Beleidskader Cloud-applicaties

BELEIDSKADER VOOR GEBRUIK VAN CLOUD-APPLICATIES (SAAS-DIENSTEN)

Auteur: Arie Elsenaar, Dienst ICT
Versie 1.0
Vastgesteld door de directeur ICT op 21 januari 2020

1. Samenvatting

Applicatiegebruik vanuit de Cloud, oftewel Software as a Service (SaaS) wordt in toenemende mate door Amsterdam UMC ingezet. Soms valt de keuze op SaaS vanwege bijvoorbeeld schaalbaarheid of kostenefficiency, soms ook omdat de gewenste leverancier alleen de SaaS-vorm biedt.
SaaS-diensten zijn onderdeel van de totale informatievoorziening van Amsterdam UMC, geleverd door derden en fysiek geplaatst buiten de grenzen van de organisatie. Dit stelt eisen aan de wijze waarop die diensten ingericht en geleverd worden en daarvoor zijn er regels en voorschriften aan verbonden.

Die regels betreffen allereerst de veiligheid. De data en de verwerking ervan dienen te voldoen aan de eisen die wet- en regelgeving daaraan stellen. Daarbij gaat het o.a. om privacy (AVG), security (NEN7510), en bij zorginformatie patiëntveiligheid (JCI, MDR/IVDR). Uitvoeren van de BIV-classificatie en aansluitend een DPIA (Data Protection Impact Analysis) vormen daarvoor de start. De Dienst ICT ondersteunt bij de technische aspecten daarvan; de functionaris gegevensbescherming (FG) bewaakt de juridische kant. Het intellectueel eigendom van de data berust bij Amsterdam UMC en de leverancier mag geen rechten op gebruik ervan claimen, zoals dat in de wereld van de sociale media, maar ook bij veel publieke Cloud-applicaties gebruikelijk is.

Naast beveiliging en privacy dient ook de continuïteit van de informatievoorziening geregeld te zijn. Dit gaat niet alleen om de beschikbaarheid (tot 24/7, afhankelijk van de aard van de applicatie), maar ook om het doorvoeren van changes. Om dat in goede banen te leiden zijn contractuele afspraken met de leverancier nodig over technische en functionele afstemming van changes.
Dit geldt vooral wanneer er sprake is van koppelingen met andere onderdelen van de informatievoorziening van Amsterdam UMC. Dan kunnen namelijk ook wijzigingen van de gekoppelde systemen impact hebben op de continuïteit van de cloudapplicatie en zijn goede afspraken tussen de partijen essentieel. De Dienst ICT brengt bij de contractvoorbereiding deze afhankelijkheden in kaart en vertaalt dat in goede contractuele afspraken.

Soms laten de leveranciers de hosting en de netwerkafhandeling door andere partijen doen. In dat geval zijn bovenstaande punten van toepassing op alle betrokken partijen, waarbij extra aandacht aan de onderlinge afhankelijkheden nodig is.

Het gebruik van een cloudapplicatie levert altijd een afhankelijkheid van de leverancier op. Naarmate de betreffende informatievoorziening belangrijker is, zijn meer maatregelen nodig om de risico's die dit met zich mee brengt te mitigeren. Zo is voor iedere SaaS-dienst een exitstrategie nodig, waarbij onder andere geregeld wordt dat de leverancier bij beëindiging van het contract meehelpt aan de omzetting van de data naar de nieuwe omgeving. Maar ook Amsterdam UMC zelf heeft verplichtingen en dient met 'goed opdrachtgeverschap' de relatie met de leverancier goed afgestemd te houden.

Om de bovengenoemde aspecten optimaal te verwerken in de contractering, is de Dienst ICT de contractpartner bij cloud-applicaties.

2. Inleiding

2.1. Aanleiding

In het verleden is op beide locaties beleid rond inzetten van cloudapplicaties (Software as a Service oftewel SaaS) ontwikkeld. De laatste jaren is het thema in een stroomversnelling geraakt. De belangrijkste reden is de AVG-wetgeving, waardoor organisaties steeds meer verantwoording moeten afleggen over het omgaan met gegevens. Opslag van gegevens in de cloud heeft daarbij extra aandacht.
Daarnaast is er een trend dat steeds meer applicaties in de cloud aangeboden worden. Bij de harmonisatie van het applicatielandschap van Amsterdam UMC wordt bovendien ook vaak naar cloudoplossingen gekeken.

Hierom is een concernbrede beleidsnota, die actuele vraagstukken bij acceptatie, implementatie, beheer en governance van SaaS-oplossingen behandelt, zeer wenselijk. Deze beleidsnota gaat dus niet over het selectieproces, maar over het gehele traject vanaf het moment van selecteren.

2.2. Doel en doelgroepen van dit document

Het doel van dit beleidskader is als volgt:

Het geven van kaders en uitvoeringsrichtlijnen voor acceptatie, implementatie, beheer en governance van cloudapplicaties (SaaS-oplossingen).

Onderdeel van de governance is het inrichten en onderhouden van de leverancierscontacten.
De doelgroepen van dit document zijn:

- opdrachtgevers, ter ondersteuning bij SaaS-projecten;
- ICT-architecten, voor de verwerking in domeinplannen en roadmaps;
- beheerders, als kader voor toetsing, invoering, beheer en beëindiging van SaaS-diensten;
- informatiemanagers, als technisch kader bij de inventarisatie van requirements;
- Inkoop en contractmanagement, als kader voor uitwerking en management van contracten.

Het document heeft een geldigheid tot eind 2021. Op basis van de bereikte doelen, het marktaanbod en de ervaringen met de SaaS-dienstverlening zal het dan aangescherpt worden.

2.3. Doelstelling SaaS-diensten

Wanneer er voor een SaaS-oplossing gekozen wordt, is die oplossing onderdeel van de totale informatievoorziening van Amsterdam UMC. Het doel dat Amsterdam UMC nastreeft is dan: een effectieve en kostenefficiënte SaaS-dienst binnen de ICT-architectuurkaders van Amsterdam UMC. Dat laatste houdt in dat de SaaS-diensten zo veel mogelijk aansluiten bij de kaders voor datakoppeling en -integratie, identitymanagement, security en privacy, deliverymanagement en leveranciersmanagement.

Soms laten de leveranciers de hosting en de netwerkafhandeling door andere partijen doen. Bij het afsluiten van het contract is het daarbij nodig om zorgvuldige afspraken over de afhandeling van incidenten te maken. In de zorg komt dit regelmatig voor. Voorbeelden zijn TimeTell, XDS, ValueCare, KLIK, Questmanager et cetera. In die gevallen zijn extra afspraken nodig om de coördinatie tussen de twee of drie partijen goed in te regelen. De eerste uitvoeringsrichtlijn gaat expliciet hierop in.

2.4. Gerelateerd beleid

Integraal van toepassing zijn alle kaders rond privacy en security inclusief AVG-wetgeving en NEN7510. Binnen de zorg komen daar nog de eisen rond patiëntveiligheid (JCI) en gebruik van medische apparatuur en programmatuur (MDR/IVDR) bij.

Overigens wijken SaaS-diensten alleen af van overige ICT-diensten voor wat betreft het ICT-platform; samen met lokaal geïnstalleerde toepassingen en werkplekapplicaties vormen ze het scala van (platform-)mogelijkheden. Alle beleid rond ICT-diensten is van toepassing; alleen vanwege het feit dat het platform in beheer is bij een externe partij, zijn er extra aandachtspunten. Dit document gaat vooral in op die aandachtspunten.

Vaak worden bij SaaS ook direct IaaS en PaaS genoemd. Dit zijn on-line infrastructuurdiensten waarbij de afnemer zijn eigen applicaties installeert en beheert; zie bijlage 1 voor meer details. Deze notitie is gericht op het afnemen van applicatiediensten. Daarmee vallen IaaS en PaaS buiten de scope.

2.5. Leeswijzer

In het volgende hoofdstuk is het beleid uitgewerkt in twee groepen: kaders en uitvoeringsrichtlijnen. De kaders bakenen het speelveld af, de uitvoeringsrichtlijnen bieden voorschriften voor acceptatie, implementatie en beheer.
In bijlage 1 is een lijst opgenomen van de belangrijkste gehanteerde begrippen en hun betekenis. Bijlage 2 bevat de documenthistorie.

3. Beleid

3.1. Kaders

3.1.1. SaaS-diensten zijn compliant aan wet- en regelgeving rond privacy en security

Beschrijving	De gevraagde SaaS-dienst dient aantoonbaar te voldoen aan alle eisen die vanuit wet- en regelgeving rond privacy en security eraan gesteld worden.
Rationale	Gebruik van SaaS-diensten impliceert beslissingen over de plaats van data-opslag en –verwerking, onderwerpen waaraan strikte voorwaarden rond informatiebeveiliging gesteld worden.
Consequenties	Voor elke keuze wordt een BIV-classificatie uitgevoerd. Waar nodig wordt een DPIA opgesteld, en wordt als onderdeel van de contractering een verwerkersovereenkomst opgesteld. Waar het privacygevoelige data betreft, vindt toetsing door de FG plaats. Dit alles leidt tot een lijst van maatregelen die getroffen moeten worden om de SaaS-dienst te laten voldoen aan wet- en regelgeving. De leverancier speelt hierin vanzelfsprekend een belangrijke rol. Hij zal de benodigde maatregelen moeten nemen om die rol ook volledig waar te maken. Dit vereist deskundigheid bij de leverancier, maar ook ervaring met dit soort maatregelen. Er kan verondersteld worden dat die aanwezig zijn wanneer de leverancier gecertificeerd is, mede omdat daarbij externe audits plaatsvinden. Welke certificering relevant is, is afhankelijk van de aard van het af te nemen product. Voorbeelden: voor privacy NEN7510, 7512 of 7513, ISO27001-1 of ISO27001-2. Voor financiële data: ISEA3402 type 2. Gedurende de gehele periode van dienstverlening werken de leveranciers actief mee aan gegevensbescherming en nemen daarvoor adequate maatregelen. Zij rapporteren direct of op verzoek over de status en afwijkingen van de gegevensbescherming. Ook de logbestanden van de leverancier zijn, voor wat betreft het gedeelte van Amsterdam UMC, toegankelijk voor de Dienst ICT voor eigen analyses en rapportages. Al deze zaken vormen onderdeel van de overeenkomst met de leverancier.

3.1.2. SaaS-diensten zijn onderdeel van de totale informatievoorziening

Beschrijving	SaaS-diensten zijn integraal onderdeel van de totale informatievoorziening van Amsterdam UMC. Het beleid voor ICT-diensten is daarmee integraal van toepassing op SaaS-diensten.
Rationale	Of er voor de realisatie van de gewenste functionaliteit nu wel of niet voor een SaaS-dienst gekozen wordt, de functionaliteit is onderdeel van de informatievoorziening van Amsterdam UMC. Dit betekent dat de SaaS-dienst moet voldoen aan alle eisen rond stabiliteit en continuïteit van de totale informatievoorziening.
Consequenties	Met de leverancier worden afspraken vastgelegd over de te volgen procedure bij changes, prioriteitstelling en aankondigingstermijnen voor changes, en over de te volgen test- en acceptatieprocedure. Indien er sprake is van uitwisseling van gegevens tussen de cloudapplicatie en andere onderdelen van de informatievoorziening bij Amsterdam UMC, worden afspraken vastgelegd over uitvoering van changes rond die koppelingen, ook wanneer die change geen wijziging in de cloudapplicatie zelf betreft.

3.1.3. AMSTERDAM UMC HOUDT HET INTELLECTUEEL EIGENDOM VAN ZIJN DATA

Beschrijving	Alle gegevens die Amsterdam UMC in het kader van SaaS-diensten op de ICT-omgeving van een externe partij ter beschikking stelt, blijven het intellectuele eigendom van Amsterdam UMC
Rationale	Bescherming van het intellectuele eigendom. Voldoen aan onder meer de AVG, de Wet Bescherming Persoonsgegevens en, wanneer het de zorg betreft, de Wet op de Geneeskundige BehandelOvereenkomst.
Consequenties	Het intellectuele eigendom wordt bij elke SaaS-dienst geborgd. Leveranciers kunnen geen (mede-)eigendom claimen op de gegevens, dan wel gegevens zonder uitdrukkelijke toestemming van de eigenaar voor andere doeleinden (willen) gebruiken. Dit is geen open deur: vaak claimen leveranciers enig gebruiksrecht op de data. Daarnaast moet Amsterdam UMC kunnen beschikken over de data. Dit houdt onder andere in dat de Dienst ICT op elk gewenst moment de data met bijbehorende metadata, dus inclusief datamodel, kan downloaden voor support-, beheer- en/of securitydoeleinden. Al deze zaken vormen onderdeel van de overeenkomst met de leverancier.

3.1.4. ER ZIJN GESTANDAARDISEERDE KOPPELVLAKKEN VOOR GEGEVENSUITWISSELING

Beschrijving	Uitwisseling van gegevens tussen systemen en applicaties loopt via gestandaardiseerde koppelvlakken; dit geldt dus ook voor SaaS-diensten.
Rationale	Gegevensuitwisseling verdient extra aandacht bij ICT-diensten. Het vergroot de complexiteit, en de risico's rond security en continuïteit van ICT-diensten nemen ook toe. Bij SaaS-diensten is er sprake van een extra zorgpunt omdat de data over de grenzen van Amsterdam UMC gaan en omdat leveranciers van SaaS-diensten vaker eigen eisen stellen aan koppelvlakken. Alleen door standaardisatie is een kostenefficiënt beheer van koppelingen mogelijk. Niet gebruikmaken van standaarden betekent extra regie-inspanning en dat verhoogt de totale kosten voor de SaaS-dienst. In het inkoopproces wordt daarom ook vastgesteld welke standaarden de leverancier gaat gebruiken in zijn dienstverlening aan Amsterdam UMC.
Consequenties	De Dienst ICT voert de technische regie over alle koppelingen. Regie omvat het overzicht houden en het kunnen ingrijpen waar nodig. Hiervoor worden extra afspraken met de leverancier vastgelegd. Waar sprake is van berichtuitwisseling, wordt bij voorkeur aangesloten op de interne standaarden die Amsterdam UMC daarvoor hanteert (bijvoorbeeld HL7). Afwijking daarvan verzwaart de regierol en heeft impact op de doorlooptijd van changes die aan de betreffende berichtuitwisseling raken. De berichtuitwisseling zelf vindt bij voorkeur plaats met één concernbrede voorziening ("servicebus"); ook hier geldt dat afwijkingen de regierol compliceren. Berichtuitwisseling tussen SaaS-diensten onderling (de 'SaaS-SaaS-koppelingen') vindt plaats middels de SaaS-SaaS-broker van Amsterdam UMC. Uitwisseling via ons netwerk met bijbehorende toename van risico's (tweemaal over het

	internet) is daarmee vermeden, terwijl Amsterdam UMC wel volledig beschikt over de werking van de koppeling. Speciale aandacht is nodig voor de uitwisseling van gegevens voor gebruikersbeheer. Het bijhouden van gebruikers en hun rechten wordt zo veel mogelijk in één systematiek gedaan, om te allen tijde bevoegde toegang te borgen, en onbevoegde toegang te voorkomen. Concreet betekent dit voor de leverancier aansluiting op de standaard SCIM of zijn opvolger.

3.1.5. ER IS EEN GEZONDE SAMENWERKINGSRELATIE MET DE LEVERANCIER MOGELIJK

Beschrijving	Elke vorm van uitbesteding introduceert een nieuwe afhankelijkheid. Zolang dat tot de gewenste resultaten leidt, is dat geen probleem. Het wordt een probleem wanneer de afhankelijkheid tot ongewenste gevolgen leidt. Dit kan zich op vele manieren manifesteren, maar alles heeft te maken met de aard van de samenwerkingsrelatie. Die moet “gezond” zijn. Voor Amsterdam UMC betekent dit onder andere dat het “in control” is, en nog vrijheden heeft in zijn (vervolg-)keuzes zonder onterechte beperkingen van de kant van de leverancier. Dit is lastig te kwantificeren. Een lijst van basisvaardigheden in een individu-gericht trainingsprogramma voor “Roestvrij samenwerken” geeft een goede indruk van wat een gezonde samenwerkingsrelatie is: 1. de intentie hebben om samen te werken: inzetten voor wederzijds succes 2. oprecht zijn: een klimaat creëren waarin mensen eerlijk en open zijn 3. eigen verantwoordelijkheid: verantwoordelijkheid nemen voor de gevolgen van eigen handelen en niet-handelen. 4. zelfreflectie en -evaluatie: eigen kracht en zwakheden goed genoeg kennen om het verschil te onderkennen tussen kwaliteit van jezelf en kwaliteit van de relatie. 5. problemen oplossen en onderhandelen: de “Interest Based”-benadering gebruiken om te onderhandelen bij conflicten die onvermijdelijk in elke relatie ontstaan. Deze checklist is niet één op één over te zetten naar organisaties, maar geeft wel de onderliggende waarden aan. Wanneer er iets “schuurt” in de relatie, moet er een vooraf vastgelegde weg zijn waarlangs dit geadresseerd kan worden. Die weg wordt vastgelegd in het contract.
Rationale	Naarmate een samenwerkingsrelatie langere tijd voortduurt, neemt het risico van een ‘vendor lock-in’ toe. Omgekeerd kan een (geleidelijk) kwaliteitsverlies bij de leverancier ertoe leiden dat we stapsgewijs zelf onderdelen gaan invullen dan wel corrigeren, waardoor de uitbesteding zijn doel voorbij schiet. Ook kan de leverancier zijn businessdoelen zodanig aanpassen dat de (business-)waarde van de contracten met Amsterdam UMC voor hem lager wordt, of verandert de leverancier het businessmodel of de dienst, waardoor de dienstverlening niet langer aansluit bij de doelstellingen van Amsterdam UMC.
Consequenties	Er is voor essentiële systemen naast het operationeel-/tactisch overleg een (bij voorkeur jaarlijks) contractoverleg, waarin beide partners borgen dat de intenties van het contract nog optimaal nagestreefd worden. Mede op basis daarvan wordt besloten over eventuele verlengingen.

	Jaarlijks worden de lopende contracten beoordeeld op hun feitelijke naleving en de risico's van onbalans. Op basis daarvan worden adviezen over aanpassingen gegeven. De contracthouder beslist daarover.

3.2. Uitvoeringsrichtlijnen

3.2.1. BIJ SAAS-DIENSTEN MET MEERDERE LEVERANCIERS ZIJN EXTRA MAATREGELEN NODIG

Beschrijving	Soms laten leveranciers van SaaS-diensten de hosting en de netwerkafhandeling door andere partijen doen. Zelf bieden ze het gebruik van de applicatie aan, maar het cloudplatform (de PaaS- of IaaS-dienst) kan de opdrachtgever zelf bepalen. Vooral kleinere leveranciers kiezen voor deze weg. In dit geval zijn extra maatregelen nodig voor de coördinatie tussen de betreffende partijen waar het de compliance van de SaaS-oplossing aan wet- en regelgeving betreft.
Rationale	SaaS-diensten waarbij meerdere leveranciers betrokken zijn, leveren een versnippering van de oplossing op. Dit leidt tot een complexere beheersituatie. Immers, elk van de partijen dragen bij aan de compliance van de oplossing aan de wet- en regelgeving.
Consequenties	Bij de selectie van SaaS-diensten wordt in een vroegtijdig stadium nagegaan of hosting en netwerkafhandeling inbegrepen is. Is dit niet het geval, dan wordt een oplossing uitgewerkt waarin Amsterdam UMC rechtstreekse contacten heeft met de andere leveranciers en waarbij er met de betreffende partijen afspraken worden gemaakt (en contractueel vastgelegd) over de onderlinge coördinatie. De voorkeur gaat uit naar oplossingen waarbij gebruik gemaakt wordt van componenten die de Dienst ICT al in zijn dienstenportefeuille heeft. Dit zowel om kostenredenen als ook omdat er dan al bestaande governance is waarop aangesloten kan worden.

3.2.2. OPDRACHTGEVERS EN GEBRUIKERS BEHOUDEN HUN "SINGLE POINT OF CONTACT"

Beschrijving	Inzet van SaaS-diensten is in wezen een vraagstuk rond de inrichting van de ICT-dienstverlening. Voor een opdrachtgever of gebruiker moet het niet uitmaken of de keten uit alleen interne partijen of een mix van interne en externe partijen plaatsvindt. Daarom is het logisch wanneer opdrachtgevers en gebruikers ook voor de SaaS-dienst gebruik kunnen maken van hun reguliere contacten bij de Dienst ICT: de ICT-Servicedesk, de applicatiebeheerder, de relatiemanager.
Rationale	Eenduidige ICT-dienstverlening aan opdrachtgevers en gebruikers, onafhankelijk van een specifieke applicatie, versnelt de afhandeling van vragen en problemen.
Consequenties	De Dienst ICT is de contractpartner. Bij implementatie van de SaaS-dienst neemt de Dienst ICT het initiatief om de benodigde overlegstructuur in te richten. Daarin zijn opdrachtgever, Dienst ICT en leverancier vertegenwoordigd. Voor bepaalde zaken (denk aan functionele-acceptatieprocessen) zijn rechtstreekse contacten tussen opdrachtgever en leverancier gewenst of zelfs noodzakelijk. De Dienst ICT voert daarover de regie om bij voorkomende problemen snel en adequaat te kunnen handelen. Om het de Dienst ICT mogelijk te maken zijn regierol te kunnen uitvoeren, wordt met de leverancier afgesproken dat zij de Dienst ICT informeren over lopende contacten binnen Amsterdam UMC. Alle zaken die de leverancier betreffen worden vastgelegd in de overeenkomst.

3.2.3. TOEGANG WORDT INGEREGELD VIA DE STANDAARDOPLOSSING VAN AMSTERDAM UMC

Beschrijving	Identiteits- en toegangsmanagement (IAM, van het Engelse Identity & Access Management) is een essentieel element in het borgen van een veilige en betrouwbare informatievoorziening. Vanuit IAM-perspectief doorloopt de gebruiker bij toegang tot een applicatie drie stappen: identificatie, authenticatie en autorisatie. Voor identificatie en authenticatie wordt bij voorkeur gebruik gemaakt wordt van het instrument dat Amsterdam UMC daarvoor als standaard hanteert: federatieve authenticatie op basis van Amsterdam UMC-accounts. Bij federatieve authenticatie wordt een vertrouwde partij gebruikt om authenticatie af te handelen voor toegang tot de SaaS-dienst. Hierdoor kan eenvoudig en veilig worden ingelogd (geauthenticeerd).
Rationale	Bevoegd gebruik van systemen, waar deze zich ook ICT-technisch bevinden, wordt centraal gemanaged. Het komt de eenvoud, en daarmee de beheersbaarheid, sterk ten goede wanneer dit eenduidig is voor alle systemen. Iedere afwijking leidt tot vergroting van de complexiteit en daarmee tot vergroting van zowel kosten als risico's op dit punt.
Consequenties	Voor SaaS-diensten wordt de authenticatie geregeld via de standaardvoorzieningen van de Dienst ICT, op dit moment ADFS in de Amsterdam UMC-omgeving, Azure-AD of SURFconext. De identificator waaronder de persoonsgegevens in de SaaS-dienst worden opgeslagen is de Amsterdam UMC-ID, conform de architectuur voor IAM. In SaaS-applicaties vindt gebruikersbeheer plaats onder gebruikmaking van het Amsterdam UMC-account, waarin alle gebruikersidentiteiten en –rechten van de beide locaties zijn opgenomen. Indien er extra voorzieningen nodig zijn om dit te realiseren, worden die zodanig opgezet dat het beheer transparant en door Amsterdam UMC auditeerbaar is.

3.2.4. DE SAAS-DIENST VOLDOET AAN DE EISEN VANUIT DE BIV-CLASSIFICATIE EN DPIA

Beschrijving	Een BIV-classificatie en DPIA leidt tot aanbevelingen voor te nemen maatregelen. Voor SaaS-diensten zijn er naast de generieke maatregelen ook specifieke maatregelen nodig. Deze betreffen het datatransport (over de grenzen van Amsterdam UMC heen), data-opslag, en verificatie van de bron/locatie van de SaaS-dienst.
Rationale	Een rechtstreeks gevolg van het kader in paragraaf 3.1.1.
Consequenties	De data, de applicatie en het netwerkverkeer wordt gescheiden van die van andere klanten van de cloudapplicatie. Het datatransport wordt beveiligd conform de BIV-classificatie. Er is voldoende verificatiemogelijkheid van de bron/locatie van de SaaS-dienst. Bij voorkeur vindt dit plaats door gebruik te maken van een VPN.

3.2.5. ELKE SAAS-DIENST HEEFT EEN EXITSTRATEGIE

Beschrijving	Voor elke SaaS-dienst is een exitstrategie nodig. De exitstrategie richt zich op: • continuïteit in de beschikbaarheid van de data • continuïteit in de informatievoorziening van Amsterdam UMC

Rationale	Borging van de continuïteit van de informatievoorziening. Denk aan situaties als beëindiging van het contract, grote veranderingen in de aard van de geleverde diensten, grote veranderingen in de markt van de betreffende diensten, faillissement of overname van de leverancier, of afnemende deskundigheid bij de leverancier.
Consequenties	Voor elke SaaS-dienst is een exitstrategie inclusief exitcriteria, continuïteitsplan en “sourcing plan B” beschikbaar. In dit plan staat omschreven wat het voorkeursalternatief is, welke stappen er gezet moeten worden voor de datamigratie en welke (contractuele) afspraken er zijn met de huidige leverancier om de continuïteit van de dienstverlening te borgen. Alleen bij dwingende noodzaak neemt Amsterdam UMC diensten af van leveranciers die een goede exitstrategie moeilijk of onmogelijk maken.

3.2.6. ELKE SAAS-DIENST WORDT VOORZIEN VAN GOED OPDRACHTGEVERSCHAP

Beschrijving	Goed Werkgeverschap is een (wettelijke) verplichting van elke organisatie. Bij SaaS-diensten gelden vergelijkbare regels voor “goed opdrachtgeverschap”. Een voorbeeld van concretisering hiervan staat in het document “Benchmark Goed Opdrachtgeverschap voor ICT-inkopen”, gepubliceerd op nederlandict.nl (zie referentie). Daarin zijn onder andere de regievoering, de resultaatsturing in de vorm van meetbare prestatie-indicatoren en het op peil houden van de vereiste deskundigheid in een lijst van 21 principes uitgewerkt. Deze uitvoeringsrichtlijn is nog niet in het gewenste stadium van concreetheid. Toch is het belangrijk genoeg om er aandacht aan te besteden, vooral bij het afsluiten en verlengen van contracten. Op basis van de opgedane ervaringen zal dit punt in volgende versies van het beleidskader nader uitgewerkt worden.
Rationale	SaaS-diensten zijn een vorm van uitbesteden. Uitbesteden betekent niet dat de eigen organisatie (zowel die van de opdrachtgever als de Dienst ICT) ervan af is. Vooral bij uitbesteding van diensten is een adequate regie-organisatie noodzakelijk, om een gezonde samenwerkingsrelatie te houden en daarmee de ICT-dienstverlening op het gewenste peil te houden. Het versloffen van goed opdrachtgeverschap leidt vroeg of laat tot een te grote afhankelijkheid van de leverancier, met kansen op degradatie in de dienstverlening en/of een vendor lock-in.
Consequenties	In de aanpak voor invoering van nieuwe of wijziging van bestaande SaaS-diensten formuleren de opdrachtgever en de Dienst ICT samen doelen en activiteiten die gericht zijn op het bereiken van het vereiste niveau van Goed Opdrachtgeverschap. Criteria daarvoor worden op basis van de feitelijke situatie vooraf vastgesteld, mede aan de hand van de principes in de genoemde benchmark (zie referentie). Dit heeft ook consequenties voor de leverancier; die consequenties worden contractueel vastgelegd. Helderheid creëren over de werkwijze van Amsterdam UMC bij acceptatie en implementatie van changes, en afspraken maken over aansluiting daarop door de leverancier, zal bijvoorbeeld onderdeel zijn van het inkoopproces. Daarbij worden ook aankondigingstermijnen overeengekomen. Voorbeeld: minimaal twee weken tevoren aankondigen van onderhoudsmomenten.

Bijlage I. Begrippenlijst

Begrip	Definitie
ADFS	Active Directory Federation Services. Een voorziening van Microsoft om geauthenticeerde toegang tot systemen te krijgen zonder opnieuw in te hoeven loggen (“single sign-on”).
AVG	Algemene Verordening Gegevensbescherming, ook wel bekend onder de Engelse naam GDPR: General Data Protection Regulation. Een Europese verordening die de regels voor verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
BIV-classificatie	Classificatie voor het bepalen van het niveau van Beschikbaarheid, Integriteit en Vertrouwelijkheid van data. Dit is een belangrijk instrument om te bepalen welke maatregelen nodig zijn om te voldoen aan wet- en regelgeving.
DPIA	Data Protection Impact Assessment. Een instrument waarmee organisaties privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in kaart kunnen brengen. Het doel van de DPIA is het bepalen van de benodigde maatregelen om de onderkende privacyrisico’s zo ver als mogelijk te minimaliseren.
Exitstrategie	Het document dat aangeeft wanneer de gekozen oplossing (in dit geval de SaaS-dienst) aangepast moet worden, wat daarbij het alternatief is, hoe de continuïteit van de onderliggende diensten gewaarborgd blijven bij de transitie, en welke maatregelen er nog nodig zijn in de oude omgeving om te blijven voldoen aan alle eisen (denk aan beveiliging).
FG	Functionaris Gegevensbescherming. Een door de Raad van Bestuur aangestelde functionaris die toeziet op datagebruik en –verwerking in Amsterdam UMC.
Goed Opdrachtgeverschap	Deze term is ontstaan om het opdrachtgeverschap bij inzet van externe partijen goed in te richten. De definitie is: “Op heldere wijze de behoeften en wensen van de organisatie overbrengen op de opdrachtnemer of leverancier.” Geleidelijk is dit uitgebreid met het borgen van die belangen gedurende de looptijd van het contract. Inrichten en handhaven ervan vereist inzet van zowel de opdrachtgever als de leverancier.
IaaS	Infrastructure as a Service. Dit is infrastructuur (rekenkracht) die als een on-line dienst wordt aangeboden. De gebruiker kiest de benodigde capaciteit waarna een virtuele computer ter beschikking gesteld wordt. De gebruiker installeert en beheert vervolgens het besturingssysteem, de generieke software (‘middleware’) en de toepassingen en hij betaalt naar gebruik. Een speciale vorm van IaaS is PaaS: Platform as a Service. Daarbij levert de leverancier de virtuele computer inclusief besturingssysteem en middleware, zodat de gebruiker alleen zijn toepassing hoeft te installeren en beheren.
IAM	Identity & Access Management. Het beheer van gebruikers en hun toegangsrechten, afgestemd op de actuele rol(len) in de organisatie.
MDR/IVDR	Medical Device Regulation/In Vitro Device Regulation. Europese regels rond aanschaf en gebruik van medische apparatuur en programmatuur. In de Regels staan de veiligheids- en kwaliteitseisen vermeld die voor de hele EU van toepassing zijn. De regels zijn vastgesteld in 2017 als opvolgers van de Medical Device Directive.
PaaS	Platform as a Service. Een speciale vorm van IaaS; zie aldaar.
SaaS	Software as a Service. Dit is software die als een online-dienst (“in de cloud”) wordt aangeboden. SaaS wordt gezien als de applicatielaag van cloudcomputing. De belangrijkste kenmerken van een SaaS-dienst zijn: • de applicatie wordt niet aangeschaft; er wordt voor het gebruik betaald;

	• de applicatie wordt niet lokaal geïnstalleerd maar bij de leverancier. De toegang verloopt via internet of een privénetwerk; • de leverancier verzorgt het applicatiebeheer; • de dienst is eenvoudig op te schalen wanneer nodig.
SCIM	System for Cross-domain Identity Management. Een standaard voor automatische uitwisseling van (gebruikers)identiteiten tussen gescheiden IT-systemen. Hiermee kunnen mutaties in de gebruikers en hun rechten vanuit een bronsysteem automatisch doorgevoerd worden in de verschillende andere systemen, waaronder een SaaS-dienst.
VPN	Virtual Private Network. Dit is een techniek om het mogelijk te maken zodanige verbindingen over het internet aan te leggen dat de vertrouwelijkheid, integriteit en authenticiteit van data op hetzelfde peil zijn als bij een verbinding die volledig binnen het eigen, lokale netwerk gelegd is.

Bijlage II. Documenthistorie

Versiebeheer

Datum	Versie	Auteur	Wijzigingen
17-07-2019	0.1	Arie Elsenaar	Eerste opzet na inventarisatie bestaand beleid en bekende knelpunten beide locaties
09-09-2019	0.5	Arie Elsenaar	Aanvullingen en correcties verwerkt
17-9-2019	0.8	Arie Elsenaar	Toetsing bij AM/beide locaties
12-12-2019	0.9	Arie Elsenaar	Voorbereiding voor aanbieding aan MT
14-01-2020	0.91	Arie Elsenaar	Verwerking opmerkingen Erik Mark
21-01-2020	1.0	Arie Elsenaar	Vaststelling door de directeur ICT

Distributie

Datum	Versie	Aan	Functie of rol
17-07-2019	0.1	medewerkers ASB	Aanvullingen en correcties verzamelen
09-09-2019	0.5	medewerkers AM	Aanvullingen en correcties verzamelen
17-9-2019	0.8	ASB-overleg	Beoordeling en afstemming
12-12-2019	0.9	MT Dienst ICT	Accordering
14-01-2020	0.91	MT Dienst ICT	Accordering na aanpassing
21-01-2020	1.0	Amsterdam UMC	Publicatie op Kwaliteitsnet/Kwadraet

Referenties

Auteur	Titel	Bron
Laurens Groenewegen	Kaderdocument clouddiensten v1.0, 28-09-2015	Kwaliteitsnet locatie VUmc
Hans van den Berg	SaaS-beleid AMC v1.0, 19-02-2013	Kwadraet locatie AMC
Hans van den Berg	SaaS-beleid AMC VUmc v0.1, 31-07-2018	Conceptnotitie Hans van den Berg
Arie Elsenaar	Beleidskader sourcing v0.9, 05-11-2018	Conceptnotitie Arie Elsenaar
PBLQ	Benchmarkrapport “Goed Opdrachtgeverschap voor ICT-inkopen door de Rijksoverheid in Nederland”	https://www.nederlandict.nl/wp-content/uploads/2017/10/Benchmarkrapport-goed-opdrachtgeverschap-voor-ICT-inkopen-door-de-Rijksoverheid-in-Nederland.pdf