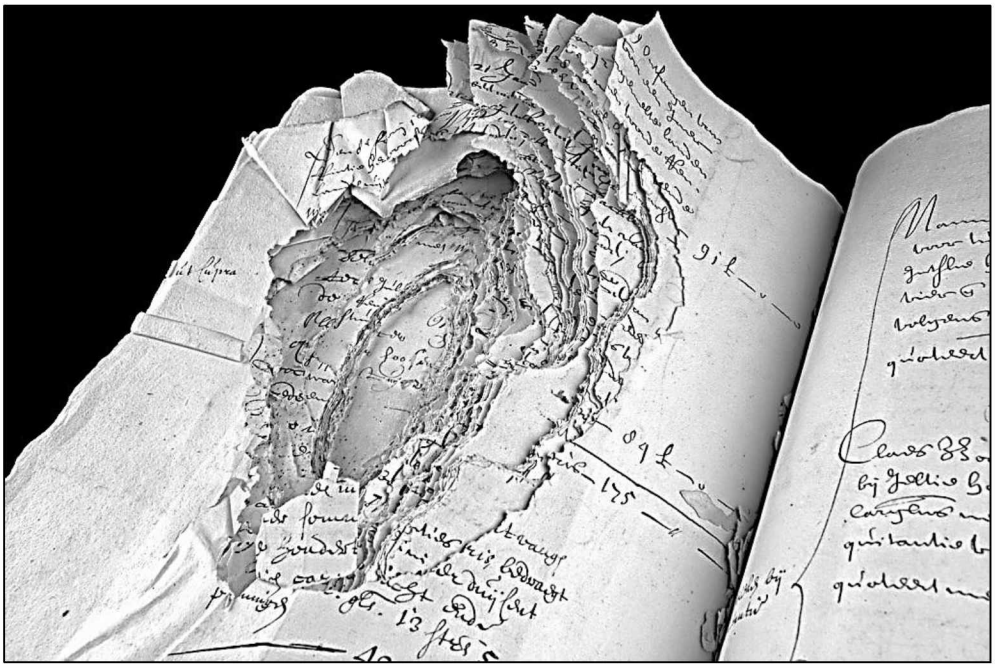
Gemeente Amsterdam

Uitfaseren applicatie? Voorkom informatieverlies!

Instructie voor analyse door Informatiebeheer



Auteurs Rens Ouwerkerk, IV Bedrijfsvoering, Team Informatiebeheer
Sjoerd Korsuize, IV Stadsdelen, Team Informatiebeheer

Versie 1.0

Datum *11 december 2017*

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1	25-1-2017	S. Korsuize, R. Ouwerkerk	Eerste versie
0.2	19-4-2017	S. Korsuize, R. Ouwerkerk	Aanpassingen na eerste review SIA (Stedelijk IB-Adviseursoverleg)
0.3	9-5-2017	S. Korsuize, R. Ouwerkerk	Aanpassingen na tweede review SIA + feedback Stadsarchief
0.4	24-5-2017	S. Korsuize R. Ouwerkerk	Aanpassingen na review vakoverleg IB
0.5	17-11-2017	S. Korsuize R. Ouwerkerk	Aanpassingen na presentatie in PLO Applicatierationalisatie/APM, vakoverleg privacy, vakoverleg functioneel beheer, projectleiders stadsdelen en vakoverleg informatiemanagement
0.9	20-11-2017	S. Korsuize R. Ouwerkerk	Vastgesteld door gedelegeerd opdrachtgever
1.0	11-12-2017	S. Korsuize R. Ouwerkerk	Vastgesteld door vakoverleg IB

Goedkeuring

Versie	Datum	Naam	Rol
0.9	6-12-2017	E. Giphart	Gedelegeerd opdrachtgever
1.0	11-12-2017	Vakoverleg IB	Opdrachtgever

Inhoud

1. Inleiding 4
2. Bepalen informatiewaarde 6
2.1 Wetgeving 6
2.2 Eigenaarschap en gebruik van de informatie 7
2.3 Vorm van de informatie 8
2.4 Verwerken onderzoeksresultaten 8
3. Bepalen strategie 9
3.1 Strategie 1: Data niet veiligstellen 9
3.2 Strategie 2: Data wel veiligstellen 9
3.3 Strategie 3: Data deels veiligstellen 9
4. Bepalen uitvoeringsmethode 11
4.1 Methoden voor strategie 1: Data niet veiligstellen 11
4.2 Methoden voor strategie 2: Data wel veiligstellen 12
4.2.1 Migreren naar doelapplicatie 12
4.2.2 Export naar los(se) bestand(en) 13
4.2.3 Handmatige invoer 14
4.2.4 Screenshots maken of uitprinten 14
4.2.5 Database veiligstellen en ontsluiten met BI-tooling 15
4.2.6 Applicatie laten draaien 15
4.2.7 Opslag data in het e-depot 15
4.3 Methoden voor strategie 3: Data deels veiligstellen 16
5. Aandachtspunten bij uitvoering 17
5.1 Bepalen wie beslisser is 17
5.2 Presenteer analyse in memo 18
5.3 Functioneel ontwerp 18
5.4 Testen 18
5.5 Verklaring van migratie 18
5.6 Archiveren export-bestanden 19
5.7 Verlaat uitzetten applicatie 19
I Appendix 20
i.i Generiek stappenplan voor migratie 20
i.ii Modelverklaring van conversie en/of migratie 23

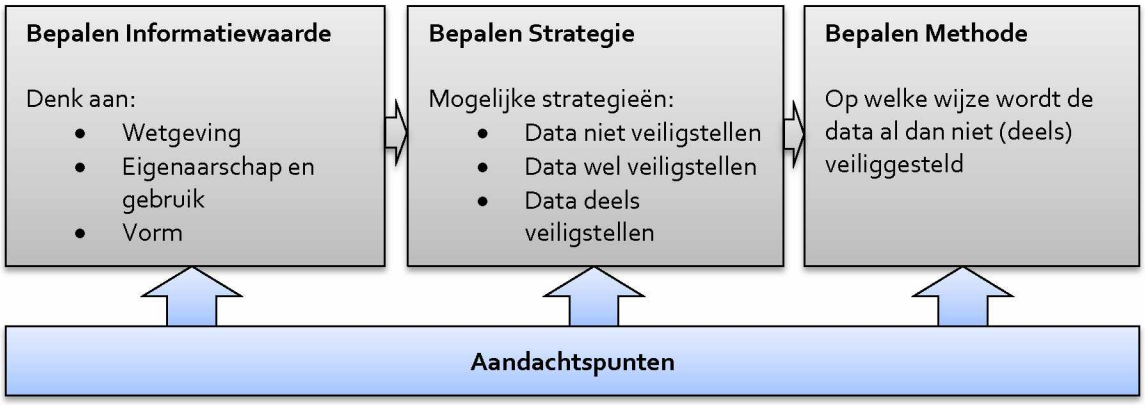
1. Inleiding

De gemeente Amsterdam kent een bewaarplicht voor alle informatie in haar applicaties, ongeacht de vorm. Dit zodat de gemeente zich kan verantwoorden en de bedrijfscontinuïteit kan waarborgen. Echter mag je informatie ook weer niet altijd onbeperkt bewaren. Zowel de Archiefwet als de Wet Bescherming Persoonsgegevens[1] geven aan hoe lang je bepaalde informatie mag bewaren en wanneer je deze zou moeten vernietigen (uitzonderingen daargelaten). In een aantal applicaties dat gebruikt wordt in de organisatie zit informatie die (tijdelijk) bewaard dient te worden op grond van dergelijke wetgeving. Om te voorkomen dat deze informatie onterecht vernietigd wordt op het moment dat de applicatie "uitgezet" wordt of dat deze juist langer wordt bewaard dan toegestaan, is het nodig om hier een check op uit te voeren. Naast wetgeving kan informatie ook van belang zijn in de uitvoer van processen. Ook hierom is een check op informatie in de uit te zetten applicatie nodig. Bovendien mogen we geen informatie vernietigen zonder toestemming van de gemeentearchivaris. Als een applicatie wordt uitgezet moet duidelijk zijn wat er met de informatie uit die applicatie moet worden gedaan. Om verlies van informatie te voorkomen, is een protocol noodzakelijk met verschillende disciplines van Informatievoorziening en de rve ICT. Het is essentieel dat ook Informatiebeheer – de specialist voor het bewaren en vernietigen van informatie – altijd wordt geraadpleegd bij het uitzetten van applicaties.

In dit document staat uiteengezet welke acties Informatiebeheer neemt om informatieverlies te voorkomen bij het uitzetten van applicaties en migreren van data. Als inhoudelijk kader bij de uitvoering, worden in dit document enkele best practices en praktijkvoorbeelden genoemd.

In Hoofdstuk 2 wordt ingegaan op de uit te voeren analyse om te bepalen in hoeverre informatie in een uit te faseren applicatie van waarde is. In Hoofdstuk 3 wordt uitgelegd welke strategieën denkbaar zijn, namelijk data niet veiligstellen, wel veiligstellen of deels veiligstellen. In hoofdstuk 4 wordt vervolgens uiteengezet welke methoden er per respectievelijke strategie mogelijk zijn om informatie niet, wel, of deels veilig te stellen. Hoofdstuk 5 gaat nader in op enkele aandachtspunten bij de uitvoer, bijzondere aandacht is hier voor hoe Informatiebeheer ondersteunt. Schematisch ziet het er als volgt uit:

[1] Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG is een geharmoniseerde Europese privacywetgeving.



Let op: de instructie die hier wordt beschreven vindt plaats als onderdeel binnen een overkoepelend traject, waarin een verzoek is binnengekomen om een applicatie uit te faseren. Dit overkoepelende traject vindt plaats onder de coördinatie van de Informatiemanager of projectleider.[2] Actueel is de Applicatierationalisatie. Echter, de instructie voor de uit te voeren analyse is ook toepasbaar op andere situaties waarin besloten is dat een applicatie in aanmerking komt voor uitfasering.

[2] Zie: Rob Ruck, *Procesbeschrijving uitzetten van applicaties* (Amsterdam 2017).

2. Bepalen informatiewaarde

Data vertegenwoordigen een bepaalde informatiewaarde. Data en informatie zijn strikt genomen niet synoniem, maar worden voor het gemak in dit stuk wel als zodanig gebruikt.[3] Om de informatiewaarde te kunnen bepalen, moet een aantal aspecten worden onderzocht. Zo is er de wetgeving waaronder de informatie valt. Verder is van belang om te weten hoe het zit met het gebruik en eigenaarschap van de informatie. Voorts is de vorm van de informatie van belang (gaat het bijvoorbeeld om een verwijzing naar papier, om digitale documenten of om een database). Tot slot komt het beheer van de informatie aan bod. Bij elk van de thema's is een aantal vragen geformuleerd. Degene die de analyse uitvoert voor het onderdeel Informatiebeheer draagt er zorg voor dat de vragen beantwoord worden. Dit wil niet zeggen dat de verantwoordelijk analist van Informatiebeheer zelf alle vragen moet of kan beantwoorden. In een aantal gevallen moet het antwoord namelijk komen van andere partijen dan het Informatiebeheer zelf. De informatiebeheerder die de analyse uitvoert betrekt de relevante betrokken partijen. Dit zijn bijvoorbeeld de gebruikers, privacy en information security officers, functioneel beheer, een informatiemanager en/of -architect.

Per thema volgt hier een overzicht van de te stellen vragen. Tevens wordt erbij vermeld welke deskundigen er iets over kunnen zeggen. Het structureel doorlopen van de vragen is een goede check om te bepalen of alle thema's relevant voor het informatiebeheer meegenomen worden. De vragenlijst is bedoeld als handreiking. In de praktijk zullen zich, afhankelijk van de specifieke casus, meer of juist minder vragen voordoen. De indeling is niet chronologisch, onderdelen kunnen parallel aan elkaar worden uitgezocht.

Deze analyse leidt tot een uitvoeringsstrategie. De mogelijke uitvoeringsstrategieën worden nader beschreven in hoofdstuk 3.

2.1 Wetgeving

Kaders voor het bewaren en vernietigen zijn deels vastgelegd in wetgeving. Daarom is het noodzakelijk om de wettelijke aspecten van de informatie te analyseren. Deze kennis zit niet alleen bij Informatiebeheer, daarom biedt deze paragraaf een aanzet tot bespreekpunten met andere IV-disciplines.

Punten te bespreken met de Informatieanalisten IB, Privacy Officers en Information Security Officers uit het betreffende domein om inzicht te krijgen in aspecten van wetgeving:

[3] Er bestaan wettelijke en beleidsmatige richtlijnen voor het eigenaarschap van informatie. Daarmee is ook het eigenaarschap van data belegd. Informatie is weliswaar niet hetzelfde als data, maar data vormen de bouwblokken voor informatie. Data worden verzameld en vastgelegd vanuit inhoudelijke processen en vertegenwoordigen daarmee een informatiewaarde binnen die processen. Een informatie-eigenaar kan zijn rol niet invullen als hij geen zeggenschap heeft over de applicatiedata. De facto is de informatie-eigenaar daarmee tevens de dataeigenaar.

- Welke bewaartermijn kent de informatie? Hier kan natuurlijk sprake zijn van meerdere bewaartermijnen;
- Is er sprake van persoonsgegevens (onderscheid hierin gewoon en bijzonder)?
    - Zo ja: vernietiging na einde bewaartermijn is urgent;
- Kunnen persoonsgegevens voortijdig worden vernietigd zonder informatieverlies?*
    - Zo ja: overweeg opschonen van de data;
- Is er een doorlopende machtiging tot vernietiging (verkregen van de gemeentearchivaris)?
- Is de informatie ook nog ergens anders? Zo ja:
    - Waar dan?
    - In welke vorm?
        - Is het één-op-één dezelfde data, of geaggregeerd?
        - Gaat het om data of om rapportages?
    - Wat is de status? Kopie, back-up, of origineel?

* Wettelijke bewaartermijnen gaan over informatie. Er is een verschil tussen "informatie" en "gegevens". Informatie is duiding. In sommige gevallen kunnen gegevens vernietigd worden, zonder dat dit informatieverlies tot gevolg heeft. Voorbeeld: tijdens de behandeling van een zaak, kan het nodig zijn om over iemands IBAN-nummer te beschikken: gedurende het proces is dat gegeven informatie. Na afhandeling van de zaak, is het alleen nog maar nodig om vast te leggen dat een betaling heeft plaats gevonden. Het IBAN-nummer is dan een gegeven dat geen informatie meer vertegenwoordigd zoals bedoeld in de Archiefwet. En kan dus ook verwijderd/vernietigd worden.[4]

2.2 Eigenaarschap en gebruik van de informatie

De manier waarop informatie gebruikt wordt, stelt eisen aan de wijze waarop de informatie veiliggesteld moet worden. Dit kan namelijk op meer en minder gebruiksvriendelijke wijze, elk met eigen kostenplaatje. Om hierin de juiste keuze te kunnen maken, is inzicht nodig in het gebruik van de informatie. Kennis hierover ligt vaak mede bij informatiearchitecten, keteninformatiemanagers, clusterinformatiemanagers en informatieanalisten. Aspecten die hierbij onderzocht moeten worden zijn:

- Inhoudelijke beschrijving van de informatie: bij welk proces hoort het?
- Wie is de eigenaar/wie zijn de eigenaren van de informatie?[5]
- Waar wordt de informatie voor gebruikt?
- Welk effect heeft eventueel informatieverlies? / Wat is de impact op de kwaliteit van de procesuitvoering?
- Welke risicoprofiel is van toepassing op de informatie?
- Wie maken gebruik van de informatie?

[4] Richard van den Belt en Rens Ouwerkerk, *Bewaartermijnen Archiefwet versus Wbp: notitie voor vakoverleg privacy* (16 november 2017).
[5] De wettelijke term is 'beheerder'. B&W zijn zorgdrager en zij wijzen (in het Besluit informatiebeheer) beheerders aan. Deze beheerders zijn 'eigenaren' van de informatie.

- Hoeveel gebruikers zijn er? [Dit heeft impact op de vorm van de te kiezen oplossing]
- Wat is de gebruiksfrequentie? [Dit heeft impact op de vorm van de te kiezen oplossing]
- Zit de informatie in een keten, hoe is de context?
- Is de informatie nodig voor rapportages?
- Gaat het om lopende zaken en/of afgesloten zaken?
- Zijn er koppelingen met andere informatiebronnen en/of –systemen?
- Is de informatie ook nog ergens anders?

  Indien ja:
  - Waar / in welke applicatie?
  - Is dit één-op-één dezelfde informatie?
  - Heeft de informatie in die andere omgeving een andere context, of maakt deel uit van een ander werkproces, die/dat leidt tot een andere waardering c.q. bewaartermijn?

2.3 Vorm van de informatie

De vorm waarin informatie is opgeslagen bepaalt mede welke mogelijkheden er zijn om de data veilig te stellen. Daarom moet gekeken worden naar een aantal aspecten hiervan. Kennis hierover zit vaak bij functioneel beheer:

- Gaat het om documenten en/of data?
- Is er sprake van verwijzingen naar papier?
- Is er inzicht in het datamodel?
- Zijn de verplichte elementen uit de Metadatastandaard ingericht?
- Wat is de lifecyclestatus van de applicatie?
- Is de applicatie ARA-III-compliant?
- Zijn er koppelingen en wat doen die?
- Om wat voor soort bestanden gaat het?
- Welke bestandsformaten worden gebruikt?
- Is de applicatie een SAAS-oplossing of wordt die intern gehost?
- Is de informatie ook nog ergens anders? Zo ja: waar? Is dit 1-op-1 dekkend?
- Betreft het een authentieke bron?

2.4 Verwerken onderzoeksresultaten

Nadat alle informatie is verzameld, wordt deze geïnterpreteerd zodat een beeld ontstaat van de informatiewaarde. In dit stadium stel je vast of informatie wel, niet of deels veiliggesteld moet worden. In het volgende hoofdstuk volgt een toelichting op de strategieën.

3. Bepalen strategie

In het vorige hoofdstuk is beschreven hoe op grond van een analyse de informatiewaarde van een uit te faseren applicatie kan worden bepaald. De resultaten van deze analyse leiden tot een beslissing wat te doen met de informatie in een uit te faseren applicatie, welke strategie te volgen bij de uitfasering. Er zijn drie mogelijke uitvoeringsstrategieën:

1. Data niet veiligstellen;
2. Data wel veiligstellen;
3. Data deels veiligstellen.

Binnen elke strategie zijn meerdere uitvoeringsmethoden mogelijk. Deze worden nader uitgewerkt in hoofdstuk 4.

3.1 Strategie 1: Data niet veiligstellen

Als uit de analyse blijkt dat de informatie geen waarde meer heeft voor de informatieconsumenten, dan is het vernietigen of verwijderen van informatie een goede optie.
Er is een verschil tussen vernietigen en verwijderen.
Verwijderen wil zeggen dat de informatie in een systeem niet als originele informatie wordt beschouwd, er is dan sprake van kopiegegevens. Feitelijk blijft de informatie nog beschikbaar in de authentieke bron. Daardoor is geen sprake van formele vernietiging, maar slechts van verwijdering. Het is niet nodig om een machtiging van de gemeentearchivaris te verkrijgen. Deze keuze kan wel tot gevolg hebben dat de betreffende informatie voor specifieke doelgroepen niet meer (goed) toegankelijk is.
Vernietigen wil zeggen dat informatie uit de authentieke bron wordt verwijderd. Daarmee is sprake van formele archiefvernietiging zoals bedoeld in de Archiefwet. Hiervoor is een machtiging van de gemeentearchivaris vereist.
Verwijderen zit vaak in de optionele sfeer, vernietigen is meer formeel en volgt meestal uit een wettelijke vernietigplicht.

3.2 Strategie 2: Data wel veiligstellen

De uitkomst van de analyse kan zijn dat alle data beschikbaar moeten blijven. Als dat het geval is, dan is de volgende vraag hoe dit te doen. Daarvoor zijn verschillende methoden denkbaar. Deze worden in het volgende hoofdstuk beschreven. Wat de meest geschikte methodiek is, hangt van de specifieke omstandigheden af.

3.3 Strategie 3: Data deels veiligstellen

Uit de analyse kan blijken dat slechts een deel van de informatie in een systeem relevant is om mee te nemen. In zo'n geval kan het zinvol zijn om "schoon door de poort" te migreren. Dit betekent in het migratietraject extra analysewerk. Er moet beschreven worden welke onderdelen

gemigreerd worden en met welke filterwaarden deze elementen van de niet-relevante onderdelen gescheiden kunnen worden.
Een voordeel van deze strategie is dat gebruikers in de doelsituatie alleen relevante gegevens ter beschikking hebben. De gedachte is: hoe kleiner de hooiberg, hoe sneller de speld gevonden wordt. De toegankelijkheid van relevante informatie wordt hierdoor vergroot.
Bij de uitvoering zijn uiteraard ook de activiteiten zoals beschreven in de vorige twee paragrafen aan de orde.

4. Bepalen uitvoeringsmethode

De keuze om data wel of niet veilig te stellen is afhankelijk van de gebruikswaarde die de informatie vertegenwoordigt. Wanneer geconcludeerd wordt dat de informatie in een uit te faseren applicatie nog van waarde is – een inzicht dat verkregen is na het uitvoeren van de analyse in het tweede hoofdstuk – dan zijn er diverse manieren om die veilig te stellen. In de uitvoering zijn er verschillen in de methoden ten aanzien van de kosten, doorlooptijd en benodigde capaciteit. De vraag is daarbij telkens of de investering in een migratietraject opweegt tegen de voordelen van het optimaal toegankelijk houden van informatie. Welke methode het meest geschikt is, hangt daardoor mede af van de eisen die gesteld worden aan onder meer de beschikbaarheid en toegankelijkheid, afgezet tegen de inspanning die nodig is om de oplossing te realiseren. Het is kortom verstandig om een kleine business case op te stellen waarmee de informatie-eigenaar geadviseerd wordt om de beste keuze te maken.

4.1 Methoden voor strategie 1: Data niet veiligstellen

In strategie 1 wordt de data uit de uit te faseren applicatie niet veiliggesteld. Als sprake is van originele informatie, dan is de consequentie dat de informatie vernietigd dient te worden. In deze paragraaf wordt beschreven hoe dit in zijn werk gaat.

Bij de vernietiging van gegevens, moet de informatie-eigenaar (rve-directeur of stadsdeelsecretaris) een machtiging tot vernietiging hebben. Als een doorlopende machtiging aanwezig is, zijn hiervoor geen extra maatregelen nodig anders dan het volgen van de reguliere richtlijnen voor vernietiging met doorlopende machtiging. In andere gevallen, begeleidt IB het proces door de aanvraag op te stellen. In de aanvraagbrief wordt vermeld:
- Om wat voor gegevens gaat het?
- Om hoeveel gegevens gaat het uitgedrukt in MB, GB of TB?
- Op welke grond komen de gegevens voor vernietiging in aanmerking?

Wat betreft de derde vraag volstaat meestal een verwijzing naar de betreffende categorie in de selectielijst.
Een uitzondering hierop zijn separate gegevensbestanden waarin persoonsgegevens zijn vastgelegd, deze bestanden zijn een bouwblok om informatie mee te creëren. Vanuit privacy-wetgeving is het soms nodig om deze te vernietigen zodra het belang is vervallen. De selectielijst voorziet hier niet (altijd) in. In 2016 heeft zich een casus voorgedaan die als precedent geldt op dit gebied: er zijn persoonsgegevens verzameld voor de distributie digitale stempassen voor de ondernemingsraadverkiezingen. Belangrijk was dat niet het individuele stemgedrag te reproduceren was vanuit archiefgegevens. De archiefinspectie heeft desgevraagd aangegeven dat ook in dergelijke gevallen sprake is van vernietiging onder de Archiefwet. De gemeentearchivaris heeft een machtiging verstrekt op basis van een bewaartermijn van drie maanden, zonder dat de selectielijst dit uitgangspunt (goed) onderschreef. De Wbp prevaleerde hier boven de Archiefwet.

De aanvraag tot het verstrekken van een machtiging tot vernietiging moet worden ondertekend door de informatie-eigenaar.

Na vernietiging wordt de verklaring van vernietiging opgesteld. Hierin wordt aangegeven op welke wijze de informatie is vernietigd. Eventueel kan verwezen worden naar een door een leverancier opgesteld certificaat van vernietiging (in geval van SAAS), of een mailbevestiging van rve ICT dat de gegevens onherstelbaar zijn vernietigd.
Een aandachtspunt hierbij is het back-upprotocol. Wanneer het nodig is om een back-up terug te zetten waarin reeds vernietigde gegevens staan, dan zal de vernietiging als onderdeel van het recoveryproces opnieuw moeten worden uitgevoerd. IB maakt hier een procesafspraak over met de functioneel beheerder.

De verklaring van vernietiging wordt ondertekend door de informatie-eigenaar en een kopie wordt verstuurd naar de gemeentearchivaris.[6]

4.2 Methoden voor strategie 2: Data wel veiligstellen

Er zijn verschillende manieren om informatie beschikbaar te houden. Sommige methoden zorgen voor een betere toegankelijkheid, maar zijn complexer en duurder in de uitvoering. Welke methodiek het meest geschikt is, hangt af van verschillende factoren. Als informatie relatief weinig wordt geraadpleegd door een kleine doelgroep, dan kan een functioneel suboptimale oplossing tegen lagere kosten of mindere inspanning de overweging waard zijn. De kwalitatief beste methodiek is, alle belangen afwegend, niet altijd de meest geschikte.

In deze paragraaf worden verschillende methodieken beschreven om informatie veilig te stellen. Bij elke methodiek is een schema toegevoegd met te verwachten complexiteit op verschillende factoren. Deze zijn vanuit ervaring opgesteld en geven een algemene indruk over de specifieke methodiek, maar in de praktijk zijn er per casus verschillen. De schema's geven een indicatie, maar mogen niet a priori als waarheid worden beschouwd in het analyseproces.

De verschillende methoden zijn in deze paragraaf in willekeurige volgorde beschreven. De Appendix bevat een stappenplan dat kan helpen bij het kiezen van een geschikte manier om data veilig te stellen.

4.2.1 Migreren naar doelapplicatie

Een voor de hand liggende manier om informatie uit een oud systeem beschikbaar te houden, is een volwaardige migratie naar de doelapplicatie. Daarmee blijft informatie toegankelijk voor de gebruikers vanuit het systeem dat in de doelsituatie hun werkproces ondersteunt. Er moet een mapping plaatsvinden van het datamodel uit het oude systeem met het datamodel van het nieuwe

[6] Zie ook: Procedure Selectie en Vernietiging, *Stadsarchief Amsterdam*: https://www.amsterdam.nl/publish/pages/734150/procedures-selectie1.pdf.

systeem: er moet zorgvuldig worden afgewogen welke database-elementen van belang zijn en in welke velden in het nieuwe systeem de waarden getoond moeten worden. De complexiteit hiervan is onder meer afhankelijk van de omvang en kwaliteit van de database die gemigreerd moet worden. Een praktische belemmering is dat het datamodel niet altijd beschikbaar is. Hoe je een migratie uitvoert verschilt per situatie. Vaak is hiervoor de inzet van een of meer softwareleveranciers nodig. Bij een migratie is het test- en acceptatieproces belangrijk. Een ander aandachtspunt is het in stand houden van onderlinge samenhang en verwijzingen.

Indicator	Waardering	Opmerking
Doorlooptijd	-	Mappen datamodellen, testtraject
Kosten	-	Inzet leverancier(s) nodig
Technische complexiteit	-	Afhankelijk van kwaliteit database
Autorisaties	++	
Afhankelijkheden	-	Inzet leverancier(s) nodig
Toegankelijkheid	++	
Herbruikbaarheid	-	Data verweven in logica specifieke applicatie

4.2.2 Export naar los(se) bestand(en)

Informatie uit applicaties die uitsluitend gegevens in een database bevatten en geen documenten, kan meestal worden geëxporteerd naar losse gegevensbestanden. Bijvoorbeeld een .csv- of .xml-bestand dat vervolgens weer ingelezen kan worden in een andere applicatie, of een .xls- of .pdf-bestand waarin de gegevens op een begrijpelijke manier worden gepresenteerd. Een export kan in sommige gevallen vanuit de applicatie zelf worden gemaakt, in andere gevallen is het nodig om een rapportagetool op de database te zetten.
Een voordeel van deze methode is dat deze relatief eenvoudig te realiseren is tegen lage kosten. Een nadeel van deze methode is dat de informatie op een weinig gebruiksvriendelijke wijze beschikbaar wordt gesteld. Bovendien is een locatie nodig (bijvoorbeeld de G-schijf of een DMS) waar het bestand wordt opgeslagen, met 'alleen lezen'-rechten om onbedoeld of ongeautoriseerd wijzigen of verwijderen te voorkomen. Gegevens verliezen immers hun informatiewaarde als de integriteit van die gegevens niet aangetoond kan worden.
Deze methode vooral geschikt als de raadpleegfrequentie laag is en de gebruikersorganisatie klein, vanwege de beperkingen in weergave en toegankelijkheid.

Indicator	Waardering	Opmerking
Doorlooptijd	++	
Kosten	++	
Technische complexiteit	+	
Autorisaties	-	Maatwerk. Autorisaties alleen op complete bestand mogelijk
Afhankelijkheden	-	Exportfunctionaliteit/kennis datamodel, alleen toepasbaar voor gegevens en niet voor migratie van documenten

Toegankelijkheid	-	Data niet ontsloten via GUI
Herbruikbaarheid	+	

4.2.3 Handmatige invoer

Een vorm van migratie is het handmatig overtikken van gegevens uit het ene systeem in het andere systeem. Deze methode is vooral geschikt als het gaat om een relatief kleine dataset.
Een aandachtspunt bij deze methode is extra kwaliteitscontrole (bovenop de generieke maatregelen die in het volgende hoofdstuk worden genoemd): door middel van bijvoorbeeld (steek)proeven of het vierogenprincipe moet worden vastgesteld of de informatie in het doelsysteem één-op-één overeen komt met de bron.
Een nadeel van deze methode is dat deze relatief arbeidsintensief is. De informatie-eigenaar zal hier capaciteit of inhuurbudget voor vrij moeten maken.

Indicator	Waardering	Opmerking
Doorlooptijd	--	Arbeidsintensief, niet geschikt voor grote volumes
Kosten	-	Hoe groter volume, hoe hoger de kosten
Technische complexiteit	++	
Autorisaties	++	Maakt gebruik van autorisatiemodel nieuwe applicatie
Afhankelijkheden	+	
Toegankelijkheid	++	Maakt gebruik van zoekfunctionaliteit nieuwe applicatie
Herbruikbaarheid	-	Data verweven in logica specifieke applicatie

4.2.4 Screenshots maken of uitprinten

In sommige applicaties wordt alle relevante informatie rondom een zaak in één scherm getoond. Hier kunnen prints of printscreens van worden gemaakt. Dit is alleen werkbaar als sprake is van een beperkt aantal relevante registraties.
Het uitprinten is vooral geschikt als sprake is van een hybride situatie (papier en digitaal naast elkaar) waarbij het uitgangspunt is dat het papieren dossier leidend is.
Het maken van screenshots heeft als voordeel dat geen kennis van het datamodel nodig is. Een nadeel is dat de screenshots niet goed doorzoekbaar zijn. Hoe meer registraties, hoe ongeschikter deze methode.

Indicator	Waardering	Opmerking
Doorlooptijd	-	Afhankelijk van volume
Kosten	+	
Technische complexiteit	++	
Autorisaties	-	Maatwerk
Afhankelijkheden	+	
Toegankelijkheid	-	Screenshots zijn niet doorzoekbaar
Herbruikbaarheid	-	Informatie is niet in de vorm van gegevens beschikbaar

4.2.5 Database veiligstellen en ontsluiten met BI-tooling

Databases die zich (vanwege omvang of complexiteit) niet lenen voor een export naar een bruikbaar bestand, kunnen ontsloten worden met BI-tooling. Vaak voorkomende zoekvragen kunnen met standaardrapportages worden ingesteld. Voor zoekvragen die minder standaard zijn, moet op maat een rapport gemaakt worden. Deze methode is daarom vooral geschikt als de raadpleegfrequentie laag is of als de zoekvragen voorspelbaar zijn.

Indicator	Waardering	Opmerking
Doorlooptijd	+	
Kosten	+	
Technische complexiteit	+	
Autorisaties	-	Alert zijn op persoonsgegevens in de database
Afhankelijkheden	+	
Toegankelijkheid	--	Toegang via rapportages: maatwerk
Herbruikbaarheid	+	

4.2.6 Applicatie laten draaien

Soms kan het slim zijn om de oude applicatie beschikbaar te houden, naast de nieuwe. Er worden dan wel additionele kosten gemaakt voor licenties en technisch en functioneel beheer, al kan het aantal licenties in veel gevallen worden verminderd. Hoe langer een oude applicatie blijft draaien, hoe minder vanzelfsprekend de aanwezigheid van applicatiekennis is. Dit is een risico voor de toegankelijkheid. Deze methode is daarom minder geschikt naarmate de informatie langer beschikbaar moet blijven. Ook is deze methode minder geschikt als een applicatie aan het eind van de levenscyclus is, omdat daarmee het risico bestaat dat die "omvalt". Bij onderzoek naar deze methode moet altijd bij rve ICT nagevraagd worden of de applicatie ARA-III-compliant is.

Indicator	Waardering	Opmerking
Doorlooptijd	++	
Kosten	-	Kosten voor licenties, technisch en functioneel beheer
Technische complexiteit	-	Verouderde applicaties draaiend houden kan lastig zijn
Autorisaties	+	
Afhankelijkheden	++	
Toegankelijkheid	-	Meerdere systemen naast elkaar, kennis verouderd
Herbruikbaarheid	-	Data verweven in logica specifieke applicatie

4.2.7 Opslag data in het e-depot

Het Stadsarchief heeft met het e-depot een voorziening in huis die gespecialiseerd is in de duurzame opslag van informatie. Deze voorziening is primair bedoeld voor de opslag van informatie die permanent te bewaren is, met als doel die beschikbaar te stellen aan de buitenwereld. Een optie kan zijn om data in het e-depot op te slaan, bijvoorbeeld als vervroegde

overbrenging. Een voordeel van deze methode is dat de toegankelijkheid van informatie voor de burger hiermee wordt bevorderd. In de toekomst zal het e-depot wellicht breder ingezet gaan worden, waarmee ook uitplaatsing van op termijn te vernietigen informatie een mogelijkheid wordt. Aan de hand van een intakegesprek met medewerkers van het Stadsarchief kan worden bepaald of het e-depot voor een specifieke casus een oplossing kan bieden.

Indicator	Waardering	Opmerking
Doorlooptijd	-	Nog geen bewezen oplossing, mogelijk kinderziekten
Kosten	+	
Technische complexiteit	-	Er is mogelijk maatwerk nodig op de raadpleeginterface
Autorisaties	+	
Afhankelijkheden	+	
Toegankelijkheid	++	
Herbruikbaarheid	+	

4.3 Methoden voor strategie 3: Data deels veiligstellen

De derde strategie is het deels veiligstellen van de data. Feitelijk is dit een combinatie van de strategieën 1 en 2. Dit geldt ook voor uitvoer van de methoden die op deze respectievelijke strategieën van toepassing zijn. Enerzijds moet gekeken worden naar de wijze waarop het daarvoor in aanmerking komende deel van de informatie veiliggesteld kan worden (strategie 2), anderzijds moet er oog zijn voor de correcte vernietiging van informatie die niet veiliggesteld hoeft te worden (strategie 1).

5. Aandachtspunten bij uitvoering

Zodra bepaald is welke strategie van toepassing is en welke methode hierbij gebruikt wordt, is het tijd voor de uitvoer. In dit hoofdstuk wordt uitgewerkt welke stappen gezet moeten worden.

5.1 Bepalen wie beslisser is

Een belangrijke vraag is, wie moet uiteindelijk de knoop doorhakken over de te volgen strategie? Formeel is dit de familie-eigenaar, als eindverantwoordelijke voor het applicatieportfolio in zijn of haar familie. Echter, de applicatie-eigenaar is niet in alle gevallen ook de informatie-eigenaar. En in één applicatie kan informatie van verschillende eigenaren zitten. De praktijk is dat er vanuit de applicatie-eigenaar afstemming wordt georganiseerd met de informatie-eigenaar of informatie-eigenaren om tot een gezamenlijk besluit te komen.

De Archiefwet, in Amsterdam uitgewerkt in het Besluit Informatiebeheer 2010, bepaalt dat het organisatieonderdeel dat een dossier heeft gevormd, verantwoordelijk is voor het beheer. Dat betekent dat bij een reorganisatie waarbij een taak van het ene organisatieonderdeel wordt overgedragen aan het andere, de latende partij eigenaar blijft van de afgesloten dossiers die in een draaiende applicatie kunnen zitten. Dit is van belang bij het opruimen van de legacy van voor de reorganisatie van 2015: als geen sprake is van een generieke applicatie, maar de taakuitvoering volledig belegd is bij het organisatieonderdeel van de familie-eigenaar, dan kan het besluitvormingsproces vereenvoudigd worden door overdracht van informatie uit te voeren. Hiervoor is een verklaring van overdracht nodig.

Informatie kan bovendien als onderdeel van een ketenproces relevant blijken voor een andere belanghebbende dan de informatie-eigenaar. Een eenvoudig voorbeeld uit de praktijk: in het personele domein werd een applicatie gebruikt om tijdens een reorganisatie het proces "belangstellingsregistratie" te ondersteunen, waarbij medewerkers belangstelling konden tonen voor een vacante functie. Wanneer de matching succesvol was verlopen, dan werd de relevante informatie in een aanstellingsdocument vastgelegd en overgedragen naar het personeelsdossier (in een andere applicatie). Wanneer geen match werd gemaakt, zou de informatie vernietigd moeten worden zodra de beslissing onherroepelijk was. In een aantal gevallen werd bezwaar gemaakt. Daarmee was de informatie niet meer relevant voor het proces "in- en uitdiensttreding", maar wel voor het proces "bezwaar en beroep". De uitkomst van het proces "bezwaar en beroep" kan vervolgens weer leiden tot een nieuwe zaak in het proces "in- en uitdiensttreding". Een belangrijke vraag is dus: kan de informatie die ontstaan is vanuit het ene proces nog een rol spelen in een ander proces. Daarbij de beperking in ogenschouw nemend dat persoonsgegevens alleen mogen worden gebruikt voor het doel waarvoor ze verzameld zijn.

5.2 Presenteer analyse in memo

Wanneer de analyse is uitgevoerd – waaruit blijkt welke strategie gevolgd wordt en welke methode hierbij gebruikt wordt – zal de beslisser een keuze moeten maken. Stel een memo op gericht aan de beslisser met daarin de volgende opbouw:
- Inleiding (wat is het probleem en wie is de probleemeigenaar);
- Inhoudelijke beschrijving van de informatie (inhoud en vorm);
- Belang van de informatie (voor wie van belang, hoe vaak van belang, waarom van belang);
- Wettelijk kader (bewaartermijnen, vernietigplicht, privacywetgeving);
- Strategie (wel of niet migreren en hoe migreren, voor- en nadelen per variant);
- Advies methode (op welke wijze data al dan niet (deels) veiligstellen).

Houd bij het opstellen van de memo rekening met de lezer. In sommige gevallen is het slim om te verwijzen naar specifieke wetsartikelen, of daaruit te citeren, in andere gevallen kun je juridisch jargon juist beter mijden. Bedenk bij het opstellen van de strategieën en methoden dat de beslisser waarschijnlijk wil weten hoeveel capaciteit en budget vereist is voor de uitvoering. Het is dan ook slim om hierover af te stemmen met de rol waar de financiële onderbouwing belegd is, bijvoorbeeld de projectleider of informatiemanager.

5.3 Functioneel ontwerp

Voor een migratie naar een doelapplicatie (zie §4.2.1) wordt vaak een functioneel ontwerp gemaakt. In het functioneel ontwerp wordt beschreven welke database-elementen worden meegenomen met de migratie en welke niet. Tevens wordt beschreven op welke wijze deze elementen worden ingelezen in de doelapplicatie en hoe de gegevens daar worden getoond. IB heeft in dit proces een rol als kwaliteitsbewaker en denkt mee over welke metagegevens van belang zijn voor de toegankelijkheid en het beheer.

5.4 Testen

In sommige gevallen kan IB een bijdrage leveren aan het testtraject, vooral als het gaat om migratie van gegevens die van belang zijn voor het informatiebeheer. In het testtraject controleert IB of die gegevens volledig en bruikbaar zijn na de migratie.

5.5 Verklaring van migratie

Na acceptatie door de opdrachtgever, wordt een verklaring van migratie opgesteld zoals bedoeld in Art. 25 sub 2 van de Archiefregeling. Een afschrift wordt ter informatie verstrekt aan de Gemeentearchivaris.

5.6 Archiveren export-bestanden

Als gekozen wordt voor een export, dan kan IB adviseren over de beheeromgeving (locatie) waar de exportbestanden worden opgeslagen. Houd er hierbij rekening mee dat een archief de meeste waarde heeft als die toegankelijk is voor de business. De bestanden (uitsluitend) opslaan in een afgeschermde omgeving bij IB of functioneel beheer heeft daarom niet de voorkeur.

5.7 Verlaat uitzetten applicatie

Als gekozen wordt om een oude applicatie nog een bepaalde tijd beschikbaar te houden, is het soms nodig om jaarlijks een deelverzameling te vernietigen. Ook moet worden vastgelegd wanneer de applicatie definitief uit kan, waarbij op dat moment een machtiging en verklaring tot vernietiging voor de informatie in de applicatie nodig zijn. Een keuze moet worden gemaakt vanuit welk kwaliteitssysteem dit wordt bewaakt en wie hierin de lead heeft: bijvoorbeeld de APM'er vanuit Blue Dolphin of de IB'er vanuit het Beheerplan Informatiehuishouding.

I Appendix

i.i Generiek stappenplan voor migratie

Dit stappenplan biedt op hoofdlijnen een houvast bij het opstellen van een migratiestrategie en het bepalen vaan een migratiemethode. Het is bedoeld als hulpmiddel voor informatiebeheerders en niet als beleidskader: niet alle praktijksituaties zullen aansluiten op de hier beschreven methodiek.

In de kolom "Actoren" is aangegeven op welke momenten het verstandig is om af te stemmen met een bepaalde andere vakdiscipline.

Stap	*Actoren*
Stap 0: Bepaal de vorm van de informatie die voor migratie in aanmerking komt	
Alleen documenten	
Alleen gegevens	
Documenten inclusief (meta)gegegevens	
Stap 1: Schat in of veiligstellen data wel/niet nodig is	
Zijn gegevens nodig vanuit archiefbeheerperspectief?	
Gaat het om originele (archiefwaardige) informatie?	
Waarvan de wettelijke bewaartermijn nog niet is verstreken?	
Zo ja: veiligstellen moet, ga verder met stap 2	
Zo nee: ga verder met de volgende criteria	
Gaat het om informatie die vereist is als de toegang tot papieren archieven?	
Zo ja: veiligstellen moet, ga verder met stap 2	
Zo nee: ga verder met de volgende criteria	
Zijn gegevens nodig vanuit businessperspectief?	
Is informatie nog onder handen (lopende zaken)?	
Valt informatie binnen een reguliere rapportageperiode?	
Zo ja: veiligstellen moet, ga verder met stap 2	
Zo nee: ga verder met de volgende criteria	
Wordt informatie wordt nog regelmatig geraadpleegd?	
Zo nee: niet veiligstellen. Vernietigen m.b.v. vernietigingsprotocol	
Zo ja: ga verder met de volgende criteria	
Mag informatie nog gebruikt worden (doelbinding)	PO
Zo nee: niet veiligstellen. Vernietigen m.b.v. vernietigingsprotocol	
Zo ja: ga verder met de volgende criteria	
Is er een positieve business case voor migratie?	
Zo nee: niet veiligstellen. Vernietigen m.b.v. vernietigingsprotocol	
Zo ja: ga verder met stap 2	

Stap 2: Schat in welke methode het meest geschikt is[7]			
Methode	1	Migratie naar doelapplicatie	FB
		Van toepassing als gegevens nodig zijn om proces in de doelapplicatie uit te kunnen voeren	
Methode	2	Gegevens exporteren naar los(se) bestand(en)	FB
		Van toepassing als er geen documenten gemigreerd hoeven te worden, en er in de doelsituatie geen of heel beperkte logica op de data wordt toegepast	
Methode	3	Handmatige invoer	
		Van toepassing als het gaat om een beperkte hoeveelheid informatie	
Methode	4	Screenshots maken of uitprinten	
		Veiligstellen van informatie in records kan door het maken van screenshots, die eventueel kunnen worden uitgeprint en toegevoegd aan het papieren dossier	
Methode	5	Database veiligstellen en toegankelijk houden met BI-tooling	FB, BI
		Van toepassing als de data nog wel relevant is, maar in de praktijk nauwelijks gebruikt wordt	
Methode	6	Oude applicatie laten draaien	FB, LM
		Van toepassing als informatie niet lang meer bewaard hoeft te blijven en weinig wordt geraadpleegd door een kleine gebruikersgroep	
Methode	7	Overbrengen naar of uitplaatsen in e-depot Stadsarchief	FB, SAA
		Van toepassing als informatie voor overbrenging in aanmerking komt	
Stap 3: Migratieplan schrijven			
Methode	1	Migratie naar doelapplicatie	
	Stap 1	Opvragen datamodel uit te faseren applicatie	FB
	Stap 2	Plotten van het "oude" datamodel op dat van de doelapplicatie	FB
	Stap 3	Bedenk of er naast migratie ook conversie nodig is, bijvoorbeeld om documenten die langdurig bewaard moeten worden om te zetten naar duurzame bestandsformaten	
	Stap 4	Bedenk of er nog acties nodig/mogelijk zijn ten aanzien van quick&dirty-dataschoning voorafgaand aan de migratie	
	Stap 5	Migreren en testen	
	Stap 6	Procesafspraken tussen FB en IB over het beheer van de data ten aanzien van (toekomstige) schoning en vernietiging	FB
	Stap 7	Acceptatie en inbeheername	
Methode	2	Gegevens exporteren naar los(se) bestand(en)	
	Stap 1	Exporteer de data naar een leesbaar bestand	FB
	Stap 2	Bepaal waar het bestand wordt opgeslagen, voor hoe lang het bestand beschikbaar moet blijven en wie het beheert en t.z.t. vernietigd, richt autorisaties in	

[7] Combinaties zijn mogelijk.

Methode	3	Handmatige invoer	
	Stap 1	Regel resources	
	Stap 2	Voer kwaliteitscontrole uit	
	Stap 3	Acceptatie en inbeheername	
Methode	4	Screenshots maken of uitprinten	
	Stap 1	Regel resources	
	Stap 2	Leg documenten vast in dossiers	
Methode	5	Database veiligstellen en toegankelijk houden met BI-tooling	
	Stap 1	Bepaal of er schoning van de database plaats moet vinden en hoe deze kan worden uitgevoerd	FB
	Stap 2	Ontwerp standaardrapportages waarmee de data gebruikt kan worden	BI
	Stap 3	Beleg het beheer van de data ten aanzien van beschikbaarheid (wie heeft toegang nodig en hoe is die toegang georganiseerd) alsook toekomstige schoning en vernietiging	BI
Methode	6	Oude applicatie laten draaien	
	Stap 1	Bepaal of er schoning van de database plaats moet vinden en hoe deze kan worden uitgevoerd	
	Stap 2	Bepaal hoeveel licenties nodig zijn en richt autorisaties in	FB, LM
	Stap 3	Leg vast wanneer de applicatie definitief uitgezet kan worden	APM
Methode	7	Overbrengen naar of uitplaatsen in e-depot Stadsarchief	
	Stap 1	Voer een intakegesprek met het Stadsarchief	SAA
	Stap 2	Maak afspraken over toegang tot de informatie	SAA
	Stap 3	Procesafspraken met SAA maken over beheer van de data	SAA
	Stap 4	Opvragen datamodel uit te faseren applicatie	FB
	Stap 5	Plotten van het "oude" datamodel op dat van de doelapplicatie	FB/SAA
	Stap 6	Voer waar nodig conversie uit om documenten die langdurig bewaard moeten worden om te zetten naar duurzame bestandsformaten	
	Stap 7	Migreren en testen	
	Stap 8	Acceptatie en inbeheername	
Stap 4: Verklaring van migratie opstellen			
	Stel een verklaring van migratie op en stuur ter kennisname naar SAA		

FB = Functioneel Beheer
PO = Privacy Officer
BI = Business Intelligence
LM = Leveranciersmanagement
APM = Applicatieportfoliomanagement
SAA = Stadsarchief Amsterdam

i.ii Modelverklaring van conversie en/of migratie

Verklaring van conversie en/of migratie

Gelet op artikel 25 lid 2 van de Archiefregeling

Gezien het migratieplan, testplan met de testverslagen waaruit blijkt dat;
• Het de archiefbestanden betreft ..... (beschrijf welk databestand het betreft);
• Er geen onacceptabele afwijkingen zijn opgetreden aan de inhoud, structuur, vorm, authenticiteit, samenhang en ordeningsstructuur van de gemigreerde en/of geconverteerde data;
• De gemigreerde en/of geconverteerde data in nieuw systeem toegankelijk, vindbaar en raadpleegbaar zijn;
• De data uit het oude systeem zodanig zijn verwijderd dat ze niet meer gereproduceerd kunnen worden anders dan met het doelsysteem.

..... (naam) verklaart in de rol van directeur van het organisatieonderdeel .....dat de gegevensconversie van ..... (oude systeem) naar ..... (doelsysteem) is voltooid en uitgevoerd volgens het migratieplan.