

# Assumpties & Uitsluitingen

Uno Automatiseringdiensten B.V. — Raamovereenkomst Catering- en  
Horecadiensten voor Gemeente Middenstad

Datum: 11/5/2025

## Aannames & Uitsluitingen — Raamovereenkomst ICT-beheer en Cloud (NVAO)

### Scopekader en definities

- Scopeafbakening: deze aanbieding ziet uitsluitend op diensten voor beheer, onderhoud en beveiliging van cloud- en infrastructuuroplossingen voor NVAO, met gebruik van Microsoft Azure in Nederlandse datacenters (regio West Europe/NL). Geen catering/horeca-activiteiten.
- Contracttype: diensten binnen een raamovereenkomst, gunning op EMVI.
- KO-conformiteit: ISO 27001 (geldig certificaat) en VOG voor alle ingezette medewerkers op NVAO-locaties of met toegang tot NVAO-data.

### Aannames (SMART, uitvoerbaar per startdatum T0)

- A1 Toegangsvoorzieningen: NVAO verstrekt binnen 5 werkdagen na T0 de benodigde bevoegdheden, netwerktoegang en contactgegevens van sleutelpersonen. Meetbaar: accounts actief en getest (E-02). Impact bij overschrijding: SLA-timers starten pas na toegang.
- A2 Regie en acceptatie: NVAO wijst per T0 een product owner (0,2 FTE) aan die binnen 2 werkdagen wijzigingen/acceptaties fiatteert. Doel: doorlooptijd changes  $\leq$  5 werkdagen (K3).
- A3 Documentatie: actuele systeem-/netwerkdokumentatie, CMDB, licentie-overzichten en dataclassificaties worden uiterlijk T0+10 werkdagen geleverd. Zonder dit geldt "best effort" beheer en risico R-01 neemt toe.
- A4 Dataplatform: workloads draaien op Azure West Europe (NL). Afwijking (andere regio/third party) alleen na schriftelijke akkoord en DPIA-impactbeoordeling (R-03).
- A5 Onderhoudsvensters: minimaal 2 geplande onderhoudsmomenten per jaar, ieder met  $\geq$  10 werkdagen voorafmelding. Doel: non-disruptive updates, beschikbaarheid  $\geq$  99,8% (K2).
- A6 24/7 beschikbaarheid: Uno levert 24/7 monitoring en incidentafhandeling voor kritieke incidenten. Responstijd  $\leq$  1 uur, oplostijd  $\leq$  4 uur (K1/K4).
- A7 Rapportages: beveiligingsincidenten per kwartaal gerapporteerd; ernstige datalekken binnen 24 uur na ontdekking aan NVAO gemeld (AVG-incidentmelding).
- A8 Scope van hardware en applicaties: hardwareleveringen en applicatieontwikkeling zijn uitgesloten; onboarding van bestaande systemen valt in scope.
- A9 Licenties en cloudkosten: Microsoft/Azure-licenties en verbruikskosten (compute, storage, egress) zijn voor rekening van NVAO, tenzij vooraf schriftelijk als "inbegrepen" vastgelegd.

### Juridische uitsluitingen en randvoorwaarden

- J1 Data-rol en AVG: NVAO is verwerkingsverantwoordelijke; Uno is verwerker. Een ondertekende verwerkersovereenkomst (conform AVG en ISO 27001 Annex A-controles) is voorwaarde voor aanvang productiebeheer.
- J2 Aansprakelijkheid: aansprakelijkheid beperkt tot het totaal aan door NVAO betaalde vergoedingen over de laatste 12 maanden, met uitsluiting van gevolgschade/indirecte schade en datareconstructiekosten, behoudens opzet/grove schuld of dwingend recht.
- J3 SLA-remedies: bij SLA-onderprestatie gelden uitsluitend de in het (te sluiten) raamcontract overeengekomen service credits als enige en exclusieve remedie, behoudens dwingend recht.
- J4 Overmacht/derden: verstoringen door derden (o.a. Microsoft Azure, internetproviders) en overmacht zijn uitgesloten van boete/credits; Uno faciliteert escalaties en herstel.
- J5 Wijzigingsbeheer: scopewijzigingen verlopen via change control met vooraf schriftelijke goedkeuring van NVAO; pas na akkoord worden planning en eventuele kosten geactiveerd.
- J6 Audit en testen: security-audits/pen-tests door of namens NVAO zijn 1x per 12 maanden inbegrepen mits 15 werkdagen vooraf afgestemd en zonder productieonderbreking; additionele audits op separate

opdracht.

