E-depot Achterhoek

Continuïteitsplan

2015

Werkgroep Continuïteitsplan

- Monique Dekker (Waterschap Rijn en IJssel)
- Eleonore Manning (Erfgoedcentrum Achterhoek en Liemers)
- Wouter Oenema (gemeente Doetinchem)
- Hans Mannaert (DiVault)
- Marian van de Wetering (gemeente Lochem)

Deelnemende partijen

Inhoud

Managementsamenvatting

Doel

Dit document is een kennisproduct dat vervaardigd is als onderdeel van het project E-depot Achterhoek. Het doel van het continuïteitsplan is het geven van een overzicht van de regelingen die nodig zijn om de digitale archiefbescheiden in het e-depot te beveiligen tegen bedreigingen.

Een bedreiging of calamiteit is een (on)gewenste gebeurtenis die zodanige negatieve gevolgen heeft, dat de voortgang van de vitale bedrijfsprocessen van het e-depot wordt verstoord en de dienstverlening niet kan worden voortgezet.

Het kunnen bedreigingen zijn die voorkomen bij alle partijen die deel uitmaken van het e-depot: de beheerorganisatie, de zorgdrager (aanbieder) en de leverancier van de e-depot-bewaaromgeving. Het kunnen geplande en ongeplande bedreigingen zijn.

Aanpak

Er is een overzicht gemaakt van de bedreigingen en calamiteiten die de voortgang en dienstverlening van het e-depot kunnen verstoren. Per bedreiging is geïnventariseerd wat de afzonderlijke risico's zijn voor de beheerorganisatie, zorgdrager en leverancier. Per risico is een categorie en factor bepaald en vastgelegd hoe we het risico kunnen beperken. We hebben beschreven waarin (Gemeenschappelijke Regeling, Archiefverordening of Contract-leverancier) en hoe de te nemen maatregelen en acties moeten worden vastgelegd. Ook is er bepaald voor welke maatregelen de beheerorganisatie, de zorgdrager en de leverancier verantwoordelijk zijn en wie ze uitvoert.

Conclusie en aanbevelingen

Het continuïteitsplan is een tactisch plan waarin we maatregelen en acties beschrijven die nadere operationele uitwerking vragen in de overeenkomsten die de e-depotpartners sluiten en de plannen die ze opstellen.

De werkgroep adviseert de maatregelen op te nemen in:
- de Gemeenschappelijke Regeling tussen zorgdragers en beheerorganisatie;
- de Archiefverordening van de afzonderlijke zorgdragers;
- het contract (SLA) tussen de leverancier en de beheerorganisatie.

Door het ontbreken van uitgebreide juridische en (inkoop) technische kennis binnen de werkgroep zijn de beschreven maatregelen niet in detail uitgewerkt voor de bovengenoemde regelingen.

De werkgroep adviseert:
- na vaststelling van het continuïteitsplan juristen en inkopers te vragen om de voorgestelde maatregelen verder uit te werken in de bovengenoemde regelingen.
- voor de continuïteit van het e-depot onderzoek te doen naar de mogelijke consequenties van de verschillende soorten overeenkomsten tussen zorgdragers en beheerorganisatie;
- de brancheverenigingen Archiefinstellingen Nederland (BRAIN) te verzoeken de Model Archiefverordening aan te passen aan de inrichting en het gebruik van e-depots.

1 Algemeen

Dit document is een kennisproduct dat vervaardigd is als onderdeel van het project E-depot Achterhoek.

1.1 Doel continuïteitsplan

De opdracht voor dit kennisproduct is in het projectplan E-depot Achterhoek als volgt beschreven:

Continuïteitsplan: na dit project moet duidelijk zijn welke eisen gesteld moeten worden aan een e-depot en de leverancier om overstappen mogelijk te maken, bijvoorbeeld bij calamiteiten, faillissement of beëindiging van een samenwerking.

In de beschrijving van de opdracht wordt alleen gesproken over het mogelijk maken van 'overstappen': de 'exit-strategie'. In Eisen Duurzaam Digitaal Depot (ED_3)[1] wordt een bredere definitie van een continuïteitsplan gegeven, namelijk: Een continuïteitsplan regelt hoe de beheerorganisatie de opgenomen archiefbescheiden veilig kan stellen.

Na discussie binnen de werkgroep en overleg met de projectgroep en de opdrachtgever is besloten het volgende uitgangspunt te hanteren voor het continuïteitsplan:

Het continuïteitsplan beschrijft wat er geregeld moet worden om de opgenomen archiefbescheiden veilig te stellen tegen bedreigingen. Dit kunnen bedreigingen zijn die voorkomen bij alle partijen die deel uitmaken van het e-depot: de externe leverancier van de e-depotbewaaromgeving, de beheerorganisatie en de zorgdrager. Het kunnen geplande (bijv. taakoverdracht) en ongeplande (bijv. faillissement of storingen) bedreigingen zijn.

Een bedreiging of calamiteit is een (on)gewenste gebeurtenis die zodanige negatieve gevolgen heeft, dat de voortgang van de vitale bedrijfsprocessen van het e-depot wordt verstoord en de dienstverlening niet kan worden voortgezet.

1.2 Scope

Het continuïteitsplan beschrijft niet hoe de beheerorganisatie het e-depot moet beheren. De uitwerking van dat beleid staat in de kennisproducten 'Bewaar en beheerstrategie E-depot Achterhoek' en 'Beschikbaarstelling E-depot Achterhoek'. De uitvoering van het beleid wordt regelmatig getoetst, zie kennisproduct 'Toetsingskader E-depot Achterhoek'.

Het continuïteitsplan beschrijft niet aan welke eisen de aanbieder moet voldoen bij het aanleveren van archieven, zie hiervoor kennisproduct 'Toepassingsprofiel E-depot Achterhoek'. Het continuïteitsplan is ook geen beveiligingsplan, ontruimingsplan of bedrijfsnoodplan. Het continuïteitsplan beschrijft wat er geregeld moet worden om de opgenomen archiefbescheiden veilig te stellen tegen bedreigingen. Het is een tactisch plan waarin we maat-

1 Eisen Duurzaam Digitaal Depot (ED_3), versie 2 december 2012 van de Landelijke Vereniging van Provinciale Archiefinspecteurs (LOPAI).

regelen en acties beschrijven die nadere operationele uitwerking vragen in de door de e-depotpartners te sluiten overeenkomsten en op te stellen plannen.

1.3 Leeswijzer

In hoofdstuk 2 is een overzicht opgenomen van mogelijke bedreigingen aan de kant van de zorgdrager, de beheerorganisatie en de IT-leverancier. Hierin zijn tevens de verschillende risico's opgenomen. Ook wordt beschreven waarin te nemen maatregelen en acties moeten worden vastgelegd.

In hoofdstuk 3 gaan we uitvoeriger in op de te nemen maatregelen om bedreigingen te beperken. Daarbij gaan we in op de acties die moeten worden uitgevoerd na een calamiteit. De vraag 'wat kan waar en door wie worden geregeld en welke kwetsbaarheden blijven?' staat hierin centraal.

In hoofdstuk 4 gaan we in op de vraag: wanneer en door wie moet het continuïteitsplan in werking worden gesteld?

2 Bedreigingen en risico's E-depot Achterhoek

Het e-depot is 'het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer, databeveiliging en aanwezige hard- en software dat duurzaam beheren en raadplegen van digitale archiefbescheiden mogelijk maakt'.

De vitale bedrijfsprocessen van het e-depot zijn:
- opname van archiefbescheiden;
- duurzaam beheer van archiefbescheiden;
- beschikbaar stellen van archiefbescheiden;
- bedrijfsvoeringprocessen.

Om de 'normale' continuïteit van deze processen te borgen, is een aantal kennisproducten opgesteld. Dit zijn het Toepassingsprofiel met eisen aan de op te nemen archiefbescheiden, het Toetsingskader, het vastgestelde beleid in de kennisproducten Beheer- en bewaarstrategie en Beschikbaarstelling, het Architectuuroverzicht en het inzicht in de financiële consequenties (Kostenoverzicht).

Daarnaast moet ook de continuïteit van de vitale processen bij bedreigingen worden gewaarborgd. Dit zijn vragen die gesteld kunnen worden.
- Welke bedreigingen of calamiteiten kunnen voorkomen?
- Welke risico's lopen de verschillende partners bij het e-depot?
- Wat kan/moet er geregeld worden om bedreigingen te beperken en welke acties moeten worden uitgevoerd na een calamiteit?

In de tabel hieronder beschrijven we de verschillende bedreigingen die kunnen voorkomen bij de partners van het e-depot. Ook wordt in het kort aangegeven waar maatregelen (acties) moeten worden opgenomen om de bedreiging te kunnen beperken. Daarbij gaan we in op uit te voeren maatregelen na een calamiteit. Op deze maatregelen en acties gaan we in hoofdstuk 3 uitvoeriger in.

Als partners van het e-depot worden onderscheiden:
- ZD: De zorgdrager: aanbieder en ook gebruiker van de op te nemen archiefbescheiden.
- BO: De beheerorganisatie.
- LC: De IT-leverancier: de ondernemer en leverancier van de bewaaromgeving.
- Gebruikers (burgers en bedrijven): risico's m.b.t. beschikbaarheid van de archiefbescheiden voor de gebruiker zijn beschreven bij de risico's voor de zorgdrager in zijn rol als gebruiker.

Per bedreiging is aangegeven welk soort risico de bedreiging oplevert en hoe hoog dit risico wordt ingeschat (weging). We maken een onderscheid tussen de volgende risico's[2].

2 Indeling overgenomen van: Concept Ontwerpselectielijst voor gemeenten en intergemeentelijke organen 2016 v0.9

- Bestuurlijk-politiek risico (BP): het potentiële nadeel dat de organisatie ondervindt in de kwaliteit van sturing van de organisatie en de publieke verantwoording over de hierover genomen beslissingen.
- Operationeel risico (O): het potentiële nadeel dat de organisatie ondervindt in de kwaliteit en mogelijkheden van de uitvoering van de door de organisatie gestelde doelen.
- Juridisch risico (J): het potentiële nadeel dat de organisatie ondervindt, doordat de belangen van de organisatie niet behartigd kunnen worden in geschillen met derde partijen.
- Financieel risico (F): het potentiële nadeel dat de organisatie ondervindt in de vorm van extra uitgaven, kosten of de vermindering van inkomsten.

De weging van het risico is op basis van kans * impact:

Kans/Impact	Klein (1)	Middel (2)	Groot (3)
Klein (1)	Zeer laag (1)	Laag (2)	Middel (3)
Middel (2)	Laag (2)	Middel (4)	Hoog (6)
Groot (3)	Middel (3)	Hoog (6)	Zeer hoog (9)

3 Maatregelen en acties om bedreigingen te voorkomen

Het continuïteitsplan beschrijft wat er geregeld moet worden om de opgenomen archiefbescheiden veilig te stellen tegen bedreigingen. Het is een tactisch plan waarin we maatregelen en acties beschrijven die nadere operationele uitwerking vragen in de door de e-depotpartners te sluiten overeenkomsten.

Hierna beschrijven we per overeenkomst welke maatregelen en acties verder moeten worden uitgewerkt.

De opstellers van het continuïteitsplan hebben onvoldoende juridische en inkooptechnische kennis om de maatregelen en acties helemaal zelf uit te werken.
Het is raadzaam om na het vaststellen van het continuïteitsplan hiervoor advies te vragen aan juristen en inkopers van de pilotorganisaties.

3.1 Gemeenschappelijke regeling

Het uitgangspunt voor dit continuïteitsplan is dat tussen alle zorgdragers en de beheerorganisatie een Gemeenschappelijke Regeling wordt afgesloten. Op dit moment zijn er ook zorgdragers die met de beheerorganisatie een Dienstverleningsovereenkomst (DVO) hebben afgesloten.

Geadviseerd wordt om – voor de continuïteit van het e-depot – onderzoek te doen naar de mogelijke consequenties van de verschillende soorten overeenkomsten tussen zorgdragers en beheerorganisatie.

In de Gemeenschappelijke Regeling tussen de zorgdragers en de beheerorganisatie moeten voorwaarden worden opgenomen over de volgende onderwerpen:

In geval van opheffing, samenvoeging of splitsing beheereenheid van een zorgdrager

ZD Eigenaarschap niet duidelijk
Toegang niet geregeld (nieuwe archiefvormende beheereenheid)
BO Vaste kosten gelijk t.o.v. minder volume
LC Continuïteit leverancier niet zeker

Omdat alleen een beheereenheid[4] bij een zorgdrager kan worden opgeheven, samengevoegd (met een andere beheereenheid) of gesplitst, blijft de zorgdrager dezelfde. Een gevolg kan zijn dat toegangsrechten moeten worden gewijzigd. Ook moet de nieuwe organisatie van de zorgdrager worden vastgelegd voor nieuw over te brengen archiefbescheiden.

Voor de beheerorganisatie en de leverancier kan het opheffen van een beheereenheid (opheffen taak) financiële consequenties hebben. Er zullen minder archiefbescheiden worden aangeboden.

4 Model Archiefverordening BRAIN:
Beheereenheid is een door burgemeester en wethouders als zodanig aan te wijzen organisatieonderdeel, zelfstandig belast met de documentaire informatievoorziening.

Bij opname van te vernietigen archiefbescheiden moet vastgelegd worden wie verantwoordelijk is voor al opgenomen, nog te vernietigen archiefbescheiden.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:
- de zorgdrager verantwoordelijk is voor het tijdig melden van wijzigingen in toegang tot en het beheer van de al opgenomen archiefbescheiden;
- de zorgdrager verantwoordelijk is voor eventuele financiële consequenties van de wijziging.

Overdracht van één of meer taken van een zorgdrager aan een ander overheidsorgaan of rechtspersoon

ZD Eigenaarschap niet duidelijk
Toegang niet geregeld
Nieuw archiefvormend overheidsorgaan of rechtspersoon
BO Vaste kosten gelijk t.o.v. minder volume
LC Continuïteit leverancier niet zeker

Als taken worden overgedragen aan een ander overheidsorgaan of rechtspersoon die geen partner is van het e-depot, moet eventueel toegang worden geregeld voor al overgebrachte archiefbescheiden. Ook moeten verwijzingen worden opgenomen naar archiefbescheiden van het andere overheidsorgaan of rechtspersoon.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:
- afspraken moeten worden vastgelegd over het eigenaarschap van en toegang tot de al overgebrachte archiefbescheiden en mogelijke wijzigingen daarin;
- de latende zorgdrager verantwoordelijk is voor eventuele financiële consequenties van de wijziging (ook bijv. afkoop indien alle taken worden stopgezet bij opheffing zorgdrager).

Aandachtspunten:
- Wat als dit aan het einde van de looptijd van de Gemeenschappelijke Regeling gebeurt?
- Wat als de nieuwe zorgdrager een ander e-depot aanwijst?

Opheffen beheerorganisatie

ZD Geen beheeromgeving
Kennisverlies over beheer e-depot
Geen toegang
LC Continuïteit leverancier niet zeker

Bij het opheffen van de beheerorganisatie moet een andere beheerorganisatie alle taken en de gehele dienstverlening overnemen. Het kan zijn dat niet alle partners kiezen voor dezelfde nieuwe beheerorganisatie. Ook het contract met de leverancier vervalt bij opheffing van de beheerorganisatie.

In de Gemeenschappelijke Regeling moet worden opgenomen dat een opvolgingsplan (of liquidatieplan) wordt opgesteld waarin:
- duurzame toegang tot en beheer van de archiefbescheiden wordt geregeld;
- de financiële gevolgen van de opheffing in beeld worden gebracht;
- een regeling wordt getroffen om kennisverlies te voorkomen.

Deelname nieuwe zorgdrager(s) aan e-depot

ZD Verminderde dienstverlening.
BO Inrichting beheerorganisatie niet berekend op meer deelnemers
LC Capaciteit leverancier niet toereikend

Nieuwe deelnemers aan het e-depot moeten voldoen aan de voorwaarden tot deelname zoals is vastgelegd in het Toepassingsprofiel. Nieuwe deelnemers betekent een toename van de aangeboden data. De beheerorganisatie en de leverancier moeten hiervoor toegerust zijn.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:

- vóór deelname van nieuwe zorgdragers de organisatorische en financiële consequenties voor de beheerorganisatie en de leverancier in beeld moeten zijn gebracht;
- de dienstverlening voor oude (en nieuwe) zorgdragers op hetzelfde peil moet blijven;
- besluiten tot deelname van nieuwe zorgdragers aan het e-depot door het Algemeen Bestuur worden genomen.

Uittreden zorgdrager(s) uit Gemeenschappelijke Regeling en daarmee uit e-depot

ZD Tekort begroting beheerorganisatie
Hogere bijdrage overblijvende deelnemers
BO Tekort begroting
LC Continuïteit leverancier niet zeker

Het uittreden van zorgdragers uit de Gemeenschappelijke Regeling en het e-depot kan grote financiële consequenties hebben voor de overblijvende partners en de leverancier.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:

- het voornemen tot uittreden tijdig (minimaal een jaar) voor het einde van de looptijd van de Gemeenschappelijke Regeling moet worden gemeld;
- de beheerorganisatie in dat geval de financiële consequenties van het uittreden in kaart brengt en voorlegt aan het Algemeen Bestuur;
- de beheerorganisatie tijdig de IT-leverancier op de hoogte brengt van de voorgenomen wijziging.

Overstap beheerorganisatie naar andere e-depot-leverancier (beëindiging contract)

ZD Verminderde dienstverlening
BO Beschadiging of verlies data door exporteren en importeren
Geen of gebrekkige ondersteuning door voormalige leverancier

Overstap van de beheerorganisatie naar een andere e-depotleverancier kan grote gevolgen hebben voor de beschikbaarheid van gegevens en archiefbescheiden. Dit kan ontstaan door beschadiging of verlies van informatie tijdens het exporteren en het importeren van gegevens in een nieuw e-depotsysteem.

In de Gemeenschappelijke Regeling moeten worden opgenomen dat:

- het voornemen tot beëindiging van het contract met de IT-leverancier tijdig (minimaal 1 jaar voor afloop of beëindiging) moet worden voorgelegd aan het Algemeen Bestuur;
- de beheerorganisatie een plan van aanpak opstelt en voorlegt aan het Algemeen Bestuur voor deze overstap.

Wijzigingen of wensen tot wijzigingen metadata en/of opslagformaten bij zorgdrager of beheerorganisatie

ZD Gebrekkige toegankelijkheid archiefbescheiden
Kosten voor aanpassing koppelingen
BO Gebrekkige beschikbaarstelling archiefbescheiden

Wijzigingen van metadata en/of opslagformaten kunnen grote gevolgen hebben voor de toegang tot en de beschikbaarheid van de archiefbescheiden. Ook kan het invloed hebben op de inrichting van de informatieverwerkende systemen bij de zorgdrager, de koppeling daarvan met het e-depot en de inrichting van het e-depot zelf.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:
- wensen of voornemens tot wijzigingen van metadata en/of opslagformaten moeten worden besproken in het (nog in te richten) SIO[5] en voorgelegd aan het Algemeen Bestuur;
- de beheerorganisatie een impactanalyse opstelt voor de voorgenomen wijziging.

Informatie onvoldoende beveiligd

ZD Ongeoorloofde toegang tot o.a. privacygevoelige informatie of ongeautoriseerde aanpassingen in creatiefase
Beschadiging van archiefbescheiden
BO Ongeoorloofde toegang tot o.a. beperkt openbare informatie
Beschadiging van archiefbescheiden

Onvoldoende beveiliging van de informatie kan ongeoorloofde toegang tot en problemen met de beschikbaarheid van de archiefbescheiden tot gevolg hebben.

In de Gemeenschappelijke Regeling moet worden opgenomen dat:
- de beheerorganisatie verantwoordelijk is voor het hebben en onderhouden van een actueel informatiebeveiligingsplan;
- de beheerorganisatie toeziet dat de IT-leverancier een actueel informatiebeveiligingsplan heeft.

3.2 Archiefverordening

In de archiefverordening van de zorgdrager moet worden opgenomen dat het e-depot is aangewezen als bewaaromgeving van de digitaal te bewaren archiefbescheiden van de zorgdrager.

Ook afspraken over eventuele uitplaatsing van te vernietigen archiefbescheiden moeten in de archiefverordening worden opgenomen.

Geadviseerd wordt om BRAIN te vragen de Model Archiefverordening aan te passen aan de inrichting en het gebruik van e-depots.

In de huidige Model Archiefverordening is opgenomen dat de zorgdrager tijdig mededeling doet aan de archivaris van een aantal wijzigingen. Bij deelname aan een e-depot is het doen van een mededeling onvoldoende, omdat de impact van de wijzigingen groter kan zijn dan in een analoge omgeving. De zorgdrager moet daarom tijdig specifieke informatie verstrek-

5 SIO: Strategisch Informatie Overleg.

ken aan de beheerorganisatie over de wijziging en in overleg met de beheerorganisatie de wijzigingen doorvoeren. Zo nodig moet vooraf een impactanalyse en een implementatieplan worden opgesteld.

Het gaat om de volgende wijzigingen:

Opheffing, samenvoeging of splitsing beheereenheid zorgdrager

ZD Eigenaarschap niet duidelijk
Toegang niet geregeld (nieuwe archiefvormende beheereenheid)
BO Vaste kosten gelijk t.o.v. minder volume
LC Continuïteit leverancier niet zeker

Overdracht van één of meer taken van een zorgdrager aan een ander overheidsorgaan of rechtspersoon

ZD Eigenaarschap niet duidelijk
Toegang niet geregeld
Nieuwe archiefvormend overheidsorgaan of rechtspersoon
BO Vaste kosten gelijk t.o.v. minder volume
LC Continuïteit leverancier niet zeker

Uittreden zorgdrager(s) uit Gemeenschappelijke Regeling en daarmee uit e-depot

ZD Tekort begroting beheerorganisatie
Hogere bijdrage overblijvende deelnemers
BO Tekort begroting
LC Continuïteit leverancier niet zeker

Aanschaf nieuwe informatie verwerkende applicaties (duurzaam te bewaren informatie) door zorgdrager

ZD Kosten voor nieuwe koppelingen
Geen koppeling mogelijk

Wijzigingen of wensen tot wijzigingen metadata en/of opslagformaten bij zorgdrager of beheerorganisatie

ZD Gebrekkige toegankelijkheid archiefbescheiden
Kosten voor aanpassing koppelingen
BO Gebrekkige beschikbaarstelling archiefbescheiden

In de archiefverordening van de zorgdragers moet opgenomen worden dat:

- de zorgdrager verantwoordelijk is voor tijdig informeren van de beheerorganisatie van (het voornemen tot) een wijziging;
- de zorgdrager en beheerorganisatie verantwoordelijk zijn voor het zo nodig opstellen van een impactanalyse en implementatieplan.

3.3 Contract leverancier/Service Level Agreement (SLA)

Voor de beheerorganisatie is van belang om de eisen die zij stelt aan de continuïteit en de kwaliteit van de dienst helder te hebben en deze eisen op te nemen in het contract/SLA met de leverancier. Daarnaast dient de beheerorganisatie afspraken op te nemen die haar in staat stellen om te beoordelen of de leverancier daadwerkelijk voldoet en blijft voldoen aan de afspraken. Hierbij kan gedacht worden aan de volgende zaken.

Naleving van wet- en regelgeving

- Moeten hiervoor aanvullende zaken geregeld worden?
  De leverancier moet aan kunnen tonen dat hij en zijn eventuele partners aan de geldende eisen voldoen.

Beheersbaarheid van processen en systemen

- Voldoet de leverancier aan de beveiligingseisen die in de eigen organisatie gelden?
  De eigenaar blijft verantwoordelijk en moet daarom in staat zijn om vast te stellen of dit op de juiste wijze is ingevuld door de leverancier; recht op audit.
- Zijn de beheerprocessen bij de leverancier afdoende ingericht?
  Disaster recovery plan; backupstrategie; 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.

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 voorkomens bij vernietiging.

Overdracht

- Is portabiliteit aantoonbaar gegarandeerd?
  Gebruik van standaardtechnologieën en –oplossingen (richtlijnen afspreken); eigenaarschap en toegang tot gegevens bij overname of faillissement (Escrow-regeling; oprichten van een stichting).

In het overzicht worden de volgende bedreigingen en risico's genoemd:

Opheffing, samenvoeging of splitsing beheereenheid zorgdrager

LC Continuïteit leverancier niet zeker

Overdracht van één of meer taken van een zorgdrager aan een ander overheidsorgaan of rechtspersoon

LC Continuïteit leverancier niet zeker

Opheffen beheerorganisatie

LC Continuïteit leverancier niet zeker

Deelname nieuwe zorgdrager(s) aan e-depot

LC Capaciteit leverancier niet toereikend

Uittreden zorgdrager(s) uit Gemeenschappelijke Regeling en daarmee uit e-depot

LC Continuïteit leverancier niet zeker

Overstap beheerorganisatie naar ander e-depot-leverancier (beëindiging contract)

BO Beschadiging of verlies data door exporteren en importeren
Geen of gebrekkige ondersteuning door voormalige leverancier

Faillissement leverancier

ZD Eigenaarschap archiefbescheiden kan betwist worden
BO Geen toegang tot of verlies van archiefbescheiden

Overname leverancier

BO Wijziging contractvoorwaarden

Aflopen contract met leverancier (verlenging)

BO Wijziging contractvoorwaarden
Leverancier wil niet verlengen
LC Aanbestedingsprocedure
Wijziging contract
Einde contract

Wijzigingen of wensen tot wijzigingen metadata en/of opslagformaten bij zorgdrager of beheerorganisatie

ZD Gebrekkige toegankelijkheid archiefbescheiden

Verminderde of geen beschikbaarheid archiefbescheiden door storingen of calamiteiten

ZD Informatie niet tijdig beschikbaar
Probleem tijdens uitplaatsen/overbrenging
BO Verstoort de dienstverlening
LC Niet goed voor het imago

Informatie onvoldoende beveiligd

BO Ongeoorloofde toegang tot o.a. beperkt openbare informatie
Beschadiging van archiefbescheiden
LC Niet goed voor het imago

In de Service Level Agreement (en/of contract) tussen de beheerorganisatie en de leverancier moeten daarom afspraken worden opgenomen over de volgende zaken.

- Contractuele afspraken over het te leveren service niveau, beschikbaarheid en kosten.
- Contractuele afspraken over aanpassingen (o.a. beëindiging) van de dienstverlening.
- Contractuele afspraken over onderhoud, calamiteiten en escalaties.
- Contractuele afspraken over taken en verantwoordelijkheden SLA-partijen.
- Operationele afspraken over opname, toegang, wijzigingen, etc.
- Verplichting beheerorganisatie bij opheffen van deze organisatie .
- Deelname nieuwe zorgdrager(s) aan e-depot.
- Uittreden zorgdrager(s) uit e-depot.
- Overstap zorgdrager naar ander e-depot.
- Exit-strategie bij overstap beheerorganisatie naar andere leverancier.
- Het tijdig voeren van nieuwe contractbesprekingen.
- Goede (geteste) exit-strategie (zie bijlage 1).
- Stichting of Escrow regeling.
- Het tijdig informeren (minimaal een jaar voor afloop of beëindiging) van wijzigingen bij de beheerorganisatie.

4 Verantwoordelijkheden partners E-depot Achterhoek

In het vorige hoofdstuk zijn de maatregelen beschreven die nodig zijn om de continuïteit van het e-depot op lange termijn te borgen. In dit hoofdstuk is beschreven wie verantwoordelijk is voor welke maatregelen.

4.1 De zorgdrager

- Verantwoordelijk voor de informatie en de kwaliteit van de informatie.
- Opdrachtgever Gemeenschappelijke Regeling.
- Beleid omtrent software inrichting/keuzes (als informatievormer).

4.2 De beheerorganisatie

- Verantwoordelijk voor de beheerorganisatie en omgeving waarin informatie duurzaam wordt bewaard.
- Inrichten ED_3 beheerorganisatie.
- Opstellen Gemeenschappelijke Regeling.
- Opstellen Liquidatieplan.
- Opstellen Noodplan.
- Stellen van (kwaliteits)eisen aan de diensten van de IT-leverancier en op basis daarvan overeenkomen van een dienstenniveau met de IT-leverancier (dit wordt vastgelegd in de SLA).
- Stellen van eisen ten aanzien van een vangnet in het geval van faillissement IT-leverancier.

4.3 De IT-leverancier

- Gedelegeerde verantwoordelijkheid voor het beheersysteem waar informatie duurzaam wordt bewaard.
- Uitvoeren SLA.
- Vangnet in het geval van faillissement ('continuïteitstichting' of Escrow) regelen.

Bijlage 1. Exit-strategie

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

Tenminste opnemen (zo helder en gedetailleerd mogelijk beschrijven):

- Scope en duur van de ondersteuning die de leverancier gaat leveren aan transitie.
  - Plan met beschrijving benodigde tijd, taken en verantwoordelijkheden voor een overdracht (zie voorbeelden post-termination assistance).
  - Voor een goede overgang moet de leverancier bereid zijn om samen te werken met de afnemer en eventuele andere leveranciers en bereid zijn om de service voor een bepaalde tijd te continueren na beëindiging.
- Afspraken over de kosten of de kostenverdeling voor de ondersteuning
  - 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).
- Afspraken over de wijze waarop de data wordt overgedragen.
  - Eisen aan hoe de data beschikbaar komt (platform: platform onafhankelijk formaat; drager).
- 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.
  - Wat en tegen welke kosten?
  - Wat gebeurt er met bezittingen 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 exit-plan te controleren en te updaten gedurende de looptijd.

Bijlage 2. Afkortingen en begrippen

Afkortingenlijst

ADA	Aangeboden digitaal archiefstuk
BDA	Beschikbaar digitaal archiefstuk
BRAIN	Branchevereniging Archiefinstellingen Nederland
DA	Digitaal Archiefstuk
DRP	Disaster Recovery Plan (Calamiteiten Herstel Plan)
DVO	Dienstverleningsovereenkomst
ECAL	Erfgoedcentrum Achterhoek en Liemers
ED3	Eisen Duurzaam Digitaal Depot
GR	Gemeenschappelijke regeling
ICTU	ICT Uitvoeringsorganisatie overheidsdiensten
KING	Kwaliteits Instituut Nederlandse Gemeenten
DMS	Document Management Systeem
LOPAI	Landelijk Overleg van Provinciale Archiefinspecteurs
OAIS	Open Archival Information System (ISO 14721)
ODA	Opgenomen digitaal archiefstuk
PDCA	Plan Do Check Act cyclus
RAZ	Regionaal Archief Zutphen
RMA	Record Management Applicatie
SIO	Strategisch Informatie Overleg
SLA	Service Level Agreement
TMLO	Toepassingsprofiel Metadatering Lokale Overheden
WRIJ	Waterschap Rijn en IJssel
XML	Extensible Markup Language

Begrippenlijst

Aanbieder	De aanbieder is, in het OAIS-model, de organisatie die de digitale archiefbescheiden aanbiedt aan het e-depot.
Adapter	Een hulpmiddel dat twee delen verbindt die niet zonder meer aan elkaar passen.
Aggregatieniveau	Het niveau waarop een record kan worden beschreven.
Archiefstuk	Informatieobject, ongeacht zijn vorm, met de bijbehorende metadata ontvangen of opgemaakt door een natuurlijke en/of rechtspersoon bij de uitvoering van taken en bewaard om te voldoen aan wettelijke en/of administratieve eisen en/of maatschappelijke behoeften.
Audit	Onderzoek naar het functioneren van een bedrijf als geheel of op onderdelen.
Audit trails	Controletrajecten.
Baseline Informatie-huishouding Gemeenten	De Baseline Informatiehuishouding Gemeenten is beoogd als het algemene, voor alle gemeenten en voor alle onder-

	delen van de gemeente - ook samenwerkingsverbanden en uitvoerende diensten - geldende normenkader voor informatiebeheer, dat de toegankelijkheid en betrouwbaarheid van overheidsinformatie bevordert.
Bewaaromgeving	Het geheel van ruimten, apparatuur, programmatuur en systeemprocedures waarmee de beheerorganisatie in staat is digitale informatie te beheren.
Bitdiepte	Of Kleurdiepte. Meeteenheid voor de hoeveelheid kleuren die een enkele punt kan weergeven.
Compressietechniek	Techniek om de omvang van een bestand te verkleinen.
Conformiteit	In overeenstemming met.
Contextinformatie	Metadata die een beschrijving geven van de relaties tussen brongegevens en hun omgeving.
Conversie	Omzetting of overzetting van gegevens in een ander bestandsformaat.
Decryptiesleutel	Een hulpmiddel voor het weer leesbaar maken van vercijferde gegevens.
Digitale archiefbescheiden	Archiefbescheiden die uitsluitend met besturingsprogrammatuur of toepassingsprogrammatuur geraadpleegd kunnen worden (Archiefregeling). Meervoud van digitaal archiefstuk (ED_3). De aangeboden (ADA), opgenomen (ODA), ter beschikking gestelde (BDA) duurzaam te bewaren en beheren digitale informatie-objecten inclusief de bijbehorende metadata.
Digitaal archiefstuk	Het DA is het enkelvoud van digitale archiefbescheiden.
Digitaal bronbestand	Bestand dat door de zorgdrager wordt aangeleverd aan de beheerorganisatie van het e-depot.
Digitale handtekening	Een methode voor het bevestigen van de juistheid van de digitale informatie.
E-conservator	Een functionaris verantwoordelijk voor de opname, toegankelijkheid en duurzaam behoud van digitale archiefbescheiden in het e-depot.
E-depot	Het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer, databeveiliging en aanwezige hard- en software dat duurzaam beheren en raadplegen van digitale archiefbescheiden mogelijk maakt.
ED_3	Eisen Duurzaam Digitaal Depot is binnen de Nederlandse archiefwetgeving een toetsingskader voor langetermijnbeheer van blijvend te bewaren digitale informatie.
Emulatie	Nabootsen en reconstrueren van originele hard- en software zodat de originele computerbestanden in hun oorspronkelijk formaat raadpleegbaar zijn.
Encryptietechniek	Het coderen van gegevens op basis van een bepaald algoritme. De versleutelde gegevens kunnen later weer gedecrypteerd worden.

Escrow overeenkomst	Afspraak tussen een softwarehuis en zijn klant om de software te plaatsen in handen van een onafhankelijke derde, die deze bewaart en in een omschreven situatie overdraagt aan een of meer andere personen.
Eventplan	Plan waarin een activiteit of gebeurtenis is opgenomen die in de toekomst moet/zal gebeuren.
Extensible Markup Language	XML is een standaard van het World Wide Web Consortium voor de syntaxis van formele opmaaktalen waarmee men gestructureerde gegevens kan weergeven in de vorm van platte tekst.
Fallbackscenario	Terugvalscenario. Een alternatieve werkwijze als de reguliere werkwijze als gevolg van een incident niet meer tot het gewenste resultaat leidt.
ICT-strategie	Een document over de bijdrage van ICT aan de doelstellingen en de continuïteit van de organisatie.
Identity management	Het geheel van processen en hulpmiddelen waarmee een identiteit kan worden geverifieerd en kan worden gekoppeld aan de juiste toegangsrechten.
Integriteitsinformatie	Metadata waarmee de fysieke integriteit van de brongegevens gecontroleerd kan worden.
ISO 14721	Space data and information transfer systems – Open archival information system (OAIS) – Reference model.
ISO 16363	Space data and information transfer systems – Audit and certification of trustworthy digital repositories.
Liquidatieplan	Een plan waarin staat wat er moet worden geregeld om een organisatie/bedrijf op te heffen.
Logging	Het vastleggen in een log, bijvoorbeeld een systeemlog of een securitylog, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.
Malware	Is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Computervirus, spyware, computerworm, Trojaans paard, etc.
Metadata	Metadata zijn gegevens (data) over gegevens (data). Naast de gegevens over inhoud, structuur en vorm van archiefbescheiden moeten bij digitale archiefbescheiden ook de technische kenmerken (bijv. bestandsformaat, soft- of hardwareafhankelijkheden) worden vastgelegd en bewaard. Dit is van belang om de omstandigheden waarin de data zijn gemaakt en bewaard te kunnen herleiden en daarmee de digitale archiefbescheiden te allen tijde te kunnen reconstrueren.
Metadataschema	Logische structuur die het verband aangeeft tussen elementen van metagegevens, doorgaans door regels vast te stellen voor het gebruik en beheer van metagegevens, vooral met betrekking tot de semantiek, de syntaxis en de keuzevrijheid (mate van verplichting) van waarden.

Migratie	Overzetting van gegevens en toepassingsprogrammatuur naar een ander platform, met behoud van authenticiteit, integriteit, betrouwbaarheid en bruikbaarheid.
NEN-ISO 23081	Informatie en documentatie - Processen voor informatie- en archiefbeheer – Metagegevens voor archiefbescheiden.
NEN-ISO 15489	Informatie en documentatie – Informatie- en archief-management.
NEN-ISO 27001	Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen.
NEN 2082	Eisen voor functionaliteit van informatie- en archief-management in programmatuur.
NEN-ISO 16175	Informatie en documentatie: principes en functionele eisen voor archiefbescheiden in een elektronische kantooromge-ving.
Ontsluitingsinformatie	Metadata, voornamelijk bestaande uit inhoudelijke be-schrijvingen, die het vinden, ordenen en opvragen van het opgenomen digitale archiefstuk (ODA) in de bewaaromge-ving mogelijk maken. De ontsluitingsinformatie is specifiek voor de bewaaromgeving bij de opname als een soort index gegenereerd of toegekend en wordt gewoonlijk afgeleid van de beheerinformatie.
Opvolgingsplan	Plan waarin wordt geregeld wat er moet gebeuren als de beheerorganisatie ophoudt te bestaan.
Overbrenging	Procedure waarbij een zorgdrager van een overheidsorgaan archiefbescheiden overdraagt aan de archiefbeheerder van een archiefbewaarplaats.
Pixel	Een gekleurde punt op het beeldscherm van de computer of in een digitaal beeld. Veel punten bij elkaar geven een beeld.
Portabiliteit	Mate van integratie met de bestaande IT-infrastructuur.
Preservering	Proces van bewaren en beheren binnen het archiefsysteem. Het geheel van activiteiten gericht op de zorg voor het tech-nische en intellectuele behoud van archiefdocumenten.
Recovery	Herstellen van data na dataverlies.
Relatie-informatie	Metadata die brongegevens en beheerinformatie van het di-gitale archiefstuk (DA) als één logisch geheel verbinden voor identificatie en gebruik.
Representatie-informatie	Metadata die nodig zijn om het digitale bronobject reproduceerbaar (leesbaar) en juist interpreteerbaar te maken. Dit kan een beschrijving van hard- en software of een samen-vatting/beschrijving van de juiste interpretatie van het digitaal bronobject zijn.
Resolutie	Term om het aantal gebruikte pixels op bijvoorbeeld een beeldscherm te beschrijven. Hoe hoger dat aantal, hoe hoger de maximale resolutie van het scherm.

Security scans	Een scan om zwakke punten in de informatiebeveiliging te laten zien.
Semantiek	Wetenschap die zich bezighoudt met de betekenis van symbolen en in het bijzonder van taal en woorden.
Syntax	De vorm en structuur van de informatie.
Toegangsinformatie	Metadata die (wettelijke) beperkingen van de toegang tot brongegevens beschrijven en tevens de bij opname overeengekomen voorwaarden voor toegang en verspreiding bevatten. Hieronder vallen auteursrechten, licentierechten, technische beperkingen, openbaarheidsbeperkingen en toegangscontrole.
Uitplaatsing	Het plaatsen van te bewaren en te vernietigen digitale archiefbescheiden in een e-depot voordat deze moeten worden overgebracht of vernietigd.
Validatie	Het controleren van een waarde op geldigheid of juistheid.
Verwijzingsinformatie	Metadata, die de unieke kenmerken ('identifiers') voor de brongegevens bevatten en eenduidige verwijzing naar brongegevens mogelijk maakt, ook voor externe systemen.
Virtual machine	Een computerprogramma dat een computer nabootst.
Zaakgericht werken	Een concept dat helpt om digitaal te werken en te archiveren.
Zorgdragers	Degene die bij of krachtens de wet is belast met de zorg voor de archiefbescheiden (Archiefwet 1995, art. 1).