

Nota van Inlichtingen

Marktconsultatie 'IT dienstverlening'

Datum: 11 juli 2025
Kenmerk: NIPV2025-EA-04009

In deze Nota van Inlichtingen geeft de Aanbestedende Dienst antwoord op de gestelde vragen die in het kader van de marktconsultatie 'IT dienstverlening' zijn geplaatst.

Vraag nr.	Document / Vraag nr.	Vraag	Antwoord
1.	Locatie van de uitvoering	Is het toegestaan dat (delen van) de gevraagde IT-dienstverlening worden uitgevoerd vanuit een locatie buiten Nederland, bijvoorbeeld vanuit Bulgarije, mits wordt voldaan aan alle gestelde eisen op het gebied van beveiliging, compliance, samenwerking en bereikbaarheid?	Op dit moment heeft het NIPV hierover nog geen definitief standpunt ingenomen. De marktconsultatie is juist bedoeld om de mogelijkheden en praktijkervaringen vanuit de markt te verkennen. Wij nemen deze input mee in onze verdere afwegingen bij het opstellen van het Programma van Eisen (PvE). Daarbij zullen onder andere aspecten als informatiebeveiliging, compliance met relevante wet- en regelgeving, bereikbaarheid, taalvaardigheid en samenwerking met de interne organisatie worden meegewogen.

2.	Transitie & Exit - Lessons Learned	Zijn er specifieke aandachtspunten of lessons learned uit vorige ICT-transities die we in onze aanpak moeten meenemen?	Ja, op basis van eerdere ICT-transities zijn er enkele belangrijke lessons learned die het NIPV nadrukkelijk wil meegeven. Een van de meest cruciale succesfactoren is een goede samenwerking tussen het IT team van het NIPV en de IT-dienstverlener. Daarbij is het essentieel dat de dienstverlener proactief optreedt en de regie neemt in projecten. Het NIPV verwacht dat de IT-dienstverlener niet alleen uitvoerend is, maar ook richtinggevend en adviserend optreedt, met oog voor de organisatiecontext en de eindgebruikers. Heldere communicatie, eigenaarschap en een gezamenlijke focus op resultaat zijn daarbij onmisbaar om uitdagingen tijdig te signaleren en effectief aan te pakken.
3.	Transitie & Exit - Exitstrategie	Heeft NIPV eisen of voorkeuren m.b.t. exitstrategie en overdracht van beheer bij toekomstige leverancierwissels?	Ja, het NIPV stelt concrete eisen aan de exit strategie en de overdracht van beheer om een naadloze overgang naar een eventuele toekomstige leverancier te waarborgen. Deze eisen zijn gericht op het minimaliseren van risico's, het waarborgen van continuïteit van dienstverlening en het behouden van kennis en documentatie. De specifieke eisen en voorwaarden met betrekking tot de exitstrategie zullen worden opgenomen in het Programma van Eisen (PvE) van de aanbesteding. De IT-dienstverlener wordt geacht hieraan volledig medewerking te verlenen en actief bij te dragen aan een zorgvuldige overdracht. Het NIPV ontvangt in de antwoorden ook graag het standpunt en/of voor en nadelen vanuit de markt met betrekking tot dit punt.
4.	Scope & Integratie - Legacy / SaaS-integratie	Zijn er bijzondere eisen of beperkingen voor integratie met bestaande, minder gangbare SaaS-applicaties of middleware binnen NIPV?	Ja, Het NIPV maakt gebruik van Exact Synergy als centrale ingang voor alle interne aanvragen, waaronder ook de IT-dienstverlening. Dit systeem fungeert als Single Point of Contact (SPOC) voor medewerkers richting ondersteunende diensten. Om de gebruikerservaring eenduidig en efficiënt te houden, is het van belang dat de IT-dienstverlener werkt vanuit dit systeem, of dat er een functionele integratie wordt gerealiseerd tussen Exact Synergy en het eigen ticketsysteem

			van de dienstverlener. Deze integratie moet zorgen voor een naadloze afhandeling van meldingen en verzoeken, zonder dat dit ten koste gaat van de gebruiksvriendelijkheid of de beheersbaarheid van de dienstverlening.
5.	Scope & Integratie - Rapportages & tooling	Is er een voorkeur voor bestaande rapportage- of monitoringtools bij NIPV, of kunnen marktpartijen hier zelf oplossingen voor voorstellen?	Het NIPV heeft geen voorkeur voor specifieke rapportage- of monitoringtools. Aangezien de dienstverlener een belangrijke rol zal spelen in de monitoring en opvolging van de dienstverlening, staat het NIPV nadrukkelijk open voor advies en voorstellen vanuit de markt over de meest geschikte tooling. Wel is het van belang dat voorgestelde oplossingen goed aansluiten op onze bestaande IT-omgeving, die primair is gebaseerd op Microsoft-technologieën en het gebruik van Microsoft Cloud-diensten (zoals Microsoft 365 en Azure). Integratie met deze omgeving en ondersteuning van bestaande standaarden op het gebied van beveiliging, compliance en beheer zijn daarbij belangrijke randvoorwaarden.
6.	Organisatiemodel & Governance - Regiemodel bij percelen	Indien de opdracht in percelen wordt verdeeld: Hoe ziet NIPV de samenwerking tussen leveranciers? Wordt een “lead supplier” rol gewenst?	Het NIPV heeft niet de intentie om de opdracht in percelen te verdelen. Het doel is om de gevraagde dienstverlening onder te brengen bij één integrale IT-dienstverlener, zodat er sprake is van duidelijke verantwoordelijkheden, optimale samenhang en efficiënte aansturing.
7.	Organisatiemodel & Governance - Deelname overleg	Wordt van de leverancier verwacht dat hij actief deelneemt aan regievergaderingen of klankbordgroepen binnen NIPV? Zo ja, met welke frequentie en op welk niveau?	Het NIPV verwacht van de IT-dienstverlener een proactieve rol in de samenwerking, inclusief een informerende en adviserende houding richting de organisatie. Deelname aan regievergaderingen of klankbordgroepen kan hier onderdeel van uitmaken, afhankelijk van de aard van de dienstverlening en de fase van het project of beheer. Het NIPV staat open voor een passende invulling hiervan en laat zich graag adviseren door de marktpartijen op basis van diens ervaring met vergelijkbare trajecten. Daarbij is het van belang dat de gekozen overlegstructuur bijdraagt aan transparantie, sturing op resultaat en een goede afstemming tussen partijen.
8.	Samenwerking & SLA - Kritische KPI's/SLA-issues	Zijn er performance indicatoren of SLA-elementen waar NIPV op basis van eerdere ervaringen extra aandacht voor heeft?	Ja, op basis van eerdere ervaringen hecht het NIPV bijzondere waarde aan de response- en oplostijden van vraagstukken en incidenten. Deze KPI's zijn cruciaal om de kwaliteit van de dienstverlening te waarborgen en moeten qua

			snelheid en effectiviteit volledig aansluiten bij de beleving van eindgebruikers, zoals zij die gewend zijn van een interne IT-servicedesk.
9.	Samenwerking & SLA - Innovatie-KPI's	Staat NIPV open voor voorstellen om aanvullend op standaard SLA's ook innovatie- of verbeterdoelen/kpi's op te nemen?	Ja, het NIPV staat hier zeker voor open. Het NIPV ziet het opnemen van innovatie- en verbeterdoelen/KPI's als een waardevolle aanvulling op de standaard SLA's. Deze doelen kunnen bijdragen aan continue verbetering van de dienstverlening en stimuleren de IT-dienstverlener om hierin een proactieve en initiërende rol te vervullen. De inhoud en formulering van dergelijke KPI's dienen in gezamenlijk overleg te worden bepaald, zodat deze realistisch, meetbaar en afgestemd zijn op de doelstellingen van de organisatie. Het NIPV nodigt de marktpartijen uit om op basis van ervaring en best practices voorstellen te doen voor een passende invulling.
10.	Security & Compliance-praktijk - SOC/SIEM-verantwoordelijkheid	Werkt NIPV met een eigen Security Operations Center (SOC), of wordt verwacht dat dit door de leverancier wordt ingevuld?	Het NIPV maakt gebruik van een externe SOC-leverancier voor de monitoring, detectie en triage van beveiligingsincidenten. Deze partij bewaakt de IT-omgeving continu op mogelijke dreigingen en afwijkingen. De opvolging van security-incidenten die voortkomen uit deze monitoring wordt echter belegd bij de IT-dienstverlener. Van de dienstverlener wordt verwacht dat hij adequaat handelt op meldingen vanuit het SOC, en dat hij beschikt over de benodigde processen, expertise en capaciteit om incidenten tijdig en effectief af te handelen, in afstemming met de opdrachtgever en conform geldende beveiligings- en compliance-eisen.
11.	Security & Compliance-praktijk - Audits en compliance	Zijn er komende security-audits of compliance-trajecten die invloed hebben op inrichting of eisen aan de dienstverlening?	Ja, er zijn diverse richtlijnen en wettelijke kaders die van invloed zijn op de inrichting en eisen aan de dienstverlening. Het NIPV houdt bij alle keuzes rekening met relevante normen en wetgeving, waaronder: - ISO 27001 (informatiebeveiliging) - BIO (Baseline Informatiebeveiliging Overheid) - NIS2.0-richtlijn - Data Act

			- AI Act Als zelfstandig bestuursorgaan (ZBO) volgt het NIPV daarnaast de adviezen op van onder andere het Ministerie van Justitie en Veiligheid (JenV). De keuzes met betrekking tot de inrichting van de dienstverlening worden altijd afgestemd met de interne teams op het gebied van security, privacy en compliance. Eventuele audits of compliance-trajecten kunnen invloed hebben op de eisen aan de dienstverlening en het is van belang dat de IT-dienstverlener hier flexibel en zorgvuldig op inspeelt.
12.	Flexibiliteit & Innovatie - Structurele innovatie	Heeft NIPV voorkeur voor structurele innovatie-initiatieven/periodieke marktupdates, of verwacht men deze op ad-hoc-basis?	Het NIPV heeft een duidelijke voorkeur voor een structurele en proactieve benadering ten aanzien van innovatie-initiatieven en marktontwikkelingen. Het NIPV verwacht dat de IT-dienstverlener ons hierin actief meeneemt en begeleidt, onder andere door het periodiek delen van relevante marktinzichten, technologische ontwikkelingen en best practices. Het doel is om gezamenlijk te blijven anticiperen op veranderingen en kansen in de markt, en zo continu te werken aan een toekomstbestendige en wendbare IT-omgeving. Ad-hoc-initiatieven kunnen aanvullend zijn, maar vormen geen vervanging voor een structurele aanpak.
13.	Flexibiliteit & Innovatie - Pilots/co-creatie	Staat NIPV open voor pilotprojecten/co-creatie op het gebied van nieuwe technologieën met de leverancier?	Het NIPV staat nadrukkelijk open voor pilotprojecten en co-creatie op het gebied van nieuwe technologieën, mits deze initiatieven toegevoegde waarde bieden voor de business. Innovatie wordt gezien als een belangrijk middel om de organisatie vooruit te helpen, en de Cloud transitie is daar een concreet voorbeeld van. Deze transitie had mede als doel om beter aan te sluiten bij technologische ontwikkelingen en om ruimte te creëren voor vernieuwing. Wel geldt dat nieuwe technologieën en initiatieven altijd moeten passen binnen het geldende beleid op het gebied van informatiebeveiliging, privacy en compliance. Eventuele pilots of co-creatietrajecten dienen daarom in goed overleg met het NIPV te worden afgestemd en vooraf getoetst op deze aspecten.
14.	Contractvorm & Looptijd -	Kan NIPV inzicht geven in de gewenste minimale of optimale contractduur en of er optiejaren voorzien zijn?	Het NIPV overweegt verschillende scenario's met betrekking tot de looptijd van de overeenkomst. Wij willen de markt graag betrekken bij deze afweging en

	Contractduur & opties		nodigen u daarom uit om uw visie te delen. Daarom hebben wij hierover een aanvullende vraag toegevoegd aan de marktconsultatie.
15.	Gebruik van Derden - Inzet partners/derden	Indien delen van de dienstverlening door specialistische partners worden uitgevoerd: Zijn er eisen aan certificering, datalocatie of contractuele borging?	Ja, indien de IT-dienstverlener gebruikmaakt van specialistische partners voor (delen van) de dienstverlening, geldt dat deze partners minimaal moeten voldoen aan dezelfde eisen en voorwaarden als de hoofdaannemer. Deze vereisten worden gespecificeerd in het Programma van Eisen (PvE) dat onderdeel zal zijn van de aanbesteding. Dit betreft onder andere eisen op het gebied van certificering, datalocatie, informatiebeveiliging, privacy en contractuele borging. De hoofdaannemer blijft te allen tijde verantwoordelijk voor de naleving van deze eisen door eventuele onderaannemers of partners.

Bijlagen:

- Marktconsultatie IT Dienstverlening versie 2. Wijziging: Onder 3.5 'Inrichting van de opdracht' is één vraag toegevoegd (zie het antwoord op vraag 14 van deze Nota van Inlichtingen.)