- J7 Intellectuele eigendom: Uno behoudt IE op templates, scripts en tooling; NVAO krijgt een niet-exclusief gebruiksrecht voor de contractduur.
- J8 Personeelscreening: inzet van medewerkers is afhankelijk van tijdige VOG-verkrijging; NVAO aanvaardt eventuele startvertraging indien screening-termijnen nationaal oplopen.
- J9 Vrijwaring licenties: NVAO staat in voor rechtmatige inzet van eigen licenties. Uno levert op verzoek bewijs van naleving voor door Uno geleverde licenties.
- J10 Exports/sovereignty: exportrestricties en data-soevereiniteitsregels worden gevolgd; verzoeken die daarmee conflicteren worden afgewezen.

#### Financiële consequenties en prijsafspraken

- F1 Prijszekerheid: tarieven voor basis-scope zijn vast gedurende de contractperiode conform ingediende prijsbijlage (pricing locked). Indexatie en prijsaanpassingen zijn alleen mogelijk indien contractueel overeengekomen.
- F2 Meerwerk: werkzaamheden buiten de must-haves/SLAs (bijv. extra onderhoudsvensters, spoedchanges op verzoek, on-site inzet buiten calamiteiten) worden alleen uitgevoerd na schriftelijke opdracht; kosten vooraf geoffreerd en pas na akkoord uitgevoerd.
- F3 Azure-kosten: gebruik, opslag, back-up, archivering, data-egress en cross-region replicatiekosten komen voor rekening van NVAO. Keuzes met significante kostenimpact (bijv. extra-retentie) worden vooraf ter goedkeuring voorgelegd.
- F4 On-site interventies: 24/7 remote-respons is inbegrepen. On-site inzet is niet inbegrepen en wordt enkel op verzoek en na akkoord uitgevoerd als meerwerk.
- F5 Garantietermijn: 12 maanden functionele garantie op projectmatige configuraties die binnen deze opdracht zijn opgeleverd; garantie omvat herstel van gebreken die aan Uno toerekenbaar zijn.

#### Kwaliteit en bewijsvoering

- ISO en processen: Uno is gecertificeerd voor ISO 27001 en ISO 9001. Bewijs: actuele certificaten op naam van Uno Automatiseringsdiensten B.V. beschikbaar op verzoek (E-05).
- VOG: VOG-bewijzen worden beheerd en op verzoek ingezien (E-06).
- Logging en metrics: NOC-logs, Azure-availability-metrics, ticketdata en change-logs worden maandelijks gedeeld (E-01 t/m E-04).

#### KPI-definities (samengevat)

- K1 Responstijd storingen: ≤ 1 uur (24/7).
- K2 Beschikbaarheid: ≥ 99,8% per kalendermaand, excl. aangekondigd onderhoud.
- K3 Doorlooptijd standaard changes: ≤ 5 werkdagen.
- K4 Oplostijd kritieke incidenten: ≤ 4 uur.

#### Kruisverbanden W-xx ↔ KPI ↔ Risico ↔ Bewijs

- W-01 24/7 monitoring en triage → KPI: K1, K4 → Risico: R-02 (toegang), R-07 (derden) → Bewijs: E-01 NOC-incidentlog en escalaties.
- W-02 Incidentbeheer (ITIL) → KPI: K1, K4 → Risico: R-04 (security) → Bewijs: E-02 Ticketrapportage en P1/P2-postmortems.
- W-03 Change & release management → KPI: K3 → Risico: R-06 (wijzigingsstop) → Bewijs: E-03 CAB-notulen, change-kalender.
- W-04 Availability management → KPI: K2 → Risico: R-03 (Azure-outage) → Bewijs: E-04 Azure SLA-metrics, uptime-rapport.

