Regionaal Archief
Alkmaar

Continuïteitsbeleid e-depot Alkmaar

September 2021

1. Inleiding

Sinds juli 2019 heeft het Regionaal Archief Alkmaar (RAA) een technisch werkende e-depotvoorziening. Het e-depot is een nieuwe dienst binnen het RAA voor het borgen van de duurzame toegankelijkheid van born digital en gedigitaliseerde te bewaren informatieobjecten, die binnen het werkgebied van het RAA zijn opgemaakt. Omdat het gaat om te bewaren informatieobjecten, worden deze na verloop van tijd in de bronapplicatie vernietigd. Daarmee worden de organisaties binnen het werkgebied, en andere gebruikers van de openbare informatie die in het e-depot staat opgenomen, afhankelijk van de mate waarin de objecten te benaderen en in te zien/te lezen zijn. Met andere woorden; zij worden afhankelijk van de continuïteit van het e-depot en van de bijbehorende dienstverlening. In dit stuk zijn de beleidsuitgangspunten opgenomen die de continuïteit van het e-depot en van de dienstverlening garanderen.

1.1 Wat is continuïteit en discontinuïteit?

Om uitgangspunten op te stellen rondom continuïteit is het belangrijk om eerst helder te hebben wat continuïteit, en in het verlengde daarvan discontinuïteit, voor het RAA inhoudt.

Het RAA hanteert de volgende definitie als het gaat om het e-depot: *'Het e-depot is het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer, databeveiliging en de aanwezigheid van hard- en software dat het duurzaam beheren en raadplegen van digitale archiefbescheiden mogelijk maakt'.*[1]

Deze definitie laat zien dat een e-depot meer is dan een technische oplossing. Het betreft een samenhang van techniek, financiën, beheer, kennis en dienstverlening. Wanneer een van deze elementen wordt verstoord, dan is er in de ogen van het RAA sprake van discontinuïteit. Continuïteit is voor het RAA in dat opzicht, dat de techniek, financiën, het beheer en de kennis dermate ingericht en up-to-date zijn, dat de dienst (zijnde het e-depot) met bijbehorende dienstverlenende processen, te allen tijde doorgang kan vinden.

1.2 Reikwijdte

Dit stuk bevat de beleidsuitgangspunten voor de continuïteit van het e-depot en de bijbehorende dienstverlening. Zowel het e-depot als de bijbehorende dienstverlening zijn niet alleen afhankelijk van de software van het e-depot zelf, maar ook van andere systemen en mechanismen. Dit beleidsdocument bevat ook uitgangspunten die deze systemen betreffen. In het kader van het e-depot en de bijbehorende dienstverlening zijn deze systemen onderdeel van de bedrijfskritische-applicaties, oftewel de applicaties die nodig zijn om de dienstverlening rondom het e-depot te kunnen continueren.

[1] Deze definitie is afkomstig van het Nationaal Archief en door ons overgenomen: Wat is een e-Depot? | Nationaal Archief.

Buiten de reikwijdte

Het continuïteitsbeleid is een beleidsstuk. Dat betekent dat er uitgangspunten zijn opgenomen die verdere uitwerking hebben in praktische plannen en procedures die niet in dit beleidsplan zijn opgenomen. Voorbeelden hiervan zijn:

- Continuïteitsplan;
- Exitstrategie;
- Calamiteitenplan;
- Aansluitvoorwaarden;
- Procedures;
- Preserveringsbeleid;
- Beschrijving van producten en diensten;
- Informatiebeveiligingsbeleid en –plan;

Deze producten zijn door het RAA apart opgesteld. Het continuïteitsbeleid heeft natuurlijk wel betrekking op deze documenten. Indien een van de bovenstaande documenten de continuïteit van een van de elementen van het e-depot garandeert, dan zal hiernaar verwezen worden.

Dit continuïteitsbeleid is daarmee tevens geen plan waarin risico's en bedreigingen worden beschreven die het e-depot en de bijbehorende dienstverlening overstijgen. Denk hierbij aan het opheffen van de gemeenschappelijke regeling RHCA, of het uittreden van één of meerdere aangesloten organisaties. Dergelijke scenario's zijn dermate ingrijpend, dat ze meer gevolgen hebben dan enkel voor het e-depot en de bijbehorende dienstverlening. Wanneer een dergelijk scenario zich voordoet, zal er dan een actieplan worden opgesteld om ervoor te zorgen dat de informatieobjecten die in het e-depot opgenomen zijn, niet verloren gaan of niet meer toegankelijk zijn.

1.3 Verantwoordelijkheden

Het calamiteitenbeleid heeft betrekking op meerdere partijen die gebruik maken van het e-depot. Dit zijn:

- De beheerorganisatie: het RAA
- De zorgdragers: de organisaties die onderdeel uit maken van de gemeenschappelijke regeling van het RAA
- De leverancier en gegevensverwerker: het RAA neemt bij een leverancier de software met verschillende diensten af met betrekking tot het e-depot

De zorgdrager is:

1. verantwoordelijk voor de informatie en de kwaliteit van de informatie die overgedragen of overgebracht wordt aan het RAA voor opname in het e-depot.
2. als archiefvormer verantwoordelijk voor het opstellen en vaststellen van beleid omtrent software-inrichting en -keuzes. Wanneer er gebruik gemaakt wordt van het e-depot van het RAA, dan dient ook rekening gehouden te worden met de aansluitvoorwaarden zoals het RAA deze heeft vastgesteld.

De beheerorganisatie is:

3. verantwoordelijk voor het beheren van archiefwaardige informatieobjecten; hiermee wordt bedoeld dat het RAA verantwoordelijk is voor de duurzame toegankelijkheid op de lange termijn van de informatieobjecten die in het e-depot zijn opgenomen.
4. verantwoordelijk voor de continuïteit van de elementen waar een e-depot uit bestaat (zoals opgenomen in paragraaf 1.1) en de bijbehorende dienstverlening.
5. verantwoordelijk voor de beheerorganisatie en de omgeving waarin de archiefwaardige informatieobjecten duurzaam worden bewaard;
6. verantwoordelijk voor het opstellen van plannen en procedures die uitvoer geven aan het continuïteitsbeleid.
7. verantwoordelijk voor het opstellen en uitdragen van (kwaliteits)eisen aan de diensten van de leverancier en op basis daarvan het opstellen van een Service Level Agreement (SLA) met de leverancier van de bewaar- en beheeromgeving;
8. verantwoordelijk voor het stellen van eisen ten aanzien van een vangnet in het geval van faillissement van de leverancier.

De leverancier is:

9. verantwoordelijk voor het beheren van het beheersysteem waarin de informatieobjecten staan opgeslagen;
10. verantwoordelijk voor het uitvoeren van de SLA;
11. verantwoordelijk voor het regelen van een vangnet in het geval van faillissement (escrowregeling; zie bijlage 2).

Binnen het continuïteitsbeleid vormen de verantwoordelijkheden van de beheerorganisatie de kern van dit document. In de volgende hoofdstukken is vastgelegd hoe elk van deze verantwoordelijkheden is ondervangen om de continuïteit van het e-depot, de overige bedrijfskritische applicaties en de bijbehorende dienstverlening te garanderen.

1.4 Evaluatie van het beleid

Het RAA heeft sinds een aantal maanden de applicatie Nuclino is gebruik. Dit is een webbased programma waarmee het eenvoudiger wordt om beleidsstukken en – plannen te publiceren. Vanwege het Wiki-vormige karakter is het mogelijk om beleidsstukken op te delen en per onderdeel te publiceren. Gezien de aard van dit programma heeft het RAA het uitgangspunt dat beleidstukken en –plannen via Nuclino worden gepubliceerd en daarmee, indien nodig, op onderdelen kunnen worden aangepast. Dit kan voorkomen wanneer bepaalde uitgangspunten nog niet geheel zijn uitgewerkt.

Eens in de 2 jaar zal het continuïteitsbeleid in zijn geheel worden gereviewed. Omdat via Nuclino het stuk in onderdelen is opgeknipt, is het mogelijk om het stuk via een scrumtraject te updaten. Per sprint zal een onderdeel worden gereviewed en aangepast.

2. De continuïteit van de duurzame toegankelijkheid

2.1 Inleiding

In het voorgaande hoofdstuk is beschreven welke verantwoordelijkheden het RAA als beheerorganisatie heeft als het gaat om de continuïteit van het e-depot en de bijbehorende dienstverlening. In dit hoofdstuk wordt dieper ingegaan op het e-depot zelf en hoe het zich verhoudt tot andere systemen binnen het RAA. Ook zal dit hoofdstuk duidelijk maken wat er aan beleidsdocumenten en plannen is opgesteld om de continuïteit van het e-depot en de bijbehorende dienstverlening te garanderen.

2.2 De continuïteit van de techniek

Het e-depot is een combinatie van verschillende elementen die erop toezien dat de duurzame toegankelijkheid van informatieobjecten, worden gegarandeerd. De elementen software en hardware worden door het RAA afgenomen bij Picturae BV in Heerhugowaard. De software draagt de naam Archivematica en deze wordt ontwikkeld door Artifactual. Archivematica is open source software die door Picturae wordt aangeboden als dienst waarbij extra onderdelen zijn toegevoegd voor specifiek de Nederlandse markt. Omdat de software open source is, kan Picturae daar zelf op voortbouwen en wordt daarom op sommige punten door Picturae zelfstandig doorontwikkeld. Daarnaast heeft Picturae een overeenkomst met Artefactual om grote aanpassingen aan de software samen te bewerkstelligen. Deze aanpassingen zijn dan beschikbaar voor alle Archivematica-gebruikers. Daarnaast wordt bij Picturae een opslaglocatie afgenomen. Alle informatieobjecten die in het e-depot worden opgenomen, komen op deze opslaglocatie van Picturae terecht.

Naast Archivematica, neemt het RAA ook het collectiebeheersysteem en het archiefbeheersysteem van Picturae af, namelijk Memorix Maior en Memorix Archieven. In Memorix Maior komen de bestanden terecht van de informatieobjecten die in het e-depot zijn opgenomen. Via het DAM, dat onderdeel is van Memorix Maior, kan vervolgens een afgeleide beschikbaar worden gesteld van zowel het object als van de metadata. In Memorix Archieven zijn de metadata die zijn gemapped naar EAD beschikbaar en kunnen daar eventueel worden beheerd. Dat betekent dat de continuïteit van het e-depot, en de duurzame toegankelijkheid van de informatieobjecten die daarin zijn opgenomen, niet alleen afhangt van Archivematica en de fysieke opslaglocaties die door Picturae wordt aangeboden, maar ook van de werking van Memorix Maior en Memorix archieven.

Om de continuïteit van de archival storage en collectiebeheersysteem waar het e-depot uit bestaat, te garanderen, zijn afspraken gemaakt. Dit betekent dat de daadwerkelijke verantwoordelijkheid voor het uitvoeren van deze afspraken bij de leverancier van de software is komen te liggen. Deze verantwoordelijkheid en afspraken zijn in de volgende stukken vastgelegd:

- Het Informatiebeveiligingsbeleid: dit beleidsstuk ondervangt de informatiebeveiliging voor de gehele organisatie, en daarmee ook voor het e-depot. Daar waar het de fysieke beveiliging van de opslaglocaties en de technische beveiliging van de informatieobjecten betreft, onderschrijft het beleid de verantwoordelijkheid van de leverancier. Informatiebeveiligingsaspecten die voortkomen uit menselijk handelen, zijn de verantwoordelijkheid van het RAA.
- De Service Level Agreement (SLA): deze overeenkomst is gesloten tussen het RAA en Picturae nadat Picturae tot leverancier van de e-depotoplossing van het RAA was aangewezen. Hierin zijn alle technische aspecten van het e-depot ondervangen die te maken

hebben met storingen, doorontwikkeling en het eventueel beëindigen van het contract met Picturae.
- De Exit-strategie: deze strategie is breder dan alleen de techniek, maar bevat veel technische aspecten. De strategie ondervangt op welke wijze de data kan worden veiliggesteld op het moment dat het RAA ervoor kiest om een andere e-depotvoorziening af te nemen bij een andere leverancier, of wanneer Picturae ervoor kiest om een andere software aan te gaan bieden dan Archivematica en het RAA niet in deze verandering mee wil gaan. In bijlage 2 staat opgenomen welke aspecten er benoemd moeten zijn in de exitstrategie.

Proces ondersteunende applicaties

Naast Memorix Maior en Archivematica, zijn er ook andere applicaties die worden gebruikt voor de uitvoer van verschillende processen die betrekking hebben op het e-depot. Zo wordt er gebruik gemaakt van:

- Een applicatie die het mogelijk maakt om gegevens uit te wisselen via een FTP-server.
- Een applicatie die het mogelijk maakt om TopX-bestanden te maken.
- Een applicatie die het mogelijk maakt op bestandsformaten de verifiëren. Deze applicatie zit ingebakken in het programma op TopX-bestanden te vormen.

De genoemde applicaties zijn open source, wat voor- en nadelen kan hebben. Aan de ene kant zijn ze daarmee multi-inzetbaar, aan de andere kant bestaat het gevaar dat er aanpassingen gedaan worden die de applicatie onbruikbaar maakt voor het RAA. Ook kan het zijn dat de applicaties ineens niet meer worden ondersteund of geüpdate.

Voor het RAA zijn de proces ondersteunende applicaties wel belangrijk, maar niet cruciaal. Mocht een applicatie niet meer werken, dan zijn er andere tools die de leemte op kunnen vullen of kan het werk met de hand worden uitgevoerd.

2.3 De continuïteit van de dienstverlening

Het vorige hoofdstuk gaf een definitie van wat het e-depot is. Naast techniek, zijn er andere elementen te onderscheiden die ook deel uitmaken van de e-depotoplossing van het RAA. Valt een van deze elementen om, dan is de continuïteit van het e-depot in het geding. Het beheer van deze elementen is benoemd in de bovengenoemde verantwoordelijkheden 4, 5 en 6. Deze verantwoordelijkheden benoemen expliciet de randvoorwaarden die nodig zijn om het e-depot en de dienstverlening rondom het e-depot, draaiende te houden.

Deze randvoorwaarden zijn door het RAA ondervangen door het maken van afspraken. Deze afspraken zijn vervolgens vastgelegd in beleid. Onderstaande beleidsdocumenten staan elders opgeslagen en zijn openbaar beschikbaar zodat iedereen die geïnteresseerd is, de stukken kan lezen. Daarom is hieronder alleen een lijst opgenomen van de stukken waar het om gaat.

- Preserveringsbeleid <link>
- Aansluitvoorwaarden <link>
- Stappenplan aansluitingen <link>
- Informatiebeveiligingsplan <link>
- Informatieanalyse <link>
- Parkeerprocedure <link>

Bovenstaande stukken gaan voornamelijk in op de eisen die aan de informatieobjecten worden gesteld, voordat ze opgenomen kunnen worden in het e-depot. Zo geven de aansluitvoorwaarden weer hoe een export er uit moet zien en het Stappenplan op welke wijze aan opname in het e-depot wordt gerealiseerd. Het preserveringsbeleid geeft weer wat er met de informatieobjecten gebeurt tijdens en na opname in het e-depot. Het Informatiebeveiligingsplan laat op zijn beurt zien hoe het RAA omgaat met informatiebeveiliging zoals staat omschreven in de BIO (2019). In de parkeerprocedure staat uitgelegd hoe informatieobjecten worden veiliggesteld op het moment dat nog niet helemaal duidelijk is hoe deze in het e-depot opgenomen moeten worden, of wanneer een extra bewerkingsslag nodig is om dit voor elkaar te krijgen.

Afwijken van de voorwaarden

Het kan voorkomen dat tijdens de informatieanalyse of tijdens het bewerken van de informatieobjecten, duidelijk wordt dat niet kan worden voldaan aan de eisen die normaliter aan een informatieobject worden gesteld om opname in het e-depot mogelijk te maken. Ook kan naar voren komen dat het niet wenselijk is om helemaal te voldoen aan de gestelde eisen, omdat hiermee waardevolle informatie verloren gaat. In dergelijk gevallen wordt gekeken of het mogelijk is om het informatieobject alsnog op te nemen in het e-depot en wat er dan nodig is om de duurzame toegankelijkheid te garanderen (bijvoorbeeld op welke wijze kan het informatieobject worden uitgelezen en welke vorm heeft het dan). Mocht een afwijking vaker voorkomen, dan worden uitgangspunten en keuzes rondom het accepteren van deze afwijking opgenomen in het betreffende beleid.

Wanneer blijkt dat een afwijking ervoor zorgt dat een informatieobject niet opgenomen kan worden in het e-depot, dan zal gekeken worden of er toch aanpassingen worden gedaan om het informatieobject opneembaar te maken. Wijzigingen hieromtrent worden bijgehouden in de metadata en zijn daarmee terugvindbaar.

2.4 Continuïteit van de duurzame toegankelijkheid

Het RAA stelt niet alleen eigen beleid op, maar probeert ook zo veel mogelijk aan te sluiten op landelijke standaarden. Op dit moment conformeert het RAA zich aan:

- Het **OAIS-model** voor de inrichting van het e-depot en de werkprocessen rond opnamen van informatie objecten in het e-depot.
- De **Handreiking voorkeursformaten** van het Nationaal Archief, om de bestandsformaten van de op te nemen informatieobjecten te standaardiseren.
- Het **Toepassingsprofiel metadata lokale overheden** (TMLO) wordt door het RAA ingezet als standaard metadatamodel.
- Naast het TMLO, maakt het RAA ook gebruik van **TopX** om de informatieobjecten inclusief de metadata in het e-depot op te kunnen nemen. TopX is de machineleesbare variant van het TMLO, waarvoor de XML-syntaxis wordt gebruikt.

Door te conformeren aan deze standaarden, ondervangt het RAA de verantwoordelijkheid nummer 4, en maakt het voor de zorgdrager mogelijk om verantwoordelijkhedennummer 1 en 2 , zoals beschreven in paragraaf 1.1, uit te voeren. Met andere woorden, door te conformeren aan deze landelijke standaarden schept het RAA duidelijkheid en eenduidigheid over de manier waarop born digital informatieobjecten door de aangesloten organisaties, gestructureerd en gemetadateerd moeten worden om een eenvoudige opname in het e-depot te kunnen realiseren. Daarnaast zorgen

deze standaarden ervoor dat de duurzame toegankelijkheid op de informatieobjecten na opname is gewaarborgd, en dat de data als geheel overgeplaatst kunnen worden naar een andere e-depotvoorziening mocht dit nodig zijn.

Het RAA is zich ervan bewust dat standaarden en handreikingen veranderen. Daarom houdt het RAA ontwikkelingen hieromtrent bij en onderzoekt op welke manier wijzingen consequenties hebben voor of toegepast kunnen worden op het e-depot. Op het moment van schrijven in de opvolger van het TMLO, het MDTO, vastgesteld. Het RAA is bezig om in kaart te brengen wat de gevolgen zijn voor het RAA en in het verlengde daarvan het e-depot wanneer deze nieuwe handreiking zal worden geïmplementeerd.

2.4 De continuïteit van kennis, mensen en middelen

Techniek en dienstverlening zijn twee aspecten binnen de definitie van het e-depot waar het RAA de continuïteit al zo veel mogelijk heeft geborgd. Deze aspecten kunnen echter geen doorgang vinden wanneer er een tekort is aan kennis, mensen en middelen. Als organisatie heeft het RAA al vroeg de basis gelegd om digitalisering, en in het verlengde daarvan het e-depot, goed in te bedden in de organisatie. De afgelopen jaren is het e-depot daarom consequent meegenomen in de begroting en is er regelmatig gekeken of er behoefte is aan versterking binnen het team dat het e-depot ontwikkeld en de aansluitingen op het e-depot realiseert.

Aan het inbedden van de mensen en middelen, liggen de volgende documenten ten grondslag:

- **Meerjarenbeleidsplan RAA**: het RAA stelt eens in de drie jaar een meer jaren beleidsplan op. Dit document zet de visie en de uitgangspunten van de werkzaamheden van het RAA op een rijtje. Het meerjarenbeleidsplan geeft ook de uitgangspunten weer rond digitalisering van archieven en de voorzieningen die daarvoor nodig zijn. Hierbij krijgt het e-depot een plek binnen die visie, samen met de mensen en middelen die daarvoor nodig zijn.
- **Meerjarenbegroting RAA**: de meerjarenbegroting bekijkt over meerdere jaren op basis van welke uitgangspunten de financiële middelen van het RAA ingezet gaan worden. Op deze manier is over een langere periode gegarandeerd dat er financiële middelen zijn gereserveerd voor de het e-depot en voor de dienstverlening die daaraan gelieerd is.
- **Jaarlijkse begroting RAA**: naast een meerjarenbegroting, wordt er door het RAA ook een jaarlijkse begroting opgesteld. Ook hierin wordt vastgelegd hoeveel digitale dienstverlening gaat kosten en hoeveel financiële middelen er nodig zijn voor het e-depot en de dienstverlening daar omheen.

Het behoud van kennis als het gaat om de inrichting van het e-depot en andere concepten die te maken hebben met de duurzame toegankelijkheid van digitale informatieobjecten, is minder makkelijk te vatten in beleid. Het RAA heeft daarom als uitgangspunt dat kennisdeling van fundamenteel belang is voor de doorontwikkeling van de e-depotvoorziening en voor het garanderen van de duurzame toegankelijkheid van de informatieobjecten die in het e-depot zijn opgenomen.

Kennis vergaren en –delen wordt op de volgende manieren gedaan:

- **Monitor Digitale Informatie**: de monitor digitale informatie (MDI) is in het leven geroepen in het kader van de ingebruikname van het e-depot. Bij het RAA was er geen zicht op de hoeveelheid digitale informatie die zich binnen de gemeenschappelijke regeling bevindt. Dit

betekende dat het lastig werd om in te schatten wat voor datasets in het e-depot geplaatst zouden gaan worden. De monitor is een vragenlijst die om het jaar bij de organisaties wordt uitgezet. Hierin nemen de organisaties ten minste op welke digitale informatie er voor overbrenging in aanmerking komt en welke informatie mogelijk als risico wordt gezien. Op basis hiervan gaat het RAA met de organisaties in gesprek om te kijken waar het RAA mogelijk een oplossing kan bieden.

- **Gebruikersoverleg Picturae Archivematica gebruikers**: twee keer per jaar vindt er een overleg plaats met alle gebruikers van de e-depotsoftware die door Picturae wordt geleverd en ondersteund. Tijdens dit overleg houden gebruikers elkaar op de hoogte en worden ze ingelicht door de leverancier over nieuwe releases en toekomstige ontwikkelingen. Naast het algemene overleg zijn er ook verschillende werkgroepen opgericht rond ontwikkelwensen van de gebruikers. Deze werkgroepen werken de ontwikkelwensen verder uit en gaan in overleg met Picturae over de daadwerkelijke ontwikkeling en implementatie. Uitgangspunt hier is dat het samen laten ontwikkelen van oplossingen kosten en tijd bespaart, evenals meer gewicht geeft aan de wensen die er zijn.
- **Kennissessies met andere archiefinstellingen**: het RAA neemt regelmatig contact op met collega archiefinstellingen om kennis en ervaring te delen. Soms zijn de onderwerpen breed, maar soms gaat het ook om specifieke vragen en ontwikkelingen waar het RAA op dat moment mee te maken heeft.
- **Opleiden van medewerker**s: medewerkers binnen het RAA krijgen de ruimte om zichzelf door te ontwikkelen in het vakgebied en om de meest recente ontwikkelingen bij te houden. Zo is het mogelijk om cursussen te doen waarbij op een specifieke ontwikkeling wordt ingezoomd om een volledige opleiding te volgen om kennis te vergaren danwel bij te spijkeren. Binnen het vakgebied worden ook webinars aangeboden en ook hier nemen medewerkers van het RAA aan deel.

3. Verantwoording en uitwerking van het beleid

3.1 Verantwoordingsmechanismen

In de voorgaande paragrafen is vastgelegd welke afspraken het RAA heeft gemaakt en heeft opgenomen in verschillende beleidsstukken als het gaat om het garanderen van de continuïteit van het e-depot en de bijbehorende dienstverlening. Naast het beleid is er ook een stuk planvorming en uitvoer. Beide aspecten kennen een verantwoordingsmechanisme welke hier onder is beschreven;

- **Algemeen bestuur (AB)**: een keer per jaar vindt er een vergadering plaats van het algemeen bestuur. Tijdens dit overleg wordt er een update gegeven van de stand van zaken rond het e-depot. Met deze stand van zaken wordt er verantwoording afgelegd over eventuele afwijkingen, worden successen gecommuniceerd en geeft het AB goedkeuring op de voorgenomen ontwikkelingen.
- **Jaarrekening:** 1 keer per jaar maakt het RAA een jaarrekening op. Hierin staat beschreven wat er met de budgetten is gebeurd die voor de verschillende taken van het RAA zijn gereserveerd. Het e-depot is apart opgenomen in deze jaarrekening. De jaarrekening wordt gepresenteerd aan het AB, die op- of aanmerkingen kan plaatsen en de jaarrekening vaststelt.
- **Verantwoording richting gebruikers**: de gebruikers van het e-depot zijn uitsluitend organisaties die vallen binnen het werkgebied van het RAA. Op verschillende manieren worden de organisaties op de hoogte gehouden van de ontwikkelingen en worden ze betrokken bij de opname van datasets in het e-depot. Zo wordt er eens in de 8 weken een nieuwsbrief rondgestuurd, vindt er twee keer per jaar een algemene bijeenkomst plaats en wordt er een á twee keer per jaar een bezoek afgelegd om met de organisaties afzonderlijk en persoonlijk over het e-depot te praten.

3.2 Uitwerking van het beleid

Naast het hebben van beleidsuitgangspunten, is het zaak om handen en voeten te geven aan het beleid. Uiteindelijk is het de bedoeling dat dit beleid aan de basis staat van de continuïteit van de e-depotvoorziening van het RAA. Om dit te realiseren zijn er verdere plannen en procedures nodig die meer in detail beschrijven wat er moet gebeuren op het moment dat er discontinuïteit optreedt. Hieronder is beschreven in welke producten de concretisering van het beleid vorm krijgt of al heeft gekregen.

Het continuïteitsplan

In het continuïteitsplan worden de verschillende bedreigingen en risico's beschreven die zich bij de zorgdragers, de beheerorganisatie of de leverancier voor kunnen doen. In het stuk wordt tevens aangegeven waar maatregelen moeten worden getroffen om de bedreiging zo goed mogelijk te kunnen voorkomen en welke maatregelen al getroffen zijn. Daarmee is het continuïteitsplan een stuk dat handen en voeten geeft aan het continuïteitsbeleid door te beschrijven hoe de uitgangspunten daadwerkelijk zijn uitgewerkt of worden uitgevoerd.

Het e-depotcontract

Het RAA is een gemeenschappelijke regeling waarbij tien gemeenten en drie gemeenschappelijke regelingen zijn aangesloten. De gemeenschappelijke regeling is juridisch opgetekend in een overeenkomst die geldt voor alle aangesloten organisaties. Binnen deze regeling zijn er nagenoeg geen voorzorgsmaatregelen opgenomen met betrekking tot specifieke zaken zoals een e-depot. De afspraken die zijn gemaakt betreffen de diensten die het RAA in zijn algemeenheid levert en gaan niet specifiek in op deelaspecten hiervan. Er is daarom besloten om met alle organisaties die aansluiten op het e-depot een aanvullend e-depotcontract af te sluiten dat betrekking heeft op het beheer van de informatieobjecten in het e-depot. Dit kan aangepast worden afhankelijk van waar het e-depot voor wordt gebruikt.

Het RAA heeft in 2020 een e-depotcontract opgesteld dat als basis kan dienen voor verschillende soorten overeenkomsten. Zo kan deze worden aangepast zodat hij gaat gelden voor te vernietigen of te bewaren informatieobjecten, of voor overgedragen of uitgeplaatste informatieobjecten. Belangrijk bij alle e-depotcontracten, onafhankelijk waar ze betrekking op hebben, is dat verantwoordelijkheden over en weer goed worden vastgelegd. Dit is ook belangrijk in het kader van de AVG.

Ook organisaties die geen onderdeel uitmaken van de gemeenschappelijke regeling kunnen ervoor kiezen om over te brengen informatieobjecten onder te brengen in het e-depot van het RAA. Voor deze organisaties zal een aangepaste versie van het e-depotcontract worden opgesteld. Elementen die bij aangesloten organisaties in de gemeenschappelijke regeling zijn vastgelegd, zullen bij niet-aangesloten organisaties worden opgenomen in het e-depotcontract.

Service Level Agreement E-depot

De Service Level Agreement (SLA) is al genoemd in hoofdstuk als een van de documenten waarmee de technische continuïteit van het e-depot wordt gegarandeerd. In dat hoofdstuk wordt verwezen naar de algemene SLA die het RAA en Picturae hebben ondertekend. Naast deze algemene SLA, wordt er op het moment van schrijven een specifieke SLA opgesteld door Picturae die het e-depot en de dienstverlening van Picturae daaromheen, betreft. In deze SLA wordt meer ingegaan op de doorontwikkeling van Archivematica, de ondersteuning die het RAA mag verwachten daarin en ondersteuning als het gaat om calamiteiten. Hierbij wordt voornamelijk technische storingen of een aanval van hackers bedoeld.

Toetsing van de leverancier

Een extra maatregel die het RAA hanteert om de continuïteit de garanderen als het gaat om bedreigingen met betrekking tot de leverancier, is toetsing. De beheerorganisatie toetst zelf of de leverancier voldoet en blijft voldoen aan de afspraken die zijn vastgelegd in de SLA. Hoe deze

toetsing wordt uitgevoerd en op welke punten er wordt getoetst, is opgenomen in het calamiteitenplan. In de bijlage 1 is een lijst opgenomen die als uitgangspunt dient om de geleverde diensten van de leverancier te kunnen toetsen.

Exit-strategie

Wanneer er eenmaal voor een e-depotoplossing is gekozen, dan is deze keuze niet in beton gegoten. Een van de onderdelen bij de aanbesteding van de vraag naar dataportabiliteit, oftewel is het mogelijk om de reedsopgenomen informatieobjecten in het e-depot op te pakken en in een andere oplossing te plaatsen. Om dit voor elkaar te krijgen is er meer nodig dan alleen een vinkje bij de aanbesteding. Om een goede overgang naar een nieuwe oplossing mogelijk te maken, is een exit-strategie nodig. In bijlage 2 staat opgesomd waar een exit-strategie aan moet voldoen om het risico op informatieverlies zo veel mogelijk te beperking.

Procedures en werkbeschrijvingen

Dit continuïteitsbeleid is geschreven op een moment dat het e-depot, en alles wat erbij komt kijken, nog in een beginfase staat. Er is daarom op dit moment nog maar weinig bekend over mogelijke calamiteiten en wat eraan gedaan kan worden. Mocht een calamiteit zich voordoen, dan het RAA zoveel mogelijk op de huidige kennis en ervaring handelen om de calamiteit zo snel mogelijk het hoofd te bieden. Dit betekent dat op basis van voortschrijdend inzicht en verdere ervaringen onderdelen van dit beleid en van de uitvoer van dit beleid, verdere stukken zullen worden opgesteld. Het RAA onderkent verschillende bedreigingen en de risico's die daaruit volgen. Deze, samen met de reeds getroffen maatregelen, zijn verder uitgewerkt in een continuïteitsplan.

Bijlage 1 Lijst toetsingselementen leverancier

1. Naleving van wet- en regelgeving

- Voldoet de leverancier aan wet- en regelgeving? Kan de leverancier hieraan voldoen of moeten hiervoor aanvullende zaken geregeld worden?
- De leverancier moet kunnen aantonen dat hij en zijn eventuele partners aan de geldende eisen voldoen.

2. Beheersbaarheid van processen en systemen

- Voldoet de leverancier aan de beveiligingseisen die in de eigen organisatie gelden?
- De beheerorganisatie blijft verantwoordelijk voor de systemen en processen en moet daarom in staat zijn vast te stellen of dit op de juiste wijze is ingevuld door de leverancier; recht op audit. Moet in staat zijn om vast te stellen of de processen en de systemen op een juiste wijze zijn ingevuld.
- Zijn de beheerprocessen bij de leverancier afdoende ingericht?
- Disaster recovery plan; back-upstrategie; periodiek testen van recovery.
- Goedkeuringsproces voor wijzigingen; voldoende testen van wijzigingen voordat ze in productie worden genomen; werken met fallbackscenario om wijzigingen terug te kunnen draaien; detectie van kwetsbaarheden; uitvoeren securityscans; toegangsbeheer; audittrails en logging.

3. Gegevensbescherming

- Is controleerbaar of verwerking van gegevens plaatsvindt op een veilige en legale manier, conform geformuleerde eisen?
- Opgeslagen of verwijderde gegevens zijn niet toegankelijk voor derde partijen; opslag alleen in afgesproken rechtsgebieden; beveiliging van gegevenstransport; verificatie van correcte overdracht; permanente verwijdering van alle voor vernietiging in aanmerking komende informatie.
- Hoe zit het met weerbaarheid tegen gijzelsoftware en hacken?

4. Overdracht

- Is portabiliteit aantoonbaar gegarandeerd?
- Het gebruik van standaardtechnologieën en –oplossingen (richtlijnen afspreken).
- Eigenaarschap en toegang tot gegevens bij overname of faillissement (escrowregeling; oprichten van een stichting).

Bijlage 2: Opzet exitstrategie

Een exit-strategie moet zowel een migratie naar een andere leverancier als naar de interne ICT-omgeving van het de beheerorganisatie beschrijven. Om een exit uit te kunnen voeren is het noodzakelijk om intern kennis op te bouwen en te behouden over de dienst.

Ten minste opnemen in de exitstrategie (zo helder en gedetailleerd mogelijk beschrijven):

- Reikwijdte en duur van de ondersteuning die de leverancier gaat leveren aan de transitie.
  - Plan met beschrijving benodigde tijd, taken en verantwoordelijkheden voor een overdracht.
  - Voor een goede overgang moet de leverancier bereid zijn samen te werken met de afnemer en eventuele andere leveranciers en bereid zijn de service voor een bepaalde tijd te continueren na beëindiging.

- Afspraken over de kosten of de kostenverdeling voor de ondersteuning vanuit de leverancier aan de beheerorganisatie.
  - Kosten die in rekening gebracht worden in verband met afschrijving van investeringen dienen elk jaar verlaagd te worden (vraag of dat hier aan de orde is).
  - Wanneer de dienstverlening door de leverancier wordt beëindigd dan is een export kosteloos.

- Afspraken over de wijze waarop de data worden overgedragen.
  - Eisen aan hoe de data beschikbaar komen (bijvoorbeeld: platform onafhankelijk formaat; drager).
  - De export moet zo geschieden dat alle contextinformatie die nodig is om een nieuwe import mogelijk te maken en om de authenticiteit van de data vast te stellen onderdeel van de export zijn.
  - Afspraken maken over wie e export uit kan voeren/uit gaat voeren en wat de kosten zijn.

- De data worden tijdens een export op geen enkele manier gewijzigd
- Afspraken over vernietiging van gegevens bij de leverancier na overdracht.
- Afspraken over overname van bezittingen of contracten met derden die de afnemer nodig heeft om de dienst te kunnen (laten) continueren.
  o Wat en tegen welke kosten?
  o Wat gebeurt er met software en diensten die met andere klanten worden gedeeld?

- Afspraken over mogelijkheden tot inhuur van het personeel dat de dienst heeft geleverd.

- Verplichting van de leverancier om kennis over de diensten over te dragen (wat gebeurt er met specifieke IP voor het leveren van de dienst?).

- Verplichting voor beide partijen om periodiek het exitstrategie te controleren en te updaten gedurende de looptijd.