Service Level Agreement
Managed Service Provider (MSP)

GGD GHOR Nederland

Inhoudsopgave

1. Inleiding 3
1.1 Document informatie 3
1.2 Opdrachtgever en opdrachtnemer 3
1.3 Doel van deze SLA 4
1.4 Context en achtergrond 4
1.5 Contractperiode 4
1.6 Scope van de dienstverlening 5
1.7 Uitgangspunten 6
1.8 Definities en begrippen 6
1.9 Rollen en verantwoordelijkheden 7

2. Servicevensters en beschikbaarheid 9
2.1 Service center 9
2.2 Beschikbaarheidsniveaus 9
2.3 Reparatie en vervanging van producten 10

3. Incident-, Request-, en Problem Management 11
3.1 Incident management 11
3.2 Reactietijden en oplostijden (MSP-minimum) 12
3.3 Service niveaus 12
3.4 Request Management 12
3.5 Problem Management 13

4. Escalatieprocedure 14

5. Change- en Releasemanagement 15
5.1 Changeproces 15
5.2 Classificatie van wijzigingen 15
5.3 Change Authority Board 16
5.4 Onderhouds- en release vensters 16
5.5 Patchmanagementproces 18

6. Security en Compliance 19
6.1 Informatieplicht wet- en regelgeving 19

7. Configuratie management en Asset management 20
7.1 Configuratie management 20
7.2 Asset management 20
7.3 Rollen en verantwoordelijkheden 20
7.4 Procesafspraken 20
7.5 Gegevens aan te leveren door opdrachtnemer 21

8. Rapportages en overleg 22
8.1 Rapportages 22
8.2 Overlegstructuur 22

9. Wijzigingen SLA, Audits en Exit 24

Akkoordverklaring 25

1. Inleiding

1.1 Document informatie

Dit document beschrijft de overeengekomen servicelevels tussen de Opdrachtgever en Leverancier, inclusief de verantwoordelijkheden, prestaties en beschikbaarheid van de IT-diensten.

- **Versie:** 0.1 – *Concept voor afstemming met SLM en Inkoop- en Contractmanagement (IC&M)*
- **Datum:** [in te vullen]
- **Opdrachtgever:** GGD GHOR Nederland
- **Opdrachtnemer:** [in te vullen]

Documentatiebeheer

De Opdrachtnemer draagt er gedurende de gehele looptijd van de overeenkomst zorg voor dat GGD GHOR Nederland toegang heeft tot actuele, volledige en correcte documentatie van alle geleverde diensten en systemen.

Deze documentatie omvat ten minste:

- **Functionele documentatie** (beschrijving van processen, gebruikershandleidingen, werkinstructies);
- **Technische documentatie** (architectuur, systeemconfiguraties, interfaces, netwerkdocumentatie, onderhouds- en back-upprocedures);
- **Wijzigings- en releasegeschiedenis;**
- **Contactgegevens** van relevante MSP-rollen en ondersteuningsstructuren.

De Opdrachtnemer zorgt ervoor dat deze documentatie tijdig wordt bijgewerkt na iedere wijziging, release of aanpassing, en stelt deze digitaal beschikbaar via een door Opdrachtgever goedgekeurd platform of documentatieportaal. Eventuele documentatieformaten of templates worden door GGD GHOR Nederland aangeleverd of goedgekeurd.

1.2 Opdrachtgever en opdrachtnemer

Deze Service Level Agreement (SLA) bevat de Service Level afspraken tussen Opdrachtgever en Opdrachtnemer inzake de levering, het beheer en de ondersteuning van managed services. Deze SLA wordt overeengekomen door:

GGD GHOR Nederland, gevestigd en kantoorhoudende te Zwarte Woud 2, 3524 SJ Utrecht, rechtsgeldig vertegenwoordigd door [naam vertegenwoordiger], hierna te noemen: **'Opdrachtgever';**

En

[Naam MSP], gevestigd te [adres], rechtsgeldig vertegenwoordigd door [naam vertegenwoordiger], hierna te noemen: **'Opdrachtnemer'**;

Overwegende dat:

Deze SLA maakt onlosmakelijk deel uit van de Overeenkomst tussen Opdrachtgever en Opdrachtnemer en bevat aanvullende afspraken over de geleverde diensten.

De definities uit de Overeenkomst zullen op gelijke wijze in deze SLA worden gebruikt.

In deze SLA worden de kwalitatieve en kwantitatieve afspraken, met betrekking tot het beheer en onderhoud van de managed services van GGD GHOR Nederland, vastgelegd.

De praktische aspecten van afstemming tussen Opdrachtgever en Opdrachtnemer met betrekking tot de overeengekomen dienstverlening zijn opgenomen in het Dossier Afspraken en Procedures (DAP). In het DAP zijn de werkafspraken en procedures op het koppelvlak tussen Opdrachtgever en Opdrachtnemer vastgelegd. Het DAP maakt integraal deel uit van deze SLA.

1.3 Doel van deze SLA

Deze Service Level Agreement (SLA) legt de afspraken vast tussen GGD GHOR Nederland en de Managed Service Provider (MSP) voor het leveren van managed services. Het doel is om continuïteit, voorspelbaarheid en kwaliteit van ICT-dienstverlening te waarborgen, zodat medewerkers optimaal kunnen werken binnen een veilige en stabiele digitale omgeving.

1.4 Context en achtergrond

GGD GHOR Nederland is de landelijke koepelorganisatie van 25 GGD'en en GHOR's en ondersteunt de publieke gezondheid en veiligheid. Na de COVID-19-pandemie heeft de organisatie gekozen voor een strategische ICT-transitie: het uitfaseren van de eigen IV-voorzieningen en het omschakelen naar managed services.

Deze transitie stelt GGD GHOR Nederland in staat om:

- Schaalbaar en flexibel op te schalen van circa 300 FTE naar maximaal 1.000 FTE in crisissituaties;
- Gestandaardiseerd en efficiënt te werken volgens ITIL v4-principes en moderne IT-servicemanagement (ITSM)-processen;
- Compliance en informatiebeveiliging te borgen conform BIO, AVG, NEN-ISO 27001/27002 en de GIBIT 2023-richtlijnen;
- Continuïteit en voorspelbaarheid te realiseren door duidelijke afspraken met de MSP over prestaties, beschikbaarheid en kwaliteit van dienstverlening.

