



Bijlage ICT randvoorwaarden bij aanbestedingen

Omschrijving van de huidige technische infrastructuur gebruikt door de gemeenten Gouda, Waddinxveen en Zuidplas en de eisen die worden gesteld voor het in gebruik nemen van een nieuwe applicatie.

Deze aanbesteding is alleen ten behoeve van gemeente Waddinxveen

Inhoudsopgave

1.	Voorwaarden systeemomgeving	4
1.1	Algemeen	4
1.2	Netwerk	6
1.3	RDBMS	6
1.4	Servers, storage en backup	6
1.5	Werkplek	7
1.6	Internet	7
1.7	Web applicaties	8
1.8	Applicatiesoftware	8
1.9	Kantoorautomatisering	8
1.10	Dataopslag	9
1.11	Backup	9
1.12	Virtualisatie	9
1.13	Beveiliging	9
1.14	Monitoring	10
2.	Extra voorwaarden levering als SaaS.....	11

Versiehistorie

versienr	datum	auteur	Status
versie 1	21-06-2011	Sjaak	gekopieerd uit beschrijving techn. Infrastructuur, bijwerken nodig
Versie 2	14-11-2012	Ingmar	Bijgewerkt, ter revisie rondgestuurd.
Versie 3	19-11-2012	Jaap	Bijgewerkt, ter revisie rondgestuurd.
Versie 4	19-02-2013	Ingmar	Bijgewerkt, niet rondgestuurd
Versie 5	24-06-2013	Ingmar	Bijgewerkt, ter controle naar unix-dba en windows-citrix gemaild.
Versie 6	12-09-2013	Ingmar	Bijgewerkt nav divers commentaar.
Versie 7	05-03-2014	Ingmar	Bijgewerkt met cloud beleid
Versie 8	01-04-2014	Jaap	Bijgewerkt met storage paragraaf
Versie 9	01-06-2014	Ingmar	Onderwerp Oracle bijgewerkt
Versie10	02-06-2014	Robert	Onderwerp fat clients + XP verwijderd en Oracle aangepast
Versie11	31-10-2014	Velen	Bijgewerkt naar actuele situatie
Versie 12	25-11-2016	Velen	Bijgewerkt naar actuele situatie
Versie 13	18-01-2017	Velen	Gemeenten Zuidplas en Waddinxveen ingevoegd
Versie 14	22-03-2017	Sjaak	1 ^e 2 paragrafen samengevoegd en aangepast, SaaS-voorwaarden als aparte paragraaf toegevoegd
Versie 15	27-03-2017	Velen	Halfjaarlijkse check door collega's
Versie 16	7-12-2017	Annemieke	Halfjaarlijkse check door collega's
Versie 17	19-12-2018	Annemieke	Bijgewerkt naar actuele situatie (nav input collega's)
Versie 18	16-01-2019	Annemieke	Opmerkingen Ingmar verwerkt
Versie 19	06-11-2019	Velen	Halfjaarlijkse check door collega's, Nagios toegevoegd
Versie 20	11-12-2019	Annemieke	Redudante internetverbinding, user authentication, user provisioning en MobileDeviceManagement toegevoegd

1. Voorwaarden systeemomgeving

1.1 Algemeen

De volgende indeling van soorten applicaties / systemen wordt gebruikt:

- Web-based
- Windows Client-server.
- Stand-alone: op een lokale PC of server. Installatie op afstand (rdp, vnc) moet mogelijk zijn
- Installatie van data en programmatuur op storage (inclusief installatie onder AppV, Citrix XenDesktop, Citrix XenApp).
- Apps ontsloten door Microsoft Intune
- Apps ontsloten door Tools4Ever HelloID
- Applicaties zijn bij voorkeur web-enabled
- Applicaties zijn Citrix XenApp-enabled.

Applicaties zullen in het technische kader moeten passen. Met name de centrale installatie op de storage en het voldoen aan de standaard gebruikte (besturings)software op serverplatforms en de clients.

We verwachten een duidelijke en inzichtelijke documentatie voor gebruikers, het applicatiebeheer en het systeembeheer. Hetzelfde geldt voor de mogelijke foutboodschappen, voor zover deze betrekking hebben op het besturingssysteem of RDBMS.

Er dient een duidelijke scheiding te zijn in systeembeheer en applicatiebeheer. Systeembeheer draagt zorg voor het uitvoeren van updates en heeft hiervoor de benodigde rechten. Applicatiebeheer draagt zorg voor contact met de leveranciers, het coördineren van updates/upgrades en het oplossen van functionele vragen van gebruikers.

De door de leverancier aan te bieden applicatie en eventuele hardware dient aan te sluiten op de binnen de gemeenten Gouda, Waddinxveen en Zuidplas geldende standaarden ten aanzien van de ICT-infrastructuur. In onderstaand overzicht zijn de vigerende ICT-standaarden weergegeven en daar waar van toepassing en nu reeds bekend welke standaarden zijn gepland. Gemeente Gouda host in twee eigen datacenters de ICT-infrastructuur van de drie gemeenten. Indien de cellen zijn samengevoegd, is het omschreven van toepassing op alle drie de gemeenten.

Tenzij expliciet anders vermeld, hanteren de gemeenten de open standaarden uit de lijsten van het Forum Standaardisatie.

gemeente Gouda		Waddinxveen	Zuidplas
Centrale hardware/software	Citrix XenApp 7 op Xenserver 7		
	Citrix Xendesktop 7 op Xenserver 7		
	Intel based hardware		
	Windows server 2012R2, Windows server 2016R2 en Windows server 2019.		
	Alle XenApp servers draaien op Windows Server 2016R2.		Xenapp servers op Windows server 2008R2, uiterlijk Q1 2020: 2016R2.
	Linux CentOS 7.x		
	VMware ESXi 6.7		
Decentrale hardware	Dell Wyse 3040 thin client with ThinOS BTX	Dell 5012-D10D thin client with ThinOS	Dell Wyse 3040 thin client with ThinOS BTX
	Ricoh MP C5503 printers/multifunctionals (copy, print, scan, fax)		
Netwerk	TCP/IP (LAN), NFS/iSCSI (storage). Cisco		
RDBMS	Oracle 12.2.0.1 (=Oracle 12cR2) (op x64 Oracle Linux 6 op Oracle VM) zowel als single database als met de single tenant architectuur standaard Oracle home onder Standard Edition Two met bijbehorende functionaliteit, opties mogelijk : Oracle Intermedia, Oracle XML DB, Oracle JVM, Oracle APEX, MD/locator. Oracle 12.1.0.2 (=Oracle 12cR1) als single database In 2020: overgang van Oracle Linux 6 naar Oracle linux 7		
	SQL 2014 op een cluster		
Kantoorautomatisering	Microsoft Office 2016 ProfessionalPlus 2016 (on-premise) docx als standaard formaat.		
Oracle client	Oracle 12 (64 of 32 bits)		
Middleware	Oracle Web Logic Suite met Forms 12 Oracle APEX (op Linux) Oracle Grid Control 13G		
Mail	Exchange 2013, Outlook 2013		
Internet	Cisco FTD firewall/IPS, Sophos Endpoint, Cisco Ironport Mail	Cisco FTD firewall/IPS, Sophos Endpoint, Cisco Ironport Mail	Cisco FTD firewall/IPS, Sophos Endpoint, KPN mail
Identity management Access management	Tools4Ever IAM Tools4Ever HelloID		
Mobile Device Management	Smartphones interne medewerkers: Microsoft Intune Chromebooks: Google G-Suite		

1.2 Netwerk

Datacommunicatie binnen de gemeenten is gebaseerd op de facto industriestandaards. Verschillende vestigingen van de gemeente zijn middels glasvezel met elkaar verbonden, waarover datacommunicatie plaats vindt via het Ethernet protocol. Er is sprake van een geswitched en gerouteerd netwerk (ISO laag 2 en 3). De interne gebouwbekabeling UTP cat6a, de bekabeling van outlet naar werkplek op basis van UTP cat5E.

De ICT-omgeving wordt gehost vanuit twee datacenters op twee verschillende locaties. Volgens de constructie active-active. Deze twee locaties zijn via redundante glasvezels op laag 2 verbonden met een snelheid van 30Gbit (lan) en 8 Gbit (storage). De Storage, Oracle, UCS omgeving zijn dubbel uitgevoerd per locatie. Iedere locatie is met een aantal aanpassingen in staat autonoom te draaien.

1.3 RDBMS

Oracle 12cR2 op Oracle VM is de database-standaard. Voor de architectuur van Oracle wordt een aangepaste OFA-standaard gehanteerd. Een uitgangspunt is verder dat alle productie-applicaties 1 op 1 gekopieerd worden naar de test-omgeving, daarbij gebruik makend van exact dezelfde instance-benamingen. De kopieslag gebeurt door het maken van snapshots, c.q. flexcloning. De databases worden in een metrocluster (gespiegelde opslag) via NFS gekoppeld. Vanwege een uniforme structuur zijn deze (qua back-end) makkelijk te migreren naar een andere server. Voor het platform wordt gebruik gemaakt van virtuele Oracle Linux-servers (virtualisatiesoftware: Oracle VM). Deze zijn op hun beurt makkelijk onderling 'verschuifbaar' naar een ander fysiek platform. Door het gebruik van NFS, OracleVM en een uniforme structuur tussen de OTP-straten en op het filesysteem/volumes wordt een grote mate van flexibiliteit in uitwijkmogelijkheden bereikt. De uitrol van nieuwe databases verloopt via een uniforme procedure en kan eenvoudig aan het beheersgrid (Oracle grid control) en backup-mechanisme worden toegevoegd. Als uitgangspunt voor nieuwe systemen/applicaties wordt daarom ook Oracle12cR2 gehanteerd. Oracle 12c databases worden bij voorkeur volgens de Oracle singletenant configuratie geïmplementeerd.

Naast Oracle 11g/12c is Microsoft SQL Server 2014 als database software in gebruik voor enkele specifieke toepassingen. Het inzetten van Postgress als RDBMS is onderzocht maar wordt niet ondersteund.

1.4 Servers, storage en backup

Voor alle onderdelen van de infrastructuur geldt dat deze zo veel mogelijk gescheiden worden neergezet per functionaliteit. Zo als hierboven beschreven wordt de database in een aparte omgeving neergezet. De applicatieservices, en printservices worden beschikbaar gesteld via virtuele servers die opereren onder VMware ESXi 6.7. Afhankelijk van de applicatie kan een virtuele server worden uitgerust met o.a. Windows server 2016. Uitrol gebeurt via een standaard procedure. De meeste virtuele servers beschikken over een productie- en testvariant. In principe geldt dat voor 1 applicatie een aparte virtuele omgeving wordt ingericht. Deze zijn eenvoudig te klonen. Een backup van deze virtuele servers gebeurt in principe via een volledige totaal-backup (Commvault). Het beheer van een dergelijke applicatieserver worden gedelegeerd aan de applicatiebeheerder.

Fileservices worden via het CIFS protocol aangeboden door de dubbel uitgevoerde Netapp filers. Voor toepassingen dient rekening te worden gehouden met deze software en plugins. Backup van deze filers gebeurt d.m.v. Commvault. Er worden vier maal per dag snapshots gemaakt zodat bestanden door de gebruiker tot enkele dagen terug zelf zijn te herstellen naar een vorige versie. Het restoren vanaf backup/tape is daarmee beperkt tot uitzonderingsgevallen.

De hardware onderliggend aan de VMware en de Citrix omgeving is Cisco UCS op basis van Intel based servers. Deze servers zijn via een 40Gbit connectiviteit in de infrastructuur opgenomen.

1.5 Werkplek

Een standaard werkplek bestaat uit een thin client van het merk Dell (voorheen Wyse). Op deze Dell thin client wordt met behulp van Citrix XenApp een desktop aangeboden. Een aantal gebruikers hebben naast Citrix XenApp ook nog Citrix XenDesktop tot hun beschikking. XenDesktop dient vooral voor het aanbieden van een desktop met grafisch zware applicaties. Alle werkplekken hebben toegang tot internet.

Er zijn een aantal manieren om applicatiesoftware te installeren:

- Netwerkschijf
- Applicatieserver
- Centrale Citrix image XenApp 7.15 (vDisk) tbv de algemene desktop voor iedereen
- Centrale Citrix image XenDesktop 7.6 (vDisk) tbv de grafische zware (CAD) applicaties

Bovenstaande lijst is gerangschikt van wenselijk naar onwenselijk. Met behulp van de RES Workspace manager wordt een gepersonaliseerde desktop aan gebruikers aangeboden. Er moet bij de planning van een nieuwe toepassing daarom rekening worden gehouden met benodigde tijd voor installatie van de software, het inleren van RES en het uitvoeren van een testtraject in samenwerking met systeem- en applicatiebeheer.

Een standaard werkplek bezit de volgende eigenschappen:

Eigenschap	Instelling
Desktop resolutie	1920*1080 of 1920*1200
Platform	Windows server 2016
Java	8
Kantoorautomatisering	Zie paragraaf 1.9
Monitor	standaard 1 per werkplek, helft van de werkplekken 2
PDF reader	Adobe Acrobat reader DC (2017.009)
Browser	Internet Explorer 11, Firefox, Chrome
Plugins	Java, Flash en .NET zijn beschikbaar

1.6 Internet

De internet verbinding gaat via een firewall (Cisco FTD2100) en dan, afhankelijk van de route, naar Gemnet of internet.

De internet verbinding is een glas verbinding via JNET (medio 2020 wordt de internetverbinding redundant via eGem uitgevoerd), 200 Mbit synchroon Gouda, 100 Mbit voor Waddinxveen en 100 Mbit voor Zuidplas. De Firewalls gebruiken ook IP/URL filters en IPS functionaliteit.

Voor externe mailtoegang is er een OWA/Activesync in de DMZ (deze wordt uitgefaseerd). Via een secure https verbinding is het mogelijk mail en agenda te raadplegen. Daarnaast hebben de gemeenten de mogelijkheid tot "thuiswerken" via een Citrix portal waar zowel een XenApp sessie als een XenDesktop sessie gestart kan worden.

Voor extern <-> intern berichtenverkeer wordt OpenTunnel van Jnet gebruikt als gateway en digikoppelingsadapter.

Met leveranciers waarmee over veel poorten of op veel adressen gecommuniceerd moet worden, of waarbij de beveiliging niet via SSL ingeregeld kan worden, kan er een VPN tunnel worden gemaakt. Maar dit is alleen als de gemeente Gouda hier het voordeel van ziet. De mail gaat via ironport spamfilters in DMZ, voorzien van SPF, DKIM, DMARC en TLS.

1.7 Web applicaties

Interne web applicaties draaien hetzij op internet information server (IIS) versie 7.0 van Microsoft of Apache Tomcat op Windows server 2016 of Linux (Cent-OS).

Oracle WebLogic Suite is in gebruik als webapplicatie server voor Oracle Forms applicaties. Oracle technologie heeft Oracle Linux op Oracle VM als standaardplatform.

1.8 Applicatiesoftware

Applicatiesoftware wordt op file- en applicatieservers gescheiden naar toepassing. Services, batches en draaiende programmatuur draaien op de applicatieserver, alsmede ook html- en xml-bestanden draaiend op een web-server. Voor de file-based bestanden kunnen deze terecht komen op een Oracle Server of filer die mbv het CIFS protocol wordt gemount op een Windows-desktop.

De rechten op de bovengenoemde shares, mappen en bestanden hierbinnen zijn geregeld via de applicatie- en afdelingsgroepen van Windows 2012R2 Active Directory.

LET OP: het maximale aantal tekens van mappen op de Windows-omgeving mag 255 tekens zijn en inclusief document-benaming 260 tekens.

Applicaties die gebruik maken van extreem lange mapstructuren of documentbenamingen worden daarom niet ondersteund.

Versiebeheer

Versiebeheer is in principe een verantwoordelijkheid van de applicatiebeheerder. In het geval van grotere applicaties worden nieuwe ontwikkelingen, aanpassingen, updates en fixes altijd getest in een (identieke) testomgeving. Pas na toestemming en goedkeuring van de applicatiebeheerder wordt software in de productieomgeving geplaatst. De applicatiebeheerder dient bij de installatie op de productieomgeving aanwezig te zijn. Tijden gaan in overleg. Systeembeheer verricht technische ondersteuning bij de uitvoering van updates op het gebied van datamanagement of aanpassingen in de database en verricht controle op de handhaving van het OTAP-principe. Aanpassingen ten gevolge van nieuw ontwikkelde koppelingen of maatwerptoeepassingen dienen zoveel mogelijk in een aparte ontwikkelomgeving te geschieden. Voor gewennings- of opleidingstoepassingen is het mogelijk een opleidingsomgeving te gebruiken.

1.9 Kantoorautomatisering

De gestandaardiseerde kantoorautomatiseringomgeving maakt gebruik van Microsoft Office ProfessionalPlus 2016 on-premise. Koppelingen van de applicatie met de kantoorautomatiseringomgeving moet derhalve via genoemde suite plaats vinden. Het ODF wordt via Office ondersteund.

Als mailserver wordt Exchange 2013 gebruikt. Het email berichtenverkeer vanuit de applicatie moet via deze server worden afgehandeld. Het van buitenaf komende emailverkeer wordt gescand op bijlagen en virussen. Alleen Office en pdf documenten worden doorgelaten. In 2020 wordt een migratie naar een hogere versie onderzocht.

Standaard kunnen gebruikers downloaden. Het downloaden van executables is niet mogelijk. Alleen bepaalde applicatiebeheerders hebben de mogelijkheid om alles te downloaden bijvoorbeeld tbv. updates, release documentatie en dergelijke. Uitvoeren van vreemde executables is standaard onmogelijk op de werkplek. Pas na goedkeuring (whitelisting) door systeembeheer kan een nieuwe executable uitgevoerd worden.

1.10 Dataopslag

De dataopslag gebeurt op een NetApp omgeving, bestaande uit een metrocluster met 2 nodes. De nodes zijn verdeeld over 2 locaties. Beide nodes zijn in staat om de resources van de andere over te nemen om in geval van uitwijk op 1 locatie te kunnen werken. Elke node bestaat uit een FAS8040 met een aantal diskshelvs en zijn middels fiberswitches met elkaar verbonden.

De dataopslag wordt gebruikt voor kantoordata (CIFS), VMware (NFS), UNIX (iSCSI), Oracle (NFS) en diverse andere databases zoals MSSQL. In totaal omvat de dataopslag zo'n 80Tb. Het opslagsysteem is voorzien van een multistore licentie voor dataopslag van meerdere organisaties.

Voor Exchange is een andere opslagsysteem in gebruik. Op elke voorgenoemde locatie staat een AFF200. De hoeveelheid data op deze filers is ca 30Tb.

Om de datagroei nog enigszins te beperken wordt gebruik gemaakt van thin-provisioning en deduplicatie. Ten behoeve van het opbouwen van een test- en/of ontwikkelomgeving wordt er gebruik van gemaakt van flexclone technologie. Daarnaast gebruiken we snapshot technologie voor het snel kunnen maken van backups. Zo'n backup wordt eventueel met behulp van snapvault overgebracht naar een backupfiler (FAS2240).

1.11 Backup

Voor centrale backups wordt gebruik gemaakt van een SAN-systeem. Commvault is de software die hiervoor wordt gebruikt. De aan te bieden hard- en software moet hierop aan sluiten. Het SAN maakt geen deel uit van het servernetwerk, op dit moment worden backups via switches naar de tape-robot getransporteerd. Dagelijks worden incremental backups gemaakt van alle centrale systemen. Alle voor productie ingezette servers worden meegenomen in de dagelijks backup. Wekelijks vindt een full-backup plaats. Als middel om de backups te kunnen streamen wordt gebruik gemaakt van staging (disk-2-disk-principe). Backups worden (afhankelijk van de behoefte direct of later naar tape weggeschreven. Aan het einde van de maand wordt de data van de backupfiler naar tape weggeschreven.

Daarnaast worden van alle bedrijfskritische systemen dmv Oracle archive logging online mutaties bewaard. De maximale verlies-tijd van database transacties wordt daarmee theoretisch beperkt tot 10 minuten.

Voor deze backup wordt gebruik gemaakt van een NetApp filer FAS2240 met in totaal zo'n 124Tb aan opslag

Het NAS-systeem op de filer maakt online-snapshots mogelijk. Van alle CIFS volumes wordt dan ook 4 per dag een snapshot gemaakt. Ook voor LUN of NFS-gebaseerde opslag is het mogelijk op relatief snelle wijze een kloon of snapshot te maken.

1.12 Virtualisatie

Applicatieservers worden gevirtualiseerd op een VMware-omgeving. De VMware hosts maken gebruik van meerdere gezamenlijk datastores op het NAS. Door deze configuratie is een High Availability omgeving gecreëerd waarin de ene VMware host de virtuele machines van de andere host over kan nemen. De VMware hosts zijn voorzien van VMware Infrastructure 6.7 (ESXi 6.7) en staan fysiek gescheiden over twee locaties. De locaties zijn door middel van glas aan elkaar gekoppeld.

De Oracle databases worden gevirtualiseerd op een Oracle VM omgeving, waarbij virtuele VM's zijn toegewezen aan de diverse gemeentes die worden gehost.

1.13 Beveiliging

Functionele organisatie

Functies zijn gesplitst in gebruikers, applicatiebeheerders en systeembeheerders.

Systeem- en databasebeheer zorgt voor het uitvoeren van updates in samenspraak met de applicatiebeheerder en de leverancier.

Applicatiebeheer zorgt voor alle zaken binnen de applicatie (toekennen van menu's, privileges etc.) In deze volgorde worden de rechten op de systemen geregeld.

De gebruiker heeft geen mogelijkheden om op de centrale servers (Windows en Unix) andere dingen te doen dan alleen het opstarten van applicaties of het wegschrijven van data of bestanden. De applicatiebeheerder heeft een aantal extra mogelijkheden. In principe kan niemand anders dan de systeembeheerders op de Windows servers en/of Unix-prompt wezenlijke wijzigingen aanbrengen.

Systeembeheer heeft de volledige rechten op alle systeem- en applicatie-software. Een aparte rol is weggelegd voor de leverancier die voor aparte doeleinden remote kan inloggen op het systeem. Dit gebeurt via een Citrix XenApp-portal. De leverancier moet een account hebben op het netwerk met een aan het account administratief gekoppeld 06 nummer om SMS te ontvangen.

Technische organisatie

Van buitenaf is het netwerk beschermd door een firewall. Hiermee is toegang tot en van het Internet geregeld. Koppelingen met landelijke voorzieningen, ketenpartners en leveranciers gaan encrypted en/of via Gemnet. Tevens wordt voor sommige functionaliteiten zoals de portal (via 2FA) en webmail de Netscaler voor hardening gebruikt.

Het downloaden door gebruikers vanaf internet is beperkt tot documenten. Alle binnenkomende bestanden worden gescand. Alleen Office en Acrobat Reader bestanden worden via de mail als bijlagen doorgelaten. Alle bijzondere bestanden worden gescand en worden alleen op verzoek van de gebruiker en na goedkeuring van de postmaster doorgezonden. Als het niet mogelijk is om een bijzonder bestand te scannen, wordt het bestand in quarantaine geplaatst en wordt de verantwoordelijkheid bij de eindgebruiker gelegd.

Voor het beschikbaar houden van de technische infrastructuur zijn maatregelen getroffen voor continuïteit en/of beheerste shutdown.

De gemeente heeft grote delen van de technische infrastructuur dubbel uitgevoerd en een eigen uitwijk ingericht. Deze uitwijk kan voor een groot deel in werking treden binnen één uur. Alleen herstel van externe verbindingen duurt langer.

Om de mobiele apparatuur goed te kunnen beveiligen, maken de gemeenten gebruik van G-Suite voor het beheren van de persoonsgebonden chromebooks en Intune voor de smartphones van de vaste medewerkers. Zowel on-premise als cloud applicaties zijn, met behulp van HelloID van Tools4Ever, met de on-premise infrastructuur gekoppeld, waarbij bijvoorbeeld het SAML of het OpenID protocol wordt gebruikt. HelloID van Tools4Ever wordt zowel gebruikt als Identity- en Accessmanagement als Access Governance als Service automation.

1.14 Monitoring

De ICT-infrastructuur wordt pro-actief gemonitord met behulp van Nagios. Naast servers en koppelingen, worden onderdelen van applicaties zoveel mogelijk in de monitoring opgenomen.

2. Extra voorwaarden levering als SaaS

Een SaaS-oplossing moet aan onderstaande voorwaarden voldoen:

- Er is de garantie dat data binnen de grenzen van de Europese Economische Ruimte (EER) wordt opgeslagen (zowel primaire opslag als eventuele back-ups en uitwijklocaties) zodat ze onder de Europese wetgeving valt;
- De gemeente moet ten allen tijd kunnen beschikken over (al) onze eigen informatie;
- Afspraken moeten worden vastgelegd in een contract, een SLA en (bij persoonsgegevens) een verwerkersovereenkomst. Vervolgens dienen deze afspraken te worden gemonitord door jaarlijkse audits.
- Er moet een exit-strategie zijn vastgelegd.

In het contract dient aandacht te zijn voor de volgende zaken:

- Specifieke beveiligingsmaatregelen afkomstig uit een risicoanalyse (inclusief een dataclassificatie) of de BIO
- De data blijft (in zoverre niet openbaar) te alle tijde eigendom van de gemeente en mag niet door de aanbieder dan wel door derden worden gebruikt
- Het voldoen aan wettelijk vastgestelde bewaartermijnen inclusief vernietiging na een bepaalde termijn (achieveving en vernietiging van gegevens, inclusief persoonsgegevens).
- Het verplicht melden van datalekken en andere beveiligingsincidenten aan de gemeente binnen een redelijke termijn
- Looptijd van het contract
- Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven
- Software licenties (van wie zijn deze en mogen deze in een Cloud worden gebruikt)
- Conversie van gegevens
- Overdracht van gegevens van- en naar de Cloud-omgeving
- Vernietiging van gegevens bij contract beëindiging
- Continuïteit van het systeem: Er zijn continuïteitsplannen voor het herstel van incidenten, zoals aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven
- Overdracht naar een andere leverancier
- Back-up, in- of uitwijk voorzieningen
- Locatie gegevens en programmatuur
- Geheimhoudingsovereenkomst
- Encryptie, versleutelen van gegevens: bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiervoor de relevante artikelen uit de BIO.
- Het gebruik maken van multi factor authenticatie
- Onderaanneming en overdracht van rechten en plichten (of geen onderaanneming toestaan)
- Opschortingsrecht
- Naleving wet- en regelgeving
- Logging gegevens kunnen opvragen en inzien
- Het recht om audits te mogen (laten) uitvoeren over alle afspraken
- Welk recht van toepassing is
- Exit regels: wat als de gemeente wil stoppen met de SaaS-applicatie of de gegevens/diensten wilt migreren naar een andere provider?

In een Service Level Agreement (SLA) worden beheerafspraken vastgelegd. De SLA maakt onderdeel uit van het contract.

Er wordt een verwerkersovereenkomst opgesteld als er sprake is van het verwerken van persoonsgegevens. Hierin worden alle rechten en plichten van de leverancier en gemeente vastgelegd.