- W-05 Security operations (patching, hardening) → KPI: K2 → Risico: R-04 → Bewijs: E-07 Patchcompliance-rapporten.
- W-06 Rapportages en reviews (maandelijks) → KPI: K1–K4 → Risico: R-01 (documentatie) → Bewijs: E-08 Maandrapporten, PDCA-actielijst.
- W-07 Onboarding & acceptatie (T0–T0+30 dgn) → KPI: K3 → Risico: R-01, R-02 → Bewijs: E-09 Acceptatieformulieren.
- W-08 Onderhoudsvensters (≥2/jaar) → KPI: K2 → Risico: R-06 → Bewijs: E-10 Aangekondigde onderhoudsberichten.
- W-09 Dataprotectie (back-up/retentie) → KPI: K2 → Risico: R-04 → Bewijs: E-11 Back-upjobsucces, restore-tests.
- W-10 Compliance (ISO/AVG) → KPI: K1–K4 indirect → Risico: R-05 → Bewijs: E-05 Certificaten, E-12 DPIA/SoA.

#### Risico's en beheersmaatregelen (samenvatting)

- R-01 Onvolledige documentatie → Maatregel: intake + gaplist binnen 10 werkdagen; escalatie bij blocker. KPI-impact: K2/K3. Bewijs: E-09.
- R-02 Vertraagde toegang → Maatregel: pre-boarding en toegangsmatrix; tijdelijke read-only monitoring. KPI-impact: K1. Bewijs: E-02.
- R-03 Azure-regionale storing → Maatregel: redundancy binnen NL-regio, optionele DR; duidelijke RTO/RPO-afspraken. KPI-impact: K2. Bewijs: E-04/E-11.
- R-04 Security-incident/malware → Maatregel: EDR/NDR integratie, patching-cadans, 24/7 triage; melding < 24 uur. KPI-impact: K1/K2. Bewijs: E-07/E-08.
- R-05 VOG niet tijdig → Maatregel: vroegtijdige aanvraag; tijdelijke vervanging. KPI-impact: n.v.t., maar startvertraging mogelijk. Bewijs: E-06.
- R-06 Change freeze/vergunningswindow → Maatregel: kalenderafstemming; noodchange-proces. KPI-impact: K3/K2. Bewijs: E-03.
- R-07 Afhankelijkheid derden (telco/app-leveranciers) → Maatregel: heldere demarcatie en escalatiepaden. KPI-impact: K1/K4. Bewijs: E-01/E-02.

#### PDCA-borging

- Plan: vastleggen SLA's, KPI's, securitycontrols, rollen en demarcatie (contract + PvA).
- Do: leveren 24/7 monitoring, incident/change-processen, onderhoud en rapportage.
- Check: maandelijkse KPI/SLA-rapporten, kwartaal security-rapporten, managementreview.
- Act: verbeteracties met eigenaar, deadline en effectmeting; doorvoeren via CAB.

#### Conformiteit met aanbestedingseisen

- Must-haves: SLA-responstijd < 1 uur, 24/7 support, beschikbaarheid ≥ 99,8%, ≥ 2 onderhoudsmomenten/jaar, Azure NL, periodieke securityrapportage — allen opgenomen in A1–A8, W-01 t/m W-10, KPI K1–K4 en bijbehorende bewijzen E-01 t/m E-12.

#### Juridische en operationele consequenties bij afwijkingen op aannames

- SLA-klokken pauzeren bij ontbrekende toegang (A1) en bij freezes buiten onze regie (R-06).
- Extra werkzaamheden door gebrekkige documentatie (A3) of ad-hoc wijzigingen worden uitsluitend na change-goedkeuring uitgevoerd en kunnen leiden tot meerwerk (F2).
- Verplaatsing naar niet-NL datacenters (A4) vereist DPIA en kan additionele kosten en doorlooptijd veroorzaken (F3).

#### Benodigde input:

- Gegevens van NVAO-product owner en escalatiecontacten.
- Toegangsmiddelen en autorisaties per rol (beheeraccounts, VPN/firewall-toegang).
- Volledige en actuele CMDB, netwerkdiagrammen, back-upbeleid en dataclassificaties.
- Overzicht van betrokken derde partijen en contractuele escalatiepaden.
- Bevestiging van Azure-regio-keuze (West Europe/NL) en gewenste back-up/retentieprofielen.

Benodigde input: