



Bijlage 7 – Service level agreement

Gemeente Almere



INHOUD

1	Inleiding	4
1.1	Doel	4
1.2	Vastlegging van partijen en goedkeuring	4
1.3	Ingangs- en einddatum	4
2	Governance	5
2.1	Verlengingsproces	5
2.2	Beëindigingsproces	5
2.3	Ontbinding en garanties	5
2.4	Wijzigingsproces	6
3	Dienstverlening, doelen en resultaten	7
3.1	Ambitie	7
3.2	Doelen en resultaten	7
3.3	Dienstverlening – SaaS Toegang en Regie	8
3.3.1	Software, onderhoud & beheer	8
3.3.2	Contactpunten	8
3.3.3	ITIL procesmanagement	8
3.4	Wijkteams	9
3.4.1	Opdracht wijkteams	9
3.4.2	Dienstverlening	9
3.5	Buiten de scope	10
3.6	Vitale bedrijfsfuncties, processen en activiteiten	10
3.7	Integratie	10
3.8	Business impact bij verlies van de dienst	10
3.9	Gebruiksresultaat	11
3.10	Kwaliteit	12
3.11	Dienstverleningstijden	12
3.12	On site ondersteuning	12
3.13	Infrastructuur	13
3.14	Wijzigingen	13
3.15	Eigendom	13
4	Communicatie	15
4.1	Contactpersonen gemeente en leverancier	15
4.2	Dienstrapportages	16
4.3	Uitzonderingen en klachten	17
4.4	Tevredenheidsonderzoeken	17
4.5	Servicebeoordelingen	17
4.6	Geheimhouding	17
5	Dienstenniveau	18
5.1	Beschikbaarheidsdoelstellingen	18
5.2	Opslagbeheer	18
5.3	Productie- en testomgeving	19
5.4	Aantasting van systemen en operationele processen	19
5.5	Betrouwbaarheidsdoelen	19
5.6	Capaciteit/prestatiedoelstellingen en garanties	19
5.6.1	Capaciteit & schaalbaarheid	19
5.6.2	Responstijden	20
6	Beveiligingseisen	22
6.1	Authenticatie & Autorisatie	22

6.2	Cryptografie	22
6.3	Gebruiksapparatuur	22
6.4	Incidentbeheer en rapportage	22
6.5	Logging en monitoring	23
6.6	Auditing	23
6.7	Vulnerability management	24
6.8	Databeheer	25
6.9	Afscherming van gegevens	25
6.10	Dataclassificatie	25
6.11	Gegevens mirroring, back-up/restore	26
6.12	Datalevenscyclus	26
6.13	Gegevensoverdraagbaarheid	26
7	Bescherming persoonsgegevens	27
7.1	Gezugscode, normen, standaarden en certificeringen	27
7.2	Doelbinding	27
7.3	Dataminimalisatie	27
7.4	Gebruiksbeperkingen	28
7.5	Openheid, transparantie en kennisgeving	28
7.5.1	Verantwoording	28
7.5.2	Geografische locatie van gegevens	28
7.5.3	Interventies	29
7.1	Meldplicht AVG inbreuk	29
8	KPI's Performanceniveau	30
10	Kosten	35
10.1	Prijzen	35
10.2	Betalingsvoorwaarden	35
10.3	Sancties	35

1 Inleiding

Deze SLA beschrijft de door de opdrachtnemer geleverde producten en/of diensten en de daarbij overeengekomen service en/of kwaliteitsniveau, zoals deze door de opdrachtnemer aan de gemeente wordt aangeboden.

1.1 Doel

Doel van de SLA is bindende kwalitatieve en kwantitatieve afspraken te maken over de kwaliteitsparameters voor het te realiseren dienstenniveau en over de rapportage daarover, met als doel om de kwaliteit en uitvoering van de producten en dienstverlening te monitoren en te verbeteren.

1.2 Vastlegging van partijen en goedkeuring

Hier worden de contactgegevens van zowel de vertegenwoordiger van de leverancier van de dienst (Opdrachtnemer) als van de afnemer (Opdrachtgever) vermeld. Dit zijn meestal de personen die goedkeuring geven aan de SLA en namens beide partijen de SLA ondertekenen.

- Vertegenwoordiger leverancier
Hier worden de contactgegevens van de vertegenwoordiger van de leverancier (Opdrachtnemer) van de dienst vermeld, meestal is dit de service level manager.
- Vertegenwoordiger gemeente
Hier worden de contactgegevens van de vertegenwoordiger van de gemeente (Opdrachtgever) vermeld.
- Goedkeuring
De goedkeuring van de SLA is de gezamenlijke verantwoordelijkheid van de gemeente en de Opdrachtnemer (service level manager).

1.3 Ingangs- en einddatum

Hier worden de ingangs- en einddatums van de SLA beschreven, tevens wordt aangegeven of er een (tussen)evaluatie plaatsvindt.

De Overeenkomst treedt in werking op [datum contractondertekening] . De looptijd van de overeenkomst voor het leveren, implementeren en onderhouden van een ICT prestatie (SaaS oplossing) ter ondersteuning voor Toegang en (casus)Regie loopt tot en met 01-04-2027 (4 jaar).

De initiële looptijd van de live operationele SaaS-dienstverlening is 01-04-2023 tot 1-04-2027, na inwerkingtreding van de Overeenkomst op [datum contractondertekening].

Op het moment van de eerste verlenging kan een synchronisatie plaatsvinden met de looptijd van de aanbesteding Software WMO en Backoffice dienstverlening Wmo en Jeugd als BPO, hetgeen een bekorting van 3 tot 6 maanden kan betekenen. De looptijd van de Gebruiksrechten is minimaal gelijk aan de looptijd van de Overeenkomst. Na afloop van de voornoemde looptijd wordt de overeenkomst slechts op verzoek van Opdrachtgever verlengd. Opdrachtgever geeft uiterlijk zes (6) maanden voor einde looptijd aan de Overeenkomst te verlengen.

De Overeenkomst heeft een maximale duur van 12 jaar en mag vier (4) maal worden verlengd. Bij verlenging wordt de Overeenkomst verlengd met een periode van twee (2) jaar.

De looptijd van de Gebruiksrechten is minimaal gelijk aan de looptijd van de Overeenkomst. De SLA maakt onderdeel uit van de Overeenkomst, de looptijd is gelijk aan de looptijd van de Overeenkomst.

2 Governance

Governance is het proces waarbij de dienstverlening wordt bestuurd en gecontroleerd. Het belangrijkste aandachtspunt is de manier waarop wijzigingen en updates van een dienst worden beheerd. Of het wijzigingsverzoek nu afkomstig is van de gemeente die de dienst afneemt of van de dienstleverancier, maakt niet uit. Dit zal verder worden uitgewerkt in de DAP.

2.1 Verlengingsproces

De overeenkomst kan 4 keer verlengd worden met 2 jaar. De verlengingen kunnen uitsluitend door opdrachtgever uiterlijk 6 maanden voorafgaand aan het aflopen van de overeenkomst worden ingeroepen, middels een verlengingsbrief getekend door de budgethouder van de gemeente Almere.

2.2 Beëindigingsproces

Het beëindigingsproces vindt plaats wanneer de gemeente die de dienst afneemt of de dienstleverancier, ervoor kiest om de overeenkomst te ontbinden.

De beëindiging kan uitsluitend door opdrachtgever uiterlijk 6 maanden voorafgaand aan het aflopen van de overeenkomst worden ingeroepen, middels een [(aangetekend) schrijven.

De uitstapmomenten kunnen enkel worden ingeroepen door wijzigingen in:

- wet- en regelgeving;
 - technologische ontwikkelingen;
- middels een [aangetekend] schrijven.

Het beëindigingsproces wordt vastgelegd in een exit-plan (te vinden in het Dossier Afspraken en Procedures (DAP)). Het exit-plan is binnen een half jaar na contractondertekening gereed en wordt vervolgen ieder kwartaal geactualiseerd. Vaststelling en goedkeuring van het exit-plan zal geschiede door Opdrachtgever of een vertegenwoordiger van Opdrachtgever. Het exit-plan stelt de gemeente in staat om de gemeentelijke gegevens binnen een aangegeven tijdsperiode veilig te stellen voordat de dienstleverancier de gemeentelijke gegevens uit systemen van de dienstleverancier wist (inclusief back-ups, hiervoor geldt mogelijk een ander tijdschema). De richtlijnen zoals opgenomen in de bijlage Richtlijn Overdragen en Migreren zijn van toepassing en moet aan worden voldaan.

De opdrachtnemer moet bij beëindiging van de overeenkomst aantoonbaar alle archiefbescheiden, en bijbehorende metadata, overdragen aan de gemeente conform tevoren afgesproken procedures en bestandsformaten. Opdrachtnemer verwijdt daarna aantoonbaar alle archiefbescheiden en metadata uit de beheeromgeving.

De leverancier dient minimaal de gegevens beschikbaar te stellen die voor opdrachtgever nodig zijn om aan de wettelijke verplichtingen en lokale afspraken te voldoen.

2.3 Ontbinding en garanties

Indien gedurende de looptijd van de overeenkomst blijkt dat Opdrachtnemer niet voldoet aan één of meerdere minimeisen, terwijl Opdrachtnemer heeft verklaard dat hij aan alle minimeisen voldoet,

dan wordt dit als niet-nakoming van de overeenkomst aangemerkt en zal de Opdrachtnemer in gebreke worden gesteld, tenzij correcte werking en nakoming blijvend onmogelijk is.

De gevolgen van het niet halen van Service Levels kan resulteren in (gedeeltelijke) ontbinding van de Overeenkomst in ieder geval na meerdere meetperiodes achtereenvolgens niet halen van dezelfde Service Levels. Gemeente heeft het recht om de geleden schade te verhalen. Betaalde sancties (als onderdeel van de afgesproken maatregelen) worden in mindering gebracht op de eventueel te betalen schadevergoeding.

2.4 Wijzigingsproces

Wijzigingen op de in het SLA vastgelegde regelingen, prestaties en rapportages kunnen zowel een incidenteel als een blijvend (structureel) karakter hebben. Wijzigingen op de SLA worden in het SLA-overleg tussen de beslissingsbevoegde vertegenwoordigers van de gemeente en Opdrachtnemer(service level manager) afgestemd. Wanneer één van de partijen aanleiding ziet om wijzigingen in de SLA aan te brengen, doet deze partij hiertoe een schriftelijk voorstel aan de andere partij. Vervolgens treden de partijen hierover in overleg. Een tussentijdse aanpassing van de SLA verkrijgt rechtskracht na overeenstemming en ondertekening door de daartoe bevoegde vertegenwoordigers (Zie Dossier Afspraken en Procedures (DAP)) van beide partijen.

3 Dienstverlening, doelen en resultaten

3.1 Ambitie

De gemeente Almere optimaliseert en moderniseert de informatievoorziening en uitvoerende dienstverlening binnen het Sociaal Domein.

De ambitie van de gemeente Almere is om een SaaS informatievoorziening Toegang en Regie (voorportaal) in aansluiting op de Wmo processen en dienstverlening Backoffice Wmo en Jeugd als BPO in Sociaal Domein, voor de Gemeente Almere en haar ketenpartners te realiseren die:

- aansluit bij de behoefte in de maatschappij, de eindgebruikers, op het gebied van dienstverlening en goede zorg;
- invulling geeft aan de behoefte van de medewerkers van gemeente en partners en de eisen die aan hen gesteld worden;
- de gemeente in staat stelt te voldoen aan het beleid van integrale en vroegtijdige Toegang en regie;
- de gemeente in staat stelt de data die gegenereerd wordt, in te zetten voor Business Intelligence en het 'voorspellen' van de zorgbehoefte in de stad.

3.2 Doelen en resultaten

Het doel van deze aanbesteding is om te komen tot een aanbieder die "SaaS Informatievoorziening Toegang en Regie (voorportaal)" in aansluiting op Wmo processen en dienstverlening Backoffice Wmo en Jeugd als BPO in het Sociaal Domein aanbiedt, die de gemeente in staat stelt optimale hulp en ondersteuning aan inwoners met een ondersteuningsbehoefte te bieden, waarbij de inwoners centraal staan.

Het resultaat van deze aanbesteding is een optimaal functionerende "SaaS Informatievoorziening Toegang en Regie (voorportaal)" in aansluiting op Wmo processen en dienstverlening Backoffice Wmo en Jeugd als BPO in het Sociaal Domein, die voldoet aan de gestelde eisen.

Het resultaat van deze aanbesteding draagt bij aan de realisatie van de volgende doelen:

- De Wijkteams zijn in staat om regie (zie definities) te voeren over casussen;
- Inwoners kunnen een actieve rol vervullen in hun proces door toegang tot en uitoefening van AVG rechten op hun eigen gegevens;
- De gemeente faciliteert de integrale samenwerking tussen interne en externe dienstverleners rondom de inwoner;
- De gemeente beschikt over gegevens en informatie om te kunnen sturen, verantwoorden en voorspellen;
- De gemeente heeft inzicht in effectiviteit van subsidies en beleid;
- We vinden voor elke hulpvraag een passende oplossing door belanghebbenden toegang te geven tot de relevante en toegestane informatie;
- Naadloze integratie met de oplossing(en) als gevolg van eerdergenoemde aanbesteding ICT Prestatie Wmo en Dienstverlening BPO.
- De gemeente kan proactief in spelen op landelijke ontwikkelingen en te voldoen aan de wettelijke- en regelgevende taken;
- Verlaging van de administratieve lasten voor zowel de klanten, zorgaanbieders als de gemeentelijke organisatie zelf;
- Er is een optimale samenwerking tussen zorgleveranciers, inwoners en ketenpartners;

- Innovatieve inzet van dataoplossingen middels artificial of business intelligence (AI/BI) teneinde een verschuiving te bewerkstelligen binnen de zorgverlening van reactief naar preventief;
- Gebruikers zijn volledig opgeleid gedurende de looptijd van de overeenkomst;
- Soepele implementatie transitie beheer;

3.3 Dienstverlening – SaaS Toegang en Regie

3.3.1 Software, onderhoud & beheer

Beschikbaar stellen van een SaaS informatievoorziening Toegang en Regie (voorportaal) in aansluiting op de Wmo processen en dienstverlening Backoffice Wmo en Jeugd als BPO in Sociaal Domein overeenkomend met de aanbestedingsdocumenten.

De Opdrachtnemer is verantwoordelijk voor het onderhoud en ondersteuning:

- Correctief Onderhoud
- Preventief Onderhoud
- Innovatief Onderhoud
- Gebruiksondersteuning en trainingen

Het technisch beheer (infrastructuur) wordt uitgevoerd door de Opdrachtnemer. Ook het applicatie beheer (doorontwikkeling en onderhoud van de applicatie) wordt door Opdrachtgever uitgevoerd.

Gemeente Almere voert het functioneel beheer (behoeftemanagement, testen, transitie, gebruiksondersteuning, wijzigingenbeheer, etc.) uit.

3.3.2 Contactpunten

Voor het uitvoeren van de dienstverlening wat o.a. staat beschreven in de paragrafen 2.1, 2.2. en 2.3 van deze SLA draagt de Opdrachtnemer zorg voor het bereikbaar en beschikbaar zijn van (verschillende) contactpunten. Contactpunt voor o.a.:

- vragen van (interne en externe) gebruikers over de software (ICT helpdesk), mogelijk via de interne ICT organisatie van gemeente Almere (ICTAR);
- contact m.b.t. de uitvoering van dienstverlening Opdrachtnemer i.r.t. de overeenkomst tussen Opdrachtnemer en Opdrachtgever;
- het melden van een datalek (procedure 24/7 beschikbaar).

3.3.3 ITIL procesmanagement

De opdrachtgever werkt vanuit de regieorganisatie conform het ITIL versie 4 (IT Infrastructure Library) procesmanagement framework. Van de opdrachtnemer wordt verwacht dat er aansluiting plaatsvindt op minimaal de volgende actieve processen:

- Incident management: voor het dagelijks beheren van onverwachte incidenten en het zo spoedig mogelijk herstellen van de dienstverlening,
- Problemen management: voor het structureel aanpakken c.q. wegnemen van trends in incidenten, of naar aanleiding van monitoring en/of logging informatie van de opdrachtnemer,
- Change management: voor het gecontroleerd en gestructureerd doorvoeren van wijzigingen binnen de omgeving,
- Release management: voor het onderhouden van applicatie- en infraversies, ook wel life cycle management genoemd en het bijhouden van de End of Life cycli van alle toeleveranciers en haar producten,

- Capacity management: voor het beheren en controleren van de capaciteit van alle aanwezige systemen binnen de kaders van dit SLA en hier tijdig en adequaat op inspelen door uitbreidingen en/of aanpassingen via change management door te voeren,
- Continuous service improvement: voor het continu toepassen van verbeteringen binnen de kaders van dit SLA.

Door in het DAP nadere afspraken over deze, en eventueel aanvullende processen te maken, garandeert de opdrachtnemer dat er door middel van een bewezen methode beheer en regie kan worden gevoerd over de dienstverlening.

3.4 Wijkteams

De Wijkteams hebben een laagdrempelige toegang waar inwoners met hun vragen op sociaal-maatschappelijk gebied terecht kunnen. Het wijkteam kijkt, samen met de inwoner, welke oplossingen de inwoners zelf kan inzetten en welke rol het netwerk om de inwoners heen kan spelen bij een antwoord op de vraag. Ook wordt gekeken welke informele en collectieve oplossingen voorhanden zijn die (mogelijk aanvullend) ingezet kunnen worden. Indien nodig leidt het wijkteam toe naar individuele, professionele ondersteuning of zorg. Hiertoe werken de MEE-IJsseloevers, de VMCA, De Schoor en de gemeente Almere samen binnen het Consortium Sociale Wijkteams Almere.

3.4.1 Opdracht wijkteams

De opdracht van de Sociale Wijkteams Almere is:

1. Versterking van de burgerkracht/ samenlevingsopbouw;
2. Vraagverheldering en vroeg signalering;
3. Inzet en ontwikkeling van algemene/collectieve activiteiten;
4. Spin in het web zijn ten aanzien van samenwerking en voorzieningen in de wijk;
5. Kortdurende begeleiding en triage (doorgeleiding van complexe/meervoudige zaken);
6. Toegang tot individuele Wmo-voorzieningen (in nauwe samenwerking met de afdeling Zorg & Welzijn) geven.

3.4.2 Dienstverlening

De dienstverlening van de wijkteams bestaat uit:

- Meldingen uit de wijk oppakken. 'Oppakken' betekent een van de volgende keuzes:
 - direct afhandelen, informatie en advies geven
 - keukentafelgesprek
 - verwijzen
- Wijkteam spreekuur;
- Kortdurende begeleiding;
- Waakvlamcontact;
- Collectieven opzetten;
- Administratief spreekuur organiseren;
- Signaleren en vragen van inwoners oppakken;
- Faciliteren bewonersinitiatieven en faciliteren vrijwilligers zoeken/koppelen;
- Netwerken op basis van doelen/speerpunten jaarplan.

3.5 Buiten de scope

Buiten het bereik van deze Service Level Agreement (en aanbesteding) vallen:

- De software voor Wmo processen;
- Backoffice dienstverlening (BPO).

Bovenstaande maakt wel onderdeel van de totale keten en staat daarmee in direct verband met het proces Toegang en Regie.

3.6 Vitale bedrijfsfuncties, processen en activiteiten

De geïdentificeerde vitale bedrijfsfuncties (niet limitatief), processen en activiteiten zijn terug te vinden als bijlage van het DAP. De Gemeente Almere hanteert hierbij de lijst van bedrijf kritische applicaties- en processen, waarbij de top 30 hiervan onderdeel uitmaken van de primaire bedrijfsprocessen.

Het gehele proces van toegang & regie

- Vanaf de start van het proces, beoordelen van de (individuele/collectieve) vraag en toeleiding ervan en de softwarematige ondersteuning daarvan.

Verwerking bedrijf- en persoonsgegevens

- Tijdens de processen worden er financiële-, persoonsgegevens en bijzondere persoonsgegevens verwerkt om de aanvraag te kunnen behandelen en uitvoeren. Zowel gemeente als Opdrachtnemer voldoen aan de BIO. Ook de medewerkers en/of onderaannemers van de Opdrachtnemer dienen zich te houden aan de BIO, waaronder het hebben van een Verklaring omtrent gedrag (VOG) voordat hij toegang mag/kan krijgen tot de kritische applicaties en/of informatie. Ter verduidelijking Opdrachtnemer gelden alle (relevante) BIO normen waar "Dienstenleverancier" als verantwoordelijke(n) (in de laatste kolom van de tabellen) is aangegeven. (M.a.w. deze BIO-normen zijn de eisen van de opdrachtgever). Alle kandidaten (medewerkers), betrokken medewerkers van Opdrachtnemer en ingehuurd personeel dienen hun verantwoordelijkheden te begrijpen, geschikt te zijn voor de rollen waarvoor zij worden overwogen, om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Omdat inwoners toegang hebben tot hun eigen gegevens vallen die, conform BIO, tot de definitie van 'gebruiker'.

Er dient door leverancier periodiek een risico inventarisatie plaats te vinden en de mitigerende maatregelen dienen te worden nagevolgd, zowel op informatieveiligheid, privacy en derdenrekening(en).

3.7 Integratie

De ICT Prestatie dient naadloos te integreren met Software Wmo conform het Programma van Eisen. Vragen die bij de wijkteams zijn binnengekomen en zijn bestemd voor Wmo consultants dienen te worden doorgezet. Andersom dienen betrokken inwoner(s) en wijkteam medewerkers inzicht te kunnen hebben in de voortgang van de aanvraag via de inwonerportaal.

3.8 Business impact bij verlies van de dienst

Bij verlies van de dienst verliest de gemeente overzicht in de zorgvragen die in Almere liggen, kan de inwoner niet zelf regie uitvoeren op zijn/haar dossier en persoonsgegevens, worden de administratieve

lasten verhoogd, kan het voorkomen dat de gemeente niet rechtmatig handelt, vertragen procedures of krijgen inwoners niet altijd de juiste hulp of staan te wachten terwijl er misschien andere zorg voor handen is. Het kan ervoor zorgen dat de veiligheid of zorg van de inwoners van Almere in het geding komt. De dienstverlening aan de inwoners heeft de hoogste prioriteit.

3.9 Gebruiksresultaat

De dienstverlening en software voldoet aan de voorwaarden welke zijn opgenomen in de aanbestedingsdocumenten en aan het onderstaande (niet limitatieve) gebruiksresultaat:

- Een implementatieplan, aansluitend op het Implementatieplan van de opdrachtgever;
- Livegang op 1 april 2023 na positieve acceptatietest (fatale termijn);
- Beschikbaarheid van de Toegang en regie software
- Bereikbaarheid van de (ICT) Helpdesk
- Bereikbaarheid van de contractmanager
- Korte doorlooptijden afhandelen incidenten/vragen interne en externe gebruikers
- Het naar alle tevredenheid van gebruikers spoedig oplossen van Issues/ klachten
- Tevreden (eind)gebruikers
- Een secure verwerking van gegevens/data.
- Voldoet aan de certificering/normen welke van toepassing zijn verklaard in de totale overeenkomst.

De partijen evalueren de dienstverlening op onder andere de volgende indicatoren, waarover verantwoord dient te worden door de opdrachtnemer:

- % beschikbaarheid van de Toegang en regie software op zowel technische paramaters, als ook het eindgebruikersperspectief;
- Bereikbaarheid van de ICT supportgroepen van de opdrachtnemer;
- aantal klachten en categorie klachten en van welke rol, inclusief de afhandeling hiervan;
- % afname klachten;
- % toename van inwoners met toegang tot hun persoonlijke informatie;
- Beoordeling klanttevredenheid van gebruikers m.b.t. software en dienstverlening
- Optimale verwerkingssnelheid van berichten.

De partijen evalueren de kwaliteit van dienstverlening en eventuele verbetermogelijkheden door regelmatig middels een PDCA cyclus de processen te beoordelen. Het betreft onder andere (niet limitatief) de volgende processen en zullen nader worden uitgewerkt in de DAP:

- Proces rapportage, op volledigheid/juistheid rapportages welke zijn overeengekomen met de opdrachtnemer en/of voortkomen uit de verantwoording van de diverse indicatoren;
- Proces wijzigingsbeheer, de mate waarin het wijzigingsbeheerproces is uitgevoerd en is afgestemd op de exploitatieorganisatie van de gemeente; welke categorieën wijzigingen de opdrachtnemer autonoom binnen zijn eigen wijzigingsbeheerproces mag doorvoeren, en over welke wijzigingen afstemming met het wijzigingsbeheerproces van de gemeente plaatsvindt;
- Proces afhandeling klachten;
- Proces toegang;
- Proces actief contractmanagement
- Proces onderhoud en beheer
- Proces audit

De (nul)meting kan enkelzijdig of gezamenlijk worden uitgevoerd en leiden tot een optimalisatie of verbeterplan.

3.10 Kwaliteit

Aan onderstaande kwaliteitsnormen, geldige certificeringen et cetera dient de Opdrachtnemer, inclusief alle door haar in te zetten personeel en derden, te voldoen:

- ISO27001;
- ISO27701;
- NEN-ISO 16175;
- NEN 7513;
- BIO;
- i-standaarden;
- informatiemodel RSGB.

3.11 Dienstverleningstijden

De gemeente Almere hanteert in beginsel een plaats- en tijdsafhankelijk werken beleid. De standaard kantoortijden zijn van maandag tot en met vrijdag op 07:00 uur – 19:00 uur (tijdszone Amsterdam), met uitzondering van algemeen erkende feestdagen.

De dienstverleningstijden van de Opdrachtnemer zijn van maandag tot en met vrijdag 08:30 – 17:00 uur, uitgezonderd algemeen erkende Nationale feestdagen. In hoofdstuk 4 staan de bereikbaarheid-, respons-, & oplostijden.

De dienstverlening is Nederlandstalig en er is sprake van persoonlijk (warm)contact (we willen weten met wie we te maken hebben) via telefoon/e-mail/chat/ticketsysteem en/of nader af te stemmen andere communicatie kanalen.

De opdrachtnemer dient op bovengenoemde tijden ondersteuning te leveren aan interne en externe gebruikers.

Voor prio1 meldingen is de dienstverlening 24/7/365 beschikbaar middels een standby/piket dienst, dit wordt nader uitgewerkt in hoofdstuk 4.

In samenspraak met Opdrachtnemer en Opdrachtgever wordt deze paragraaf nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.

3.12 On site ondersteuning

In voorkomende gevallen dient de functioneel beheerder op locatie van de gemeente ondersteund te worden in het beheer en onderhoud van de Software Toegang en Regie door een onsite support medewerker van de opdrachtnemer. Hiervoor dient een standaard verzoek ingericht te worden via een producten- en dienstencatalogus dat door de opdrachtnemer wordt aangeboden en valt onder de standaarddienstverlening.

3.13 Infrastructuur

Vanwege de aard van de opdracht (SaaS) worden er geen aanpassingen gedaan aan de werkplek Almere, uitgezonderd koppelingen met de gemeentelijke systemen welke noodzakelijk zijn voor een optimale procesflow en samenwerking.

3.14 Wijzigingen

Planbaar onderhoud geschiedt uitsluitend buiten standaard kantoortijden. Ongepland onderhoud geschiedt in overleg met gemeente Almere. Voorzienbare, planbare mutaties, zoals landelijke wijzigingen of aanpassingen in Almeers beleid dienen 3 maanden van tevoren aangegeven en binnen 3 maanden worden doorgevoerd. Incidentele mutaties, binnen 1 week na melding doorvoeren. Regelmatig terugkoppeling over voortgang en einde. Het wijzigingsproces zal worden uitgewerkt en toegevoegd worden aan het DAP. Tevens biedt GIBIT PvE hoofdstuk 8 een leidraad voor de invulling van wijzigingen- en release beheer, waaronder (onder andere):

- Het moment van het verrichten van Onderhoud wordt in onderling overleg bepaald. uitgangspunt daarbij is dat Onderhoud op zodanige wijze plaatsvindt dat dit minst verstorend is voor de bedrijfsprocessen van Opdrachtgever. Onderhoud dat verstorend is of kan werken voor de bedrijfsprocessen van Opdrachtgever wordt bovendien tijdig vooraf aangekondigd.
- Indien en voor zover leverancier bewijst dat een storing of gebrek niet aan hem toerekenbaar is, is hij niet verplicht tot herstel daarvan. Indien opdrachtgever niettemin opdracht geeft tot het pogen tot voornoemd herstel, is leverancier gerechtigd de kosten gemoeid met het herstel separaat door te berekenen.

Er worden met de opdrachtnemer relatieve normen overeengekomen voor hoog volume producten/aantal geraakte gebruikers voor te laat/niet leveren.

3.15 Eigendom

Alle rechten van intellectuele eigendom op de krachtens de Overeenkomst door Leverancier ter beschikking gestelde ICT Prestatie berusten uitsluitend bij Opdrachtnemer of diens licentiegever(s). Alle rechten op de met de ICT Prestatie van Opdrachtgever afkomstige verwerkte gegevens (blijven) rusten bij Opdrachtgever, ongeacht waar deze gegevens staan opgeslagen en ongeacht of de gegevens na initiële ontvangst zijn bewerkt of niet.

Opdrachtnemer verleent een Gebruiksrecht op de ICT Prestatie aan de Opdrachtgever en aan de overige rollen zoals opgenomen in de aanbestedingsdocumenten en aan eventuele Derden die namens de Opdrachtgever opereren. Het Gebruiksrecht omvat in ieder geval het recht de ICT Prestatie (en alle daarin besloten liggende informatie/kennis) te gebruiken voor het Overeengekomen gebruik, alsmede voor testdoeleinden, met inbegrip van alle daarvoor redelijkerwijs noodzakelijke al dan niet tijdelijke verveelvoudigingen en openbaarmakingen. Het Gebruiksrecht omvat niet het recht zelf exploitatiehandelingen te verrichten, tenzij anders overeengekomen.

De Software Toegang en Regie dient een standaard oplossing te zijn en geen softwarematig maatwerk te bevatten. Functionaliteit die specifiek voor deze aanbesteding ontwikkeld zou moeten worden, dient in de eerstvolgende release opgenomen te zijn als standaardfunctionaliteit.

Indien in uitzondering door beide partijen alsnog maatwerk wordt overeengekomen, dient deze in de eerstvolgende release opgenomen te zijn als standaardfunctionaliteit. Niet alleen voor Almere, ook voor andere klanten van opdrachtnemer. Indien eerstvolgende release niet realistisch is, dan geldt zo spoedig mogelijk in overleg.

4 Communicatie

Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken dienstenniveaus en het doorvoeren van veranderingen en verbeteringen (bijvoorbeeld vastgelegd in verbeterplannen), is regelmatig overleg op diverse organisatieniveaus noodzakelijk.

Opdrachtgever en Opdrachtnemer hanteren minimaal onderstaande communicatiestructuur:

Strategisch:

- Periodiek (4x per jaar) afstemmen van ontwikkelingen:
 - o Wet- en regelgeving;
 - o Project en diensten portfolio Opdrachtgever en Opdrachtnemer;
 - o Financieel beleid Opdrachtgever;
 - o Informatiebeveiliging en privacy compliance;
 - o Informatie en technische architectuur.
 - o Trends en marktontwikkelingen.
- Is partner om gezamenlijk actief deel te nemen aan landelijke ontwikkelingen.

Tactisch:

- Periodiek (2x per kwartaal) afstemmen over:
 - o Contractuele zaken;
 - o Projecten (eisen, oplossingen, borging) en wijzigingen (impact, wijzigingsbeheerproces);
 - o Diensten behoefte Opdrachtgever en dienstencatalogus Opdrachtnemer.
 - o Bespreken van de SLA rapportage en de hieraan gekoppelde acties

Operationeel:

- Dagelijks afstemmen over aanvragen die niet geautomatiseerd kunnen worden behandeld, service requests, incidenten en het bewakings-/beheerproces.

Een nadere concretisering van deze overlegvormen is opgenomen in het Dossier Afspraken en Procedures (DAP).

4.1 Contactpersonen gemeente en leverancier

De Governance met betrekking tot o.a. de overleggen, rollen, mandaat en daarbij horende contactpersonen worden opgenomen in de DAP en continu bijgehouden/aangepast afhankelijk van de rolatie.

In de DAP zal worden opgenomen welke de door de gemeente opgegeven rollen, contact kunnen opnemen met de Opdrachtnemer. In de basis mogen alle gebruikers contact opnemen met de Opdrachtnemer, tenzij anders gezamenlijk overeengekomen in de DAP.

Conform het escalatiematrix opgenomen in de governance in de DAP, kan er omhoog worden geëscaleerd.

De volgende rollen zullen o.a. nader worden uitgewerkt in de DAP met de daarbij horende contactpersonen:

Opdrachtgever	Opdrachtnemer
---------------	---------------

Contract board: Groep met personen die vraageigenaar zijn en/of contracteigenaar. O.a.: ▪ Afdelingsmanager Zorg & Welzijn en ICTAR ▪ Teammanager Zorg & Welzijn en ICTAR	Contract board: Groep met personen die leveringseigenaar zijn en/of contracteigenaar.
Contractmanager	Contractmanager
Realisatie- en verificatiemanager: ▪ Service Demand Manager ▪ Senior cluster Sociaal en Publiek ▪ Functioneel- en Technisch beheer ▪ ITIL (IT Infrastructure Library) procesmanagement ▪ Security management ▪ Project management ▪ Architectuur ▪ Business Information Manager ▪ Informatie architecten ▪ CISO ▪ Privacy Coördinator	Realisatie- en verificatiemanager: ▪ Security management, CISO ▪ Project management ▪ Architectuur ▪ Privacy officer
Gebruikers	Productie

4.2 Dienstrapportages

Maandelijks, als onderdeel van de overeenkomst, rapporteert (mits anders overeengekomen) de leverancier aan de gemeente over de normen en indicatoren in deze SLA.

We verwachten van de leverancier ook dat hij proactief mee denkt en advies geeft over verbeteringen in de werkwijze van de gemeente.

De rapportages (niet limitatief), de exacte inhoud en frequentie worden in samenspraak met opdrachtnemer vastgesteld, de hierna volgende tabel geeft een beeld.

Rapportage	Betreft
Algemeen	In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door Opdrachtnemer te leveren/geleverde diensten en specificaties van de software en dienstverlening, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.
(Informatiebeveiliging) incidenten	Een (informatiebeveiliging) incident is een enkele of een reeks van ongewenste of onverwachte gebeurtenissen die een aanzienlijke kans hebben om de bedrijfsvoering te compromitteren of verstoren en een bedreiging vormen voor de informatiebeveiliging. O.a. meldingen/ signalen zwakke plekken in informatiebeveiliging van interne en externe gebruikers en (poging tot) ongeautoriseerde toegang en getroffen maatregelen.
Service Level Agreement	Leverancier zal periodiek aan Opdrachtgever rapport uitbrengen over de nakoming door hem van de overeengekomen Service Levels/KPI's . Zie ook

	artikelen 8.13, 8.14 en 21 van de GIBIT2020 en de daarbij horende verbeterplannen
Capaciteits- en prestatierapportage	Inzicht in alles wat te maken heeft met de afgenomen ICT prestatie en de daarbij horende dienstverlening.
Standaard operationele data	Voor de Software Toegang en Regie geldt dat het systeem standaard operationele rapportages levert om te kunnen sturen op de beschreven processen die het systeem ondersteunt.
Verbeteringen en aanbevelingen	Conform het continuous service improvement proces vanuit ITIL (IT Infrastructure Library) , zal de opdrachtnemer per proces in de maandrapportage SMART verbeteringen en aanbevelingen aandragen aan de opdrachtgever. In samenspraak zullen hier acties aan gekoppeld worden die wederom SMART gedefinieerd worden en onder verantwoordelijkheid van de opdrachtnemer worden uitgevoerd en gerapporteerd aan de opdrachtgever.

4.3 Uitzonderingen en klachten

In overleg met Partijen (Opdrachtnemer en Opdrachtgever) of op initiatief van één Partij wordt er geëscaleerd. Het ultieme doel van een escalatie is gemanagede issue- of probleemoplossing. In het geval een escalatie niet tot volle tevredenheid wordt opgelost worden de geschilstappen vanuit de GIBIT voorwaarden toegepast. De procedure wordt in samenspraak met de leverancier nader uitgewerkt na gunning en is te vinden in het DAP.

4.4 Tevredenheidsonderzoeken

De procedure voor het meten van de tevredenheid wordt in samenspraak met de leverancier nader uitgewerkt na gunning en is te vinden in het DAP.

4.5 Servicebeoordelingen

De procedure voor het meten van de dienst wordt in samenspraak met de opdrachtnemer nader uitgewerkt na gunning en is te vinden in het DAP. De meting dient op regelmatige basis plaats te vinden. Verbeteringen worden in gezamenlijkheid doorgevoerd. Dit begint met een aanleiding wat resulteert in een verbetervoorstel. De procesmanager/-eigenaar besluit met de opdrachtnemer eventueel tot doorvoeren van de verandering.

4.6 Geheimhouding

Een verwerkersovereenkomst maakt deel uit van deze overeenkomst. De verwerker zorgt dat de personen die onder zijn verantwoordelijkheid werkzaam zijn en toegang hebben tot de persoonsgegevens op een of andere schriftelijke manier zijn gehouden aan de geheimhoudingsplicht. De volledige verantwoordelijkheid ligt bij de verwerker.

In artikel 15 van de GIBIT zijn voorwaarden opgenomen m.b.t. geheimhouding voor beide partijen.

5 Dienstenniveau

In dit hoofdstuk worden de kwalitatieve en kwantitatieve dienstenniveaus vastgelegd voor de beschikbaarheids- en betrouwbaarheidsdoelen. Op basis van deze dienstenniveaus vindt monitoring plaats van het geleverde dienstenniveau in relatie met het afgesproken niveau.

5.1 Beschikbaarheidsdoelstellingen

De beschikbaarheid van de Software Toegang en Regie dienstverlening is als volgt:

Beschikbaarheid	Waarde
Servicewindow 1 ma/vr 08:30 – 17:00	98,5%
Servicewindow 2	96,0%

De ICT prestatie moet voor interne en externe gebruikers beschikbaar zijn gedurende Servicewindow 1. Planmatig onderhoud vindt plaats buiten Servicewindow 1 en wordt niet meegenomen in berekening van de beschikbaarheid (in Servicewindow 2).

Servicewindow 2 betreft alle dagen en uren buiten Servicewindow 1, inclusief nationaal erkende feestdagen.

Het niet beschikbaar zijn is niet beperkt tot uitvallen gehele applicatie, ook wanneer de applicatie niet volgens overeengekomen prestatie niet functioneert, zoals bijvoorbeeld wanneer aanvragen niet verwerkt kunnen worden, en/of onderzoeken niet uitgevoerd kunnen worden of mutaties niet verwerkt kunnen worden of informatie niet correct wordt opgehaald/weergegeven etc. De Opdrachtnemer is verantwoordelijk voor het secuur rapporteren over de daadwerkelijke beschikbaarheid.

Bij niet beschikbaar van de applicatie, melding hoe te handelen voor de gebruiker.

Indien er onderhoud is, melding op het scherm inclusief de tijd waarop de dienst wederom beschikbaar gesteld wordt.

Buiten de Servicewindow 1 is er een mogelijkheid om Prioriteit 1 meldingen te kunnen doorgeven middels een standby/piketdienst van de Opdrachtnemer.

5.2 Opslagbeheer

Voor de gemeente is van belang dat er zodanige infrastructurele maatregelen zijn getroffen dat de voortgang en kwaliteit van de dienstverlening niet wordt aangetast. Er zijn aantoonbare adequate maatregelen genomen tegen:

- Beschadiging of verlies van (persoons)gegevens;
- Onbevoegde wijziging van (persoons)gegevens;
- Ontvreemding van (persoons)gegevens;
- Onnodige verdere verwerking van (persoons)gegevens.

het minimaliseren van opslag in de omgeving van de opdrachtgever. Daar waar de opdrachtgever moet besluiten over het wel/niet archiveren of verwijderen van opslag, zal dit door de opdrachtnemer Van de opdrachtnemer wordt verwacht dat er structurele opschoningprocessen ingericht zijn, teneinde

compleet en volledig worden aangediend als casus, waarop de opdrachtgever een besluit over kan nemen.

5.3 Productie- en testomgeving

Naast de productie omgeving heeft de gemeente de beschikking over een omgeving waarin wijzigingen kunnen worden getest. In deze tweede omgeving kan de impact van wijzigingen op het gehele proces worden getest. Wijzigingen mogen pas in productie worden genomen na goedkeuring van de opdrachtgever. Tevens kan deze omgeving gebruikt worden om incidenten na te bootsen waarbij de impact in productie onduidelijk is. De synchronisatie tussen productie en test moet een continu afgesproken proces zijn, waarbij de omgevingen representatief moeten zijn voor de hiervoor geschetste doeleinden.

5.4 Aantasting van systemen en operationele processen

Vanuit de ICT regieorganisatie zal er overleg plaatsvinden over structurele trends, bijvoorbeeld vaak voorkomende (herhaalde) incidenten. Hierbij wordt conform het problem management proces van ITIL versie 4 (IT Infrastructure Library) een plan voor onderzoek opgesteld, een rootcause analyse opgeleverd, een actielijst met verwijzingen naar wijzigingen (change management proces) en een evaluatie van dit geheel. In het DAP worden de raakvlakken tussen opdrachtnemer-gever met betrekking tot het problem management proces, nader uitgewerkt. Hiermee trachten wij de aantasting van systemen en operationele processen, op een gecontroleerde en gestructureerde wijze, aan te sturen in samenwerking met de leverancier.

5.5 Betrouwbaarheidsdoelen

De betrouwbaarheidsdoelen die worden vereist zijn 100% op:

Doel	Norm
Mean Time Between Failures (MTBF)	> 2 uur
Mean Time Between Service Incidents (MTBSI)	> 4 uur

Indien de opdrachtnemer lager dan 100% scoort, zal dit door middel van verbeteracties en aanbevelingen in het Service Level Rapportage (SLA rapport maandelijks), worden opgenomen en bewaakt zolang dit het gewenste niveau van 100% weer bereikt. In het geval van het niet behalen van de afgesproken verbeterdeadline, zullen beide partijen door middel van een verbeterplan (continuous service improvement plan van ITILversie 4(IT Infrastructure Library)) de noodzaak en urgentie verhogen en daarmee adequaat inspelen op de niet-gehaalde deadline.

5.6 Capaciteit/prestatiedoelstellingen en garanties

Capaciteitsbeheer is zodanig geregeld dat de gevraagde dienstenniveaus gehaald en onderhouden kunnen worden op basis van de scope van de opdracht. Houdt hierbij rekening met het feit dat op mogelijke groei van de capaciteitsvraag wordt geanticipeerd en dat de specifieke capaciteitsbehoefte per systeem is vastgelegd.

5.6.1 Capaciteit & schaalbaarheid

In de gemeente Almere wonen ruim 216.000 inwoners en het aantal interne gebruikers is naar verwachting 250. Gemeente Almere heeft als doelstelling voor 2050 om naar 350.000 inwoners te groeien. Op basis hiervan verwacht de opdrachtgever dat de opdrachtnemer in de prognose van de

groei rekening houdt met capaciteit en schaalbaarheid van systemen en processen. Hiervoor dient via de afgesproken governance tijdig en volledig gerapporteerd te worden, zodat de opdrachtgever op advies van de opdrachtnemer toekomstvast beslissingen kan nemen. Veranderingen in de organisatiedoelstellingen worden door middel van de strategische overleggen kenbaar gemaakt en hierop dient in de tactische- en operationele lagen geanticipeerd te worden, waarbij de verantwoordelijkheid voor de impactbepaling op de dienst primair bij de opdrachtnemer ligt.

5.6.2 Responstijden

Er kan onderscheid worden gemaakt in soorten vragen met oplossingstermijnen (bijv.: PDC niet actueel, moet snel worden opgelost).

Op basis van urgentie wordt de responsetijd bepaald.

Prioriteit	Aanmeldtijd bereikbaarheid	Responsetijd	Oplostijd	Servicewindow (zie paragraaf 5.10)
1; kritiek	< 5 minuten	< 15 minuten	< 4 uur	1 & 2
2; hoog	< 5 minuten	< 15 minuten	< 8 uur	1
3; middel	< 5 minuten	< 30 minuten	< 16 uur	1
4; laag	< 5 minuten	< 30 minuten	In overleg < 40 uur	1

Definitie Prioriteit:

Prioriteit	Urgentie	Impact (op gebruikers)
P1 - Kritiek	Bedrijfs- en/of missie kritische processen of applicaties liggen stil of worden ernstig verstoord	Een zeer ernstige productie verstoring die ofwel alle gebruikers raken ofwel het functioneren van de gemeente Almere
P2 – Hoog	Bedrijfs- en/of missie kritische processen liggen stil of worden ernstig verstoord. Er is eventueel een Workaround beschikbaar.	Een ernstige productie verstoring die ofwel alle gebruikers raken ofwel het functioneren van de gemeente Almere
P3 - Middel	Bedrijfs- en/of proces-ondersteunende processen liggen stil of worden ernstig verstoord.	Beheerdienst(en) is deels niet beschikbaar voor een middelgrote groep gebruikers (10 tot 49 gebruikers). Of Beheerdienst(en) is in zijn geheel niet beschikbaar voor een kleine groep gebruikers (0 tot 9 gebruikers).
P4 - Laag	Bedrijfs- en/of proces-ondersteunende processen ondervinden minimaal of geen hinder.	Beheerdienst(en) is deels niet beschikbaar voor een selecte groep gebruikers of een individuele gebruiker (0 tot 9 gebruikers).

Definitie van bereikbaarheid:

Dit is de tijd dat de melder/klant moet wachten voordat hij iemand van vlees en bloed aan de lijn krijgt (of via de andere overeengekomen communicatie kanalen).

Definitie van Responstijd:

Responstijd is de tijd die de opdrachtnemer nodig heeft om inhoudelijk te reageren op eventuele vragen of problemen die klanten hebben.

Definitie van Oplostijd:

Het tijdsverloop (inclusief Responstijd) waarbinnen een gedetecteerde of gemelde Storing (al dan niet tijdelijk middels een Workaround) opgelost dan wel gerepareerd is.

In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.

6 Beveiligingseisen

Zaken waar nader afspraken over gemaakt dienen te worden zijn:

- Specifieke beveiligingsmaatregelen om de normen en afspraken uit deze SLA te halen. Denk hierbij aan back-up/restore en encryptie/sleutelbeheer;
- Procedure van beveiliging van systemen, diensten en data;
- Maatregelen bij het schenden van beveiligingsprocedures;
- Aanspreekpunt bij beveiligingsincidenten;
- Betrouwbaarheid van de dienst;
- Autorisaties rollen/rechten 3 of 6 maanden overzichten van gebruikers en hun rechten;
- Totale governance tussen opdrachtnemer en opdrachtgever;
- Jaarlijks audit laten uitvoeren en de resultaten en opvolgacties op de gevonden kwetsbaarheden delen met de opdrachtgever.

6.1 Authenticatie & Autorisatie

Toegang tot de inwonerportaal verloopt als volgt:

- Interne gebruikers: via de gemeente, Microsoft Azure Active Directory, autorisatie verloopt via rol gebaseerde toegang in IAM (Role-based access control);
 - Voor beheerders van Gemeente Almere zal door middel van Single Sign On (SSO) geauthentiseerd toegang tot het beheerdeel van het portaal verzorgd worden
- Externe gebruikers: via DigiD, eHerkenning of vergelijkbaar.

6.2 Cryptografie

Hoogst mogelijke mate van versleuteling, in geheel versleuteld, leverancier mag methode aangeven, minimaal 256bit.

6.3 Gebruiksapparatuur

Opdrachtnemer is verantwoordelijk voor het instrueren van de interne gebruikers en voor de naleving van veiligheidsmaatregelen dat onbeheerde apparatuur voldoende beschermd is. Opdrachtgever draagt deze zelfde verantwoordelijkheid voor de interne gebruikers van de Gemeente Almere.

- Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
- Een onbemende werkplek is altijd vergrendeld.
- Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.
- Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.
- Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.
- Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.

6.4 Incidentbeheer en rapportage

Een (informatiebeveiligings)incident is een enkele of een reeks van ongewenste of onverwachte gebeurtenissen die een aanzienlijke kans hebben om de bedrijfsvoering te compromitteren of verstoren

en een bedreiging vormen voor de informatiebeveiliging. Incidentbeheer bestaat uit de processen voor het detecteren, rapporteren, beoordelen, reageren op, omgaan met, en leren van (informatiebeveiligings)incidenten. Hoe informatiebeveiligingsincidenten worden behandeld door de dienstleverancier wordt in samenspraak met de Opdrachtgever nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie. De procedure zal worden opgenomen in de DAP.

6.5 Logging en monitoring

Logging is het vastleggen van gegevens met betrekking tot de werking en het gebruik van een dienst. Monitoring is het vaststellen van de status van één of meer parameters van een dienst. Logging en monitoring zijn de verantwoordelijkheid van de Opdrachtnemer.

Registraties (records) in logbestanden zijn belangrijk voor de gemeente bij het analyseren van incidenten, zoals inbreuken op de beveiliging en fouten van de dienst, alsook bij het monitoren van het dagelijkse gebruik van de dienst.

Een logregel bevat minimaal:

- a. de gebeurtenis;
- b. de benodigde informatie die nodig is om het incident met hoge;
- c. mate van zekerheid te herleiden tot een natuurlijk persoon;
- d. het gebruikte apparaat;
- e. het resultaat van de handeling;
- f. een datum en tijdstip van de gebeurtenis.

Zie voor overige voorwaarden artikel 12.4 van de Baseline Informatiebeveiliging Overheid BIO.

De opdrachtgever meld direct en rapporteert over onbevoegd toegang tot (persoons)gegevens.

Door middel van het SLR (Service Level Report) wordt de opdrachtgever (pro)actief geïnformeerd en geadviseerd over (genomen of te nemen) maatregelen in de omgeving die naar aanleiding van logging en monitoring naar boven komen. Op verzoek, kan de opdrachtgever rapportage over de logging en monitoring opvragen bij de opdrachtnemer.

6.6 Auditing

Door middel van (ad hoc en periodieke) audits kan de opdrachtnemer met onafhankelijk verkregen bewijs aantonen dat de Software Toegang en Regie voldoet aan de criteria die door de gemeente zijn gesteld. De audits zijn er op gericht om het vertrouwen in de dienst te verhogen. De informatie benodigd voor en verkregen door de audits (zoals rapportages) zijn actueel en beschikbaar. De volgende audits zijn *minimaal* maar niet limitatief overeengekomen:

- Audit op de verwerking van persoonsgegevens:
De verwerker is op grond van de AVG verplicht om mee te werken aan de uitvoering van een audit. Partijen maken vooraf afspraken over de frequentie van de uit te voeren audits. Als de verwerker op basis van een certificering kan aantonen dat het beveiligingsniveau voldoende is, kan een audit achterwege blijven. Hiervoor dienen de scope en de verklaring van toepasselijkheid van de certificering wel de verwerking volledig dekken.

- Audit op de naleving van de wezenlijke verplichting uit hoofde van de Overeenkomst:
Opdrachtgever kan de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de GIBIT 2020 en de daarmee samenhangende overeenkomsten (SLA, verwerkersovereenkomst, etc.), alsmede de juistheid van toegezonden facturen, binnen een redelijke termijn door een onafhankelijke ter zake deskundige aan geheimhouding gebonden derde te laten controleren.
- Audit op certificering:
De opdrachtnemer dient in het bezit te zijn van een door een onafhankelijke instanties opgestelde verklaring dat de ondernemer aan kwaliteitsnormen ISO9001 2015, ISO27001 (informatiebeveiliging), ISO27701 (privacy), NEN-ISO 16175 (informatiebeheer), NEN 7513 (logging) en de BIO voldoet, te weten een geldig certificaat of aantoonbaar gelijkwaardig. Als gelijkwaardig wordt erkend een geldig ander keurmerk en/of een verklaring, uitgebracht door een onafhankelijke instantie die voldoet aan de Europese normenreeks voor certificering, waarmee de opdrachtnemer aantoont volledig te voldoen aan de gestelde eisen (uit bovengenoemde regelingen) die ten grondslag ligt aan het gevraagde certificaat.
- Audit op informatiebeveiliging:
 - Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.
 - Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. Er is een (onafhankelijke) interne audit procedure die minimaal jaarlijks toetst op het ongewijzigd bestaan van logbestanden.
 - De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.
- Audit voortkomend uit wettelijke verplichtingen:
Voor zover Opdrachtgever afhankelijk is van Opdrachtnemer voor de uitvoering van (wettelijke verplichte) audits, zal Opdrachtnemer alle noodzakelijke medewerking verlenen aan de uitvoering van deze audits. De kosten voor deze medewerking worden gedragen door Opdrachtgever.

Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.

6.7 Vulnerability management

Een kwetsbaarheid is een zwakke plek in een dienst, informatiesysteem, beveiligingsprocedures van het systeem, interne controles, of de implementatie die kan worden misbruikt door een bedreiging. Het beheer van kwetsbaarheden betekent dat informatie over technische kwetsbaarheden van informatiesystemen die wordt gebruikt tijdig moet worden verkregen en de blootstelling aan dergelijke kwetsbaarheden dient te worden geëvalueerd en er dienen passende maatregelen genomen te worden om de bijbehorende risico's te beperken. De opdrachtnemer scant minimaal twee keer per week op vastgestelde momenten op een zodanig tijdstip dat het representatief is met in achtneming dat het de performance van het systeem niet negatief mag beïnvloeden, op kwetsbaarheden. Beveiligingsupdates (patches) worden op de kortst mogelijke termijn toegepast na testen.

De opdrachtgever wordt volledig geïnformeerd over gevonden kwetsbaarheden en de opvolgende acties hieraan, via het SLR (Service Level Report).

6.8 Databeheer

Opdrachtnemer verklaart zich bereid om Opdrachtgever desgewenst toe te staan het gebruik van de ICT Prestatie na de beëindigingsdatum voor een redelijke periode te verlengen, indien de werkzaamheden overeenkomstig het Exit-plan niet tijdig zijn afgerond. Hiervoor zal een vergoeding in rekening worden gebracht naar rato van de laatst geldende gebruiksvergoedingen (waarbij noodzakelijke verlengingen van Derdenprogrammatuur volledig kunnen worden doorbelast), tenzij de niet-tijdige afronding van de Exit-werkzaamheden toerekenbaar is aan Leverancier (de verlenging is dan gratis).

Leverancier zal de door hem ten behoeve van Opdrachtgever verwerkte gegevens waarop op grond van de Gemeentelijke ICT-kwaliteitsnormen althans de Overeenkomst een bewaartermijn van toepassing is gedurende de looptijd van de Overeenkomst (i) aantoonbaar voor de duur van die bewaartermijn bewaren en (ii) niet verwijderen dan na toestemming van Opdrachtgever.

Leverancier is in staat archiefbescheiden te migreren naar archiefsystemen van Opdrachtgever conform de vereisten in de het Programma van Eisen en de Gemeentelijke ICT kwaliteitsnormen. Leverancier verricht de werkzaamheden voor het daadwerkelijk migreren van archiefbescheiden tegen de in de Overeenkomst bepaalde condities en maken onderdeel uit van de fixed fee voor implementatie.

Indien op het moment van opschorting, opzegging of ontbinding van de Overeenkomst de Opdrachtnemer archiefbescheiden van Opdrachtgever onder zich heeft die vanwege de plaatsing en inrichting van de ICT Prestatie niet tevens berusten onder de Opdrachtgever als zorgdrager, dan verplicht Opdrachtnemer zich te handelen als zou hij een kennisgeving hebben ontvangen onder artikel 11 lid 1 Archiefwet 1995 (ongeacht of de betreffende archiefbescheiden zijn opgenomen in Derdenprogrammatuur).

6.9 Afscherming van gegevens

Het is voor de gemeente van groot belang om afspraken te maken over de wijze waarop met zijn gegevens wordt omgegaan. De beveiligingseisen zijn hier primair gericht op de vertrouwelijkheid en in mindere mate de integriteit van de gebruikersgegevens. De leverancier zal zowel binnen de verwerkingsorganisatie als voor de afscherming van de diensten en applicatie gebruik dienen te maken van afdoende logische toegangsbeveiliging. De logische toegangsbeveiliging wordt jaarlijks door een deskundige en onafhankelijke auditor gecontroleerd.

Eisen met betrekking tot het afschermen van gegevens in de SLA betreffen onder andere:

- classificatie van gegevens;
- integraal systeem van logische beveiliging;
- rapportage van inbreuken;
- periodieke audit van de logische toegangsbeveiliging.

De verantwoordelijkheid voor de logische (digitale) toegangsbeveiliging wordt gewaarborgd door de opdrachtgever.

6.10 Dataclassificatie

Dataclassificatie is een beschrijving van gegevensklassen die zijn geassocieerd met de dienst:

- gemeentelijke gegevens;
- gegevens van de inwoners
- gegevens afgeleid van de dienst.

De gemeentelijke gegevens zijn geclassificeerd op beveiligingsniveau BBN2. De maatregelen die de leverancier dient te nemen zijn in lijn met de betreffende eisen uit de BIO.

6.11 Gegevens mirroring, back-up/restore

Zijn opgenomen in de KPI's.

Kritische prestatie indicator	Tijd
Recovery Point Objective	24 uur
Recovery Time Objective	Binnen 16 werkuren

Recovery Point Objective is de maximaal toegestane tijd tussen laatste backup en het incident. RPO specificeert alleen de acceptabele tijdsperiode.

Recovery Time Objective is de maximale hoeveelheid tijd dat een bedrijfsproces kan worden verstoord, na een ramp, zonder onaanvaardbare gevolgen voor de bedrijfsvoering.

6.12 Datalevenscyclus

In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA met name op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.

De leverancier dient in staat te zijn om gegevens te verwijderen wanneer de bewaartermijn is verstreken en gegevens op te halen/vragen/verwijderen nadat een verwijder verzoek is ingediend.

6.13 Gegevensoverdraagbaarheid

De leverancier dient het mogelijk te maken dat gegevens overdraagbaar zijn voor inwoners en naar andere gemeenten. In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA met name op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.

7 Bescherming persoonsgegevens

Deze paragraaf richt zich op het vaststellen van passende dienstniveau-doelstellingen met betrekking tot die situaties waarbij de dienstleverancier als een gegevensverwerker (bewerker) fungeert, namens de gemeente (verantwoordelijke).

7.1 Gedragscodes, normen, standaarden en certificeringen

De gemeente, als verantwoordelijke voor de verwerking, moet de verantwoordelijkheid voor het naleven van de toepasselijke wetgeving inzake gegevensbescherming accepteren. Met name heeft de gemeente de plicht om de rechtmatigheid van de verwerking van persoonsgegevens te beoordelen en een opdrachtnemer te selecteren die de naleving van de toepasselijke wetgeving begeleid/faciliteert.

In dit verband moet de opdrachtnemer alle noodzakelijke informatie beschikbaar stellen, ook in het kader van de naleving van het principe van transparantie, zoals hierna beschreven. Dergelijke informatie omvat informatie die kan helpen bij de beoordeling van de dienst, zoals gedragscodes met betrekking tot de bescherming van persoonsgegevens, normen of certificeringsregelingen waar de dienst aan voldoet.

7.2 Doelbinding

Het principe van doelbinding vereist dat persoonsgegevens alleen worden verwerkt ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met de vastgestelde doelbinding. Hieraan gekoppeld zijn verplichtingen tot dataminimalisatie, zorg voor de kwaliteit van gegevens, terughoudendheid met verdere verwerking en een beveiligingsverplichting. Daarom moet het doel van de verwerking voorafgaand aan het verzamelen van persoonsgegevens worden vastgesteld voor de verwerking door de verantwoordelijke, die tevens de betrokkene daarvan op de hoogte moet stellen.

Wanneer de verantwoordelijke besluit om de data extern te verwerken, moet ervoor worden gezorgd dat persoonsgegevens niet (illegaal) voor andere doeleinden worden verwerkt door de dienstleverancier, of één van zijn onderaannemers.

De dienstleverancier geen persoonsgegevens, op grond van de overeenkomst met de gemeente, voor eigen doeleinden, zonder de uitdrukkelijke toestemming van de gemeente verwerken. Een dienstleverancier die persoonsgegevens van de gemeente voor eigen doeleinden verwerkt zonder een expliciet mandaat van de gemeente, kwalificeert zich als een verantwoordelijke voor de gegevensverwerking in eigenbelang en zal daarom aan alle relevante verplichtingen moeten voldoen. Het overzicht met verwerkingsdoeleinden, die niet door de gemeente zijn gewenst/geëist, wordt in samenspraak nader gedefinieerd.

7.3 Dataminimalisatie

De gemeente is verantwoordelijk en dient zich ervan te verzekeren, dat persoonsgegevens worden gewist (door de dienstleverancier en eventuele onderaannemers), waar ze ook zijn opgeslagen, zodra deze niet meer nodig zijn voor de specifieke doeleinden. Verder kan het voorkomen dat tijdelijke gegevens worden aangemaakt op het moment dat gebruik wordt gemaakt van de dienst, en dat deze om technische redenen niet onmiddellijk kunnen worden verwijderd op het moment dat ze niet meer worden gebruikt. Periodieke controles moeten aantonen (garanderen) dat dergelijke tijdelijke gegevens effectief zijn verwijderd na een vooraf bepaalde periode. Aangezien (persoons)gegevens redundant op verschillende servers op verschillende locaties bewaard kunnen worden, moet men zeker zijn dat elk exemplaar daarvan onherroepelijk wordt gewist.

7.4 Gebruiksbeperkingen

De Opdrachtnemer, in haar hoedanigheid als gegevensverwerker (verwerker), moet de gemeente op de meest doelmatige wijze informeren over een (juridisch bindend) overheidsverzoek om gebruikersinformatie (persoonsgegevens) in verband met een strafrechtelijk onderzoek. Hierbij is de Opdrachtnemer verplicht om deze gegevens aan de rechtshandhaver of overheidsinstantie beschikbaar te stellen, tenzij anders is verboden, zoals een wettelijk verbod om de vertrouwelijkheid van het onderzoek te behouden.

7.5 Openheid, transparantie en kennisgeving

Alleen als de Opdrachtnemer de gemeente informeert over alle relevante kwesties, is de gemeente in staat om te voldoen aan haar verplichtingen als verantwoordelijke met betrekking tot de verwerking van persoonsgegevens om de rechtmatigheid van deze verwerking te beoordelen. Bovendien moet de Opdrachtnemer de informatie beschikbaar stellen die de gemeente in staat stelt om de betrokkenen te voorzien van een adequate kennisgeving met betrekking tot de verwerking van hun persoonsgegevens, zoals door de wet is vereist.

Transparantie betekent onder andere dat de gemeente bewust wordt gemaakt van het feit dat de Opdrachtnemer gebruik maakt van onderaannemers om de betreffende dienst aan te kunnen bieden. Er is toestemming van de gemeente noodzakelijk (die kan zijn vormgegeven in een voorafgaande algemene toestemming) voor het gebruik van onderaannemers. De gemeente kan zich verzetten tegen veranderingen in de lijst met onderaannemers. Om deze bepalingen uit te voeren, moet de lijst van onderaannemers ter beschikking worden gesteld aan de gemeente.

7.5.1 Verantwoording

Op het gebied van gegevensbescherming, heeft verantwoording vaak een brede betekenis en beschrijft het vermogen van partijen om aan te tonen dat zij passende maatregelen hebben genomen om de bescherming van gegevens te garanderen.

In deze context is het afleggen van verantwoording vooral van belang om lekken van persoonsgegevens te onderzoeken. De ICT-infrastructuur dient hiervoor betrouwbare logging en monitoring mechanismen te bieden, zoals beschreven in deze SLA.

Bovendien dient opdrachtnemer bewijsstukken te kunnen overleggen dat ze passende en doeltreffende maatregelen hebben genomen die de beginselen met betrekking tot gegevensbescherming ondersteunen. Bijvoorbeeld procedures om de identificatie van alle gegevensverwerkingen te verzekeren, om adequaat op toegangsverzoeken te reageren, het aanstellen van een functionaris gegevensbescherming (data privacy officer), et cetera.

Zowel gemeenten als de verantwoordelijken voor de gegevensverwerking, dienen in staat te zijn om de opzet en bestaan, mogelijk ook de werking, van de noodzakelijke maatregelen aan bevoegde toezichthoudende autoriteiten te tonen.

De Opdrachtnemer moet de gemeente op de hoogte brengen als er een datalek heeft plaatsgevonden als dit invloed (impact) heeft op de gemeentelijke gegevens. Daartoe dient de dienstleverancier over een beleid op het gebied van datalekken te beschikken waarin de procedures voor het vaststellen van en communiceren over datalekken is beschreven.

7.5.2 Geografische locatie van gegevens

Persoonsgegevens die worden verwerkt door uitbesteding kunnen worden overgedragen naar derde landen, waarvan de wetgeving niet een adequaat niveau van gegevensbescherming garandeert. Dit impliceert ook dat persoonsgegevens kunnen worden verstrekt aan buitenlandse wetshandhaving diensten zonder geldige EU rechtsgrond.

Om deze risico's te minimaliseren, zal de gemeente controleren of de Opdrachtnemer de rechtmatigheid van de grensoverschrijdende overdracht van gegevens garandeert. Bijvoorbeeld door de beveiliging van dergelijke gegevensoverdrachten te borgen door middel van safe harbour overeenkomst/regelingen, Europese Gemeenschap (EG)-modelclausules of bindende bedrijfsvoorschriften, naargelang de situatie.

Daartoe zal de gemeente geïnformeerd dienen te worden over de locatie waar de gegevens verwerkt worden, zoals ook vereist in de hierboven genoemde beginselen van openheid en transparantie.

In de dienstverlening is geborgd dat er geen doorgifte/overdracht/opslag/backup van persoonsgegevens buiten de EER plaatsvindt.

7.5.3 Interventies

De AVG geeft de betrokkene het recht van toegang, correctie, wissen, blokkeren en bezwaar. Daarom dient de gemeente te controleren of de Opdrachtnemer geen technische en organisatorische obstakels opwerpt met betrekking tot deze eisen, ook in gevallen dat de gemeentelijke gegevens verder worden verwerkt door onderaannemers.

De Opdrachtnemer is verplicht om de gemeente op een tijdige en efficiënte wijze te ondersteunen bij het uitvoeren van de rechten van de betrokkene.

7.1 Meldplicht AVG inbreuk

Het is belangrijk dat de verwerker de verwerkingsverantwoordelijke zo snel mogelijk op de hoogte brengt van een (vermoedelijke) inbreuk. Het gaat er daarbij om dat de verwerker de verwerkingsverantwoordelijke direct informeert zodra er voldoende redenen zijn om aan te nemen dat er sprake is van een inbreuk. Als er sprake is van verdachte activiteiten, hoeft er geen sprake te zijn van een inbreuk. Zodra de verwerker wel kennis heeft van de inbreuk, moet hij die binnen 24 uur melden bij de verwerkingsverantwoordelijke. De termijn van 24 uur is een maximale termijn.

De termijn van 72 uur die de verwerkingsverantwoordelijke heeft om de inbreuk te melden bij de toezichthoudende autoriteit begint te lopen, zodra de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk. Dus als de inbreuk heeft plaatsgevonden bij de verwerker en deze meldt het aan de verwerkingsverantwoordelijke, heeft laatstgenoemde pas op dat moment kennis genomen van de inbreuk en begint de meldingstermijn van 72 uur te lopen.

Verwerkingsverantwoordelijke moet zorgen voor een 24/7 bereikbaarheid om zo een melding via het afgesproken kanaal in ontvangst te kunnen nemen. Als een verwerker is aangesloten bij de IBD, kan verwerker ervoor kiezen om een inbreuk ook te melden via IBD. De IBD is een CERT en is erop ingericht om in geval van een inbreuk direct alle betrokken gemeenten te informeren.

8 KPI's Performanceniveau

In de vorige paragrafen zijn de prestatie-eisen welke aan de te leveren diensten gesteld worden beschreven. Om vast te stellen of beide partijen zich aan de overeengekomen afspraken houden, zal de dienstverlening gemeten moeten worden. Elke prestatie-eis dient vertaald te worden in één of meer kritieke/kritische prestatie-indicatoren (KPI). Vervolgens dient voor elke KPI een norm bepaald te worden, de meetinstrumenten en de bijbehorende gevolgen.

De boetes worden niet in geld geïnd. De boetes worden in samenspraak op basis van onderstaande regels toegewezen aan een innovatie- en functionele-verbeteringsvoorziening 'fonds'. Uit dit fonds kan de gemeente Almere aanspraak maken op inzet van Opdrachtnemer o.b.v. de bij de inschrijving bepaalde uurtarieven. De boetes ontslaan natuurlijk niet de plicht van Opdrachtnemer om in de volgende meetperiode te voldoen aan de overeengekomen KPI (groen).

Let op daar waar hierboven is beschreven dat een boete direct opeisbaar is, zal deze boete door opdrachtgever worden verrekend met de maandelijkse vergoeding.

KPI	Norm	Meetinstrument + meetfrequentie	Gevolg
Aanmeldtijd bereikbaarheid	Maximaal 5 minuten	Loggegevens Resultaat audits Gemiddelde wachttijden 1x per kwartaal	<= 5 minuten = Groen = Conform overeengekomen serviceniveau.
			>5 <= 7,5 minuten= Oranje = wijkt af van overeengekomen serviceniveau = Plan van aanpak.
			> 7,5 <= 10 minuten Rood = wijkt sterk af van overeengekomen serviceniveau = Acuut plan van aanpak en boete van € 1.000,- per maand voor de maanden waarin deze norm niet is gehaald.
			> 10 minuten of geen verbetering van rood naar oranje of van oranje naar groen = direct opeisbare/verrekenbare boete van € 2.000,- per maand voor de maanden waarin deze norm niet is gehaald en escalatieproces.
Responstijd (Kritiek P1 & Hoog P2)	Maximaal 15 minuten	Loggegevens Resultaat audits Gemiddelde responstijd 1x per kwartaal	<= 15 minuten = Groen = Conform overeengekomen serviceniveau.
			>15 min <= 20 min = Oranje = wijkt af van overeengekomen serviceniveau = Plan van aanpak.
Responstijd (Middel P3 en Laag P4)	Maximaal 30 minuten		>20 min <= 30 min = Rood = wijkt sterk af van overeengekomen serviceniveau = Acuut plan van aanpak en boete van € 1.000,- per maand per categorie voor de

			maanden waarin deze norm niet is gehaald. >30 min of geen verbetering van rood naar oranje of van oranje naar groen = direct opeisbare/ verrekenbare boete van € 2.000,- per maand voor de maanden waarin deze norm niet is gehaald en escalatieproces.
Oplostijd (Kritiek P1)	Maximaal 4 uur, ook buiten kantoortijden	Loggegevens Resultaat audits Gemiddelde doorlooptijden 1x per kwartaal	<=norm = Groen = Conform overeengekomen serviceniveau.
Oplostijd (Hoog P2)	Maximaal 8 uur, binnen kantoortijden		Norm + <= 10% = Oranje = wijkt af van overeengekomen serviceniveau = Plan van aanpak.
Oplostijd (Middel P3)	Maximaal 16 uur, binnen kantoortijden		Norm +> 10% en <+ 20% = Rood = wijkt sterk af van overeengekomen serviceniveau = Acuut plan van aanpak en boete van € 1.000,- per categorie per maand voor de maanden waarin deze norm niet is gehaald.
Oplostijd (laag P4)	In overleg/ Maximaal 40 uur, binnen kantoortijden		Norm >= 20% of geen verbetering van rood naar oranje of van oranje naar groen direct opeisbare/verrekenbare boete van € 2.000,- per maand voor de maanden waarin deze norm niet is gehaald en escalatieproces.
Klachten dienstverlening	Aantal in overleg	Rapportage meldingen	<norm = Groen = Conform overeengekomen serviceniveau
			Norm + <= 10% = Oranje = wijkt af van overeengekomen serviceniveau = Plan van aanpak
			Norm + >10% en <= 20% = Rood = wijkt sterk af van overeengekomen serviceniveau = Acuut plan van aanpak en boete van € 2.500,- per maand voor de maanden waarin deze norm niet is gehaald.
			Norm + >20% of geen verbetering van rood naar oranje of van oranje naar groen direct opeisbare/ verrekenbare boete van € 5.000,- per maand voor de

			maanden waarin deze norm niet is gehaald en escalatieproces.
Beoordeling klanttevredenheid van interne en externe gebruikers m.b.t software en dienstverlening	Cijfer schaal 1-10, minimaal 8	Resultaat 1 maal per jaar beoordeling	>=8 = Groen = Conform overeengekomen serviceniveau
			>=7 en <8= Oranje = wijkt af van overeengekomen serviceniveau Plan van aanpak
			>=6 en <7 Rood = wijkt sterk af van overeengekomen serviceniveau = Acut plan van aanpak en boete van € 25.000,- per jaar.
			< 6 en geen verbetering van rood naar oranje of van oranje naar groen direct opeisbare/ verrekenbare boete van € 50.000,- per jaar en escalatieproces.

KPI	Norm	Meetinstrument + meetfrequentie	Gevolg
Beschikbaarheid tijdens Servicewindow 1	98,5% minimaal	Kwartaalrapportage door opdrachtnemer	>98,5% = Groen = Conform overeengekomen serviceniveau.
			<98,5% en > 98% = Oranje = wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en boete van € 5.000,- per maand voor de maanden waarin deze norm niet is gehaald.
			<=98% en > 97,5% Rood Acut plan van aanpak en boete van € 7.500,- per maand voor de maanden waarin deze norm niet is gehaald.
			<= 97,5% en geen verbetering van rood naar oranje of van oranje naar groen direct opeisbare/ verrekenbare boete van € 7.500,- per maand en escalatieproces
Beschikbaarheid buiten Servicewindow 1	96%	Kwartaalrapportage door opdrachtnemer	>=96% = Groen = Conform overeengekomen serviceniveau.
			<96% en > 95% = Oranje = wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en boete van € 2.500,- per maand voor de maanden waarin deze norm niet is gehaald.
			<= 95% en > 94% Rood direct opeisbare/ verrekenbare boete van € 2.500,- per maand en escalatieproces.
			<= 94 % en geen verbetering van rood naar oranje of van oranje naar groen direct opeisbare/ verrekenbare boete van € 3.750,- per maand en escalatieproces
Mean Time Between Failures (MTBF)	Maximaal 2 uur	Kwartaalrapportage door opdrachtnemer	> 2 uur wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en boete van € 2.500,- per keer dat deze norm niet is gehaald.

Mean Time Between Service Incidents (MTBSI)	Maximaal 4 uur	Kwartaalrapportage door opdrachtnemer	> 4 uur wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en direct opeisbare/ verrekenbare boete van € 2.500,- per keer dat deze norm niet is gehaald.
Mean Time to Repair (MTTR)	In overleg	Kwartaalrapportage door opdrachtnemer	Acut plan van aanpak.
Aantal storingen 3 minuten of korter	In overleg	Kwartaalrapportage door opdrachtnemer	Acut plan van aanpak.
Aantal storingen langer dan 3 minuten	In overleg	Kwartaalrapportage door opdrachtnemer	Acut plan van aanpak.
Recovery Point Objective (dataverlies)	Maximaal 24 uur	Per incident/rapportage	> 24 uur wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en direct opeisbare/ verrekenbare boete van € 10.000,- per keer dat deze norm niet is gehaald.
Recovery Time Objective tijdsverlies	Binnen 16 werkuren (twee dagen van 8 uur)	Per incident/rapportage	> 16 uur wijkt af van overeengekomen serviceniveau = Acut plan van aanpak en direct opeisbare/ verrekenbare boete van € 10.000,- per keer dat deze norm niet is gehaald.
Beveiligingsincidenten	0 (nul)	Per incident/rapportage	Acut plan van aanpak en escalatieproces.

9 Kosten

Hier worden de financiële consequenties (vergoedingen) met betrekking tot de dienstverlening beschreven. Bijvoorbeeld per gebruiker, per systeem, gerelateerd aan beschikbaarheidseisen van de dienst.

9.1 Prijzen

Uitgangspunt hierbij zijn de eisen welke door Partijen via Bijlage 3 Tarievenblad zijn overeengekomen. De nadere uitwerking op basis van het hiervoor gestelde volgt in een gezamenlijk op te stellen Dossier Financiële Afspraken.

9.2 Betalingsvoorwaarden

Facturatie van delen van het jaarbedrag vindt plaats maandelijks achteraf en vangt aan wanneer de dienstverlening daadwerkelijk wordt uitgevoerd. Het betaaltermijn van de factuur is 30 dagen vanaf de datum van ontvangst.

De eenmalige implementatiekosten (migratie, conversie en transitie) zijn gemaximaliseerd op €50.000,-. De vergoeding o.b.v. 60% van het door u geoffreerde implementatiebedrag wordt achteraf gedaan aan de hand van de voortgang ten opzichte van het overeengekomen projectplan van Opdrachtnemer. De resterende 40% van het door u geoffreerde implementatiebedrag wordt vergoed na door Opdrachtnemer opgeleverde en door Opdrachtgever geaccepteerde ingebruikname. Leverancier verzendt de factuur aan Opdrachtgever elektronisch overeenkomstig de geldende eisen voor facturatie zoals opgenomen in de Gemeentelijke ICT-kwaliteitsnormen. De e-factuur wordt in ubl-formaat aangeleverd via het open PEPPOL netwerk van Simpler Invoicing. Kosten verband houdende met e-facturatie komen voor rekening van Leverancier. Eisen waaraan factuur dient te voldoen worden uitgewerkt in de DAP.

In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.

9.3 Sancties

Bij een verlate oplevering (later dan de fatale termijn 1-4-2023) bedraagt de boete € 10.000,- per maand en is door Opdrachtgever direct opeisbaar en verrekenbaar, zolang de vertraging voortduurt.

In samenspraak met Opdrachtnemer en Opdrachtgever wordt de SLA op dit punt nader ingevuld op basis van de randvoorwaarden en minimum eisen welke ten grondslag liggen aan de door Opdrachtgever geëiste Prestaties en de door dienstleverancier te leveren/geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden/geleverd als overeengekomen Prestatie.