



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	Verlenging en beëindiging	5
2.2	Beëindigingsproces	5
2.3	Ontbinding en garanties	5
2.4	Wijzigingsproces	5
3	Dienstverlening, doelen en resultaten	6
3.1	Dienstverlening	6
3.1.1	Software Wmo	6
3.1.2	Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO)	6
3.2	Buiten de scope	6
3.3	Vitale bedrijfsfuncties, processen en activiteiten	7
3.4	Integratie	7
3.5	Business impact bij verlies van de dienst	7
3.6	Gebruiksresultaat	7
3.7	Kwaliteit	8
3.8	Dienstverleningstijden	8
3.8.1	Software Wmo	9
3.8.2	Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO)	9
3.9	On site ondersteuning	9
3.10	Infrastructuur	9
3.11	Wijzigingen	9
3.12	Eigendom	10
4	Communicatie	11
4.1	Contactpersonen gemeente	11
4.2	Contactpersonen leverancier	11
4.3	Dienstrapportages	11
4.4	Uitzonderingen en klachten	12
4.5	Tevredenheidsonderzoeken	12
4.6	Servicebeoordelingen	12
4.7	Geheimhouding, verantwoordelijkheid en concurrentiebeding	12
5	Dienstenniveau	13
5.1	Beschikbaarheidsdoelstellingen	13
5.2	Beschikbaarheidsdoelen	13
5.3	Opslagbeheer	13
5.4	Productie- en testomgeving	13
5.5	Aantasting van systemen en operationele processen	13
5.6	Betrouwbaarheidsdoelen	14
5.7	Capaciteit/prestatiedoelstellingen en garanties	14
5.7.1	Capaciteit & schaalbaarheid	14
5.7.2	Responstijden	14
5.7.3	Capaciteit- en prestatierapportage	14
6	Beveiligingseisen	15
6.1	Authenticatie & Autorisatie	15
6.2	Cryptografie	15
6.3	Incidentbeheer en rapportage	15
6.4	Logging en monitoring	15
6.5	Auditing	15
6.6	Vulnerability management	16

6.7	Databeheer	16
6.8	Afscherming van gegevens	16
6.9	Dataclassificatie	16
6.10	Gegevens mirroring, back-up & restore	17
6.11	Datalevenscyclus	17
6.12	Gegevensoverdraagbaarheid	17
7	Bescherming persoonsgegevens	18
7.1	Gedragcodes, normen, standaarden en certificeringen	18
7.2	Doelbinding	18
7.3	Dataminimalisatie	18
7.4	Gebruiksbeperkingen	18
7.5	Openheid, transparantie en kennisgeving	19
7.5.1	Verantwoording	19
7.5.2	Geografische locatie van gegevens	19
7.5.3	Interventies	20
8	Taken en verantwoordelijkheden	21
8.1	Plichten van de dienstverlener	21
8.1.1	Borging van de beheersprocessen	21
8.1.2	Logische toegangsbeveiliging	21
8.2	Plichten van de gemeente	21
8.2.1	Verantwoordelijkheden gebruikers	22
8.2.2	Monitoring van beveiligingseisen	22
8.2.3	Beperkingen, afhankelijkheden en overmacht	22
8.2.4	Aansprakelijkheden	22
9	KPI's Performanceniveau	23
10	Kosten	24
10.1	Prijzen	24
10.2	Betalingsvoorwaarden	24
10.3	Sancties	24

1 Inleiding

Deze SLA beschrijft de door de dienstleverancier geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze 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 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 25-04-2022. De looptijd van de Hosting-diensten is 01-01-2023 tot en met 31-12-2026 na inwerkingtreding van de Overeenkomst. De Overeenkomst heeft een looptijd tot 31-12-2026. 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 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.

2.1 Verlenging en beëindiging

Inschrijver moet bij beëindiging van de overeenkomst aantoonbaar alle archiefbescheiden, en bijbehorende metadata, overdragen aan de gemeente conform tevoren afgesproken procedures en bestandsformaten. Inschrijver verwijdt daarna aantoonbaar alle archiefbescheiden en metadata uit de beheeromgeving. Ook hier moet worden voldaan aan de Richtlijn Overdragen en Migreren (bijlage16). De beschrijving van de exit procedure (Bijlage Richtlijn Overdragen en Migreren) is te vinden in het Dossier Afspraken en Procedures (DAP).

2.2 Beëindigingsproces

Het beëindigingsproces vindt plaats wanneer de gemeente die de dienst afneemt of de dienstleverancier, ervoor kiest om de overeenkomst te ontbinden. Het beëindigingsproces dient een stappenplan te bevatten dat de gemeente in staat stelt 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 leverancier dient minimaal de gegevens beschikbaar stellen die voor opdrachtgever nodig zijn om aan de wettelijke verplichtingen en lokale afspraken te voldoen.

Bij faillissement van de leverancier zal de derdenrekening direct worden geblokkeerd.

2.3 Ontbinding en garanties

Indien gedurende de looptijd van de overeenkomst blijkt dat Dienstverlener (combinatie) niet voldoet aan één of meerdere minimeisen, terwijl Dienstverlener (combinatie) heeft verklaard dat hij aan alle minimeisen voldoet, dan wordt dit als niet-nakoming van de overeenkomst aangemerkt en zal de Dienstverlener (combinatie) 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 en/of de SLA('s), in ieder geval het 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 dienstleverancier (service level manager) afgestemd. Wanneer één van de partijen aanleiding ziet om wijzigingen in het 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 het SLA verkrijgt rechtskracht na overeenstemming en ondertekening door de daartoe bevoegde vertegenwoordigers van beide partijen.

3 Dienstverlening, doelen en resultaten

3.1 Dienstverlening

Software Wmo & Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO) van gemeente Almere met betrekking tot ondersteuning informatievoorziening Wmo processen en dienstverlening Backoffice processen Wmo en Jeugd als BPO in het Sociaal Domein. Gedeelte van de uitvoering ligt ook bij de BPO. Opdrachtgever heeft de ambitie om aan te sluiten op de werkwijze die gangbaar is in het land en gebruik te maken van de nieuwe mogelijkheden die de systemen bieden.

3.1.1 Software Wmo

Ondersteuning van de alle vormen van Wmo processen (intake en behandelen) door middel van standaard SaaS software. Daarbij hebben inwoners via DigiD toegang tot de gegevens betreffende hun Wmo aanvragen.

3.1.2 Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO)

De Backoffice dienstverlening Wmo en Jeugd als BPO bestaat uit werkzaamheden van de te selecteren financieel-administratieve Dienstverlener en start vanaf het moment waarop de beschikking verleend kan worden. Daarbij is de Dienstverlener verantwoordelijk voor:

- het beoordelen van de aanvraag en het beschikken of afwijzen ervan. Uitzonderingen zullen handmatig door Opdrachtgever worden beoordeeld, inclusief het afhandelen van het bezwaar erover;
- Het berichtenverkeer dat voortvloeit uit iWmo en iJeugd tussen de gemeente, de Dienstverlener en haar ICT-oplossing, de zorgaanbieders, de landelijke voorzieningen en knooppunten, het CBS, etc.;
- Controleren, verwerken/uitvoeren van facturen, declaraties en betalingen;
- Het verwerken van de uitvalprocessen;
- Operationele contractbeheer van zorgaanbieders;
- Invulling geven aan de vraagbaakfunctie voor gemeente, relevantie instanties (zoals CAK, SVB) en zorgaanbieders over aanvragen, mutaties, beschikkingen, facturen, etc.;
- Rapporteren aan de gemeente;
- Portaal voor zorgaanbieders;
- Het actief invulling geven aan de verantwoordingsverplichtingen;
- Het verrichten van de betalingen aan zorgaanbieders vanaf een derdenrekening van de gemeente;
- Het controle uitvoeringsplan.
- De PDC dient ook landelijke voorzieningen (het specifieke aanbod wat via VNG is gecontracteerd) te bevatten.
- Niet gecontracteerde aanbieders worden niet vastgelegd in PDC en aanvragen die door/aan hen worden gedaan worden altijd door gemeente beoordeeld.

Samenvattend is na het verlenen van een beschikking de Dienstverlener verantwoordelijk voor de juiste en tijdige afhandeling van de financieel/administratieve processen, inclusief alle uitzonderingen, welke na beschikking weer in de reguliere workflow van de dienstverlener terugkeren.

Hier worden specifieke functionaliteiten met betrekking tot de dienst beschreven. Deze specifieke functionaliteiten kunnen van essentieel belang zijn vanuit het perspectief van de gemeente, om gebruik te maken van deze dienst.

3.2 Buiten de scope

Buiten het bereik van de opdracht vallen:

- wijkteams, de toeleiding;
- integrale regie(multiproblematiek);

- een uitgebreide burger-/inwonerportaal, waarbij inzicht in documenten, planvorming, digitale accordering en de voortgang van Wmo dossier wel binnen de scope valt.

3.3 Vitale bedrijfsfuncties, processen en activiteiten

Vitale bedrijfsfuncties zijn start van het proces en beoordelen van de aanvraag en de toekenning ervan. Daarnaast is het beheren van de derdenrekening(en) vitaal (zoals tijdige betalingen) en dienen er passende beheersmaatregelen te worden genomen om misbruik te voorkomen (conform ISAE 3402). Tijdens de processen worden er financiële-, persoonsgegevens en bijzondere persoonsgegevens verwerkt om de aanvraag te kunnen behandelen en uitvoeren. Zowel gemeente als leverancier voldoen aan de BIO. Ook de medewerkers en/of onderaannemers van de leverancier 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 voor de softwareleverancier en BPO 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 leveranciers en ingehuurd personeel dienen hun verantwoordelijkheden begrijpen, geschikt zijn voor de rollen waarvoor zij worden overwogen, en 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).

3.4 Integratie

De Software Wmo en BPO dienstverlening moeten naadloos op elkaar aansluiten. De Software Wmo en BPO dienstverlening dienen informatie te kunnen uitwisselen met de koppelingen die in het Programma van Eisen zijn gesteld.

Financiële mutaties kunnen worden verwerkt in de gemeentelijke administratie, minimaal conform huidige situatie.

3.5 Business impact bij verlies van de dienst

Bij verlies van de dienst kan de gemeente geen aanvragen behandelen en toekennen. De dienstverlening aan de inwoners heeft de hoogste prioriteit.

3.6 Gebruiksresultaat

Over onderstaande (niet limitatieve) indicatoren dient te worden verantwoord:

- Implementatieplan, aansluitend op het Implementatieplan van de opdrachtgever;
- Livegang op 1 januari 2023 na positieve acceptatietest (fatale termijn);
- Beschikbaarheid van de Wmo software;
- Beschikbaarheid van de Backoffice dienstverlening Wmo en Jeugd als BPO;
- Bereikbaarheid van de Helpdesk WMO software en van de Helpdesk van de Backoffice dienstverlening Wmo en Jeugd als BPO.
- Betaling van declaraties binnen gestelde termijn;
- Verwerkingssnelheid van berichten;
- Doorlooptijd afhandelen incidenten/vragen zorgleveranciers.
- Doorlooptijden afhandelen incidenten/vragen opdrachtgever
- Doorlooptijden afhandelen mutaties door de leveranciers Wmo Software en de Backoffice dienstverlening Wmo en Jeugd
- Issues/ klachten
- Klanttevredenheid zorgleveranciers

- Klanttevredenheid opdrachtgever
- Secuurheid verwerking gegevens/data (foutmarge, mutaties, beschikking etc.)
- Certificering normen welke van toepassing zijn verklaard in de totale overeenkomst.

Garanties Gemeente en leverancier evalueren de dienstverlening en normen aan de hand van (onder andere):

- Het aantal klachten;
- De mate waarin het wijzigingsbeheerproces is uitgevoerd en is afgestemd op de exploitatieorganisatie van de gemeente;
- welke categorieën wijzigingen de leverancier autonoom binnen zijn eigen wijzigingsbeheerproces mag doorvoeren, en over welke wijzigingen afstemming met het wijzigingsbeheerproces van de gemeente plaatsvindt;
- Efficiënter proces/kortere doorlooptijd;
- % afname uitzonderingen;
- % afname klachten;
- % toename van inwoners met toegang tot hun Wmo informatie;
- klanttevredenheid van interne gebruikers;
- klanttevredenheid van zorgaanbieders;
- klanttevredenheid van inwoners;
- Ontvangen rapportages welke zijn overeengekomen met de inschrijver en/of voortkomen uit de verantwoording van de diverse indicatoren.

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

3.7 Kwaliteit

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

- ISO27001;
- ISO27701;
- NEN-ISO 16175;
- ISAE 3402;
- BIO;
- i-standaarden;
- informatiemodel RSGB.

3.8 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 leverancier zijn maandag tot en met vrijdag 08:00 – 18:00 uur, uitgezonderd algemeen erkende Nationale feestdagen. De dienstverlening is Nederlandstalig en er is sprake van persoonlijk 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.

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.

urgentie	Aanmeldtijd bereikbaarheid	Responsetijd	Oplostijd 24x7x365
1; urgent	< 5 minuten	< 15 minuten	< 4 uur

2; hoog	< 5 minuten	< 15 minuten	< 8 uur
3; middel	< 5 minuten	< 30 minuten	< 16 uur
4; laag	< 5 minuten	< 30 minuten	In overleg < 40 uur

Definitie van urgentie:

- Het betreft een incident met grote impact op de bedrijfsvoering van de Opdrachtgever;
- Het betreft een incident met een middelgrote impact;
- Het betreft een incident met een beperkt grote impact;
- Het betreft een incident met een hinderlijke, maar niet-direct versturende impact.

Hier worden de afspraken met betrekking tot de beschikbaarheid van de dienst vastgelegd.

Drie loketten:

1. Voor vragen van (interne en externe) gebruikers over software Wmo;
2. Voor zorgleveranciers (leveranciersportaal) door BPO dienstverlener;
3. Datalek procedure 24x7.

3.8.1 Software Wmo

Voor inhoudelijke vragen over de Wmo aanvraag is de gemeente het aanspreekpunt voor inwoners. De leverancier dient op bovengenoemde tijden ondersteuning te leveren aan interne en externe gebruikers. 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.

3.8.2 Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO)

In crisis situaties in de jeugd wordt direct geschakeld en op een later moment (tijdens kantoortijden) wordt dit administratief gerepareerd, conform overeengekomen werkprocedure welke is opgenomen in de DAP

Uitzondering die door de gemeente beoordeeld dienen te worden dienen binnen 1 werkdag bekend te worden gemaakt bij de gemeente, conform overeengekomen werkprocedure welke is opgenomen in de DAP.

Zorgleveranciers hebben minimaal tijdens bovengenoemde dienstverleningstijden en dienstverleningskanalen toegang tot de leveranciersportaal en ondersteuning.

3.9 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 Wmo.

Voor Backoffice dienstverlening Wmo en Jeugd als Business process outsourcing (BPO) is de mogelijkheid om, in uitzonderlijke gevallen, te werken op de locatie van Almere.

3.10 Infrastructuur

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

3.11 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 week na melding doorvoeren.

Regelmatig terugkoppeling over voortgang en einde.

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

3.12 Eigendom

Gemeente is eigenaar van de gegevens. De programmatuur is eigendom van de gebruikersvereniging (of vergelijkbaar) waaraan gemeente deelneemt. De software is veilig gesteld via een Escrow regeling of vergelijkbaar. Hardware is eigendom van leverancier.

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 Inschrijver hanteren minimaal onderstaande communicatiestructuur:

Strategisch:

- Periodiek (4x per jaar) afstemmen van ontwikkelingen:
 - o Wet- en regelgeving;
 - o Project en diensten portfolio Opdrachtgever en Inschrijver;
 - o Financieel beleid Opdrachtgever;
 - o Informatiebeveiliging en privacy compliance;
 - o Informatie en technische architectuur.
- 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 Inschrijver.

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

Dit kan dezelfde persoon zijn als die bij paragraaf 1.2 maar dit kan ook een operationeel/procesmanager zijn.

4.2 Contactpersonen leverancier

Hier worden de contactgegevens van de service level manager (zie paragraaf 1.2) of de (klant) manager verantwoordelijk voor het leveren van de dienst van de leverancier weergegeven. Nader te bepalen na gunning.

4.3 Dienstrapportages

Maandelijks rapporteert 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 uit onderliggende documenten zijn (niet limitatief):

- Backoffice dienstverlening Wmo en Jeugd als BPO brengt facturen in mindering op de verplichting. Er wordt hierover periodiek gerapporteerd naar opdrachtgever.
- Van zwakke plekken in de informatiebeveiliging
- Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren;
- Inschrijver zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen welke voortvloeien uit wet- en regelgeving alsmede

professioneel opdrachtnemerschap nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen onverwijld aan de gemeente worden gerapporteerd;

- Dient periodiek te kunnen rapporteren en exporteren over nader vast te stellen periode(s):
 - Inkoop: grootboeknummers per leverancier met datum (i.v.m. zorgjaar);
 - Betalingen per leverancier t.b.v. liquiditeitsprognose;
 - Correcties of verrekeningen in de administratie (memoriaalboeking).
- Leverancier zal periodiek aan Opdrachtgever rapport uitbrengen over de nakoming door hem van de overeengekomen Service Levels, waaronder in ieder geval wordt verstaan de Beschikbaarheid van de ICT Prestatie en het niveau van de diensten, waaronder het Onderhoud van de ICT Prestatie alsmede het geplande Innovatief Onderhoud;
- Na ontvangst van het rapport zal door Opdrachtgever worden vastgesteld of Leverancier zijn verplichtingen uit hoofde van het Onderhoud, waaronder de door hem gegarandeerde Service Levels, heeft gehaald, al dan niet door inschakeling van een derde overeenkomstig artikel 21;
- Backoffice dienstverlening Wmo en Jeugd als BPO legt verantwoording af over uitgaven derdenrekening.

4.4 Uitzonderingen en klachten

In overleg met Partijen (Opdrachtnemer en Opdrachtgever) of op initiatief van een 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.

4.5 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.

4.6 Servicebeoordelingen

Hier wordt de procedure beschreven voor de herziening van de dienst met de gemeente. Deze meting dient op regelmatige basis plaats te vinden. De procedure voor de herziening van de dienst is te vinden in het DAP.

Verbeteringen worden in gezamenlijkheid doorgevoerd. Dit begint met een aanleiding wat resulteert in een verbetervoorstel. De procesmanager/-eigenaar besluit met de Leverancier eventueel tot doorvoeren van de verandering.

4.7 Geheimhouding, verantwoordelijkheid en concurrentiebeding

Afspraken met betrekking tot het niet openbaar maken of aan derden beschikbaar stellen van vernomen informatie tijdens het opstellen van de SLA of het functioneren van de dienst(verlening). Denk hierbij ook aan geheimhoudingsplicht met betrekking tot informatie en in het bijzonder geheime of vertrouwelijke informatie. Ook kunnen bepalingen worden opgenomen voor bescherming tegen het overnemen van personeel (concurrentiebeding) of het rechtstreeks onderhandelen van de gemeente (buiten de dienstleverancier om) met derden over de levering van (delen van) diensten.

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 Wmo en BPO dienstverlening is als volgt:

Beschikbaarheid	Waarde
Servicewindow 1 ma/vr 08:00 – 18:00	98,5%
Servicewindow 2	96,0%

Het niet beschikbaar zijn is niet beperkt tot uitvallen gehele applicatie, ook wanneer aanvragen niet verwerkt kunnen worden, en/of onderzoeken niet uitgevoerd kunnen worden, en/of geen opdrachten en mutaties via berichtenverkeer verzonden kunnen worden.

5.2 Beschikbaarheidsdoelen

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.

5.3 Opslagbeheer

Voor de gemeente is alleen van belang dat er zodanige infrastructurele maatregelen zijn getroffen dat de voortgang en kwaliteit van de dienstverlening niet wordt aangetast. Er zijn 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.

5.4 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 (onder andere) de kunnen worden getest. Wijzigingen mogen pas in productie worden genomen na goedkeuring van de opdrachtgever.

5.5 Aantasting van systemen en operationele processen

De beveiliging tegen de aantasting van systemen en operationele processen is erop gericht om de voortgang van de verwerkingsprocessen bij de dienstleverancier te waarborgen. De deskundigheid en kwaliteit van de operationele werkzaamheden zijn van directe invloed op de reputatie van de dienstleverancier. Daarnaast kan door een onafhankelijk deskundige periodiek een oordeel gegeven worden over de algemene kwaliteit van de operationele processen. Hoewel hier sprake is van processen bij de dienstleverancier dienen er in de SLA wel degelijk uitdrukkelijke eisen gesteld te worden aan de minimale beschikbaarheid, de verwerkingssnelheid, de capaciteit en de controleerbaarheid daarvan. Ook is het van groot belang in de SLA aandacht te besteden aan de procedure die gevolgd wordt bij het uitvallen van de productie. De gemeente moet eisen stellen aan de snelheid waarmee de productieomgeving wordt hersteld of tot uitwijk wordt overgegaan. De mate waarin recovery mogelijk is, is deels afhankelijk van de door de gemeente gekozen back-upmethode.

5.6 Betrouwbaarheidsdoelen

De betrouwbaarheidsdoelen die worden vereist zijn:

Mean Time Between Failures	< 2 uur
Mean Time Between Service Incidents	< 4 uur

5.7 Capaciteit/prestatiedoelstellingen en garanties

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

5.7.1 Capaciteit & schaalbaarheid

In de gemeente Almere wonen ruim 216.000 inwoners en het aantal interne gebruikers is naar verwachting 250. Actuele cijfers over Zorg & Welzijn zijn te vinden op de openbare Monitor Sociaal Domein bij “Welke hulp en ondersteuning gebruiken Almeerders?” en de volgende “Vormen van hulp en ondersteuning”: [Jeugdhulp](#) en [Wmo-ondersteuning aan volwassenen](#).

Voordat de vakanties beginnen (met name in de zomer) neemt de caseload met ongeveer 30% toe; de dienstverlening dient deze piek op te kunnen vangen.

5.7.2 Responstijden

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.

5.7.3 Capaciteit- en prestatierapportage

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.

6 Beveiligingseisen

De uitbesteding van de backoffice processen mag niet leiden tot een aantasting van het bestaande beveiligingsniveau. Uitgaand van het feit dat voorafgaand aan de uitbesteding reeds een passend beveiligingsniveau bestond (BIO), dient dit niveau ook na de uitbesteding te worden voortgezet. De uitbesteding tot een andere of een efficiëntere uitvoering van de beveiliging leidt. 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 leverancier en opdrachtgever;
- Jaarlijks audit laten uitvoeren en delen met opdrachtgever.

6.1 Authenticatie & Autorisatie

Authenticatie van interne gebruikers verloopt via Azure, autorisatie verloopt via rolgebaseerde toegang in IAM (Role-based access control).

6.2 Cryptografie

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

6.3 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 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.

6.4 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 leverancier (software en BPO).

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. Er dient minimale automatische logging te zijn van gebruiker, datum en tijd waarop mutatie van een melding heeft plaatsgevonden (statusverandering, toevoegen activiteit, nieuwe melding, annulering melding, wijziging melding).

6.5 Auditing

Door middel van (ad hoc en periodieke) audits kan de leverancier met onafhankelijk verkregen bewijs aantonen dat de Software Wmo en BPO dienstverlening voldoen 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.

Auditing kan ook in opdracht en op kosten van Opdrachtgever worden uitgevoerd.

6.6 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 leverancier scant minimaal twee keer per week op vastgestelde momenten plaatsvinden op kwetsbaarheden. Beveiligingsupdates (patches) worden op de kortst mogelijke termijn toegepast na testen.

6.7 Databeheer

Leverancier 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 tarieven en condities, of bij gebreke daarvan tegen de reguliere tarieven van Leverancier en nader overeen te komen condities. Indien op het moment van opschorting, opzegging of ontbinding van de Overeenkomst Leverancier 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 Leverancier 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).

6.8 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.

6.9 Dataclassificatie

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

- gemeentelijke gegevens;
- gegevens van de dienstleverancier;
- gegevens afgeleid van de dienst;

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

6.10 Gegevens mirroring, back-up & restore

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.

6.11 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.

6.12 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 dienstniveaudoelstellingen 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 dienstleverancier te selecteren die de naleving van de toepasselijke wetgeving begeleid/faciliteert.

In dit verband moet de dienstleverancier 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.

In het algemeen mag 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 (bijvoorbeeld om een markt of wetenschappelijke analyse uit te voeren of om de direct marketing te verbeteren, alles uit eigen belang), kwalificeert zich als een verantwoordelijke voor de gegevensverwerking in eigen belang en zal daarom aan alle relevante verplichtingen moeten voldoen.

Het is daarom belangrijk dat het overzicht met verwerkingsdoeleinden (indien aanwezig), die niet door de gemeente zijn gewenst/geëist, is 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 dienstleverancier, 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 dienstleverancier 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 dienstleverancier 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 dienstleverancier 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 dienstleverancier 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 leverancier 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 dienstleverancier 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 wetshandhavingdiensten zonder geldige EU rechtsgrond.

Om deze risico's te minimaliseren, moet de gemeente controleren of de dienstleverancier 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 dienstleverancier geen technische en organisatorische obstakels opwerpt met betrekking tot deze eisen, ook in gevallen dat de gemeentelijke gegevens verder worden verwerkt door onderaannemers.

Het contract tussen de gemeente en de dienstleverancier moet beschrijven dat de dienstleverancier verplicht is om de gemeente op een tijdige en efficiënte wijze te ondersteunen bij het uitvoeren van de rechten van de betrokkene.

8 Taken en verantwoordelijkheden

Uitbesteden van processen leidt slechts tot een overdracht van taken en verantwoordelijkheden. De eindverantwoordelijkheid voor de processen, inclusief de beveiligingsaspecten, kan niet worden overgedragen. Ook de processen die zijn uitbesteed, blijven verbonden met de gemeente. De kwaliteit van het uitbesteede ICT-proces en de producten die daaruit voortvloeien, behouden een directe invloed op het functioneren van de gemeentelijke bedrijfsprocessen.

Uitbesteding leidt in eerste instantie tot een reductie van processen en de daaraan verbonden werkzaamheden. De totstandkoming van een uitbestedingsrelatie tussen de gemeente en dienstleverancier leidt echter ook tot het ontstaan van nieuwe beheertaken. De uitbesteding van een proces zal er in ieder geval toe leiden dat de directe operationele werkzaamheden rond het proces op de dienstleverancier zullen overgaan. In het verlengde daarvan zal er echter een gemeentelijke beheerorganisatie ingericht moeten worden om enerzijds in de communicatie met de dienstleverancier te kunnen voorzien en anderzijds het door de dienstleverancier toegezegde normniveau te controleren. Zeker als een organisatie meer delen van het proces aan verschillende dienstleveranciers heeft uitbesteed, is een vorm van Service Level Management noodzakelijk.

8.1 Plichten van de dienstverlener

Hier worden de eisen beschreven, zoals overeengekomen met de gemeente, waaraan de dienstverlener dient te voldoen.

8.1.1 Borging van de beheersprocessen

Om als dienstleverancier de kwaliteit van de operationele exploitatieprocessen te kunnen waarborgen en daarmee tevens de garantie te kunnen bieden dat de beveiligingsmaatregelen ook daadwerkelijk functioneren, is het noodzakelijk dat de dienstleverancier een adequate beheersorganisatie heeft ingericht. De werkzaamheden binnen de beheersorganisatie zijn voor het grootste deel gericht op het intern sturen van de verwerkingsprocessen.

De werkzaamheden met betrekking tot de help-/servicedesk en het service management zijn met name gericht op de externe communicatie met de gemeente. Hierover zullen in de SLA dan ook afspraken gemaakt moeten worden. Een belangrijke taak van de help-/servicedesk is het ondersteunen van de gebruikers en het registreren van incidenten. Het service management verzorgt alle verdere contacten tussen de gemeente en dienstleverancier. Het service management controleert of de afgesproken dienstenniveaus ook daadwerkelijk gehaald worden, het zogenaamde service level management.

8.1.2 Logische toegangsbeveiliging

Om na de uitbesteding het bestaande beveiligingsniveau te kunnen handhaven, is het noodzakelijk dat ook bij de dienstleverancier een adequaat systeem van logische toegangsbeveiliging is geïmplementeerd. Een dergelijk systeem zal niet alleen bescherming moeten bieden aan de technische systemen bij de dienstleverancier, maar ook aan de applicatie van de gemeente die bij de dienstleverancier functioneert. Het autorisatiebeheer bewaakt de initiële instellingen, actualiseert de autorisaties voortdurend en signaleert mogelijke inbreuken direct. Het autorisatiebeheer valt weliswaar onder de verantwoordelijkheid van de gemeente, de leverancier heeft hierop een invloed.

8.2 Plichten van de gemeente

Hier worden de eisen beschreven, zoals overeengekomen met de dienstleverancier, waaraan de gemeente dient te voldoen. In samenspraak met Opdrachtnemer en Opdrachtgever worden onderstaande paragrafen in deze SLA 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.

8.2.1 Verantwoordelijkheden gebruikers

Hier worden de verantwoordelijkheden voor de gebruikers van de dienst beschreven.

8.2.2 Monitoring van beveiligingseisen

Hier worden de beveiligingseisen beschreven die gemonitord moeten worden in relatie tot de dienst. De basis hiervoor is het contract/overeenkomst, de eventuele verwerkersovereenkomst en relevante BIO-eisen.

8.2.3 Beperkingen, afhankelijkheden en overmacht

Vastlegging van beperkingen met betrekking tot het gebruik van de te leveren diensten, de afhankelijkheid van derde organisaties en het beschrijven van situaties waarin de organisaties zich kunnen beroepen op overmacht.

8.2.4 Aansprakelijkheden

Vermelding van zowel de aansprakelijkheid voor de bij de gemeente opgestelde apparatuur en/of programmatuur als van de aansprakelijkheid van de dienstleverancier voor het functioneren van de gemeentelijke dienstverlening in relatie tot de afgenomen dienstverlening. Bijvoorbeeld in geval van storingen of calamiteiten.

9 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 volgende kpi's; bereikbaarheid, continuïteit, doorlooptijden, onderhoud, audit gegevensveiligheid, secuurheid (foutmarges, mutaties, beschikkingen etc.) worden in de volgende Nota van Inlichtingen nader uitgewerkt.

10 Kosten

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

10.1 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.

10.2 Betalingsvoorwaarden

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.

10.3 Sancties

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.