1.5 Contractperiode

Binnen vier (4) weken na voorlopige gunning levert de MSP aan GGD GHOR Nederland een definitieve Service Level Agreement (SLA) en Dossier Afspraken en Procedures (DAP). Deze definitieve SLA en DAP zijn gebaseerd op de reactie van GGD GHOR Nederland op de bij inschrijving ingediende documenten.

De definitieve SLA en DAP vormen onderdeel van de Raamovereenkomst en zijn bindend voor beide partijen gedurende de looptijd van het contract.

1.6 Scope van de dienstverlening

De MSP levert en beheert de onderstaande kantoorautomatiseringsdiensten. Deze diensten zijn geïntegreerd en worden geleverd op basis van overeengekomen servicelevels, rapportages en beveiligingsnormen.

Domein	Omschrijving
Kantoorinfrastructuur	Beheer van netwerkverbindingen (LAN/WAN/Wi-Fi), hardware en randapparatuur.
Kantoorautomatisering	Levering en beheer van Microsoft 365-diensten (Exchange, Teams, SharePoint, OneDrive), printing en audiovisuele faciliteiten.
Werkplekdiensten	Levering, beheer en onderhoud van virtuele en fysieke werkplekken (incl. on-boarding/off-boarding).
Cloudhosting	Hosting en beheer van kantoorapplicaties in de cloud, inclusief optionele applicatiehosting.
Servicedesk & Incidentmanagement	1e en 2e-lijns ondersteuning, incidentregistratie, classificatie en escalatie.
Back-up & Recovery	Back-upbeheer conform vastgestelde RPO/RTO-afspraken en herstelprocedures.
Change & Release Management	Beheer van standaard- en spoedwijzigingen via een goedgekeurde CAB-procedure.
Monitoring & Rapportage	Proactieve monitoring van systemen en maandelijkse SLA-rapportage.
Managed Hardware	Inkoop, distributie, installatie en lifecycle-management van devices (laptops, desktops, mobiele devices, randapparatuur).
Cloud Solution Provider (Software Licensing)	Levering, facturatie en beheer van softwarelicenties via een CSP-model, inclusief automatische provisioning en licentie-optimalisatie.
Managed Telecom	Levering en beheer van zakelijke telefonie, conferencing en meeting-faciliteiten.
Managed End-User Services	Gebruikersondersteuning, advies en periodieke gebruikerscommunicatie.
Integratie met ServiceNow	Volledige koppeling met ServiceNow voor servicemanagement, rapportage en workflow-automatisering.
Compliance en Security	Levering conform BIO, AVG, ISO 27001/27002 en GIBIT 2023; uitvoering van periodieke audits.
Managed Printing	Beheer, levering en onderhoud van printomgevingen, inclusief tonerbeheer, beveiligd printen en gebruiksrapportages.
Managed Meeting	Levering en beheer van meeting- en vergadertechnologie (AV-oplossingen, room booking, conferencing), inclusief proactief onderhoud.
Managed Firewalls	Beheer, configuratie en monitoring van firewalloplossingen, inclusief updates, patching en security-regels.

1.7 Uitgangspunten

De volgende uitgangspunten zijn van toepassing op de MSP-dienstverlening:

- **Servicekwaliteit:** duidelijke afspraken over service-windows, responstijden, oplostijden en escalatieprocedures (zie hoofdstuk 2 en 4).
- **Meetbaarheid:** KPI's voor beschikbaarheid, performance, incidentafhandeling en klanttevredenheid zijn contractueel vastgelegd en maandelijks gerapporteerd (zie hoofdstuk 5 en 7).
- **Servicemanagement:** volledige integratie met ServiceNow; processen van Opdrachtgever zijn leidend (zie hoofdstuk 5).
- **Continuïteit**: de MSP borgt redundantie, back-up, herstel en failover-mechanismen conform afgesproken RPO/RTO (zie hoofdstuk 2.2).
- **Flexibiliteit:** dienstverlening is schaalbaar en vendor-neutraal ingericht om vendor lock-in te voorkomen.
- **Samenwerking:** beide partijen werken samen op basis van de in hoofdstuk 7 beschreven overlegstructuur (operationeel, tactisch en strategisch), inclusief periodieke service-reviews, verbetertrajecten en innovatievoorstellen.

1.8 Definities en begrippen

Begrip	Definitie
MSP (Managed Service Provider)	De opdrachtnemer die verantwoordelijk is voor de levering van managed ICT-diensten.
Opdrachtgever (GGD GHOR Nederland)	De organisatie die de diensten afneemt en contractueel toeziet op naleving van SLA en DAP.
DAP (Dossier Afspraken en Procedures)	Document waarin alle operationele, tactische en strategische afspraken, procedures en verantwoordelijkheden zijn vastgelegd.
SLA (Service Level Agreement)	Overeenkomst waarin prestaties, beschikbaarheid en kwaliteit van dienstverlening contractueel zijn vastgelegd.
Incident	Een verstoring van de dienst of een dreiging daarvan.
Major Incident	Incident met grote impact op kritieke bedrijfsprocessen; vereist speciale aanpak.
Beveiligingsincident	Ongewenste gebeurtenis die BIV (Beschikbaarheid, Integriteit, Vertrouwelijkheid) bedreigt.
Service Request (SR)	Formeel verzoek van een gebruiker om informatie, advies of een standaardactie (bijv. accountaanmaak).
Responstijd	Tijd tussen registratie van het incident/service request en start van de oplossing.
Oplostijd	Tijd tussen start oplossen en functioneel herstel van de dienst.
KEDB (Known Error Database)	Database met bekende fouten en work arounds.
RCA (Root Cause Analysis)	Analyse om de onderliggende oorzaak van een probleem vast te stellen.
SLM (Service Level Management)	Proces voor definiëren, bewaken en verbeteren van SLA's.
Service Window	Tijdsvenster waarin de dienst gegarandeerd is volgens SLA.
Onderhoudsvenster (Maintenance Window)	Afgesproken periode voor gepland onderhoud van systemen of infrastructuur.

Begrip	Definitie
P1–P4	Prioriteitsniveaus op basis van impact en urgentie: P1 = Kritisch, P2 = Hoog, P3 = Normaal, P4 = Laag.
RPO (Recovery Point Objective)	Maximale aanvaardbare hoeveelheid dataverlies, uitgedrukt in tijd.
RTO (Recovery Time Objective)	Maximale aanvaardbare tijd om de dienst volledig te herstellen na een incident.
Change Authority (CAB)	Formele overlegstructuur die wijzigingen (non-standard, spoed, emergency) beoordeelt en goedkeurt.
Change Coördinator	Persoon die wijzigingen coördineert en bewaakt.
Standard Change	Vooraf gedefinieerde wijziging met lage impact.
Non-Standard Change	Maatwerk wijziging, vereist impactanalyse en goedkeuring.
Spoedwijziging	Wijziging om kritieke incidenten te voorkomen of op te lossen.
Emergency Change	Directe wijziging bij calamiteiten, mondelinge goedkeuring vereist.
OTAP (Ontwikkel, Test, Acceptatie, Productie)	Standaard ontwikkel- en implementatieroute voor softwarewijzigingen.
BIO (Baseline Informatiebeveiliging Overheid)	Overheidsrichtlijn voor informatiebeveiliging.
AVG (Algemene Verordening Gegevensbescherming)	Europese privacywetgeving voor verwerking van persoonsgegevens.
ISO 27001/27002	Internationale normen voor informatiebeveiliging en best practices.
GIBIT 2023	Richtlijnen voor informatievoorziening en ICT bij GGD'en en GHOR.
SLR (Service Level Rapportage)	Periodieke rapportage van prestaties, incidenten, wijzigingen, beschikbaarheid, capaciteitsbeheer, security management, afwijkingen en verbeteracties.
KPI (Key Performance Indicator)	Meetbare norm voor prestaties, zoals beschikbaarheid of incidentafhandeling.
CSAT (Customer Satisfaction Score)	Klanttevredenheidsscore, bijvoorbeeld gemeten op een schaal van 1–5 via ticket-enquêtes.
ServiceNow	Servicemanagementplatform voor registratie, monitoring en rapportage.

1.9 Rollen en verantwoordelijkheden

Dit hoofdstuk beschrijft de rollen en verantwoordelijkheden van zowel Opdrachtgever als Managed Service Provider (MSP). Het doel is om duidelijkheid te creëren over wie verantwoordelijk, aansprakelijk, geconsulteerd en geïnformeerd is bij de uitvoering van contract- en serviceactiviteiten. Deze rollen zijn gebaseerd op CATS CM, Prince II Agile en ITIL-methodieken en vormen de basis voor governance en samenwerking.

Rol	Korte omschrijving
Opdrachtgever	Vertegenwoordigt de organisatie die de opdracht geeft; verantwoordelijk voor businesscase en doelstellingen
Contracteigenaar	Formeel eigenaar van het contract binnen de organisatie; eindverantwoordelijk

Rol	Korte omschrijving
Contractmanager	Beheert het contract gedurende de looptijd; stuurt op prestaties, risico's en relatiebeheer
Leveranciersmanager	Richt zich op de relatie met de leverancier op tactisch niveau; stuurt op samenwerking en leverancierssstrategie
Contractbeheerder	Houdt administratieve kant van het contract bij: bewaakt termijnen, archief en wijzigingen
Prestatiemanager	Richt zich op het meten en beoordelen van afgesproken prestaties
Servicemanager	Zorgt voor afstemming tussen contractafspraken en operationele dienstverlening
Juridisch Adviseur	Adviseert over juridische aspecten van het contract en bewaakt compliance
Inkoopadviseur / -manager	Ondersteunt bij contractvorming en aanbestedingen
Financieel Adviseur	Adviseert over tarieven, indexaties, budgetbewaking en betalingsschema's
Business Owner / Functioneel eigenaar	Vertegenwoordigt interne klant/gebruiker; bewaakt aansluiting op functionele behoefte
Risicomanager	Identificeert en mitigeert contractrisico's
Change Manager	Beheert wijzigingen die impact hebben op contract of uitvoering
Leverancier/ Vendor	Partij die prestatie levert volgens het contract
Stakeholders (intern/extern)	Overige belanghebbenden die input geven op uitvoering en resultaten
Service Level Manager	Definieert, onderhandelt en bewaakt SLA's; coördineert communicatie tussen klant en MSP
Service Owner	End-to-end verantwoordelijk voor een specifieke dienst
Proces Owner SLM	Ontwerpt, onderhoudt en verbetert het Service Level Management-proces
Service Desk & ICT beheer	Coördineert incidenten, service requests en escalaties; bewaakt operationele prestaties

2. Servicevensters en beschikbaarheid

Dit hoofdstuk legt de afspraken vast over de beschikbaarheid van systemen, applicaties en servicedesk. Het doel is om continuïteit van de dienstverlening te waarborgen en meetbare normen vast te leggen, inclusief berekeningsmethoden en uitzonderingen.

2.1 Service center

De MSP kan de service-windows van de dienstverlening tijdelijk opschalen indien dit noodzakelijk is om kritieke incidenten op te lossen of de continuïteit van de dienstverlening te waarborgen.

- **Servicedesk telefonisch:** Maandag t/m vrijdag, 08:00 – 18:00 uur (exclusief erkende feestdagen)
- **Portal & e-mail:** 24/7 voor registratie van incidenten en service requests
- **Noodnummer (P1):** 24/7 bereikbaar voor kritieke incidenten
- **Incident-afhandelingsvenster:** Prioriteit 1 tijdens noodnummer, prioriteit 1–4 via portal/e-mail
- **Taal en ondersteuning:** Nederlands

2.2 Beschikbaarheidsniveaus

Component	Beschikbaarheid	Beschikbaarheids-venster	Onderhoudsvenster	Maximale downtime per kwartaal
Werkplekken (fysiek/virtueel)	≥ 99,5% per kwartaal	Ma–Vr 08:00–18:00	Buiten kantooruren	≤ 10,92 uur
Applicaties (Office 365, standaard apps)	≥ 99,5% per kwartaal	24/7	Buiten kantooruren	≤ 10,92 uur
Netwerk & VPN	≥ 99,8% per kwartaal	24/7	Buiten kantooruren	≤ 5,46 uur

Toelichting: Beschikbaarheid wordt gemeten tot en met het koppelvlak van de lijnverbinding met GGD GHOR Nederland. Buiten het servicevenster blijft het systeem beschikbaar voor normaal gebruik, met uitzondering van gepland onderhoud. De MSP dient voldoende redundantie te hebben ingebouwd om deze beschikbaarheid te garanderen.

Herstelparameters	Norm
RPO (Recovery Point Objective)	Maximaal 4 uur
RTO (Recovery Time Objective)	Maximaal 8 uur
Disaster Recovery Test	Minimaal jaarlijks

Opmerkingen:

- De RTO gaat in vanaf het moment dat GGD GHOR Nederland en de MSP gezamenlijk besluiten tot herstel, bijvoorbeeld het terugzetten van een back-up.
- Na onderhoud of incidenten controleert de MSP het systeem actief op beschikbaarheid en gebreken. Indien mogelijk en noodzakelijk worden deze direct hersteld.

- Beschikbaarheid wordt als volgt berekend:
  Beschikbaarheid (%) = (Aantal uren binnen servicevenster – niet-beschikbare uren) / Aantal uren binnen servicevenster × 100%

2.3 Reparatie en vervanging van producten

Bij het vervangen van hardware, software of andere producten door de Opdrachtnemer blijven alle bepalingen van de originele levering volledig van kracht. Dit omvat onder andere garanties, onderhoudsafspraken, support en beveiligingsnormen.

De Opdrachtnemer draagt er zorg voor dat vervangingen zodanig worden uitgevoerd dat de continuïteit van de dienstverlening en de afgesproken servicelevels niet worden aangetast.

Eventuele updates of configuraties die nodig zijn naar aanleiding van vervanging worden door de Opdrachtnemer uitgevoerd conform de overeengekomen processen en onderhoudsvensters.

De Opdrachtgever kan de Opdrachtnemer verzoeken advies te geven over onderwerpen die niet direct vallen onder de overeengekomen Producten en Diensten, mits deze binnen de scope van de Raamovereenkomst liggen.

3. Incident-, Request-, en Problem Management

3.1 Incident management

Opdrachtnemer hanteert een formeel vastgelegde incidentenprocedure, opgenomen als separaat document in het Dossier Afspraken en Procedures (DAP). Incidenten worden geclassificeerd op basis van impact en urgentie in vier prioriteitsniveaus (P1–P4), conform onderstaande definities.

De prioriteit wordt bepaald op basis van:

- Impact: organisatie/ afdeling/ individu;
- Urgentie: werk ligt stil/ ernstig belemmerd/ beperkt hinder/ geen hinder.

Major incident

Een Major Incident betreft een incident op diensten die kritieke bedrijfsprocessen ondersteunen. Het Major Incident Management-proces richt zich op:

- Het continueren van de dienstverlening en de primaire bedrijfsprocessen;
- Het nemen van mitigerende maatregelen tijdens een crisis om de impact te minimaliseren;
- Het herstellen van de crisis en het treffen van maatregelen ter voorkoming van herhaling.

Beveiligingsincident

Een Beveiligingsincident is een of meerdere (ongewenste of onverwachte) gebeurtenissen die een grote kans hebben om bedrijfsprocessen te bedreigen en/of een risico vormen voor de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van informatie.

Alle incidenten worden geregistreerd en opgevolgd via het centrale servicemanagementsysteem van Opdrachtgever (ServiceNow). De status van incidenten is real-time inzichtelijk voor Opdrachtgever.

Indien sprake is van een structureel probleem of herhaalde incidenten:

- Start Opdrachtnemer binnen 4 werkdagen met het oplossen van het probleem;
- Voert binnen 5 werkdagen een Root Cause Analysis (RCA) uit;
- Levert uiterlijk binnen 10 werkdagen een verbeterplan op, inclusief:
    - Oorzakenanalyse;
    - Concrete verbeteracties;
    - Planning en verantwoordelijken;
    - Risico's en mitigerende maatregelen.

Het verbeterplan wordt ter acceptatie voorgelegd aan Opdrachtgever. Opdrachtnemer rapporteert periodiek over de voortgang conform het DAP. Een incident wordt pas als opgelost beschouwd wanneer de eindrapportage door Opdrachtgever is geaccepteerd.

De escalatiemanager van Opdrachtnemer is direct aanspreekbaar bij interpretatieverschillen of structurele incidenten en bewaakt de naleving van doorlooptijden.

3.2 Reactietijden en oplostijden (MSP-minimum)

Prioriteit	Voorbeelden	Responstijd	Oplostijd
P1 – Major/Kritisch	Hele organisatie ligt stil; uitval netwerk/werkplekken	≤ 30 minuten	≤ 4 uur
P2 – Hoog	Locatie/afdeling ernstig belemmerd	≤ 30 minuten	≤ 1 werkdag
P3 – Normaal	Enkelvoudige storing; workaround mogelijk	≤ 2 uur	≤ 1 week
P4 – Laag	Vraag/kleine hinder	≤ 4 uur	≤ 2 weken

Opmerkingen:

- P1-incidenten worden altijd telefonisch gemeld via het noodnummer (24/7).
- Meting pauzeert bij wachten op klant of derde partij (vastgelegd in ticket).
- Alleen diensten binnen MSP-beheer tellen mee.

3.3 Service niveaus

De responstijden en oplostijden kunnen per incidenttype verschillen afhankelijk van het gekozen serviceniveau. Deze afspraken worden vastgelegd in de Nadere Overeenkomst tussen Opdrachtgever en Opdrachtnemer.

- **Niveau 1 – standaard:** standaard responstijden en oplostijden zoals in §3.2.
- **Niveau 2 – uitgebreid:** verbeterde responstijden voor kritieke incidenten, extra rapportage.
- **Niveau 3 – kritiek:** prioriteit bij alle P1/P2-incidenten, snellere escalatie en wekelijkse voortgangsrapportage.
- **Niveau 4 - maatwerk**: afwijkende SLA-parameters in overleg.

Opdrachtgever heeft de mogelijkheid om in de Nadere Overeenkomst af te wijken van de standaardparameters. Alle serviceniveaus worden gemonitord en gerapporteerd in de Service Level Rapportage (SLR).

3.4 Request Management

Een Standaard Service Request is een verzoek van een gebruiker voor het leveren van een vooraf gedefinieerde dienst (bijvoorbeeld accountaanmaak, rechtenwijziging of software-installatie). Het doel is om deze verzoeken effectief en gebruiksvriendelijk af te handelen, conform vooraf vastgestelde kosten, stappen en doorlooptijden. Kenmerken:

- **Gestandaardiseerd proces:** uitgevoerd volgens vooraf goedgekeurde procedures en kosten.
- **Doorlooptijden:** vastgelegd in deze SLA en/of Nadere Overeenkomst.
- **Facturering:** indien van toepassing, conform vooraf overeengekomen afspraken.
- **Registratie:** alle service requests worden vastgelegd in het door Opdrachtgever aangewezen systeem (ServiceNow).
- **Autorisatie:** alleen verzoeken van geautoriseerde personen worden in behandeling genomen. De autorisatielijst wordt door Opdrachtgever beheerd en periodiek geactualiseerd. Opdrachtnemer controleert bij elk verzoek of de aanvrager voorkomt op deze lijst en legt deze controle vast in

ServiceNow. Verzoeken van niet-geautoriseerde personen worden niet uitgevoerd, tenzij vooraf schriftelijk bevestigd door Opdrachtgever.

In het Dossier Afspraken en Procedures (DAP) wordt vastgelegd:

- De procedure voor het bijwerken van de autorisatielijst;
- De rollen en bevoegdheden van geautoriseerde personen;
- De wijze van verificatie door Opdrachtnemer.

Doorlooptijden

Type	Responstijd	Afhandeltijd
Service Request (standaard)	≤ 16 kantooruren	≤ 40 kantooruren
Service Request (spoed)	≤ 8 kantooruren	In overleg

Opdrachtnemer informeert de aanvrager proactief over de status en voortgang van het verzoek. Indien een verzoek niet kan worden uitgevoerd binnen de gestelde termijn, wordt dit tijdig gecommuniceerd inclusief reden en nieuwe planning.

3.5 Problem Management

Het doel van Problem Management is om structurele oorzaken van incidenten te identificeren en definitief op te lossen, zodat herhaling wordt voorkomen en de impact op de dienstverlening wordt geminimaliseerd.

Processtappen:

- **Detectie:** Start bij herhaalde incidenten of signalen van structurele problemen.
- **Root Cause Analysis (RCA):** Binnen 5 werkdagen na constatering voert Opdrachtnemer een RCA uit.
- **Verbeterplan:** Binnen 10 werkdagen levert Opdrachtnemer een verbeterplan op, inclusief:
  - Oorzakenanalyse;
  - Concrete verbeteracties;
  - Planning en verantwoordelijken;
  - Risico's en mitigerende maatregelen.

- **Known Error Database (KEDB):** Bekende fouten en workarounds worden vastgelegd en gedeeld met Opdrachtgever.
- **Rapportage:** Voortgang wordt periodiek gerapporteerd in de Service Level Rapportage (SLR).

Problem Management sluit aan op Continual Improvement en kan leiden tot wijzigingen via het Change Management-proces.

4. Escalatieprocedure

In geval van een tekortschietende prestatie of interpretatieverschil treden Opdrachtgever (GGD GHOR Nederland) en de Opdrachtnemer (MSP) in overleg. De escalatieprocedure kent drie niveaus, elk met een specifiek mandaat:

Eerste escalatieniveau – Accountteam/ Servicedesk
Mandaat: Operationele afhandeling van incidenten en verzoeken binnen de afgesproken servicelevels.
Verantwoordelijkheden:

- Eerste aanspreekpunt voor dagelijkse operationele issues;
- Initiëren van herstelacties bij incidenten;
- Registratie en communicatie via ServiceNow.

Tweede escalatieniveau – Functionaris
Mandaat: Bevoegd tot het toewijzen van extra middelen, personeel en het aanpassen van operationele processen.
Verantwoordelijkheden:

- Coördinatie bij structurele problemen of herhaalde incidenten.
- Opstellen van verbeterplannen en impactanalyses.
- Afstemming met Opdrachtgever over voortgang en maatregelen.

Derde escalatieniveau – Directie MSP/ Procuratiehouder
Mandaat: Eindverantwoordelijkheid voor de dienstverlening binnen de overeenkomst.
Verantwoordelijkheden:

- Besluitvorming bij escalaties met strategische impact.
- Vertegenwoordiging van MSP in strategisch overleg.
- Goedkeuring van structurele wijzigingen en exit-maatregelen.
- Vendor escalatie**:** Indien nodig escaleren naar externe leveranciers (bijv. Microsoft, hardware- of softwarepartners) om kritieke problemen op te lossen of aanvullende ondersteuning te verkrijgen.

De MSP benoemt een escalatiemanager die fungeert als aanspreekpunt bij interpretatieverschillen of structurele problemen. Deze persoon is direct aanspreekbaar en verantwoordelijk voor het bewaken van de doorlooptijden en bereikbaarheid zoals vastgelegd in de SLA en het DAP.

Indien een tekortschietende prestatie een overschrijding van een SLA-parameter inhoudt en toerekenbaar is aan de MSP, kan de Opdrachtgever boetes of service credits opleggen, conform de Nadere Overeenkomst. Bij overmacht (conform definitie in het Burgerlijk Wetboek) worden geen boetes opgelegd.

5. Change- en Releasemanagement

Het doel van Change- en Releasemanagement is om wijzigingen gecontroleerd, voorspelbaar en veilig door te voeren, met minimale impact op de continuïteit van de dienstverlening. Alle wijzigingen worden door Opdrachtnemer geregistreerd in het door Opdrachtgever aangewezen servicemanagementsysteem (ServiceNow). De processen van Opdrachtgever zijn leidend.

5.1 Changeproces

Wijzigingen op de dienstverlening worden beheerst door een formeel Changeproces.
Een normale change is een toevoeging, aanpassing of verwijdering van (een gedeelte van) de bestaande IT-services en infrastructuur, zoals:

- Periodieke wijziging (bijv. updates of onderhoud);
- Functionele wijziging (bijv. nieuwe functionaliteit);
- Technische wijziging (bijv. configuratieaanpassing).

Procesafspraken:

- Alle changes worden uitgevoerd in samenspraak met de Opdrachtnemer en de door GGD GHOR Nederland aangewezen Change Coördinator.
- Voor elke wijziging is een impactanalyse, draaiboek en rollback-plan verplicht.
- De operationele processen van de Opdrachtnemer sluiten aan op de processen van de Opdrachtgever, waarbij de processen van de Opdrachtgever leidend zijn.
- Indien een wijziging mislukt, wordt het rollback-plan direct uitgevoerd en geëvalueerd met de Change Coördinator.
- Na uitvoering informeert de leverancier de Change Coördinator over de status van de wijziging of rollback.
- Spoed- of kritieke changes (ter voorkoming of oplossing van P1) worden gecoördineerd door de Change Coördinator. De Opdrachtnemer levert achteraf alle benodigde informatie voor registratie en evaluatie.

Alle wijzigingen worden door de Opdrachtnemer geregistreerd in het door de Opdrachtgever aangewezen servicemanagementsysteem (waaronder ServiceNow).

5.2 Classificatie van wijzigingen

Wijzigingen worden geclassificeerd als:

- **Standard Change**: vooraf gedefinieerd, lage impact; onderdeel van het Request Managementproces.
- **Non-Standard Change**: maatwerk, vereist impactanalyse en goedkeuring.
- **Spoedwijziging**: noodzakelijk om kritieke incidenten (P1/P2) te voorkomen of op te lossen.
- **Emergency Change**: direct uitvoeren bij calamiteiten; mondelinge goedkeuring vereist.

Wijzigingen worden niet uitgevoerd zonder expliciete goedkeuring van de Change Authority Board van de Opdrachtgever. OTAP-route (Ontwikkel, Test, Acceptatie, Productie) wordt toegepast waar mogelijk.

Type change	Responstijd	Doorlooptijd/Oplevering	Toelichting
Change (standaard)	≤ 16 kantooruren	≤ 40 kantooruren	Vooraf gedefinieerd, lage impact
Change (spoed)	≤ 2 kantooruren	≤ 16 kantooruren	Met hogere prioriteit, afwijkende kosten mogelijk
Non-Standard Change	≤ 40 kantooruren	Planning in overleg	Impactanalyse en offerte/changeplan via CAB
Emergency Change	Zo snel mogelijk	Zo snel mogelijk	Voor kritieke situaties (P1/P2)

5.3 Change Authority Board

Alle wijzigingsverzoeken worden door de Opdrachtnemer geregistreerd in het door de Opdrachtgever aangewezen systeem (zoals ServiceNow).

Daarbij levert de Opdrachtnemer volledige en tijdige informatie over:

- Impactanalyse op beschikbaarheid, beveiliging en continuïteit;
- Risico's en beheersmaatregelen;
- Planning en verwachte doorlooptijd;
- Benodigde resources en afhankelijkheden;
- Terugvalscenario's voor het geval implementatie mislukt.

De Opdrachtgever bepaalt op basis van deze informatie of een wijziging wordt goedgekeurd, uitgesteld of afgekeurd. De Opdrachtnemer voert geen wijziging uit zonder expliciete goedkeuring van de **Change Authority Board** van GGD GHOR Nederland.

Spoedeisende wijzigingen (Emergency Changes) kunnen alleen worden uitgevoerd na mondelinge goedkeuring van de aangewezen autoriteit bij de Opdrachtgever; deze goedkeuring wordt achteraf formeel vastgelegd in de CAB-registratie.

De Opdrachtnemer is verantwoordelijk voor de uitvoering en oplevering van goedgekeurde wijzigingen en rapporteert hierover in de eerstvolgende Service Level Rapportage (SLR) en/of het operationeel overleg. Eventuele verstoringen of escalaties als gevolg van de wijziging worden onmiddellijk gemeld conform de incident- en escalatieprocedures.

5.4 Onderhouds- en release vensters

Het doel van onderhouds- en releasevensters is om wijzigingen en updates gecontroleerd en met minimale impact op de dienstverlening door te voeren. Deze afspraken volgen ITIL-principes en zijn afgestemd op de processen van GGD GHOR Nederland.

De Opdrachtnemer stemt het onderhoudsvenster van systemen en infrastructuur afzonderlijk af met de release vensters van de Opdrachtgever.

Onderhoudsvensters

Gepland onderhoud wordt uitgevoerd door de Opdrachtnemer buiten de reguliere servicevensters van de Opdrachtgever, tenzij schriftelijk anders overeengekomen. De Opdrachtnemer meldt gepland onderhoud minimaal vijf (5) werkdagen vooraf aan de Opdrachtgever, inclusief:

- Datum en tijdsduur van het onderhoud;
- Verwachte impact op systemen en gebruikers;
- Advies voor acties door de Opdrachtgever indien nodig.

Gepland onderhoud wordt niet meegenomen in de berekening van beschikbaarheid zoals beschreven in deze SLA.

Preventief onderhoud

- Wordt periodiek uitgevoerd door de Opdrachtnemer;
- Heeft lage impact en veroorzaakt geen merkbare hinder voor gebruikers;
- Dient ter voorkoming van incidenten en ter borging van continuïteit van de dienstverlening.

Spoedonderhoud

- Wordt uitgevoerd na overleg met de Opdrachtgever;
- Kan wel impact hebben op gebruikers en systemen;
- Wordt meegenomen in de beschikbaarheidsberekening en wordt uitgevoerd zo snel mogelijk om continuïteit te herstellen;
- De Opdrachtgever wordt direct geïnformeerd over planning, impact en eventuele benodigde acties.

Pandemie-afspraak:

- In geval van opschaling (bijvoorbeeld pandemie) wordt onderhoud uitgevoerd **na 23:00 uur**, in overleg met de Opdrachtgever.

Release vensters

Releases van software, updates of nieuwe functionaliteiten worden uitgevoerd door de Opdrachtnemer binnen de door de Opdrachtgever goedgekeurde releasevensters. Releases mogen alleen plaatsvinden na:

- Schriftelijke goedkeuring van de Opdrachtgever;
- Afstemming van eventuele impact op bestaande services en gebruikers.

Releases buiten de overeengekomen releasevensters zijn uitsluitend toegestaan in geval van Emergency Changes, na expliciete schriftelijke goedkeuring van de Opdrachtgever.

De Opdrachtnemer waarborgt dat alle onderhouds- en release-activiteiten zodanig worden gepland en uitgevoerd dat de continuïteit van de dienstverlening wordt gegarandeerd en de afgesproken servicelevels niet worden aangetast.

5.5 Patchmanagementproces

Security- en patchmanagement omvat het identificeren, verkrijgen, installeren en controleren van software-updates (patches). Deze patches zijn cruciaal voor:

- Het corrigeren van fouten,
- Het verbeteren van beveiliging,
- Het verhogen van functionaliteit.

De Opdrachtnemer integreert patchmanagement naadloos in de dienstverlening en maakt onderscheid tussen:

- **Standaard security patches:** automatisch toegepast zonder merkbare impact op gebruikers.
- **Specifieke patches:** vereisen vooraf een gedetailleerde evaluatie van impact en noodzaak. Implementatie verloopt via het formele Changeproces, inclusief:
  - Impactanalyse,
  - Risicobeoordeling,
  - Rollback-plan,
  - Goedkeuring door de Change Authority Board (CAB).

Type update	Vereiste actie
Kritische security-updates/ patches (CVSS ≥ 9.0)	Binnen 24 uur na publicatie geïnstalleerd door Opdrachtnemer, in afstemming met GGD GHOR Nederland
Hoge security-updates/ patches (CVSS ≥ 7.0)	Binnen 5 werkdagen na publicatie geïnstalleerd door Opdrachtnemer, in afstemming met GGD GHOR Nederland

KPI	Definitie	Norm	Frequentie
Beschikbaarheid per component	Uptime binnen venster excl. gepland onderhoud	≥ targets per §3.2	Maandelijks
Incidentafhandeling	% op tijd per prioriteit	≥ 80% binnen norm	Maandelijks
CSAT (ticket-enquête)	Gemiddelde score 1–5	> 3.5/5	Maandelijks
Patch compliance	% devices up-to-date	≥ 95% binnen termijn	Maandelijks
Back-ups geslaagd	% succesvolle back-ups	≥ 99,9%	Maandelijks

Monitoring & rapportage:

- Patchstatus wordt continu gemonitord via het servicemanagementsysteem (ServiceNow).
- Opdrachtnemer rapporteert maandelijks over patch compliance, met als doelstelling ≥ 95% up-to-date systemen binnen de gestelde termijnen.

6. Security en Compliance

De Opdrachtnemer werkt conform relevante normen en wetgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), Baseline Informatiebeveiliging Overheid (BIO), ISO/IEC 27001 en 27002, en NEN 7510 (indien van toepassing). Jaarlijks verstrekt Opdrachtnemer een onafhankelijk auditrapport of certificaatbewijs ter onderbouwing van compliance. Privacy-afspraken zijn vastgelegd in de verwerkersovereenkomst.

Onderwerp	Eis (MSP-minimum)
Toegangsbeheer	Multi-Factor Authenticatie (MFA) is verplicht voor alle beheerders. Waar mogelijk wordt gebruikgemaakt van Just-In-Time (JIT) en Just-Enough-Access (JEA) principes.
Patching (werkplekken/servers)	Critical patches worden binnen 14 dagen toegepast; High-priority patches binnen 30 dagen; overige patches conform de overeengekomen patchcyclus.
Logging & monitoring	24/7 monitoring van alle kerncomponenten. Logretentie bedraagt minimaal 90 dagen. Logging is gescheiden van andere diensten en wordt periodiek geëvalueerd.
Kwetsbaarheden	Identificatie en mitigatie van kwetsbaarheden verloopt via het formele changeproces. Kwartaalrapportages over kwetsbaarheden en genomen maatregelen worden gedeeld met Opdrachtgever.
Security-incidenten	Security Incidenten worden geclassificeerd als P1 of P2. Melding aan Opdrachtgever vindt plaats conform de termijnen in het Dossier Afspraken en Procedures (DAP) en de AVG.

6.1 Informatieplicht wet- en regelgeving

De Opdrachtnemer is verplicht de Opdrachtgever schriftelijk en tijdig te informeren over wijzigingen of nieuwe wet- en regelgeving die van invloed kunnen zijn op de uitvoering van de geleverde Producten en Diensten. De Opdrachtnemer draagt er zorg voor dat deze informatie wordt voorzien van een toelichting op de impact, eventuele risico's en concrete aanbevelingen voor mitigatie of implementatie.

De Opdrachtnemer neemt deze informatie op in het tactisch en strategisch overleg met de Opdrachtgever, zodat gezamenlijk kan worden bepaald welke acties noodzakelijk zijn om continuïteit, compliance en kwaliteit van de dienstverlening te waarborgen.

De Opdrachtgever behoudt het recht om op basis van deze informatie aanvullende richtlijnen of instructies te geven aan de Opdrachtnemer met betrekking tot de uitvoering van de Producten en Diensten.

7. Configuratie- en Asset Management

Het doel van configuratiemanagement en assetbeheer is om een volledig, actueel en betrouwbaar overzicht te hebben van alle geleverde producten en diensten, inclusief hun eigenschappen en relaties. Dit is essentieel voor continuïteit, compliance, security en effectief beheer.

7.1 Configuratie management

Configuratiemanagement waarborgt dat alle componenten van de IT-dienstverlening (zoals hardware, software, licenties, certificaten en lokale apparatuur) correct en volledig worden vastgelegd in de Configuration Management Database (CMDB) van de leverancier. Wijzigingen in de IT-omgeving worden te allen tijde tijdig en accuraat verwerkt zodat het overzicht betrouwbaar blijft.

7.2 Asset management

Assetbeheer omvat het registreren, beheren en actualiseren van alle assets binnen het Asset Register van GGD GHOR Nederland, inclusief contractuele en financiële gegevens. De GGD-assetmanager neemt hierbij het initiatief en bepaalt welke informatie noodzakelijk is voor een volledige en juiste opname in het Asset Register.

De opdrachtnemer, Product Owner en/of projectleider leveren alle relevante informatie en bijbehorende specificaties die nodig zijn om geleverde producten en diensten correct te kunnen registreren. Deze informatie kan betrekking hebben op — maar is niet gelimiteerd tot — software, hardware, certificaten, lokale apparatuur, serienummers, versienummers en gekoppelde gebruikers.

7.3 Rollen en verantwoordelijkheden

Opdrachtnemer:

- Levert alle relevante configuratiegegevens en specificaties van geleverde producten en diensten.
- Houdt de eigen CMDB actueel bij wijzigingen in de IT-omgeving.
- Informeert GGD GHOR Nederland direct over wijzigingen die impact hebben op configuratie of assetbeheer.

Opdrachtgever (GGD GHOR Nederland):

- Beheert het Asset Register en neemt het initiatief voor updates.
- Geeft wijzigingen in de IT-omgeving door aan de leverancier, zodat deze in de CMDB verwerkt kunnen worden.

7.4 Procesafspraken

- Gegevens worden aangeleverd in een door Opdrachtgever vastgesteld formaat en met een frequentie zoals vastgelegd in het Dossier Afspraken en Procedures (DAP).
- Bij wijzigingen:
  - Indien de Opdrachtnemer zelf wijzigingen doorvoert, zorgt deze voor een update in de CMDB en informeert GGD GHOR Nederland.
  - Indien GGD GHOR Nederland wijzigingen doorvoert, worden deze doorgegeven aan de Opdrachtnemer.

7.5 Gegevens aan te leveren door opdrachtnemer

De opdrachtnemer levert alle relevante configuratie- en assetgegevens aan, zodat deze volledig en correct kunnen worden opgenomen in het Asset Register van GGD GHOR Nederland. Deze informatie omvat onder andere:

Configuratie- en productgegevens:

- Serienummers en typenummers
- Hardware- en softwareconfiguraties
- Versienummers en gekoppelde gebruikers
- Licentiegegevens inclusief geldigheidsduur
- Certificaten en lokale apparatuur
- Installatie- en onderhoudsstatus
- Locatie en organisatorische toewijzing

Contractuele en financiële specificaties:

- Omschrijving (zoals type licentie, onderhoudsovereenkomst of abonnement) en aantallen
- Naam en contactgegevens van licentiegever, onderhoudsleverancier of abonnementsverstrekker
- Type support en bijbehorende contactinformatie, inclusief supportprocedure
- Uniek opdrachtnummer van GGD GHOR Nederland
- Ingangsdatum van de (nadere) overeenkomst
- Einddatum van de (nadere) overeenkomst
- Totale verwervingsprijs van de overeenkomst
- Periodieke kosten (bijv. eenmalig, jaarlijks, per kwartaal of per maand)
- Eventuele verschillen tussen contractafspraken en het daadwerkelijk gebruik door GGD GHOR Nederland op de peildatum van rapportage

De opdrachtnemer is verantwoordelijk voor de juistheid, volledigheid en tijdige aanlevering van deze informatie.

8. Rapportages en overleg

8.1 Rapportages

Opdrachtgever levert maandelijks een Service Level Rapportage (SLR) aan Opdrachtnemer. Deze rapportage wordt besproken in het operationeel overleg en vormt de basis voor tactische en strategische evaluaties.

De SLR bevat ten minste de volgende onderdelen:

- Service Level Performance (KPI's);
- Incidenten en problemen;
- Wijzigingen en releases;
- Beschikbaarheid en onderhoud;
- Capaciteitsbeheer;
- Security management;
- Afwijkingen en verbeteracties;
- Toekomstige acties en roadmap.

Opdrachtnemer is verantwoordelijk voor:

- Het leveren van input voor de SLR waar nodig;
- Het opvolgen van afspraken en acties die voortkomen uit het SLR-overleg;
- Het rapporteren over voortgang van verbeteracties in de daaropvolgende SLR.
- De structuur en het format van de SLR worden vastgelegd in het Dossier Afspraken en Procedures (DAP).

Het format en de structuur van de SLR worden vastgesteld door de Opdrachtgever en vastgelegd in het Dossier Afspraken en Procedures (DAP). De Opdrachtnemer houdt zich te allen tijde aan dit format en zorgt dat resultaten en acties correct worden uitgevoerd. Eventuele escalaties worden tijdig gemeld conform de overeengekomen procedures.

8.2 Overlegstructuur

De Opdrachtnemer verplicht zich deel te nemen aan al de door de Opdrachtgever georganiseerde overlegvormen (operationeel, tactisch en strategisch), die nodig geacht worden in het kader van de uitvoering van de Opdracht. Voor alle drie de overleggen geldt dat de Opdrachtnemer verantwoordelijk is voor de verslaglegging. Het verslag wordt binnen vijf (5) werkdagen digitaal voorgelegd aan de Opdrachtgever ter goedkeuring. De Opdrachtgever zal binnen 5 werkdagen reageren en aangeven of de gespreksverslagen al dan niet definitief opgemaakt kunnen worden en verstuurd kunnen worden naar alle deelnemers van het desbetreffende overleg.

De Opdrachtgever levert na gunning een format aan waarbinnen de verslaglegging dient plaats te vinden. Van het operationeel, tactische en strategisch overleg maakt de Opdrachtnemer het verslag.

Operationeel overleg
Operationeel overleg vindt zo vaak als noodzakelijk plaats. Dit overleg kan persoonlijk, telefonisch, per e-mail of schriftelijk plaatshebben, zowel op initiatief van de Opdrachtgever als van de Opdrachtnemer. Afhankelijk

van de behoefte en het onderwerp. Vanuit de Opdrachtgever wordt een of meerdere contactperso(o)n(en) aangesteld.

Tactisch overleg
Tactisch overleg vindt minimaal één keer per half jaar plaats. Dit overleg zal een bijeenkomst zijn van de accountmanager van de Opdrachtnemer en de Contractmanager van de Opdrachtgever. Onderwerpen die op de agenda staan zijn o.a. de prestatie op de verschillende KPI's, marktontwikkelingen, kwaliteitscontrole, etc..

Strategisch overleg
Strategisch overleg vindt minimaal één keer per jaar plaats. Dit overleg zal plaatshebben met de Contractmanager en de Teamleider van Contractmanagement van de Opdrachtgever en met de centrale contactpersoon en de commercieel directeur van de Opdrachtnemer. Tijdens dit overleg zullen naast de onderwerpen van het tactisch overleg ook verbeteringen voor efficiency, eventuele op handen zijnde prijs aanpassingen, eventuele boetes, etc. besproken worden.

Jaarlijks vindt er een evaluatiegesprek plaats tussen de aangewezen contactpersoon van de MSP en GGD GHOR Nederland. Tijdens dit gesprek worden de samenwerking, prestaties, verbeterpunten en strategische ontwikkelingen besproken. De MSP levert voorafgaand aan het gesprek een overzicht van relevante KPI's, trends en openstaande acties.

9. Wijzigingen SLA, Audits en Exit

- **Herziening SLA**: minimaal jaarlijks of eerder indien nodig; wijzigingen via addendum, wederzijds bekrachtigd.
- **Audits**: Opdrachtgever kan audits laten uitvoeren; MSP verleent medewerking en levert bewijsstukken. Kostenverdeling conform Hoofdovereenkomst/GIBIT-bepalingen.
- **Exit & overdraagbaarheid**: MSP levert exit-plan, data-export in overeengekomen formaten, overdracht documentatie en kennis, en redelijke medewerking aan transitie (exit-termijnen en vergoedingen in de Overeenkomst/DAP).

Akkoordverklaring

Aldus overeengekomen en in tweevoud ondertekend:

GGD GHOR Nederland	[Naam MSP]
Plaats: Utrecht:	Plaats: [in te vullen]
Datum:	Datum:
_____	_____
Handtekening	Handtekening
Naam:	Naam:
Functie:	Functie:

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl