INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

Service Level Agreement

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking Service Level Agreement

Versienummer

2.3.

Versiedatum

december 2019

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	Juli 2015	Eerste versie
1.0.1	Augustus 2016	Taskforce BID verwijderd, WBP vervangen door Wbp, GBA vervangen door BRP
2.0	Maart 2019	BIO update
2.1	Juli 2019	Verwijzingen aangepast en kleine aanpassingen in lay-out
2.1.1	Augustus 2019	Verwijzingen gerepareerd
2.2	Augustus 2019	Beschrijving governance aangepast en wijzigingen toegevoegd in de bijlage.
2.3	December 2019	Diverse tekstuele wijzigingen, onder andere in relatie tot AVG

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

INFORMATIE
BEVEILIGINGS
DIENST

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is om aanwijzingen te geven waar gemeenten op dienen te letten bij het afsluiten van Service Level Agreements met leveranciers.

Doelgroep

Dit document is van belang voor de CISO, inkopers, het management van de gemeente, de systemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente
- Voorbeeld Service Level Agreement

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties
15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers
18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen
18.2.3 Beoordeling van technische naleving

Wat is er veranderd ten opzichte van de BIG?

Meer beveiligingseisen en aandacht voor de keten van leveranciers, verder is er weinig veranderd ten opzichte van de BIG, in de maatregelen en controls is er een kleine nuance.

Inhoudsopgave

1. Inleiding

Een SLA, ook wel Diensten Niveau Overeenkomsten (DNO) genoemd, is een schriftelijke overeenkomst tussen twee partijen waarin afspraken over een gezamenlijk overeengekomen dienstenniveau staan tussen een aanbieder en een afnemer van een dienst of een product.

De insteek bij het opstellen van een SLA is een partnership gericht op een 'goede' samenwerking tussen gemeente en dienstleverancier. In een SLA wordt de link gelegd tussen de zakelijke behoeften/verwachtingen van de gemeente en de hiervoor benodigde diensten/technologie. De insteek dient ten allen tijde te zijn dat wordt voorkomen dat zowel de gemeente als de dienstleverancier in de stand van 'verschuilen / excuses' komen te staan. Dit kan bereikt worden door afspraken te maken over het 'wat' er geleverd dient te worden en niet over het 'hoe'. Er dienen ook afspraken gemaakt te worden over het testen van de gemaakte afspraken of anders geformuleerd aantonen dat de dienstleverancier kan voldoen aan de doelstelling.

Het opstellen van een SLA is geen eenvoudige zaak. Het resultaat van een SLA is dat de dienstleverancier kan laten zien dat de gewenste dienst wordt geleverd, op een wijze die begrijpelijk is voor de gemeente, conform vooraf gedefinieerde meetpunten en gerealiseerde resultaten. Samengevat weet de dienstleverancier wat er van hem verwacht wordt en wordt door de dienstleverancier de zakelijke behoefte van de gemeente ingevuld.

1.1. Business case

U dient vast te stellen of uitbesteding (cloudcomputing) geschikt is voor uw gemeente. Om een gedegen beslissing te kunnen nemen, dient u een business case te maken. Deze business case dient te beschrijven waarom deze dienst door de gemeente bij de dienstleverancier wordt betrokken, welke overwegingen hieraan ten grondslag hebben gelegen. Tevens dient u bij deze afweging ook in kaart te brengen wat de impact is op uw gemeentelijke- en beheerprocessen. Om het uiteindelijke transitie- en migratieproces voor uw gemeente zo soepel mogelijk te laten verlopen, moet u de wijzigingen op uw processen in kaart brengen en het verandertraject starten voordat met de migratie van uw ICT-dienstverlening kan worden gestart. Zorg dat informatiebeveiliging aantoonbaar (op basis van een risicoafweging) is meegewogen bij het besluit een externe dienstleverancier wel of niet in te schakelen.

Voorbeeld overwegingen om van een externe dienstleverancier gebruik te maken zijn hogere beschikbaarheid, samenwerking van afnemers, kostenbeheersing, verhogen dienstverlening, flexibiliteit, betere beveiliging.

1.2. Doelstelling Service Level Agreement

Het doel van de SLA is het maken en onderhouden van structurele afspraken met betrekking tot een gezamenlijk overeengekomen dienstenniveau en het rapporteren over de gerealiseerde dienstverlening. Het doel van de SLA moet uitgeschreven worden in ondubbelzinnige bewoordingen. De onderhandelingen tussen de gemeente en de dienstleverancier dient te gaan over eenheden die begrijpelijk en meetbaar zijn voor de gemeente, zoals het aantal transacties per uur of het aantal e-mails per dag en niet over CPU[1] tijd en hoeveelheden gebruikt geheugen.

1 CPU = Central Processing Unit.

Hiervoor worden prestatie indicatoren en kwaliteitseisen van een dienst of een product vastgelegd, zodat deze later kunnen worden getoetst, en ook worden hierin de rechten en plichten van zowel aanbieder als afnemer vastgelegd. De SLA structureert tevens de wijze waarop aanvragen voor nieuwe of aangepaste diensten worden afgehandeld en leiden tot nieuwe of aangepaste afspraken.

1.3. De indeling van dit document is als volgt

In hoofdstuk 2 wordt algemene en achtergrondinformatie geven van de SLA. Denk hierbij aan het doel van een SLA, de samenhang van de SLA met andere documenten in de inkoopketen en dat de afspraken in de SLA volgens het SMART-principe gedefinieerd dienen te worden.

Hoofdstuk 3 geeft een beschrijving van de klant-leverancierrelatie en een generieke opbouw van de SLA.

In bijlage 1 wordt een voorbeeld SLA beschreven. Dit voorbeeld kan worden gebruikt bij het opstellen en/of reviewen van een SLA, om te verifiëren of alle relevante aspecten zijn beschreven.

Aanwijzing voor gebruik

Deze handleiding is qua opzet geschreven om te beschrijven waaraan een goede SLA moet voldoen inclusief passende beveiligingsmaatregelen gebaseerd op de BIO. Een SLA staat niet op zichzelf, er zijn kwaliteitseisen aan de opdrachtgever en opdrachtnemer en er zijn eventueel ook aanvullende producten, zoals een Dossier Afspraken en Procedures (DAP) en een Dossier Financiële Afspraken (DFA).

2. SLA algemeen

Een SLA kan een contract zijn, maar wordt ook vaak gebruikt als instrument om afspraken vast te leggen naast een formeel (inkoop)contract. Een succesvolle SLA is een goed instrument voor de organisatie om de klant-leverancierrelatie te optimaliseren en te professionaliseren. Een SLA zorgt ervoor dat de interne vraag concreet gemaakt wordt en dat de leverancier meer levert vanuit een concurrentiepositie.

De SLA is daarom zowel een communicatie- als een sturingsmiddel, creëert een marktwerking tussen de (interne) klant en de leverancier, en zorgt voor een betere sturing op kosten. Zo brengt een SLA klant en leverancier op gezette tijden samen en dient het als een platform voor discussie over de gewenste kwaliteit en levering van diensten. Daarnaast kunnen in een SLA specifieke Kritieke/Kritische Prestatie Indicatoren of Key Performance Indicators (KPI's) worden opgenomen die de interne dienstverlening meetbaar maken, waardoor er meer op resultaat kan worden gestuurd in plaats van op inspanningsverplichtingen. Tevens kan de kostendoorbelasting van de diensten een belangrijk onderdeel van de SLA vormen, waardoor de klant meer invloed krijgt op de financiële gevolgen van zijn vraag. Een succesvolle SLA straalt hiermee professionaliteit uit en geeft uitleg over de te leveren dienstverlening, hoe deze wordt gemonitord en hoe hierover verantwoording wordt afgelegd door middel van rapportages.

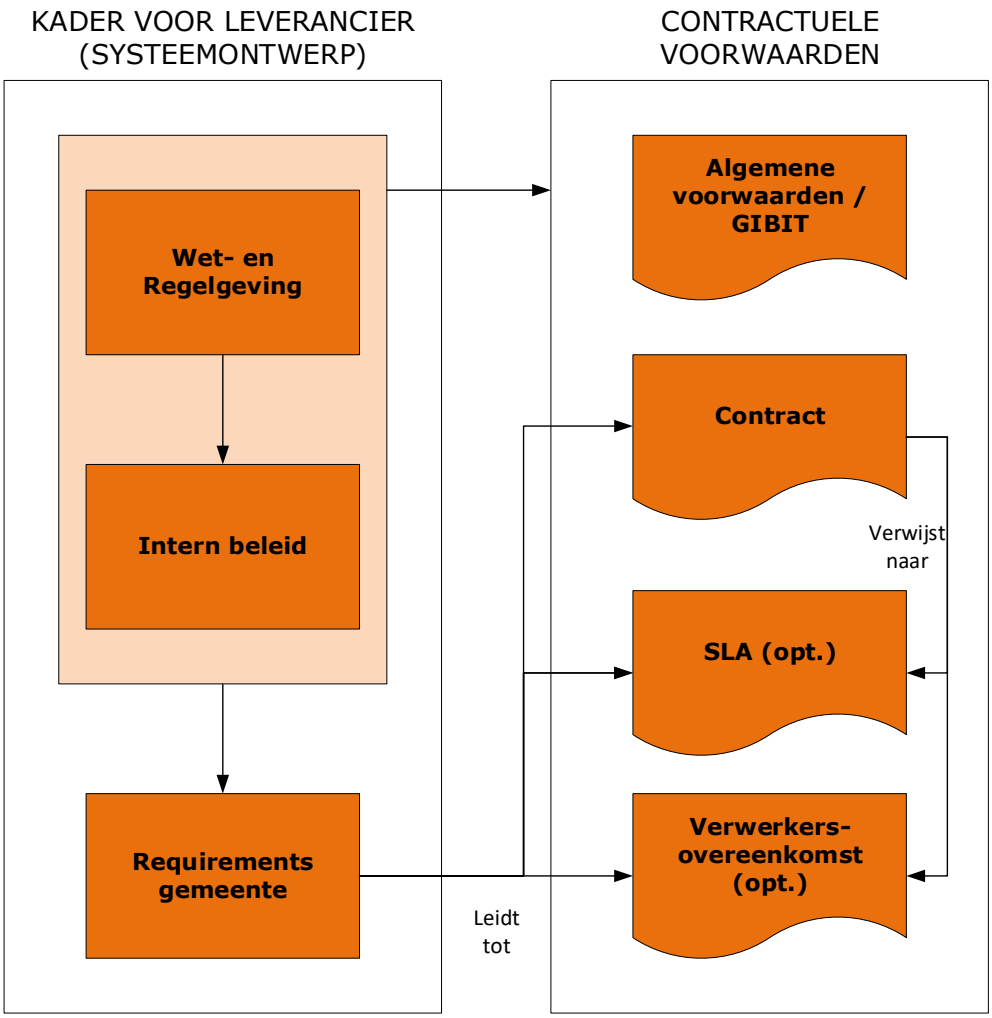
2.1. Verschijningsvormen

Een SLA kent meerdere verschijningsvormen afhankelijk van het product of de dienst die uitbesteed of ingekocht is. Daarnaast kunnen er meerdere benamingen gebruikt worden:

- Service Level Agreement (SLA)
- Service Niveau Overeenkomst (SNO)
- Diensten Niveau Overeenkomst (DNO)
- Product Level Agreement (PLA)

2.2. Plaats SLA in de inkoopketen

De SLA voor een (ICT-)dienst of service staat niet los van de hoofdovereenkomst, waarin de algemene (inkoop)voorwaarden staan beschreven en die niet afhankelijk zijn van de specifieke dienstverlening die wordt afgenomen. De vereisten voor de beveiliging van de dienst kunnen in een separate beveiligingsovereenkomst beschreven zijn of zijn opgenomen in de (hoofd-) overeenkomst. Belangrijk is steeds dat het totaal aan vereisten, alle facetten van de kwaliteit van de dienst borgen. De afspraken in het contract kunnen daarbij steeds worden geconcretiseerd in een SLA. Als verwerking van de privacygevoelige informatie plaatsvindt, is dit vastgelegd in een bewerkersovereenkomst. Dit levert voor de beveiligingsvereisten de volgende verhouding tussen de documenten op, zoals in figuur 1 weergegeven.



Figuur 1 Verhouding tussen de documenten.

2.3. SMART

De afspraken in de SLA dienen te voldoen aan het SMART-principe:

- **S**pecifiek / Simpel
  De volgende vragen kunnen helpen om de doelstelling zo duidelijk en eenduidig mogelijk te formuleren:
  - Wat willen we bereiken?
  - Wie is er bij betrokken?
  - Waar gaat het gebeuren?
  - Wanneer gebeurt het?
  - Waarom willen we het bereiken?

Voorbeeld: De beschikbaarheid van het gemeentelijke digitale portaal (wat) is op 1 januari 2020 (wanneer) met 10% toegenomen (wat) ten opzichte van 1 januari 2019 (wanneer). Tegelijkertijd zijn de kosten (wat) met 10% afgenomen.

- **M**eetbaar
  De meetbaarheid wordt meestal uitgedrukt in kwantitatieve eenheden (getallen). De meetbaarheid kan ook zichtbaar gemaakt worden door het doel te vergelijken met bestaande procedures, kwaliteitseisen, normen, handleidingen of systemen. Hierbij is het van belang of het behalen van de doelstelling meetbaar is of onder welke (meetbare) voorwaarden het doel is bereikt. Denk aan: hoeveel, hoe is dit vast te stellen.

  Voorbeeld: De beschikbaarheid van het gemeentelijke digitale portaal is op 1 januari 2020 met 10% toegenomen (getal) ten opzichte van 1 januari 2019 Tegelijkertijd zijn de kosten met 10% afgenomen (getal).

- **A**cceptabel / Aanvaardbaar
  Is de doelstelling relevant en wordt deze geaccepteerd door de betrokkenen (doelgroep en/of management)? Is er voldoende draagvlak om het doel te behalen?

  Voorbeeld: De beschikbaarheid van het gemeentelijke digitale portaal is op 1 januari 2020 met 10% toegenomen (resultaat) ten opzichte van 1 januari 2019. Tegelijkertijd zijn de kosten met 10% afgenomen (resultaat).

- **R**ealistisch / Resultaatgericht
  Hierbij is de belangrijkste vraag of de doelstelling haalbaar is. De volgende vragen kunnen helpen om de doelstelling zo realistisch en resultaatgericht mogelijk te formuleren:
  - Zijn de inspanningen niet te hoog of te laag?
  - Staan de inspanningen in relatie met het te behalen resultaat?

  Voorbeeld: De beschikbaarheid van het gemeentelijke digitale portaal is op 1 januari 2020 met 10% toegenomen (haalbaar) ten opzichte van 1 januari 2019. Tegelijkertijd zijn de kosten met 10% afgenomen (haalbaar).

- **T**ijdgebonden
  Wanneer (in de tijd) moet het doel bereikt zijn? Wat is de deadline voor de doelstelling? Welke planning hoort hierbij? Denk hierbij aan start-, eind- en eventuele tussendata.

  Voorbeeld: De beschikbaarheid van het gemeentelijke digitale portaal is op 1 januari 2020 (datum) met 10% toegenomen ten opzichte van 1 januari 2019 (datum). Tegelijkertijd zijn de kosten met 10% afgenomen.

3. Opbouw SLA

Een SLA kan, als het goed is opgezet, breder en effectiever zijn dan een contract alleen. SLA's zouden idealiter handvatten moeten bieden voor risk management en compliance rondom het managen van het uitbestedingsrisico, en het 'nieuwe' keten denken bij veel overheidsinstellingen moeten ondersteunen. Daarnaast moeten ze gericht zijn op communicatie en uitleg. SLA's zijn in dat geval meer gericht op het faciliteren van verandering en het vastleggen van 'wie doet wat', dan op het weergeven van een statisch contract tussen interne partijen.

De praktijk leert echter dat SLA's onvoldoende worden ingezet als tool bij het managen van het uitbestedingsrisico en de procesketen. Deze situatie wordt door het management veelal onwenselijk geacht met het oog op de borging van de continuïteit van de bedrijfsvoering, de integriteit van de organisatie en de kwaliteit van de dienstverlening.

De SLA als tool om het uitbestedingsrisico te beheersen

Het komt voor dat gemeenten onderdelen van hun primaire proces(-keten) dan wel van hun ondersteunende proces, bijvoorbeeld de ICT-organisatie, hebben uitbesteed aan andere concern onderdelen, dan wel aan samenwerkingsverbanden of leveranciers.

Het management van de gemeente dient, ook als processen zijn uitbesteed aan andere onderdelen binnen het eigen concern, de verschillende instanties rondom basisregistraties of DigiD te kunnen laten zien, en aan te kunnen tonen dat er voldoende maatregelen zijn getroffen om ook de risico's die inwerken op de uitbestede processen volledig te beheersen. Dat kan als partijen werken met SLA's die geen papieren tijgers zijn.

De wetgever stelt vanuit haar rol als toezichthouder eisen aan SLA's, omdat de wijze waarop een gemeente georganiseerd is, van invloed is op de kwaliteit van het proces in de hele keten van het concern. Uitbesteding wordt hierbij opgevat als het structureel laten uitvoeren van primaire processen of ondersteunende taken door een andere organisatorische of juridische entiteit van het concern, of door een onafhankelijke derde. Het gaat dan om processen en taken waaraan risico's zijn verbonden die materiële invloed kunnen hebben op de prestaties, de positie, de continuïteit en/of de integriteit van de gemeente.

Deze generieke SLA beschrijft de verplichtingen en verantwoordelijkheden van de gemeente en de leverancier van de onderhavige ICT-diensten. Het gaat hierbij om:

- Door de gemeente uit te besteden ICT-diensten aan een leverancier.
- Het afnemen van ICT-diensten door de gemeente die door een leverancier worden geleverd.

Uitgangspunt hierbij is dat zo optimaal invulling wordt gegeven aan de wensen en behoeften van de gemeente, uiteraard binnen de afgesproken kostenkaders.

Een aspect dat bijzondere aandacht verdient bij ICT-uitbesteding is de beveiliging. Wanneer een gemeente een deel van hun ICT-dienstverlening door een derde partij laat uitvoeren, wil de gemeente de zekerheid hebben dat de betrouwbaarheid van zijn informatievoorziening gehandhaafd blijft. De gemeente zal van de leverancier verlangen dat deze aantoonbaar aan de gestelde beveiligingseisen kan voldoen.

3.1. Klant-leverancierrelatie

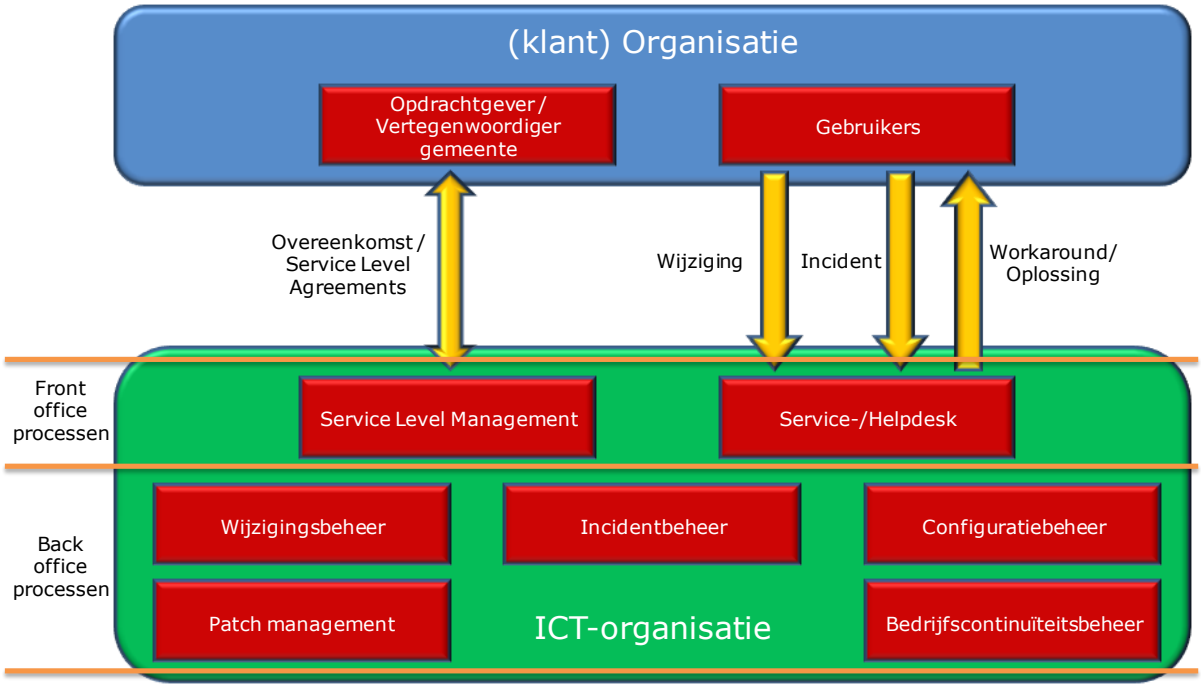
Bij uitbesteding, de overdracht van de uitvoering van diensten aan een derde partij, is de 'klant-leverancierrelatie' belangrijk. Bij de klant-leverancierrelatie zijn minimaal twee partijen betrokken. Enerzijds is er de klant (in dit geval de gemeente) die (een deel van) de uitvoering en het beheer van zijn ICT-proces heeft uitbesteed aan een derde partij. Anderzijds is er de leverancier die de uit te besteden taken en verantwoordelijkheden op zich neemt. De relatie tussen de klant en de leverancier is op enigerlei wijze geformaliseerd in een klant-leverancierovereenkomst.

Naast de aard van de klant-leverancierrelatie dienen ook afspraken omtrent de inhoud en kwaliteit van de dienstverlening te worden vastgelegd. Veelal gebeurt dit in een apart document, de SLA. De procedures waarmee klant- en leveranciersorganisaties de activiteiten coördineren zijn veelal vastgelegd in een Dossier Afspraken en Procedures (DAP), of ook wel aangeduid als Operational Level Agreement (OLA).

De klant-leverancierrelatie is van groot belang, omdat het zowel inhoud geeft aan de communicatie tussen de klant en de leverancier, als aan de structuur die daaraan ten grondslag ligt. De klant-leverancierrelatie raakt alle niveaus van de betrokken organisaties. De klant-leverancierrelatie is dan ook werkzaam op zowel strategisch niveau, waar klant-leverancierovereenkomsten (bijvoorbeeld uitbestedingsovereenkomsten met externe leveranciers) worden gesloten, als op tactisch niveau, waar de SLA's tot stand komen, als op operationeel niveau, waar de DAP's van toepassing zijn.

De kwaliteit van de diensten die de leverancier aan de klant levert, wordt in beginsel door twee elementen bepaald. Enerzijds de wijze waarop de leverancier zijn interne processen beheerst en daarmee de kwaliteit van het geleverde product kan bepalen. Anderzijds de wijze waarop de leverancier met de klant communiceert en daardoor in staat is aan de wensen van de klant te voldoen. Gewoonlijk wordt deze tweedeling bij de leverancier tot uiting gebracht door een onderscheid te maken tussen front- en backoffice processen (zie figuur 2 op de volgende pagina). In de SLA dient aan beide soorten processen zeker aandacht gegeven te worden, maar de wijze waarop zal sterk verschillen.

Voor frontoffice processen, zoals de ondersteuning door de service-/helpdesk, zullen gedetailleerde afspraken gemaakt moeten worden omtrent de kwaliteit van de dienstverlening, vertaald in bijvoorbeeld bereikbaarheid van de help-/servicedesk, openstellingstijden, responstijden, oplospercentages, et cetera. De backoffice processen behoren tot de verantwoordelijkheid van de leverancier en blijven voor de klant grotendeels 'verborgen'. De klant kan dan ook slechts een indirecte invloed uitoefenen op het functioneren en de beveiliging van deze processen. De klant kan bij deze processen in principe volstaan met het opstellen van algemeen geformuleerde normen. Op welke wijze bijvoorbeeld het incident- en probleembeheer is ingericht, is voor de klant niet van essentieel belang, wel is van belang dat de incidenten en problemen (van een bepaalde categorie) binnen een bepaalde tijd worden opgelost. Of de leverancier voor het oplossen van het incident of probleem eigen specialisten inschakelt, daarvoor gebruikmaakt van externen of misschien wel moet uitwijken naar een ander systeem, is voor de klant niet van doorslaggevend belang. Het belangrijkste is dat de in de SLA afgesproken continuïteitsnorm wordt gehandhaafd. Uit het oogpunt van kwaliteitsborging is het van belang dat er in de SLA niet alleen beveiligingsnormen worden vastgelegd, maar ook dat deze normen worden gecontroleerd. De leverancier toont door middel van rapportage aan dat de in de SLA gemaakte afspraken ook zijn nagekomen. Zeker bij frontoffice processen zal dit een effectief controlemiddel zijn. Voor backoffice processen, die minder zichtbaar zijn voor de klant, is het aan te bevelen om periodiek een onafhankelijke controle bij de leverancier uit te voeren naar de kwaliteit hiervan.



Figuur 2 Samenhang front- en backoffice processen

In de praktijk wordt hierin door de leverancier voorzien, door jaarlijks aan een onafhankelijke EDP-auditor te vragen een zogenaamde Third Party-Mededeling (TPM) af te geven. In de SLA kan worden volstaan met de afspraak dat jaarlijks een onafhankelijke audit wordt uitgevoerd.

3.2. Aanvullende producten

Een SLA kan net als andere contractvormen al snel een zeer omvangrijk product worden. Een SLA kan beter klein gehouden worden en daarbij bestaan uit één of meer bijlagen. De SLA wordt dan gezien als kapstok waaraan alles wordt opgehangen. Aangezien een SLA vaak op directieniveau getekend wordt is het handig om de SLA zelf niet te vaak te laten wijzigen, een directietraject kan namelijk lang duren.

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage 1: Opbouw/indeling SLA

Inhoudsopgave

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage 2: Template SLA

In deze bijlage wordt een verdere invulling gegeven van de opbouw zoals deze in bijlage 1 is weergegeven.

Deze template bevat een globale lijst met aandachtspunten die relevant zijn bij het opstellen van een Service Level Agreement (SLA). Het toesnijden op iedere gemeentelijke individuele praktijksituatie is ondoenlijk en er kan dan ook niet ingegaan worden op het afbreukrisico's die in uw specifieke situatie gelopen wordt. Op basis van het af te nemen product en/of dienst en eigen risicoafweging dient de gemeente te beslissen welke aandachtspunten uit deze template relevant zijn. Deze relevante aandachtspunten kunnen daarna door de gemeente gebruikt worden om de nieuwe SLA op te stellen of de SLA van de dienstleverancier te beoordelen. Het kan ook voorkomen dat bepaalde onderwerpen en/of detaillering niet in deze SLA worden beschreven maar in een ander document worden opgenomen zoals Dossier afspraken en Procedures (DAP, inkoopvoorwaarden, contract/overeenkomst of bewerkersovereenkomst. Denk hierbij aan kwantitatieve afspraken zoals aantal gebruikers. Deze aantallen kunnen in de loop van de tijd veranderen en hiervoor wil je niet telkens de SLA aanpassen.

Het is niet de bedoeling om een compleet overzicht te geven van de doelstellingen op het gebied van dienstenniveaus (Service Level Objectives (SLOs)), maar om voorbeelden te geven die kunnen worden gebruikt bij het opstellen van de eisen door de gemeenten.

i. Versiebeheer/Wijzigingshistorie

Hier worden de wijzigingen op de SLA beschreven die zijn goedgekeurd en door wie.

ii. Distributielijst

Hier worden de functies/personen opgesomd die een afschrift dienen te ontvangen van deze SLA.

iii. Leeswijzer

Hier wordt beschreven hoe dit SLA het beste gelezen kan worden, afhankelijk van de functie/taak en achtergrondkennis van de lezer.

0. Positie SLA en gerelateerde documenten

Hier wordt de samenhang beschreven tussen het contract / de overeenkomst en de SLA en de relatie met documenten die mogelijk als bijlagen op de SLA zijn bijgevoegd.

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 van de SLA

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.

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

Afspraken over het verlengen van de looptijd en het beëindigen van de SLA en tevens afspraken over het voortijdig beëindigen van de SLA (exitprocedure/-strategie). De beschrijving van de exitprocedure is te vinden in het Dossier Afspraken en Procedures (DAP).

- 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).

2.2 Ontbinding en garanties

Beschrijving van de ontbindende voorwaarden. Maar ook de garanties met betrekking tot de overdracht en vernietiging van gegevens.[2] Bijvoorbeeld het langdurig niet halen van de afgesproken dienstenniveaus.

2 Zie ook paragraaf 5.1 in dit document.

2.3 Wijzigingssproces van het SLA

Wijzigingen op de in het SLA vastgelegde regelingen, prestaties en rapportages kunnen zowel een incidenteel[3] als een blijvend (structureel)[4] 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

Aard van de uitbestede activiteiten of de ingekochte of geleverde goederen/diensten.

- Belang van de dienst
  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.

- Identificatie van essentiële componenten
  Hier wordt onder andere de essentiële hard- en software beschreven, maar ook de gemeentelijke (vitale) bedrijfsfuncties die door de dienst ondersteund worden. Deze informatie kan verkregen worden uit een door de gemeente uitgevoerde baselinetoets BIO, diepgaande risicoanalyse of classificatie van informatie verkregen informatie.

- Vitale bedrijfsfuncties, processen en activiteiten
  Hier worden de vitale gemeentelijke bedrijfsfuncties, processen en activiteiten die door de (ICT-)dienst ondersteund worden beschreven. Hierbij is input van de gemeente uiteraard onontbeerlijk. De gemeente geeft aan de dienstleverancier aan wat voor hen van belang is. Hier wordt ook vermeld of er (bijzondere) persoonsgegevens worden verwerkt.

- Overige essentiële zaken
  Hier wordt onder andere het (laten) testen van de dienst en de controle op de beveiligingsmaatregelen beschreven. In de SLA dient dan ook vastgelegd te worden welke beveiligingsmaatregelen vereist zijn, dat deze door de dienstleverancier getroffen zijn en worden nageleefd, en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook dient beschreven te zijn hoe die beveiligingsmaatregelen door de dienstleverancier te controleren zijn (bijvoorbeeld audits en penetratietests) en hoe het toezicht is geregeld.

- Business impact bij verlies van de dienst
  Hier wordt de business impact beschreven bij verlies van de dienst op basis van de resultaten van de uitgevoerde baselinetoets BIO of de handreiking classificatie.

3 Bij deze wijzigingen gaat het om een eenmalige, kortstondige afwijking van de inhoud van het SLA, waarbij het SLA als zodanig niet wijzigt.

4 Een wijziging is structureel wanneer ten gevolge van deze wijziging de inhoud van het SLA verandert.

3.2 Gebruiksresultaat

Beschrijving van het gewenste gebruiksresultaat, hier worden de kwalitatieve en kwantitatieve afspraken voor het te realiseren dienstenniveau beschreven.

3.3 Garanties

Beschrijving van de gewenste resultaten in termen van garanties, hier worden de kwalitatieve en kwantitatieve afspraken voor het te realiseren dienstenniveau beschreven.

3.4 Kwaliteit

Hier worden de kwaliteitsnormen, certificeringen et cetera beschreven waaraan de dienstleverancier dient te voldoen.

3.5 Dienstverleningstijden

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

- Support (service-/helpdesk)
  Support is de dienstverlening die door dienstleverancier wordt geleverd om incidenten, problemen en vragen van de gemeente af te handelen. Hier worden afspraken met betrekking tot reactie- en oplostijden vastgelegd.

- Beschikbaarheid van de dienst (uptime)
  Beschikbaarheid is de eigenschap dat de dienst toegankelijk en bruikbaar is op het moment dat de gemeente gebruik wil maken van de dienst. Beschikbaarheid is een belangrijke dienstniveaudoelstelling, want het beschrijft of de dienst daadwerkelijk gebruikt kan worden. Het is belangrijk om de beschikbaarheid van de dienst vast te stellen in combinatie met het belang van beschikbaarheid van de specifieke toepassing voor uw gemeente.

- Onderhoud
  Hier worden de afspraken met betrekking tot het onderhoud van de dienst vastgelegd. De uitvoering van onderhoudswerkzaamheden kan tot gevolg hebben dat de dienst niet beschikbaar is voor gebruik door de gemeente.

- Uitzonderingen op beschikbaarheid dienstverlening
  Hier worden de afspraken met betrekking tot de uitzonderingen op de beschikbaarheid van de dienstverlening vastgelegd.

- Stand-by
  Hier worden de afspraken met betrekking tot de stand-by dienstverlening vastgelegd.

