebruikers. Generieke accounts zijn niet toegestaan, tenzij expliciet goedgekeurd door BVO NL.	5.20g
	Een adequaat wachtwoordbeleid te hanteren (complexiteit, lengte, periodieke wijziging).	-
4. Operationele Beveiliging	Systemen die voor BVO NL worden ingezet te beschermen tegen malware met up-to-date anti-malware software.	5.23c
5. Incident- management	Een proces te hebben voor het detecteren, registreren en reageren op informatiebeveiligingsincidenten.	5.19i
	Alle informatiebeveiligingsincidenten die (mogelijk) impact hebben op BVO NL of haar data onverwijld, en uiterlijk binnen de contractueel afgesproken termijn, te melden aan BVO NL.	5.20j
6. Fysieke Beveiliging	Kantoren en datacenters waar BVO NL data wordt verwerkt of opgeslagen, fysiek te beveiligen tegen ongeautoriseerde toegang.	5.20v
	Alle fysieke media die vertrouwelijke data van BVO NL bevatten, veilig op te slaan en te transporteren. Bij verzending dient gebruik gemaakt te worden van een traceerbare en betrouwbare koeriersdienst.	5.19l, 5.20w
	Fysieke media die niet langer nodig zijn, op een veilige en gecertificeerde manier te vernietigen (bv. degaussing, shredding).	5.20y
7. Toetsing & Controle	Medewerking te verlenen aan de periodieke beoordelingen door BVO NL, zoals een Quick Scan of een leveranciersgesprek, om de naleving van de overeengekomen eisen te toetsen.	5.22

8. Beëindiging Relatie	Bij beëindiging van het contract alle data van BVO NL op een veilige en gecertificeerde manier te vernietigen of te retourneren, en hiervan bewijs te leveren.	5.19m, 5.20x
-------------------------------	--	--------------

Deze eisen zijn gericht op leveranciers die een hoger risico vormen vanwege de aard van de data of de criticiteit van de dienst. De focus ligt op volwassen, aantoonbare processen. De beoogde IT-partner valt hier onder.

Domein	Eis (De leverancier dient...)	Referentie waar dit in de NEN 7510 norm staat
9. Risicomanagement	Een formeel proces voor risicomanagement te hebben en periodiek risicobeoordelingen uit te voeren op de dienstverlening aan BVO NL.	5.19 Zorgspecifiek
10. Cryptografie	Alle PGI en andere vertrouwelijke data van BVO NL te beschermen met encryptie, zowel tijdens transport (in-transit, bv. TLS 1.3+) als bij opslag (at-rest, bv. full disk of database encryption), gebruikmakend van actuele, industrie-standaard algoritmes.	5.19 Zorgspecifiek
11. Wijzigingsbeheer	Een formeel wijzigingsbeheerproces te hanteren. BVO NL dient vooraf geïnformeerd te worden over significante wijzigingen in de dienstverlening, infrastructuur of sub-leveranciers.	5.20u, 5.22
12. Logging & Security Monitoring	Voldoende logging te genereren en te bewaren van gebeurtenissen op systemen die BVO NL data verwerken, om beveiligingsincidenten te kunnen onderzoeken.	5.22g
13. Kwetsbaarheden- en Patchmanagement	Een formeel vulnerability management proces te hebben voor het periodiek scannen, identificeren en classificeren van kwetsbaarheden in alle systemen die voor BVO NL worden ingezet. Een adequaat patch management proces te hebben om kritieke en hoge risico kwetsbaarheden tijdig te mitigeren, conform industrie-standaarden en/of contractueel vastgelegde termijnen.	5.19f.2, 8.8
14. Back-up en Herstel	Periodiek back-ups te maken van alle data en configuraties van BVO NL, conform de contractueel overeengekomen Recovery Point Objective (RPO).	5.20s, 5.23i
	Back-ups veilig op te slaan, fysiek en/of logisch gescheiden van de productieomgeving, en te beschermen tegen ongeautoriseerde toegang en wijziging.	-
15. Toeleveringsketen	De inzet van onderaannemers (sub-verwerkers) die BVO NL data verwerken vooraf ter goedkeuring voor te leggen aan BVO NL. De leverancier legt dezelfde beveiligingseisen op aan haar onderaannemers.	5.20l, 5.21b

16. Continuïteit	Een gedocumenteerd en getest Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP) te hebben om de beschikbaarheid van de dienst te garanderen conform de contractuele afspraken (RTO/RPO).	5.19j, 5.20s
	Een gedocumenteerde exit-procedure te hebben die beschrijft hoe, op verzoek van BVO NL, alle data op een veilige en volledige manier kan worden geëxporteerd in een leesbaar en bruikbaar formaat.	5.20z, 5.23j
17. Auditrecht	BVO NL het recht te verlenen om (of via een onafhankelijke derde) audits uit te voeren op de naleving van de overeengekomen beveiligingseisen.	5.20p
18. Data Governance	Te garanderen dat alle data van BVO NL uitsluitend wordt verwerkt en opgeslagen binnen de Europees Economische Ruimte (EER), tenzij expliciet en schriftelijk anders overeengekomen.	5.23d
19. Systeembeveiliging	Indien software specifiek voor BVO NL wordt ontwikkeld, dient dit te gebeuren op basis van secure coding principes.	-
	Processen te hebben om de integriteit en authenticiteit van software- en hardwarecomponenten te waarborgen gedurende de levenscyclus (anti-manipulatie).	5.21j
20. Incidentmanagement (Aanvulling)	Op verzoek van BVO NL medewerking te verlenen aan (forensisch) onderzoek na een incident, inclusief het veiligstellen en aanleveren van relevante logs en ander digitaal bewijsmateriaal.	NEN7513, NIS2
21. Onafhankelijke Assurance	Te beschikken over een geldige, actuele certificering voor NEN 7510 en/of ISO/IEC 27001. Als alternatief kan een SOC 2 Type II rapportage (inclusief relevante Trust Services Criteria) worden geaccepteerd.	5.20o, 5.21f

Dit zijn eisen, voor kritieke leveranciers. De focus ligt op onafhankelijke validatie, diepgaande transparantie en strategische veerkracht. De beoogde IT-partner valt hier onder.

Domein	Eis (De leverancier dient...)	NEN 7510 Ref.
22. Cryptografie (aanvulling)	Voor de opslag van zeer gevoelige data-elementen, zoals BSN-nummers en medische diagnoses, dient application-level of column-level encryptie te worden toegepast. Dit zorgt ervoor dat de data ook beschermd is tegen ongeautoriseerde toegang door (database)beheerders. Het beheer van de cryptografische sleutels dient te zijn gescheiden van de data en te voldoen aan best practices voor key management.	8.4

23. Penetratietesten	Jaarlijks een onafhankelijke penetratietest te laten uitvoeren op de omgeving die voor BVO NL wordt gebruikt. Een management-samenvatting van de resultaten en het plan van aanpak voor bevindingen dient met BVO NL te worden gedeeld.	5.21f
24. Transparantie Toelevering	Voor geleverde software of medische apparatuur een Software Bill of Materials (SBOM) en een Manufacturer Disclosure Statement for Medical Device Security (MDS2) te overleggen.	5.21 Zorgspecifiek
	Zekerheid te verschaffen dat producten functioneren zoals bedoeld, zonder ongewenste functionaliteit, en dat componenten authentiek en ongewijzigd zijn.	5.21 Zorgspecifiek
25. Strategische Veerkracht	De gedocumenteerde exit-strategie periodiek te testen en op verzoek van BVO NL de resultaten van deze test te kunnen overleggen, om aan te tonen dat een soepele overdracht van data en diensten haalbaar is binnen de afgesproken termijnen.	5.20z, 5.23j
	Voor kritieke, op maat gemaakte software een broncode escrow-regeling te treffen.	-
	Jaarlijks een hersteltest (restore test) uit te voeren om de integriteit van de back-ups en de effectiviteit van de herstelprocedure te valideren, conform de contractueel overeengekomen Recovery Time Objective (RTO). Een samenvatting van de testresultaten dient met BVO NL te worden gedeeld.	5.19j
26. Samenwerking	Een vaste, benoemde contactpersoon voor informatiebeveiliging aan te wijzen voor strategisch overleg met BVO NL.	5.20m