3.6 On-site ondersteuning

Hier worden de afspraken met betrekking tot het on-site vereiste niveau van ondersteuning (support) vastgelegd.

- Locaties/Ruimtes
  Hier worden de afspraken vastgelegd vanaf welke locaties / ruimtes met de dienst gewerkt kan worden en welke bijzonderheden hierop van toepassing zijn. Bij een SaaS-dienst gelden hiervoor hoogstwaarschijnlijk geen beperkingen aangezien deze dienst via het internet benaderd kan worden.

- Soorten gebruikers
  Hier worden de afspraken vastgelegd over welke soorten en het aantal gebruikers dat van de dienst gebruik gaat maken. Maak het gebruik van een bandbreedte mogelijk (minimaal en maximaal aantal gebruikers).

- Soorten infrastructuren
  Hier worden de afspraken vastgelegd over welke soorten infrastructuur er worden ondersteund.

3.7 Ondersteuning op afstand

Hier worden de afspraken met betrekking tot het vereiste niveau van ondersteuning (support) op afstand vastgelegd. Denk hierbij aan toegang op afstand tot systemen door de technisch beheerders van de dienstleverancier/-verlener (beheerders) maar ook aan de gemeentelijke functioneel beheerders en (eind)gebruikers. Tevens dienen afspraken vastgelegd te worden met betrekking tot de beveiliging.

- Locaties/Ruimtes
  Hier worden de afspraken vastgelegd over vanaf welke locaties/ruimtes ondersteuning op afstand kan worden geboden. Bij een SaaS-dienst gelden hiervoor hoogstwaarschijnlijk geen beperkingen aangezien het beheer van deze dienst via het internet uitgevoerd kan worden, middels een beheerinterface.

- Soorten gebruikers
  Hier worden de afspraken vastgelegd over welke soorten en het aantal gebruikers dat van de dienst op afstand gebruik gaat maken. Groepen/gebruikers die toegang tot de dienst worden toegekend. Maak het gebruik van een bandbreedte mogelijk (minimaal en maximaal aantal gebruikers).

- Soorten infrastructuur
  Hier worden de afspraken vastgelegd over welke soorten infrastructuur worden ondersteund.

3.8 Wijzigingen

Hier worden afspraken vastgelegd over het indienen van wijzigingsverzoeken door de gemeente. Te denken valt aan de verschillende categorieën wijzigingen die daarbij worden onderkend, evenals criteria voor indeling van deze categorieën en per onderkende wijzigingscategorie de tijd die geldt voor het doorvoeren van de betreffende wijziging, de wijze waarop (belangrijke) wijzigingen binnen de ICT-organisatie impact kunnen hebben voor de gebruikersorganisatie van de gemeente en de wijze waarop over wijzigingen wordt gerapporteerd.

Er dienen ook afspraken met leveranciers worden vastgelegd over:

- dat de leverancier een wijzigingsbeheerproces uitvoert en dat het wijzigingsbeheerproces bij de leverancier en bij de exploitatieorganisatie van de gemeente op elkaar zijn afgestemd, dit geldt in het bijzonder voor de wederzijdse wijzigingskalenders.
- welke categorieën wijzigingen de leverancier autonoom binnen zijn eigen wijzigingsbeheerproces mag doorvoeren, en over welke wijzigingen afstemming met het wijzigingsbeheerproces van de gemeente plaatsvindt.
- welke eisen door de gemeente worden gesteld aan de informatievoorziening over de wijzigingen bij de leverancier.

3.9 Eigendom

Hier wordt beschreven wie de eigenaar is van de gegevens, software en hardware. Hier kunnen ook afspraken met betrekking tot de intellectuele eigendomsrechten worden beschreven.

4 Communicatie tussen gemeente en dienstverlener

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. Er wordt vastgelegd wanneer gestructureerd overleg plaatsvindt, wie er aan dit overleg deelnemen en wie bij beide partijen verantwoordelijk zijn voor de onderlinge relatie. Tevens wordt een overzicht opgenomen van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten. Een nadere concretisering van deze overlegvormen is opgenomen in het Dossier Afspraken en Procedures (DAP). Denk hierbij aan tijdstippen of aanleidingen voor overleg en de betrokken personen bij overleg.

4.1 Verantwoordelijke contactpersoon gemeente

Hier worden de contactgegevens van de verantwoordelijke contactpersoon van de gemeente weergegeven. Dit kan dezelfde persoon zijn als die bij paragraaf 1.2 maar dit kan ook een operationeel / procesmanager zijn.

4.2 Verantwoordelijk (klant) manager leverancier

Hier worden de contactgegevens van de service level manager (zie paragraaf 1.1) of de (klant) manager verantwoordelijk voor het leveren van de dienst van de leverancier weergegeven.

4.3 Dienstrapportages

Hier wordt de inhoud en frequentie (interval) van de rapportage beschreven die door de dienstleverancier worden opgeleverd. Als gemeente dient u zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de afgenomen dienstverlening.

4.4 Uitzonderingen en klachten

Hier worden de procedures voor de behandeling van uitzonderingen en klachten beschreven. Bijvoorbeeld gegevens die moeten worden opgenomen in formele klachten, afgesproken responstijden en de escalatie procedure. De procedure voor de behandeling van uitzonderingen en klachten is te vinden in het Dossier Afspraken en Procedures (DAP).

- Communicatie in geval van escalaties
  Aangaande de dienstverlening welke buiten de afgesproken dienstenniveaus valt, kan geëscaleerd worden. Bijvoorbeeld: Eindgebruikers dienen altijd eerst de help-/servicedesk (escalatie niveau 1) te bellen. Overige partijen binnen de gemeente kunnen vanuit hun functie contact opnemen met hun counterpart bij de dienstleverancier. De escalatieprocedure is te vinden in het DAP en geeft onder andere aan welke personen betrokken zijn bij escalaties en welke afwijkende clausules gelden ten opzichte van het SLA (bijvoorbeeld met betrekking tot het verlenen van extra ondersteuning door de dienstleverancier).

- Communicatie in geval van geschillen
  Beschrijving van het feit wanneer onderling overleg plaatsvindt en wat de procedure is bij het optreden van onderlinge conflicten of geschillen qua afhandeling en het betrekken van derde partijen. De geschillenprocedure is te vinden in het DAP en geeft onder andere aan welke personen betrokken zijn bij geschillen (bijvoorbeeld een onafhankelijke derde instantie of persoon) en het feit of een uitspraak van een onafhankelijke geschillencommissie bindend is of niet.

4.5 Tevredenheidsonderzoeken

Hier wordt de procedure beschreven voor het meten van de tevredenheid van de gemeente. Deze meting dient op regelmatige basis plaats te vinden. De procedure voor het meten van de tevredenheid 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.

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 eisen / doelen

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

Niet beschikbaarheidsvoorwaarden

Hier worden de voorwaarden beschreven wanneer de dienst als niet beschikbaar wordt beschouwd. Houdt hierbij rekening met de omstandigheid dat de dienst op meerdere locaties wordt aangeboden en het niet beschikbaar zijn van de dienst een gevolg kan zijn van beveiligingsincidenten (bijvoorbeeld DDoS).

- Beschikbaarheidsdoelen
  De mate waarin aan de vraag naar een product wordt voldaan (servicegraad). Exacte definitie van hoe de overeengekomen beschikbaarheidniveaus wordt berekend, op basis van de afgesproken servicetijd en downtime. Dit wordt meestal uitgedrukt in een percentage en kan gemeten worden op verschillende plaatsen in de keten.

  Opslagbeheer
  Aan de opslag en verwerking van de gebruikersgegevens kunnen door de gemeente aanvullende eisen gesteld worden, bijvoorbeeld ten aanzien van de wijze van bewaren, de bewaartermijn en de wijze van vernietiging. Eventueel kunnen voor bijzonder vertrouwelijke of privacygevoelige gegevens aanvullende afspraken worden gemaakt.
  Uitval van infrastructurele voorzieningen
  De wijze waarop de facilitaire en ICT-voorzieningen zijn ingericht is de verantwoordelijkheid van de dienstleverancier. 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.

  Onvoldoende scheiding tussen ontwikkel-, test- en productieomgeving
  Het aanbrengen van scheiding tussen ontwikkel-, test- en productieomgeving is primair bedoeld om in ieder geval de productieomgeving zo veel mogelijk te isoleren van verstorende externe invloeden. Door middel van wijzigingsbeheer en autorisatiebeheer kan deze scheiding verder in stand worden gehouden. Deze werkzaamheden gebeuren volledig bij de dienstleverancier.

  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.

- Betrouwbaarheidsdoelen
  Hier worden de betrouwbaarheidsdoelen van de dienst beschreven die door de gemeente worden vereist, meestal gedefinieerd als MTBF (Mean Time Between Failures) of MTBSI (Mean Time Between Service Incidenten)

- Onderhoudbaarheidsdoelen
  Hier worden de onderhoudbaarheidsdoelen met betrekking tot de dienst beschreven.

- Niet beschikbaar in verband met onderhoud
  Hier worden afspraken beschreven die te maken hebben met onderhoud van het ICT-systeem of-dienst. Denk hierbij aan het aantal toegestane periodes van het niet beschikbaar zijn (downtime) en welke periode vereist is om het niet beschikbaar zijn door te geven aan de gemeente.

- Onderhoudsbeperkingen
  Hier worden afspraken beschreven met betrekking tot onderhoudsbeperkingen. Bijvoorbeeld toegestane onderhoudsvensters, wanneer mag er geen onderhoud plaatsvinden en procedures om de geplande onderbrekingen in de dienstverlening aan te kondigen. De procedures om de geplande onderbrekingen in de dienstverlening aan te kondigen zijn te vinden in het DAP.

- Beschikbaarheidsrapportage
  Hier worden de eisen ten aanzien van de beschikbaarheidsrapportage beschreven. Verwijs naar een bijlage waar een voorbeeld van de rapportage is opgenomen.

- Definities
  Hier worden de definities gegeven van bijvoorbeeld grote incidenten en spoedwijzigingen.

5.2 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.

- Benodigde capaciteit
  Hier worden de benodigde capaciteitseisen, op basis van de onder- en bovengrens, beschreven voor de betreffende dienst. Denk hierbij aan de eisen met betrekking tot transacties en gebruikers.
  De capaciteit geeft de maximale hoeveelheid weer van een bepaalde eigenschap (kenmerk/karakteristiek) van de dienst. Het is vaak een belangrijke waarde voor gemeenten om te weten wanneer ze gebruik gaan maken van een dienst. Relevante eigenschappen kunnen variëren, afhankelijk van de mogelijkheden die door de dienst worden ondersteund (geboden). Het is ook vaak het geval dat meerdere eigenschappen relevant zijn voor een bepaalde dienst met de bijbehorende capaciteit per eigenschap. Afspraken met betrekking tot de capaciteit dienen duidelijk in de SLA te worden beschreven voor een dienst. Merk op dat de capaciteit dienstniveaudoelstellingen verwijzen naar de capaciteiten zoals deze worden gezien door een individuele gemeente en dat reflecteert niet het totaal aan capaciteiten, die door de dienstleverancier wordt ondersteund. Vaak kan de gemeente capaciteitsgrenzen voor hun dienst(en) aanpassen door het aanvragen van een wijziging in hun abonnement.
  Er zijn een aantal dienstniveaudoelstellingen, die betrekking hebben op de capaciteit van een dienst. Het gaat hierbij ondermeer om de hoeveelheid opgeslagen data, aantal gebruikers, aantal profielen, aantal transacties, aantal servicedesk calls, aantal (gelijktijdige) hits op de website, verwachte groei van deze dienstniveaudoelstellingen et cetera.

- Responstijden
  Hier worden de eisen met betrekking tot responstijden van het ICT-systeem en –dienst beschreven. Zoals, op piektijden binnen drie seconden een antwoordbericht, verversen van een webpagina en respons geven binnen vijf seconden.
  Responstijd is het tijdsinterval tussen de door de gemeente geïnitieerde gebeurtenis (stimulus) met betrekking tot de dienst en de door de dienstleverancier geïnitieerde gebeurtenis in reactie op die stimulus.

De responstijd dienstniveaudoelstelling kan variëren afhankelijk van het moment waarop de stimulus van de gemeente gemeten wordt. Bijvoorbeeld: de meting kan worden gestart op het moment dat de gemeente de stimulus initieert op hun (mobiele) apparaat, of de meting kan starten op het moment dat het verzoek van de gemeente op het eindpunt van de dienstleverancier arriveert. Het verschil zit hem in de transporttijd over het netwerk (meestal het internet), waarop de dienstleverancier vaak geen invloed kan uitoefenen (niet zijn verantwoordelijkheid). Evenzo kan het punt waarop de reactie van de dienstleverancier gemeten wordt verschillen.

Responstijd is een belangrijk aspect met betrekking tot de gebruikerservaring van een dienst. Afhankelijk van de dienstverlening kan het zijn dat als responstijden groter zijn dan een afgesproken drempelwaarde, deze worden beschouwd als onaanvaardbaar en dat de dienst effectief gezien onbruikbaar is. Een belangrijk aspect hierbij is dat responstijden kunnen variëren afhankelijk van de aard van het verzoek aan de betreffende dienst die wordt afgenomen.

Een factor die moet worden meegenomen is dat veel diensten verschillende bewerkingen ondersteunen en dat waarschijnlijk de responstijd voor deze verschillende bewerkingen verschillen. Het is daarom noodzakelijk om voor de dienstniveaudoelstellingen met betrekking tot de responstijd duidelijk aan te geven om welke bewerkingen het gaat.

- Schaalbaarheid
  Hier worden de eisen met betrekking tot de schaalbaarheid van het ICT-systeem en –dienst beschreven. Verwachte stijging van het gebruik van de dienst op middellange en lange termijn.

- Capaciteit- en prestatierapportage
  Hier worden de eisen met betrekking tot de inhoud (capaciteit en prestatie) en frequentie (interval) van de rapportage beschreven die door de dienstleverancier worden opgeleverd. Als gemeente dient u zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de afgenomen dienstverlening.

5.3 Continuïteitseisen

Hier worden de continuïteitseisen (beschikbaarheid) met betrekking tot de dienst beschreven. Bijvoorbeeld in het geval van een calamiteit/ramp.

- Hersteltermijn minimale dienstverlening
  Hier wordt de termijn beschreven waarbinnen een verstoorde dienst op een (minimaal) vastgesteld dienstverleningsniveau hersteld dient te zijn. Om dit vast te stellen kan het noodzakelijk zijn dat de gemeente een baselinetoets BIO uitvoert.

- Hersteltermijn normale dienstverlening
  Hier wordt de termijn beschreven waarbinnen een verstoorde dienst op het normale dienstverleningsniveau hersteld dient te zijn. Ook regels opnemen over escalatie (zie ook hoofdstuk 4 Communicatie tussen gemeente en dienstverlener).

5.4 Beveiligingseisen

Het specificeren van meetbare beveiligingsdoelstellingen in SLA’s is nuttig om zowel de zekerheid (assurance) als transparantie te verbeteren. Op hetzelfde moment, zorgt het voor een gemeenschappelijke semantiek om de beveiliging van de dienst vanuit twee invalshoeken te beheren, namelijk (i) het beveiligingsniveau dat wordt aangeboden door een dienstleverancier en, (ii) het door een gemeente gevraagd beveiligingsniveau.

De aanpak die hierbij kan worden gebruikt is het analyseren van de beveiligingsmaatregelen van bekende frameworks (Bijvoorbeeld ISO 27001 of de BIO) in een of meer dienstniveaudoelstellingen. Deze dienstniveaudoelstellingen kunnen zowel kwantitatief als kwalitatief zijn. Deze paragraaf behandelt de dienstniveaudoelstellingen die betrekking hebben op de beveiliging van de dienst. Het aantal beschreven dienstniveaudoelstellingen is zeker niet uitputtend, en hou ook rekening met het feit dat wellicht niet alle doelstellingen van toepassing zijn op alle diensten.

De uitbesteding van ICT-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. Uiteraard is het geen enkel probleem als de uitbesteding tot een andere of een efficiëntere uitvoering van de beveiliging leidt. Beveiliging van systemen, diensten en data zijn hierbij belangrijke aspecten. Deze onderdelen dienen dan ook beschermd te worden tegen zowel interne als externe aanvallen. Zaken waar 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

Betrouwbaarheid van de dienst is de eigenschap van een dienst om zijn functies correct en zonder fouten uit te voeren, meestal over een bepaalde tijdsperiode. Deze categorie is meestal gerelateerd aan de beveiligingsmaatregelen: implementeren bedrijfscontinuïteitsbeheer en disaster recovery in standaarden zoals ISO 27002. Voor deze dienstniveaudoelstelling dient rekening gehouden te worden met de toegestane downtime, die onder andere bestaat uit gepland onderhoud.
Opmerking: Betrouwbaarheid omvat ook de mogelijkheid van de dienst om op een adequate manier om te gaan met storingen en het voorkomen van onbeschikbaarheid van de dienst of het verlies van gegevens in het geval van dergelijke storingen.
De doelstelling met betrekking tot betrouwbaarheid moet worden vermeld, zodat de gemeente kan beoordelen of de specifieke dienst voldoet aan hun zakelijke behoeften. Sommige databeheer dienstniveaudoelstellingen kunnen relevant zijn voor betrouwbaarheid (zie ook paragraaf 5.5).

- Authenticatie & Autorisatie

Authenticatie is de verificatie van de geclaimde identiteit van een entiteit. Bijvoorbeeld de gebruiker van de dienst. Autorisatie is het proces van controleren of een entiteit toestemming heeft voor toegang tot en het gebruik van een bepaalde bron op basis van vooraf gedefinieerde gebruikerprivileges. Authenticatie en autorisatie zijn belangrijke elementen van informatiebeveiliging die van toepassing zijn op het gebruik van diensten. De details met betrekking tot authenticatie en autorisatie dienen duidelijk te worden beschreven door middel van dienstniveaudoelstellingen.

- Cryptografie

Cryptografie is een discipline waarin gegevens worden omgezet teneinde de informatie-inhoud te verbergen, te voorkomen dat deze ongemerkt wordt gewijzigd en / of zonder toestemming wordt gebruikt. Ook bekend onder de term encryptie. Data-encryptie kan in verschillende omstandigheden worden ingezet en er zijn veel encryptiemethoden in gebruik. Deze methoden variëren in hun kracht en verschillen ook in hun kosten - zowel in termen van performance en de benodigde rekenkracht. Het is noodzakelijk om in de SLA bijzonderheden met betrekking tot betreffende encryptiemethoden te vermelden zodat de gemeente een dienst volledig kan beoordelen.

- 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 een dienstleverancier is van groot belang voor de gemeente, omdat een informatiebeveiligingsincident met betrekking tot de dienst ook een informatiebeveiligingsincident is voor de gemeente.

- 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 dienstleverancier.
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. Hiervoor is het noodzakelijk om dienstniveaudoelstellingen met betrekking tot logging en monitoring van de dienst en de bijbehorende mogelijkheden volledig te beschrijven.

- Auditing

Auditing is een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van informatie (bewijsmateriaal) over een dienst en een objectieve evaluatie hiervan om te bepalen in welke mate aan de audit criteria wordt voldaan. De noodzakelijke informatie (bewijs) en de audit criteria worden meestal bepaald door het audit- of certificeringschema die wordt gebruikt om de audit uit te voeren. Audits zijn een middel waarmee de dienstleverancier kan aantonen dat een dienst voldoet aan bepaalde criteria die van belang zijn voor de gemeente op basis van onafhankelijk verkregen bewijs. Audits zijn er op gericht om het vertrouwen in de dienst te verhogen.

- Vulnerability management

Een kwetsbaarheid is een zwakke plek in een 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 dienstleverancier is in veel gevallen de eigenaar van de informatiesystemen die zijn geassocieerd met een dienst met als gevolg dat de gemeente afhankelijk is van de dienstleverancier voor het juiste en tijdige beheer van de kwetsbaarheden voor deze informatiesystemen. De dienstniveaudoelstellingen met betrekking tot vulnerability management dienen hierin transparantie voor de gemeente te bieden.

5.5 Databeheer

Het beheren van gegevens en informatie in het tijdperk van Cloud Computing en uitbesteding heeft gevolgen voor alle organisaties. De databeheer dienstniveaudoelstellingen in dit hoofdstuk worden uitgedrukt in kwantitatieve en kwalitatieve indicatoren die betrekking hebben op de databeheer levenscyclus, en kan worden beschouwd als een aanvulling op de bestaande en van toepassing zijnde beveiliging en gegevensbescherming die wordt aangeboden door de dienstleverancier.

De databeheer dienstniveaudoelstellingen zijn onderverdeeld in vier (4) verschillende categorieën die alle aspecten van de geïdentificeerde data levenscyclus behandelen. Niet alle dienstniveaudoelstellingen zijn relevant voor elke dienst, dit is met name afhankelijk van het type dienst. Voor Cloud geldt dit voor de volgende verschillende typen: IaaS, PaaS of SaaS.

- 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 dienstleverancier zal zowel binnen de verwerkingsorganisatie als voor de afscherming van de applicatie gebruik dienen te maken van afdoende logische toegangsbeveiliging. Als aanvullende eis zou door de gemeente gesteld kunnen worden dat de logische toegangsbeveiliging jaarlijks door een deskundige en onafhankelijke auditor dient te worden 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

- Dataclassificatie
  Dataclassificatie is een beschrijving van gegevensklassen die zijn geassocieerd met de dienst:
  - gemeentelijke gegevens
  - gegevens van de dienstleverancier
  - gegevens afgeleid van de dienst

  Gemeentelijke gegevens is een gegevensklasse die onder de controle is van de gemeente. Gemeentelijke gegevens omvatten gegevens die door de gemeente zijn ingevoerd in de dienst maar ook de resultaten die voortkomen uit het gebruik van de dienst door de gemeente.

- Gegevens mirroring, back-up & restore
  Deze dienstniveaudoelstellingen categorie gaat over de mechanismen die worden gebruikt om te garanderen dat de gemeentelijke gegevens beschikbaar zijn (online of offline). De mechanismen die binnen het toepassingsgebied van deze dienstniveaudoelstelling vallen zijn verdeeld in twee veel gebruikte categorieën (i) data mirroring, (ii) back-up / restore.
  Veel gebruikte beveiligingscertificeringen bevatten specifieke beveiligingsmaatregelen die worden uitgevoerd om gegevensverlies te voorkomen.

  In veel gevallen bevatten deze zelden mogelijkheden die door de gemeente kunnen worden gebruikt om te beoordelen/controleren of de geïmplementeerde beveiligingsmaatregelen daadwerkelijk aan haar eisen voldoen. In het bijzonder met betrekking tot dienstniveaudoelstellingen op de volgende gebieden:
  - De tijdigheid (actualiteit) van de mirroring mechanismen, die wellicht rechtstreeks verband heeft met de geografische ligging van de datacenters van de dienstleverancier.
  - Concrete gegevens in verband met de frequentie en de methode die door de back-up en recovery-mechanismen van de dienstleverancier worden gebruikt.

  Voorgestelde dienstniveaudoelstellingen stellen gemeenten in staat om bijvoorbeeld hun procedures voor risicobeoordeling en bedrijfscontinuïteit bij te stellen.

De dienstniveaudoelstellingen kunnen de gemeente helpen bij het opzetten van Recovery Point Objective (RPO) and Recovery Time Objective (RTO) bij gebruik van de dienst.
Recovery Point Objective is de maximaal toegestane tijd tussen herstelpunten. RPO specificeert niet de hoeveelheid acceptabel gegevensverlies, alleen de acceptabele tijdsperiode. In het bijzonder, RPO beïnvloedt redundantie van gegevens en back-up. Een kleine RPO suggereert mirroring opslag van zowel tijdelijke als permanente gegevens, terwijl bij een grotere tijdsperiode een periodieke back-up benadering mogelijk is. Zoals met RTO, moet de gemeente het aanvaardbare RPO bepalen voor iedere dienst die ze gebruiken en ervoor zorgen dat de dienstleverancier en hun eigen disaster recovery plan (rampenherstelplannen) voldoen aan hun doelstellingen.

Recovery Time Objective is de maximale hoeveelheid tijd dat een bedrijfsproces kan worden verstoord, na een ramp, zonder onaanvaardbare gevolgen voor de bedrijfsvoering. Diensten kunnen kritische componenten zijn voor de bedrijfsprocessen. Gemeenten moeten de RTO bepalen voor elk bedrijfsproces dat afhankelijk is van de dienst en tevens moeten ze bepalen of de disaster recovery plannen (rampenherstelplannen) van de dienstleverancier en hun eigen rampenherstelplan voldoen aan hun doelstellingen.

- Datalevenscyclus
  Het volgende overzicht van dienstniveaudoelstellingen is gerelateerd aan de efficiëntie en effectiviteit van de werkwijze met betrekking tot de datalevenscyclus door dienstleverancier, met een bijzondere aandacht voor de werkwijze en mechanismen voor het verwerken en verwijderen van data. Aan de ene kant, geeft het volgende overzicht van dienstniveaudoelstellingen informatie in verband met de garanties (assurance) en actualiteit in verband met de mechanismen voor het verwijderen van gegevens. Anderzijds, worden ook kwantitatieve dienstniveaudoelstellingen beschreven in verband met de betrouwbaarheid van de dienstverlening met betrekking tot dataopslag (het ophalen/-vragen en de duurzaamheid van de opgeslagen gegevens). Verder kan het van belang zijn voor de gemeente dat deze in staat is om gegevens op te halen/vragen nadat een verwijder verzoek is ingediend. Hiervoor dienen dan ook dienstniveaudoelstellingen voor worden vastgelegd.

- Gegevensoverdraagbaarheid (dataportabiliteit)
  Het volgende overzicht met dienstniveaudoelstellingen is gerelateerd met de mogelijkheden van de dienstleverancier om gegevens te exporteren, zodat deze gegevens nog steeds door de gemeente kunnen worden gebruikt bijvoorbeeld in het geval van contractbeëindiging. Vaak richten de beveiligingsmaatregelen zich bij dataportabiliteit op het van toepassing zijnde beleid van de dienstleverancier, waardoor het moeilijk (en soms onmogelijk) is voor de gemeente om de specifieke indicatoren in verband met de beschikbare formaten, interfaces en overdrachtsnelheden te achterhalen.

5.6 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).

- 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.

- 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 eigenbelang), kwalificeert zich als een verantwoordelijke voor de gegevensverwerking in eigenbelang 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.

- 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.

Het contract tussen de gemeente en de dienstleverancier moet duidelijke bepalingen voor het wissen van persoonsgegevens bevatten. Aangezien (persoons)gegevens redundant op verschillende servers op verschillende locaties bewaard kunnen worden, moet men zeker zijn dat elk exemplaar daarvan onherroepelijk wordt gewist. Bijvoorbeeld eerdere versies, tijdelijke bestanden, et cetera.

- 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.

- 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.

  De verwerking van bepaalde bijzondere gegevenscategorieën kan de naleving van specifieke wettelijke bepalingen eisen, die niet worden gedekt door algemene normen of certificeringen. Daarom moet duidelijk binnen de SLA worden bepaald voor welke bijzondere gegevenscategorieën de dienst geschikt is.

- 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 de desbetreffende paragraaf 5.4.5 van deze SLA.
  Bovendien dienen dienstleveranciers 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.

- 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.

- 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.

5.7 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, die niet overschreden mag worden. De KPI’s moeten toetsbaar zijn, dat wil zeggen dat ze aan een aantal eisen moeten voldoen, zoals:

- Validiteit: De prestatie-indicator moet een maat zijn voor de prestatie(eis) waarin inzicht nodig is.
- Geldigheid: De prestatie-indicator moet toepasbaar zijn in de situatie waarin deze toegepast wordt.
- Eenduidigheid: De prestatie-indicator moet slechts op één manier geïnterpreteerd kunnen worden.
- Meetbaarheid: De meetwaarden van de prestatie-indicator moeten kwantitatief te bepalen zijn (er moet een meetschaal voor de indicator zijn).
- Vergelijkbaarheid: De meetwaarden van dezelfde prestatie-indicator in verschillende situaties moeten vergelijkbaar zijn. Uiteindelijk dient er voor iedere prestatie-indicator een norm bepaald te worden, oftewel een waarde die niet overschreden mag worden. Een norm kan een minimum zijn (bijvoorbeeld voor beschikbaarheid), of een maximum (bijvoorbeeld voor vertraging).

6 Taken en verantwoordelijkheden

Uitbesteden van ICT-processen leidt slechts tot een overdracht van taken en verantwoordelijkheden. De eindverantwoordelijkheid voor de ICT-processen, inclusief de beveiligingsaspecten, kan niet worden overgedragen. Ook de ICT-processen die zijn uitbesteed, blijven verbonden met de gemeente. De kwaliteit van het uitbestede 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 ICT-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 ICT-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 ICT-proces aan verschillende dienstleveranciers heeft uitbesteed, is een vorm van Service Level Management noodzakelijk.

6.1 Plichten van de dienstverlener

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

- 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.

- 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 dienstleverancier, maar de gemeente heeft hierop een aanzienlijke invloed.

6.2 Plichten van de gemeente

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

6.3 Verantwoordelijkheden gebruikers

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

6.4 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.

6.5 Addendum informatiebeveiligingsdienst voor gemeenten

Bij voorkeur heeft de dienstverlener met de IBD afspraken gemaakt over de verantwoordelijkheden met betrekking tot informatieveiligheid in het addendum Informatiebeveiligingsdienst voor gemeenten behorend bij het VNG Realisatie convenant.[5] Hier wordt aangegeven of de dienstverlener dit IBD-addendum heeft ondertekend of niet middels een ja of nee.

6.6 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.

6.7 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.

7 Kosten

7.1 Kosten dienstverlening

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

- Prijzen

De hoogte van de vergoeding die betaald moet worden dient te worden vastgelegd, inclusief grenzen aan stijgingen. Hierdoor krijgt de gemeente zekerheid met betrekking tot de jaarlijkse kosten.

- Betalingsvoorwaarden

Afspraken aangaande betaling van overeengekomen vergoedingen dienen te worden vastgelegd om onduidelijkheden en/of problemen hieromtrent te voorkomen.

7.2 Sancties, bonussen

Hier worden de regels voor sancties, bonussen met betrekking tot de dienstverlening beschreven.

8 Verklarende woordenlijst

Optioneel: In de verklarende woordenlijst wordt een uitleg gegeven van de belangrijkste begrippen die van toepassing zijn binnen de context van alle documenten behorende tot deze SLA.

8.1 Definities

8.2 Afkortingen

5 https://www.informatiebeveiligingsdienst.nl/product/addendum-informatiebeveiligingsdienst-voor-gemeenten-ibd-addendum/

9 Bijlagen

Denk aan andere SLA's, rapportageformat, contracten, beveiligingseisen et cetera.

1. Rapportage templates
    a. Contractmanagement (SLA wijzigingen)
    b. Opdrachtmanagement (dienstenniveaus op maand basis)
    c. Service-/helpdesk: openstaande en afgehandelde incidenten, status openstaande incidenten, overschrijdingen.
    d. Template voor wijzigingsverzoeken
2. Document Afspraken en procedures (DAP)
3. Onderhoudsdocumentatie
4. Beveiligingseisen uit de BIO
5. Woordenlijst/begrippenlijst

Bijlage 3: Literatuur/bronnen

Voor deze publicatie is gebruik gemaakt van onderstaande bronnen:

Titel: diverse artikelen (waaronder Inrichtingsmodel IT-beheer en Checklist Service Level Agreement SLA)
Wie: Wiebe Zijlstra
Uitgeverij: ZBC kennisbank
Link: https://zbc.nu/

Titel: Beveiliging en Service Level Agreements
Wie: diverse auteurs (Platform voor Informatiebeveiliging (PvIB))
Uitgeverij: Ten Hagen en Stam
Datum: 2001
ISBN-10: 90-440-0223-6 (niet meer leverbaar)

Titel: Cloud SLA de best practices van cloud service level agreements
Wie: Bart de Best & Pascal Huijbers
Uitgeverij: Leonon Media
Datum: 2014
ISBN-10: 90-71501-73-9
ISBN-13: 978-90-71501-73-9

In juni 2014 heeft de Cloud Select Industry Group - subgroep Service Level Agreement (C-SIG-SLA) van de Europese Commissie een SLA richtlijn gepubliceerd.6 Deze SLA richtlijn voor clouddiensten dient ook als input voor de cloud SLA standaarden die door de Internationale Organisatie voor Standaardisatie (ISO) op dit moment worden ontwikkeld.
Het gaat hierbij om een drietal standaarden, namelijk:

- ISO/IEC 19086-1 - Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 1: Overview and concepts
- ISO/IEC 19086-2 - Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 2: Metrics
- ISO/IEC 19086-3 - Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 3: Core requirements

6 https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie