Rapport

Digitaal archiefbeheer in de praktijk

Handboek

Filip Boudrez
Hannelore Dekeyser

Stadsarchief Antwerpen

Digitaal archiefbeheer in de praktijk

Handboek

Filip Boudrez
Hannelore Dekeyser

DAVID werd gefinancierd door het FWO-Vlaanderen in het kader van het Max Wildiersfonds. Het stadsarchief Antwerpen en het ICRI (KULeuven) waren de projectpartners van het DAVID-project.

Rapporten van het stadsarchief Antwerpen.
Reeds verschenen

1. *Kabinetsarchieven van de Antwerpse burgemeesters en schepenen: waarde en ordeningsplan*, Jan Anckaer, Maarten De Baere, Werner Pottier, Inge Schoups, Willem Vanneste, 2002, 50 p.
2. *Auteursrechten audiovisuele archieven. Film en geluidsarchieven,* Ann Leysen, 2003, 88 p.
3. *Krachtlijnen conserveringsbeleid. Geluidsarchieven,* Liesbeth Baaten, 2003, 47 p.
4. *E-mailarchieven. E-mails: hoe bewaren en goed archiveren,* Filip Boudrez, 2003, 64 p.

STADSARCHIEF ANTWERPEN
Venusstraat 11, 2000 Antwerpen
Tel. + 32 (0)3 206 94 11 – Fax + 32 (0)3 206 94 10
E-mail: stadsarchief@stad.antwerpen.be
eFLORISwebsite: http://stadsarchief.antwerpen.be

Leeszaal: dinsdag tot vrijdag van 8.30 tot 16.30 uur
Opvragen stukken van 8.30 tot 12.00 en 13.00 tot 15.30 uur
Administratie: maandag tot vrijdag van 8.30 tot 16.30 uur.

Eindredactie: Filip Boudrez, Hannelore Dekeyser, Inge Schoups, Roberte Van Haute, Willem Vanneste

Ontwerp en opmaak: Katrien Daemers en Jessika L'Ecluse/ Gestalte
en grafisch centrum stad Antwerpen (kaft)

Drukwerk: grafisch centrum stad Antwerpen
Verantwoordelijke uitgever: Inge Schoups, Venusstraat 11, 2000 Antwerpen
Wettelijk depotnummer: D/2004/0306/102

Inhoud

> DEEL 2: ARCHIEFLUIK

Voorwoord

Digitaal Archiveren in Vlaamse Instellingen en Diensten (DAVID) was het eerste onderzoeksproject inzake digitale archivering in Vlaanderen. Het stadsarchief Antwerpen was samen met het Interdisciplinair Centrum voor Recht en Informatica projectpartner van het DAVID-project. DAVID werd gefinancierd door het FWO-Vlaanderen in het kader van het Max Wildiersfonds. Het project liep van januari 2000 tot en met december 2003.

DAVID had tot doel te onderzoeken hoe digitale archiefdocumenten op een duurzame en betrouwbare wijze in samenhang met hun context worden gearchiveerd. DAVID zocht op basis van specifieke onderzoekscases archiveringsoplossingen voor alle types digitale archiefdocumenten. Bijzondere aandacht ging uit naar de archivering van digitale archiefdocumenten die het resultaat zijn van nieuwe technologieën zoals e-mail en internet. Buitenlandse ervaringen toonden immers aan dat archiefdiensten best vanaf de creatie van deze archiefdocumenten met hun archiveringsprocedures starten.

Voor elke onderzoekscase werd eerst het juridische kader uitgetekend. Binnen dit kader werd vervolgens een archiveringsoplossing uitgewerkt. Het onderzoek werd hierbij zoveel mogelijk aan de praktijk getoetst. De digitale archiefdocumenten van de Antwerpse stedelijke administratie vormden de praktische casussen van het project. De archiveringsstrategieën die DAVID uitwerkte, werden gaandeweg in de stadsadministratie uitgetest en geïmplementeerd. De feedback vanuit de praktijk werd teruggekoppeld naar de DAVID-rapporten.

In de loop van het project werden alle tussentijdse rapporten, richtlijnen en adviezen, artikels, voorbeelden, presentaties, enz. op de projectwebsite (http://www.antwerpen.be/david) gepubliceerd. Deze website blijft ook na het einde van het project on line beschikbaar en wordt nog zoveel mogelijk geactualiseerd.

Het DAVID-project werd afgerond met de publicatie van het vademecum *Digitaal archiefbeheer in de praktijk. Handboek*. In het eerste deel analyseert Hannelore Dekeyser (ICRI) het juridische kader waarbinnen digitale archivering gebeurt. Digitale archivering dient immers in overeenstemming te zijn met o.a. de archiveringsplicht, de openbaarheid van bestuur, de bescherming van de privacy en het auteursrecht. Het archiefluik vormt het tweede deel van het vademecum en is van de hand van Filip Boudrez (stadsarchief Antwerpen). Vertrekkend vanuit de algemene problematiek van digitaal archiveren worden de mogelijke bewaarstrategieën voor digitale archiefdocumenten geëvalueerd en wordt de DAVID-bewaarstrategie voorgesteld. Archiveringsstandaarden spelen een belangrijke rol in deze bewaarstrategie en worden in het volgend hoofdstuk toegelicht. In het laatste hoofdstuk worden twee archiveringsstrategieën voorgesteld: één voor kantoordocumenten en één voor informatiesystemen.

Voorliggend Technisch Rapport van het stadsarchief Antwerpen bevat het vademecum van het DAVID-project. Deze papieren uitgave is een tijdsopname want het is de intentie om de on line versie te blijven actualiseren.

Juli 2004

DEEL 1

JURIDISCH LUIK

A. Inleiding

In de meest eenvoudige termen uitgedrukt, stellen zich op juridisch vlak twee fundamentele vragen:
– Waarom archiveren?
– Hoe archiveren?
In het juridisch luik van dit handboek zullen deze twee vragen dieper uitgewerkt worden.

1. Waarom archiveren?

Eenvoudig gesteld zijn er drie redenen om bepaalde informatie te archiveren:
– Omdat het moet op grond van een wet.
– Omdat je het beloofd hebt in een contract.
– Omdat het in je eigen belang is.
In dit handboek wordt op de eerste plaats de wettelijke verplichting nader bekeken in deel B. Bewaren en het recht.

2. Hoe archiveren?

Eenmaal vastligt dat archiveren noodzakelijk of wenselijk is, moet men zich uiteraard afvragen hoe dit concreet te organiseren. Het recht legt een aantal beperkingen en/of verplichtingen op waaraan moet voldaan worden. De volgende prangende kwesties dringen zich op:
– Mag het archiefdocument in digitale vorm bewaard worden?
– Wat met de bescherming van de persoonlijke levenssfeer?
– Hoe zit het met de openbaarheidsverplichtingen?
– Welke impact heeft het auteursrecht?
Bovenop deze algemene kwesties kan voor elk type archiefdocument nog andere specifieke wet- en regelgeving gelden.

B. Bewaren en het recht

Bewaarverplichtingen vind je terug in verschillende wetten en regels. Hierna volgt een overzicht van een aantal juridische bewaarverplichtingen, zonder evenwel exhaustief te zijn. Zowel de overheid als particulieren moeten in heel wat gevallen documenten bewaren. Voor de overheid bestaat een algemene regeling, terwijl voor particulieren alleen bijzondere gevallen geregeld zijn. Hierna volgt een overzicht van de belangrijkste bewaarverplichtingen in de publieke en de private sector[1].

1. De publieke sector

1.1. De archiefwet

De archiefwet van 24 juni 1955[2] verplicht de overheid haar archiefdocumenten te bewaren. Het oorspronkelijk doel van de wet was het onderwijs en het wetenschappelijke onderzoek te bevorderen, door ons land met een degelijke archiefdienst toe te rusten. De uitvoering van deze kaderwet is beperkt gebleven tot het koninklijk besluit van 12 december 1957 betreffende de uitvoering van de archiefwet (archief-KB)[3]. Het Algemeen Rijksarchief houdt toezicht op de naleving van de wet.

Wie?

De archiefwet is van toepassing op alle overheden die deel uitmaken van de uitvoerende of de rechterlijke macht. Het gaat dus om rechtbanken en administraties op federaal, regionaal, provinciaal en gemeentelijk niveau. De wetgevende macht valt buiten deze regeling (art. 1 archiefwet).

Wat?

De genoemde overheden mogen hun 'archiefbescheiden' of archiefdocumenten niet vernietigen zonder de toestemming van de Algemene Rijksarchivaris (art. 5 archiefwet).
De term 'archiefbescheid' wordt niet gedefinieerd in de wet, maar het gaat om alle documenten die ongeacht hun vorm, drager of datum, naar hun aard bestemd zijn om te berusten onder de persoon, groep personen of organisatie die het document heeft ontvangen of opgemaakt uit hoofde van zijn of haar taken of ter handhaving van zijn of haar rechten[4].
Overheden mogen hun archieven niet zomaar op eigen initiatief vernietigen, maar toch moeten niet alle archiefstukken worden bewaard. De grote massa documenten die een overheid produceert maakt dit onmogelijk. Sommige documenten hebben bovendien geen enkele archiefwaarde op lange termijn. Het is niet doenbaar om telkens bij de vernietiging van een document de toestemming van de Algemene Rijksarchivaris te vragen. Uit de praktijk is een pragmatische oplossing gegroeid in de vorm van selectielijsten opgesteld door de Algemene Rijksarchivaris. Deze lijsten kan de overheid dan hanteren als richtlijn om te beslissen welke documenten worden bewaard.

Hoe?

De archiefwet verplicht de overheden, de gemeenten uitgezonderd, hun archiefdocumenten van meer dan honderd jaar oud te deponeren bij het rijksarchief. Jongere documenten die geen nut meer hebben voor de overheid kunnen op verzoek gedeponeerd worden.
Tot aan de deponering moeten de overheden hun archiefdocumenten zelf in goede, geordende en toegankelijke staat bewaren. In de praktijk bleek die termijn van honderd jaar niet haalbaar. De meeste overheden hebben geen archiefdienst die daarvoor is uitgerust. In de praktijk worden

documenten reeds neergelegd na een termijn van dertig jaar. Bescheiden die nog geen dertig jaar oud zijn, mogen op verzoek van die overheden in het rijksarchief worden neergelegd.
Overheden kunnen vrijgesteld worden van de deponeringsverplichting (art. 1 archiefwet), maar moeten dan zelf hun archief bewaren. Verschillende ministeries[5] en provincies kregen reeds zo'n vrijstelling.
Voor de gemeenten en openbare instellingen gelden andere regels. Zij moeten hun archiefdocumenten bewaren ongeacht de leeftijd ervan. Het rijksarchief kan de archieven opeisen wanneer een gemeente deze taak niet naar behoren vervult.

Opmerkingen
Sinds de staatshervorming bestaan er nog enkele andere bestuursniveaus buiten deze opgesomd in de archiefwet. Zolang de gemeenschappen en de gewesten zelf geen archiefregels uitwerken, blijft de archiefwet op hen van toepassing. Tot nu toe vaardigde alleen het Waals gewest een eigen archiefdecreet uit[6].

Meer informatie:
S. VAN DEN EYNDE, Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1, *Stadsarchief Antwerpen - ICRI K.U.Leuven, Antwerpen - Leuven, p. 11 e.v.*, *http://www.antwerpen.be/david/teksten/Rapporten/Rapport3.pdf*
F. SCHRAM, Overzicht archiefwetgeving, *http://user.online.be/~fschram/wetlijst3.html*.

1.2. Specifieke regels
In de publieke sector bestaat ook specifieke reglementering over de bewaring van bepaalde stukken. Enkele voorbeelden:
- Artikel 76 §2 Raad van State wet: "de leden van het auditoraat worden ermee belast de documentatie betreffende de rechtspraak van de Raad van State in de vorm van geautomatiseerde bestanden bij te houden, te bewaren en ter beschikking te stellen".
- Artikel 40 en 43 burgerlijk wetboek: "De akten van de burgerlijke stand worden, in iedere gemeente, ingeschreven in een of meer dubbel gehouden registers. Binnen een maand wordt het ene dubbel neergelegd in het archief van de gemeente, het andere op de griffie van de rechtbank van eerste aanleg."
- Artikel 19 § 6 lid 2 van de wet van 20 juli 1990 betreffende de voorlopige hechtenis: de griffier bewaart eensluidende afschriften van de dossiers van alle aangehoudenen op de griffie.
- Artikel 124 Hypotheekwet: De hypotheekbewaarder is gehouden een aantal registers aan te maken en te bewaren. De titel van hypotheekbewaarder wijst er reeds op dat hij of zij niet enkel moet zorgen dat de door de wet vermelde akten en titels worden overgeschreven in de registers, maar ook dat de hypothecaire bescheiden in goede staat bewaard worden. Daartoe houdt de hypotheekbewaarder een archief in zijn hypotheekkantoor[7].
- Artikel 105.4 van het reglement van de Kamer bepaalt dat de griffier, die de Kamer zelf benoemt, het archief van de Kamer bewaart[8]. Hetzelfde geldt voor de Senaat (art. 92.3 van het reglement van de Senaat)[9].

Naast deze bijzondere regels bepaalt de strafwet nog dat een nalatige bewaarder bestraft kan worden wanneer "stukken of gerechtelijke procesakten ofwel andere papieren, registers, geïnformatiseerde of magnetische dragers, akten of voorwerpen die in archieven, griffies of openbare bewaarplaatsen berusten, of die aan een openbaar bewaarder in die hoedanigheid zijn toevertrouwd, worden ontvreemd of vernietigd" (art. 240 strafwet).

2. De private sector

Een equivalent voor de archiefwet bestaat niet in de private sector. Er is wel een lappendeken van verschillende specifieke en sectoriële bewaarverplichtingen. Hierna volgen enkele voorbeelden.

2.1. Handelsrecht

Handelaars (zowel natuurlijke als rechtspersonen) zijn verplicht een voor de aard en de omvang van hun bedrijf passende boekhouding te voeren[10]. De boekhouding omvat alle verrichtingen, bezittingen, vorderingen, schulden en verplichtingen van welke aard ook. Alle gebeurtenissen die een invloed hebben op de vermogenstoestand van de onderneming moeten met andere woorden worden opgenomen in de boeken. De onderneming moet de boeken (zijnde de balans, de resultatenrekening en de toelichting) bewaren gedurende 10 jaar[11]. Bovendien moet elke boeking in de boeken steunen op verantwoordingsstukken die ook gedurende 10 jaar moeten worden bewaard[12].

2.2. Het notariaat

Notarissen moeten de minuten bewaren van alle akten die zij verlijden[13]. Hiertoe houden ze een repertorium waarin alle akten worden geregistreerd in de volgorde waarin ze zijn verleden. Deze originelen mogen ze in principe nooit uit handen geven. Indien de minuten die zij houden tenminste honderd jaar oud zijn, mogen zij hun archief overdragen aan het rijksarchief binnen de provincie waarin hun ambtsgebied is gelegen[14].

2.3. Sociale documenten

Het koninklijk besluit nr. 5 van 23 oktober 1978 legt aan de werkgever het bewaren op van de zogenaamde sociale documenten[15]. Als sociale documenten worden beschouwd: het personeelregister, de individuele rekening, het aanwezigheidsregister en de sociale identiteitskaart.
In het kader van de modernisering van de overheid worden de sociale documenten stilaan afgebouwd. Sinds 1 januari 2003 is de onmiddellijke aangifte van tewerkstelling via het internet (Dimona: https://www.socialsecurity.be/site_nl/Applics/dimona/index.htm) verplicht voor alle werkgevers, behalve in enkele uitzonderlijke gevallen. Een correcte Dimona-aangifte stelt de werkgever vrij van een aantal verplichtingen met betrekking tot het bijhouden van de sociale documenten[16]. Zo hoeft het personeelsregister niet langer aangevuld te worden. De Dimona-aangifte vervangt iedere nieuwe inschrijving in het register. Oude papieren registers moeten natuurlijk nog wel bewaard worden. Een gelijkaardige vrijstelling bestaat nog niet voor de individuele rekening, maar wordt wel in het voorruitzicht gesteld.

2.4. Vennootschapsrecht

Alle documenten waarvan de opmaak door de vennootschappenwet is voorgeschreven, dienen bewaard te worden gedurende 5 jaar vanaf de bekendmaking van de afsluiting van de vereffening van de vennootschap op de plaats die de algemene vergadering aanwijst[17]. Deze bewaringsplicht behelst onder andere de registers van de aandelen op naam, het register van de obligaties op naam, de notulen van de vergaderingen, verslagen van commissarissenrevisoren, aanwezigheidslijsten van vergaderingen, processen-verbaal van de algemene vergaderingen ...

2.5. Belastingrecht

De belastingplichtige is verplicht alle documenten te bewaren die noodzakelijk zijn voor de bepaling van het belastbaar inkomen[18]. Voor handelaars/belastingplichtigen volstaat het daarbij niet om enkel de wettelijk verplichte boekhoudkundige bescheiden of boeken te bewaren[19].

2.6. Financieel recht

De Preventiewet inzake witwassen van geld bepaalt dat bepaalde ondernemingen, zoals kredietinstellingen en verzekeringsmaatschappijen, zich dienen te vergewissen van de identiteit van hun cliënten aan de hand van een bewijsstuk op het ogenblik dat zij een zakenrelatie aanknopen waardoor de betrokkenen gewone cliënten worden[20]. Artikel 7 van die wet vereist dat een afschrift van dat bewijsstuk wordt bewaard gedurende 5 jaar na het beëindigen van de relatie.

Meer informatie:

J. DUMORTIER, Op-Slag Bewezen. Juridische mogelijkheden en moeilijkheden bij het opzetten van een elektronisch documentbeheersysteem, *Brussel, Keesing Publishers - BelAIIM, 2002, 66 p.*

H. DEKEYSER en J. DUMORTIER, 'Elektronisch archiveren', in X. (ed.), Tendensen in het bedrijfsrecht. Contracteren zonder papier, *Brussel, Bruylant, 2003, 207-236.*

3. Waarom bestaan deze wettelijke bewaarverplichtingen?

De wettelijke bewaarverplichtingen zijn ingevoerd om verschillende redenen. De archiefwet heeft onder meer als doel het onderwijs en het wetenschappelijke onderzoek te bevorderen. In de private sector vinden de bewaarplichten hun grondslag in het onmiddellijke nut van een document voor de archiefvormer of voor een derde. De latere cultuurhistorische waarde of het wetenschappelijke belang is minder doorslaggevend. Documenten worden bewaard omdat ze in de toekomst nog een functie moeten vervullen. Het recht onderscheidt vooral drie primaire functies die een archiefstuk kan vervullen:

1. controle en verantwoording
2. bewijs
3. de bescherming van de belangen van derden.

3.1. Controle en verantwoording

Documenten worden in het algemeen bewaard om de efficiëntie van de werkprocessen van een organisatie te bevorderen. Daarbovenop eist het recht de bewaring van documenten om anderen in staat te stellen controle uit te oefenen. Dit is het geval voor de bewaringsverplichtingen uit het belastingrecht, voor de sociale documenten en voor overheidsdocumenten.

Waar de boekhoudverplichting voor handelaars vooral de rechten van derden wil beschermen, wordt de plicht ten aanzien van de belastingplichtige om alle documenten (onder andere de boekhouding) te bewaren die van belang zijn om het belastbaar inkomen te bepalen, verantwoord vanuit de controlemogelijkheid waarover de belastingadministratie moet kunnen beschikken. Men moet kunnen nagaan of de aangegeven inkomsten wel overeenstemmen met de werkelijke inkomsten.

De werkgever moet de sociale documenten gedurende een bepaalde periode bewaren met het oog op een efficiënte controle op een juiste toepassing van de wettelijke bepalingen inzake tewerkstelling[21].

Overheidsdocumenten dienen in de eerste plaats te worden bewaard voor controledoeleinden omdat politici verantwoording verschuldigd zijn aan de rechtsonderhorigen door wie ze zijn verkozen om hen te vertegenwoordigen[22]. De bewaring van beleidsdocumenten maakt het mogelijk dat politici op elk moment ter verantwoording kunnen worden geroepen, zelfs verschillende legislaturen later. De archivering van deze documenten draagt dus bij tot het democratische gehalte van een samenleving. In dit verband is de reglementering omtrent de openbaarheid van bestuur van belang.

3.2. Bewijs

Het burgerlijk bewijsrecht met betrekking tot verbintenissen[23] kent aan een geschrift meer waarde toe dan aan de andere bewijsmiddelen, zoals bijvoorbeeld getuigen. Een onderhandse akte, zijnde een ondertekend geschrift dat speciaal werd opgemaakt om als bewijs te dienen, heeft bovendien meer waarde dan een ander geschrift (bijvoorbeeld een brief). Om van de bijzondere bewijswaarde van de onderhandse akte te kunnen profiteren, is het van belang dat deze akte voorhanden is op het moment dat er een betwisting ontstaat. Artikel 1341 burgerlijk wetboek stelt dat een akte voor een notaris of een onderhandse akte moet worden opgemaakt van alle zaken die de som of de waarde van 375 Euro te boven gaan. Maar het spreekt voor zich dat het niet volstaat dat er een notariële of onderhandse akte wordt opgemaakt. Wat de wetgever hier eigenlijk ook bedoeld heeft, is dat die akte aan de rechter moet kunnen worden voorgelegd op het moment dat er een verbintenis met een waarde boven de 375 Euro ter discussie staat. Artikel 1341 burgerlijk wetboek legt dus onrechtstreeks de verplichting op om akten te bewaren.

Notariële akten moeten in het archief van de notaris bewaard worden. Authentieke akten hebben een hogere bewijswaarde dan onderhandse akten. Het is immers niet toegelaten om de inhoud van een authentieke akte te weerleggen. De inhoud ervan kan enkel betwist worden door een procedure te voeren tot inschrijving wegens valsheid, wat een zeer zware strafrechtelijke procedure is. Het is dan ook het hoogste bewijsmiddel in de hiërarchie. De authentieke akte opgemaakt door de notaris heeft een dergelijke grote waarde net omdat deze bewaard wordt op een veilige plaats door een betrouwbare persoon, namelijk de notaris. Authentieke akten van andere openbare ambtenaren bieden niet altijd dezelfde waarborgen op het vlak van de bewaring[24]. Bewaring van akten is dus niet enkel vereist om het gepaste bewijs te kunnen leveren op het juiste moment, maar soms ook om een bijzondere bewijswaarde toe te kennen aan bepaalde bewijsmiddelen.

De ambtenaar van de burgerlijke stand zorgt voor de bewaring van de door hem/haar opgestelde akten. Deze akten van de burgerlijke stand zijn de instrumenten waarmee men zijn bezit van staat zal kunnen bewijzen. Iedere natuurlijke persoon leeft in bepaalde verhoudingen tot zijn medeburgers. Het geheel van deze verhoudingen wordt de staat van de persoon genoemd. Hierdoor bepaalt men de juridische toestand zowel in de familie als in de maatschappij. Gezien het belang van het bezit van staat is het noodzakelijk dat zowel de vaststelling (bijvoorbeeld door geboorte, huwelijk of overlijden) als de wijziging ervan (via erkenning, adoptie of echtscheiding) op een ondubbelzinnige wijze komt vast te staan en dat de bewijzen ervan zorgvuldig bewaard worden[25].

De preventiewet inzake de bestrijding van het witwassen van geld legt aan bepaalde financiële instellingen de plicht op om de identificatiestukken te bewaren van hun cliënten. Dit is ingegeven door de vaststelling dat malafide personen die instellingen gebruiken als kader om transacties uit te voeren met criminele bedoelingen. Het feit dat deze informatie moet gearchiveerd worden, ondersteunt de strafrechtelijke bestrijding van het witwassen. In financiële aangelegenheden kan een strafrechtelijke opsporing slechts tot een succesvolle vervolging leiden, indien er een spoor van bewijsmiddelen (paper trail) kan worden gereconstrueerd dat het bewijs van de overtreding van de strafwet levert[26]. Die archiveringsplicht in de nationale anti-witwaswetgevingen is ingegeven door de bewijsmoeilijkheden die de overheid steeds weer ondervond bij de vervolging van witwasmisdrijven.

3.3. Bescherming van de belangen van derden

De boekhouding is ontstaan als bewijsinstrument en als middel ter bescherming van derden. De boekhoudverplichtingen werden aanvankelijk enkel opgelegd aan vennootschappen met beperkte aansprakelijkheid met het oog op de bescherming van de belangen van de aandeelhouders (waaraan rekening en verantwoording moest worden afgelegd) en van de schuldeisers (die het risico inzake het verhalen van hun schuldvordering moesten kunnen inschatten)[27]. Sinds de nieuwe boekhoudwetgeving van 1975 is de boekhouding op de eerste plaats een beheersinstrument voor de onderneming. Het voeren van een boekhouding volgens precieze en eenvormige normen, is een essentiële voorwaarde voor het goede beleid van de ondernemingen, voor de harmonie in de sociale relaties binnen de bedrijven, voor de bescherming van de rechten van de schuldeisers

en voor het uitoefenen van bepaalde controles en bevoegdheden door de overheid[28]. De boekhouding verenigt met andere woorden de drie juridische bewaringscriteria in zich. De stukken waarop de boekingen in de boeken steunen, moeten gedurende 10 jaar worden bewaard om als bewijs te dienen tegenover derden en met het oog op controles door de overheid[29].
Alle vennootschappen zijn nu dan ook onderworpen aan één of andere boekhoudverplichting. De rechtspraak aanvaardt trouwens dat de beschikbaarheid van informatie met zich brengt dat men mag verwachten van een voorzichtige ondernemer dat hij bij het aangaan van een belangrijke handelsrelatie de jaarrekeningen consulteert. De boekhouding blijft dus ook nu nog een belangrijk middel ter bescherming van de belangen van derden.
De bewaringsplicht ten aanzien van vennootschapsdocumenten werd opgelegd ter bescherming van de rechten van de schuldeisers. Tot 5 jaar na de vereffening van de vennootschap kunnen zij immers rechtsvorderingen instellen tegen de vereffenaars van de vennootschap[30].
De hypothecaire inrichting in België is speciaal opgericht ter bescherming van de belangen van derden. Het verplicht houden van de hypothecaire bescheiden door de hypotheekbewaarder, zoals dit is vervat in de hypotheekwet, dient om de deelnemers aan het rechtsverkeer op de hoogte te stellen van de rechtstoestand van een onroerende goederen, omdat deze één van de belangrijkste zekerheden opleveren voor het kredietwezen. (Toekomstige) schuldeisers kunnen aan de hand van de hypothecaire registers nagaan wie er op een bepaald moment titularis is van een zakelijk recht op een onroerend goed. Ze vinden er ook informatie omtrent de mate waarin een onroerend goed bezwaard is met een zakelijk zekerheidsrecht (een voorrecht of een hypotheek).
De dossiers van alle aangehoudenen dienen op de griffie bewaard te worden ter bescherming van de rechten van verdediging van de beschuldigden. Zij mogen hun dossier inkijken op de griffie van de rechtbank waarvoor de strafvordering aanhangig is die tegen hen is ingesteld.

C. Mag digitaal archiveren?

De vraag of digitaal archiveren juridisch wel mag speelt bij veel overheden, maar ook bij bedrijven en particulieren. Het recht legt expliciet of impliciet heel wat bewaringsplichten op ten aanzien van bepaalde documenten. Veel van die documenten worden vandaag de dag aangemaakt met behulp van informaticamiddelen. Maar voldoet een digitaal document wel aan alle juridische verplichtingen? Of moet dezelfde informatie ook nog op papier bewaard worden?
Het gebeurt uiterst zelden dat een wet expliciet zegt welke vorm een document mag aannemen. Men ging er oorspronkelijk gewoon van uit dat een document een papieren stuk was. Omdat het recht meestal vaag blijft over de vorm van een document, is er veel ruimte voor interpretatie. Voor elk concreet type document moeten we uit allerlei omstandigheden afleiden of het rechtsgeldig in digitale vorm gemaakt en/of bewaard mag worden. Hierna schetsen we een conceptueel kader om dit proces te begeleiden.

1. Creatie van een digitaal document

Aan de redactie van elk document gaat een voorbereidende fase vooraf. Eerst is er een kladversie, op papier of in digitale vorm. De definitieve versie van een document wordt in de regel in digitale vorm opgesteld met behulp van een tekstverwerker. De meeste documenten worden eveneens afgedrukt.
Soms worden papieren documenten ook omgezet naar een digitale versie via allerlei scanningtechnieken. In sommige organisaties worden alle inkomende brieven ingescand en enkel nog in digitale vorm gebruikt.
In principe kunnen al deze stukken in aanmerking komen voor archivering, afhankelijk van hun archiefwaardigheid. Om te weten of digitaal archiveren afdoende is, moet in de eerste plaats naar de rechtsgeldigheid van het digitale document gekeken worden.

1.1. Het digitale document is rechtsgeldig

Indien de wet uitdrukkelijk stelt dat het digitale document rechtsgeldig is, dan mag het document uiteraard aangemaakt worden in digitale vorm. Zo'n uitdrukkelijke bepaling komt erg zelden voor. De wet tot invoering van de elektronische handtekening[31] geeft enkele voorbeelden:
– de onderhandse akte voorzien van een elektronische handtekening is ontvankelijk
– elke kennisgeving, in de zin van de toezending van een akte van rechtspleging, kan voortaan ook per e-mail gebeuren.

Wanneer een digitaal document geldig gemaakt mag worden, ligt het voor de hand dat het ook geldig in digitale vorm bewaard mag worden. Toch is dit niet noodzakelijk altijd het geval.

1.2. Alleen het papieren document is rechtsgeldig

Nog zeldzamer is het geval waar de wet uitdrukkelijk stelt dat een document op een papieren drager gemaakt moet worden. De reden is eenvoudig: papier was zo vanzelfsprekend dat een uitdrukkelijke vermelding overbodig was.
Sommige organisaties scannen papieren documenten in om praktische redenen. De digitale versie van het papieren stuk mag gearchiveerd worden, maar is voor juridische doeleinden vaak onvoldoende.

1.3. De wet zegt niets over de rechtsgeldigheid

Deze situatie is het meest voorkomende geval. Hier moet men uit de context afleiden of het document in kwestie al dan niet rechtsgeldig is in digitale vorm. De functionele equivalentie theorie dient hierbij als richtlijn. Bij elk type document moet men zich de volgende vragen stellen:

Welke vormvereisten worden opgelegd?

Vormvereisten kunnen in drie categorieën ingedeeld worden:

- uiterlijke vormvereisten: bijvoorbeeld de afmetingen en de kleur van een document, gebruik van een stempel, zegel of watermerk, de vereiste dat een geschrift wordt opgesteld
- redactionele vormvereisten: bijvoorbeeld voorkomen van een handtekening, doorlopende nummering, verplichte inhoudelijke vermeldingen, volgorde van de gegevens, parafering van elke bladzijde, layout van het document
- vereisten met betrekking tot de bewaring: bijvoorbeeld bewaren van meerdere exemplaren, de plaats van bewaring, inbewaargeving bij een derde.

Wat is het doel van elke vormvereiste?

Vormvereisten worden ingezet om de meest uiteenlopende doelstellingen te verwezenlijken. Elk type document moet apart bekeken worden in zijn juridische context om te achterhalen wat de bedoeling is van deze of gene vormvereiste. Enkele doelstellingen komen regelmatig terug en daarvan worden er hier enkele uitgelicht.

- identificatie van de betrokkenen: de handtekening is hiervan het voorbeeld bij uitstek, maar ook handgeschreven vermeldingen horen in deze categorie thuis
- integriteit van de inhoud: bijvoorbeeld de handtekening, geschrift, bewaren van meerdere exemplaren, bewaargeving bij een derde, doorlopende nummering, parafering
- controle van de inhoud: bijvoorbeeld verplichte inhoudelijke vermeldingen op het kiezersregister
- bescherming van de bestemmeling: bijvoorbeeld verplichte inhoudelijke vermeldingen met belangrijke informatie.

Kan de vormvereiste vervuld worden in een digitale context?

Bij elke vormvereiste moet men nagaan of de vormvereisten, zoals omschreven door de wet, vervuld kunnen worden in een digitaal document.

Veruit de meeste vormvereisten kunnen op zijn minst geïmiteerd worden in een digitaal document, denk aan de kleur, doorlopende nummering, volgorde van de gegevens en layout. Andere vormvereisten kunnen zonder meer in digitale vorm vervuld worden omdat de wet omschrijft hoe dit moet gebeuren. Dit is het geval voor de handtekening, de verplichte vermeldingen en het geschrift[32].

Sommige vormvereisten kunnen niet nagebootst worden, tenminste niet in de zin van de wet, bijvoorbeeld de stempel, de zegel of het watermerk. In deze gevallen is alleen het papieren document rechtsgeldig.

Is het doel van de vormvereiste vervuld in een digitale context?

Het volstaat niet dat een vormvereiste kan geïmiteerd worden in een digitaal document, het doel van de vormvereiste moet eveneens vervuld zijn. Zoniet is de digitale implementatie geen functioneel equivalent van de traditionele vormvereiste. Zoals gezegd moeten al deze vragen geval per geval onderzocht worden. Hier volgen slechts enkele voorbeelden ter illustratie.

- De doorlopende nummering: het nummeren van elk blad moet de vernietiging of invoeging van bladen voorkomen. Manipulaties zullen dan onmiddellijk opvallen. In een digitaal document kunnen ook doorlopende pagina- of bladnummers opgenomen worden. Het doel van de vormvereiste, namelijk de integriteit garanderen, wordt hiermee niet bereikt.

– Bewaring door een derde: bijvoorbeeld neerlegging bij een notaris.
  • Deze vereiste moet in eerste instantie de fysieke bewaring van een document zeker stellen. Net als bij papieren documenten, kan een derde belangrijke garanties bieden voor de bewaring van digitale documenten.
  • Vervolgens wordt een derde regelmatig ingeschakeld om manipulatie van documenten uit te sluiten. Opnieuw geldt dit evenzeer voor digitale documenten.
  • Ten slotte moet bewaring door een derde de integriteit van het document garanderen. Louter de bewaring in handen van een derde lijkt onvoldoende om de integriteit van een digitaal document te garanderen, vooral indien er speciale maatregelen genomen moeten worden om de toegankelijkheid van het document op langere termijn te garanderen.
– Verplichte inhoudelijke vermeldingen: deze vereiste kan zonder meer nageleefd worden in digitale vorm.

Bestaat er een alternatief dat de doelstelling wel vervult?

Indien blijkt dat de doelstellingen van elke vormvereiste niet vervuld zijn in een digitale context, is de digitale versie van het document niet rechtsgeldig. Er is een wetswijziging nodig om deze situatie op te lossen.

Onder impuls van de Europese Unie is reeds een eerste beperkte stap in deze richting gezet. De wet op de elektronische handel bepaalt dat "aan elke wettelijke of reglementaire vormvereiste voor de totstandkoming van contracten langs elektronische weg is voldaan wanneer de functionele kwaliteiten van deze vereiste zijn gevrijwaard"[33]. Deze wet laat toe een stap verder te gaan en een alternatief te zoeken voor elke traditionele vormvereiste die niet digitaal nageleefd kan worden.

Het toepassingsgebied van deze wetswijziging is echter beperkt. Het gaat enkel om contracten afgesloten langs elektronische weg in het kader van een dienst van de informatiemaatschappij[34]. Sommige activiteiten worden daarenboven expliciet uitgesloten, onder meer gevallen waarbij de tussenkomst van een notaris vereist is[35]. Het begrip "dienst van de informatiemaatschappij" moet erg ruim geïnterpreteerd worden, maar volgens de voorbereidende werken van de wet niet zo ruim dat overheidsactiviteiten eronder vallen[36]. Het valt af te wachten of de rechtbanken, en met name het Europese Hof van Justitie, deze interpretatie zullen volgen.

Zoals reeds vermeld, past de wetgever zelf de functionele equivalentie theorie toe bij het moderniseren van vormvereisten. De wet op de elektronische handtekening verwijst uitdrukkelijk naar de functies die een handtekening moet vervullen, met name identificatie van de partijen, toestemming met de transactie en integriteit van de akte[37]. De wet op de elektronische handel omschrijft de functies die een geschrift en verplichte handgeschreven vermeldingen moeten vervullen[38]. Een geschrift is "een opeenvolging van verstaanbare tekens die toegankelijk zijn voor een latere raadpleging"[39]. Aan de eis van een handgeschreven vermelding van degene die zich verbindt, kan worden voldaan door om het even welk procédé dat waarborgt dat de vermelding effectief uitgaat van deze laatste[40].

Dergelijke vage functie-omschrijvingen zijn uiteraard mooi in theorie, maar ze invullen in de praktijk is een ander paar mouwen. Een concrete oplossing wordt vaak gezocht in technieken gebaseerd op asymmetrische cryptografie of encryptie gebaseerd op publieke sleutels. Het voorbeeld bij uitstek is uiteraard de digitale handtekening gebaseerd op een *Public Key Infrastructure*, waaraan een zeer grote juridische waarde gehecht wordt. Dezelfde techniek wordt ingezet om elektronische aangetekende brieven te verzenden, handgeschreven vermeldingen te vervangen, documenten te dateren, enz. Vroeg of laat zal de archivaris met deze technologie geconfronteerd worden. Vandaag is nog niet helemaal duidelijk hoe digitale handtekeningen en dergelijke behandeld moeten worden. Meer onderzoek is in deze materie onontbeerlijk.

Meer informatie:

S. VAN DEN EYNDE, Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1. *http://www.antwerpen.be/david/teksten/Rapporten/Rapport3.pdf.*

P. VAN EECKE, en J. DUMORTIER, (ed.), Elektronische handel, Commentaar bij de wetten van 11 maart 2003, *Leuven, die Keure, 2003, 335 p.*

M. DEMOULIN, en E. MONTERO, 'Le formalisme contractuel à l'heure du commerce électronique' *in* La théorie générale des obligations, suite., *Commission Université-Palais (CUP), Formation permanente, Université de Liège, 2002.*

M. DEMOULIN, D. GOBERT en E. MONTERO, Commerce électronique: de la théorie à la pratique, *Brussel, Bruylant, 2003, 201 p.*

O. LIBON, en S. VAN DEN EYNDE, European Electronic Signature Standardization Initiative - Trusted Archival Services, *European Commission, 2000, 66 p., http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf.*

J. DUMORTIER, O. LIBON, A. MITRAKAS, A. RINDERLE, A. SCHREIBER, P. VAN EECKE, European Electronic Signature Standardization Initiative - Certificate Path Validation, *European Commission, 2000, 61p., http://www.law.kuleuven.ac.be/icri/publications/416CertificateValidation_Report.pdf.*

J. DUMORTIER, O. LIBON, A. MITRAKAS, R. RINDERLE, A. SCHREIBER, P. VAN EECKE, European Electronic Signature Standardization Initiative - Signature Policies, *European Commission, 2000, 43 p., http://www.law.kuleuven.ac.be/icri/publications/418SignaturePolicy_Report.pdf.*

2. Bewaring in digitale vorm

Buiten de rechtsgeldigheid om, kan het recht ook een bepaalde vorm van bewaring voorschrijven of toelaten. Meestal bestaan er geen uitdrukkelijke regels omtrent de bewaringsvorm voor documenten. In principe volstaat het om documenten te bewaren in de vorm waarin ze rechtsgeldig opgemaakt werden.

Op deze regel bestaan wel tal van uitzonderingen. Verschillende overheidsdiensten kregen het recht om hun papieren stukken om te zetten in foto- of microfotokopieën, magnetische, elektronische of optische kopieën[41]. Het gaat onder meer om stukken die enkel geldig in papieren vorm gemaakt mogen worden. De uitzonderingsbepalingen vermelden telkens dat de kopie dezelfde bewijswaarde heeft als het origineel. De originele stukken worden in de regel vernietigd. Ook al wordt een kopie bewaard, toch lijkt de toestemming van de Algemene Rijksarchivaris voor deze operatie noodzakelijk.

Naast deze uitzonderingen, blijkt dat de wetgeving niet altijd consistent is. Het kan voorvallen dat archivering in oorspronkelijke vorm toch om één of andere reden niet volstaat. Zo mag de boekhouding in digitale vorm opgesteld worden, maar volgens de boekhoudwet moet het dagboek, het centraal boek en het inventarisboek in papieren registers bewaard worden[42]. De fiscus aanvaardt de digitale versie wel, zolang de onveranderlijkheid van de boekingen gegarandeerd is.

Meer informatie:

S. VAN DEN EYNDE, Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1, *http://www.antwerpen.be/david/teksten/Rapporten/Rapport3.pdf.*

J. DUMORTIER, Op-Slag Bewezen. Juridische mogelijkheden en moeilijkheden bij het opzetten van een elektronisch documentbeheersysteem, *Brussel, Keesing Publishers - BelAIIM, 2002, 66 p.*

H. DEKEYSER en J. DUMORTIER, 'Elektronisch archiveren', *in X. (ed.)*, Tendensen in het bedrijfsrecht. Contracteren zonder papier, *Brussel, Bruylant, 2003, 207-236.*

3. Conclusie

De vraag of digitaal archiveren volstaat hangt van twee zaken af:

Is de digitale versie van het document een rechtsgeldig document?
Indien de wet uitdrukkelijk de rechtsgeldigheid vastlegt van een document in digitale vorm, is er geen probleem. Meestal zwijgt de wet hierover en moet uit de context afgeleid worden of een bepaald document geldig in digitale vorm kan opgemaakt worden. De functionele equivalentie theorie schetst het kader om deze analyse uit te voeren. Hierbij gaat men na of elke vormvereiste zoals door de wet omschreven afdoende kan vervuld worden op digitale wijze. Doorslaggevend is de vraag of het doel van de vormvereiste wel bereikt wordt. Wanneer een vormvereiste ofwel niet op digitale wijze geïmplementeerd kan worden, ofwel het doel niet bereikt is de digitale versie van een document niet rechtsgeldig. Nochtans zijn er vaak alternatieve technieken beschikbaar die het normdoel van een vormvereiste wel bereiken. Zonder wetswijziging kunnen deze alternatieven niet ingezet worden.

Mag het document uitsluitend in digitale vorm bewaard worden?
Een enkele keer legt de wet uitdrukkelijk op in welke vorm documenten bewaard moeten worden. Meestal zwijgt de wet hierover. Als uitgangspunt worden documenten bewaard in hun oorspronkelijke vorm. De wetgever voerde zelf verschillende uitzonderingen in op dit principe. Daarnaast bestaan er soms tegenstrijdige wettelijke voorschriften.

D. Openbaarheid van bestuur

De bewaring van overheidsdocumenten is uiteraard geen doel op zich, maar heeft verschillende achterliggende redenen. De efficiënte uitoefening van de dienstverlening is één reden. Een andere reden vinden we in de regels omtrent de openbaarheid van bestuur.
De openbaarheid van bestuur is op twee pijlers gebaseerd: de actieve en de passieve openbaarheid. Actieve openbaarheid houdt in dat de overheid zelf het initiatief moet nemen om de burgers te informeren over alle zaken die hen aangaan. Hier zullen we verder niet op in gaan. De passieve openbaarheid legt aan de overheid de verplichting op toegang tot alle bestuursdocumenten te verlenen. Toegang betekent bestuursdocumenten kunnen raadplegen of er een afschrift van kunnen krijgen. Dit heeft vanzelfsprekend belangrijke gevolgen voor de opbouw, het beheer en de toegankelijkheid van archief.

1. Toepasselijke wetgeving

De regelgeving inzake de openbaarheid van bestuur in België is sterk versnipperd. Enerzijds bestaat er op elk bestuurlijk niveau een specifieke wetgeving (federaal, regionaal, provinciaal en gemeentelijk), anderzijds wordt de reglementering inzake de toegang tot documenten vaak geïntegreerd in bestaande wetten.
Artikel 32 van de Grondwet geeft iedereen het recht om elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de ordonnantie.
Op federaal niveau regelt de wet van 11 april 1994 de openbaarheid van bestuur, maar vooral de uitzonderingen hierop[43].
In Vlaanderen wordt de openbaarheid van bestuur voorlopig nog geregeld door het Vlaamse decreet van 18 mei 1999[44]. Het Vlaamse Parlement heeft een nieuw decreet aangenomen[45], maar tot dit in het Staatsblad verschijnt, kan het niet in werking treden. Dit decreet wordt hierna het toekomstige decreet genoemd.
Voor het gemeentelijke en provinciale bestuursniveau was de federale wetgever oorspronkelijk bevoegd[46] om een openbaarheidsregeling uit te werken. Deze bevoegdheid vertaalde zich in de wet van 12 november 1997 betreffende de openbaarheid van bestuur in de gemeenten en provincies[47]. De bijzondere wet van 13 juli 2001 heeft deze bevoegdheid naar de gewesten overgeheveld. Het toekomstige Vlaamse openbaarheidsdecreet zal de wet vervangen voor de Vlaamse gemeenten en provincies. De wet blijft van toepassing voor het Waalse en Brusselse Hoofdstedelijke Gewest zolang zij geen eigen regelgeving uitvaardigen.
Voor een overzicht van alle openbaarheidsreglementeringen in België zie F. Schram, "Openbaarheid in wetteksten", http://user.online.be/~fschram/wetlijst1.html. De grote lijnen van al deze reglementeringen lopen gelijk. In wat volgt zal voornamelijk de Vlaamse regeling besproken worden.

2. Toepassingsgebied

2.1. Wie?

De openbaarheidsregels in het algemeen zijn van toepassing op alle organen van de uitvoerende macht. De meeste openbaarheidsregels gebruiken het begrip 'administratieve overheid'[48] zoals dit gedefiniëerd wordt door de Raad van State. In geval van twijfel heeft de Raad van State het

laatste woord over de vraag of een bepaalde instantie nu al dan niet een administratieve overheid is.

Het toekomstige Vlaamse decreet gebruikt de term 'bestuursinstantie'. Een bestuursinstantie is

a) een rechtspersoon die is opgericht bij of krachtens de Grondwet, een wet, decreet of ordonnantie
b) een natuurlijke persoon, een groepering van natuurlijke personen, een rechtspersoon of groepering van rechtspersonen die in hun werking bepaald en gecontroleerd worden door a)
c) een natuurlijke persoon, een groepering van natuurlijke personen, een rechtspersoon of groepering van rechtspersonen, voorzover zij door een bestuursinstantie in de zin van a) zijn belast met de uitoefening van een taak van algemeen belang of voorzover zij een taak van algemeen belang behartigen en beslissingen nemen die derden binden.

Daarnaast voert het toekomstige Vlaamse decreet de term 'milieu-instantie' in ter omzetting van internationale regels met betrekking tot de openbaarheid van milieu-informatie[49]. Het onderscheid is van belang omdat de overheid milieu-informatie minder kan afschermen van het publiek dan andere informatie.

De rechterlijke en de wetgevende macht zijn in principe niet onderworpen aan de openbaarheidsregels die hier beschreven worden. Er kunnen wel specifieke regels bestaan die een inzagerecht toekennen op hun documenten. Het toekomstige Vlaamse decreet verduidelijkt dat deze uitsluiting enkel geldt voor zover ze handelen in hun rechterlijke of wetgevende rol. Daarnaast kunnen er specifieke regels bestaan die een inzagerecht toekennen op hun documenten.

De federale wet op de openbaarheid is van toepassing op[50]:

– op de federale administratieve overheden
– op alle andere administratieve overheden, doch slechts voor de uitzonderingensgronden op de openbaarheid in deze wet die tot de federale bevoegdheid behoren.

Het huidige Vlaamse openbaarheidsdecreet is van toepassing op[51]:

– de administratieve overheden van het Vlaamse Gewest en de Vlaamse Gemeenschap
– alle andere administratieve overheden, doch slechts voor de uitzonderingsgronden op de openbaarheid in dit decreet die tot de bevoegdheid van de Vlaamse Gemeenschap of het Vlaamse Gewest behoren
– de verenigingen van provincies en gemeenten
– de openbare centra voor maatschappelijk welzijn en de verenigingen bedoeld in hoofdstuk 12 van de organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn.

Het toekomstige Vlaamse openbaarheidsdecreet is van toepassing op[52]:

– het Vlaamse Parlement en de eraan verbonden instellingen
– de diensten, instellingen en rechtspersonen die afhangen van de Vlaamse Gemeenschap of het Vlaamse Gewest
– de gemeenten en de districten
– de provincies
– de andere gemeentelijke en provinciale instellingen, met inbegrip van de verenigingen zonder winstoogmerk waarin één of meer gemeenten of de provincies minstens de helft van de stemmen in één van de beheersorganen heeft of de helft van de financiering voor haar rekening neemt
– de verenigingen van provincies en gemeenten, bedoeld in de wet van 22 december 1986 betreffende de intercommunales, en de samenwerkingsvormen zoals geregeld in het decreet van 6 juli 2001 houdende de intergemeentelijke samenwerking
– de openbare centra voor maatschappelijk welzijn, hierna OCMW's te noemen, en de verenigingen, bedoeld in hoofdstuk 12 van de organieke wet van 8 juli 1976 betreffende OCMW's
– de polders, bedoeld in de wet van 3 juni 1957 betreffende de polders, en de wateringen, bedoeld in de wet van 5 juli 1956 betreffende de wateringen
– de kerkfabrieken en de instellingen die belast zijn met het beheer van de temporaliën van de erkende erediensten
– alle andere instanties binnen het Vlaamse Gewest en de Vlaamse Gemeenschap.

De federale wet op de openbaarheid bij lokale overheden is van toepassing op de provinciale en gemeentelijke administratieve overheden[53].

2.2. Wat?

De openbaarheidsregels zijn van toepassing op 'bestuursdocumenten'. De term bestuursdocument moet erg breed opgevat worden. Het betreft alle beschikbare informatie ongeacht de drager of de vorm. Het gaat onder meer om schriftelijke stukken, geluids- en beeldopnamen met inbegrip van de gegevens vervat in de geautomatiseerde informatieverwerking, sommige notulen en processen-verbaal, statistieken, administratieve richtlijnen, omzendbrieven, contracten en vergunningen, registers van openbaar onderzoek, examencohiers, films, foto's, enz.[54]. Zonder twijfel vallen alle soorten digitale informatie, zoals websites, databanken, e-mail, logbestanden, en dergelijke ook binnen dit begrip.

Het enige criterium is of het informatie is waarover een overheid 'beschikt', met andere woorden die de overheid in zijn materieel bezit heeft. Dit laatste impliceert dat een burger niet van de overheid kan verlangen om op basis van bestaande gegevens een nieuw document op te stellen. Bij digitale gegevens kan men hierover discussiëren: vormen de resultaten van een bevraging van een databank een nieuw document? Zo ja, dan heeft de burger geen recht op inzage. Deze zienswijze gaat in tegen de bedoeling van de grondwet en wordt in de rechtsleer niet aanvaard. In dergelijke gevallen is het document in kwestie reeds latent aanwezig, de overheid beschikt er in zekere zin over en er is dus een recht op inzage[55].

Het toekomstige Vlaamse decreet verduidelijkt dat een instantie ook beschikt over de bestuursdocumenten die in het bezit van een personeelslid zijn, voorzover het bestuursdocument betrekking heeft op de uitoefening van de functies van die instantie. De documenten van een instantie die in een archief worden neergelegd, blijven bestuursdocumenten waarover deze instantie beschikt[56]. De archivaris mag niet beslissen over aanvragen tot openbaarmaking van deze documenten, maar moet elke aanvraag doorsturen naar de instantie die het document in het archief heeft neergelegd[57].

3. Procedure

Op de procedure kan in het kader van dit handboek digitaal archiveren niet erg diep worden ingegaan, aangezien deze problematiek niet specifiek is voor ons thema. Voor meer informatie wordt verwezen naar gespecialiseerde literatuur. Hierna worden enkel de basisprincipes geschetst.

Raadplegen van bestuursdocumenten kan enkel na schriftelijke aanvraag gericht aan de bevoegde overheid. De verzoeker moet in principe geen belang aantonen voor de raadpleging. Indien de aangeschreven overheid meent dat ze niet bevoegd is, meldt ze dit aan de verzoeker en verwijst hem/haar door naar de bevoegde overheid.

De overheid moet binnen een bepaalde termijn beslissen of ze de aanvraag inwilligt of afwijst. Afwijzingen zijn enkel mogelijk op de gronden voorzien door de wet, het decreet of de ordonnantie. Enkele voorbeelden zijn de vrijwaring van de fundamentele rechten en vrijheden van de bestuurden, de openbare orde, de veiligheid of de verdediging van het land, de persoonlijke levenssfeer, enz. Ook aanvragen die kennelijk te vaag of kennelijk onredelijk zijn, mogen afgewezen worden. De burger kan in beroep gaan tegen een afwijzende beslissen.

Meer informatie:
H. BLOEMEN, 'Het recht op openbaarheid van bestuursdocumenten: een bijzonder grondrecht', *in X. (ed.)* Mediarecht, Overheidsvoorlichting, *Brussel, Kluwer, losbladig,*
W. PAS, 'De wet van 11 april 1994 betreffende de openbaarheid van bestuur', *in X. (ed.)* Mediarecht, Overheidsvoorlichting*, Brussel, Kluwer, losbladig,*
F. SCHRAM, 'De Vlaamse openbaarheidswetgeving', *in X. (ed.)* Mediarecht, Overheidsvoorlichting, *Brussel, Kluwer, losbladig,*
F. SCHRAM, Openbaarheid van bestuur, *Brugge, Die Keure, 2003, 177 p.*

4. Verhouding met de archiefwetgeving

4.1. Archiefstukken en bestuursdocumenten

De begrippen 'archiefstuk' en 'bestuursdocument' dekken niet dezelfde lading maar overlappen elkaar wel voor een groot stuk.

- Een archiefstuk is elk document dat, ongeacht zijn vorm, drager of datum, naar zijn aard bestemd is om te berusten onder de persoon, groep personen of organisatie die het document heeft ontvangen of opgemaakt uit hoofde van zijn of haar activiteiten, zijn of haar taken of ter handhaving van zijn of haar rechten[58]. De archiefwet heeft enkel betrekking op archiefstukken van organen van de uitvoerende en de rechterlijke macht.
- Een bestuursdocument is elke informatie waarover een administratieve overheid of een instantie beschikt.

  Overlapping van de archiefwetgeving en de openbaarheidsregels komen dus enkel voor wanneer het gaat om archiefstukken van administratieve overheden of instanties. Welke regels nu uiteindelijk gelden voor deze categorie archiefstukken is niet meteen duidelijk. Hierna proberen we toch enige duidelijkheid te scheppen.

4.2. De openbaarheid van archiefstukken-bestuursdocumenten

De algemene regel is erg eenvoudig: bestuursdocumenten zijn openbaar. In principe zijn de bestuursdocumenten die gedeponeerd worden in het rijksarchief eveneens openbaar. Uitzonderingen zijn mogelijk, voor zover die in een wet, een decreet of een ordonnantie opgenomen zijn.

Verplicht gedeponeerde stukken

Archiefstukken ouder dan honderd jaar moeten in het rijksarchief gedeponeerd worden[59]. Volgens de archiefwet zijn deze stukken openbaar[60].
Op de verplichte neerlegging bij het rijksarchief kunnen evenwel uitzonderingen verleend worden[61]. Het Ministerie van Buitenlandse zaken en het Ministerie van Landsverdediging kregen zo'n vrijstelling. De archiefwet zegt niets over de openbaarheid van deze stukken. De federale wet op de openbaarheid is in deze gevallen van toepassing[62]. De archiefvormer beslist zelf over de toepassing van de uitzonderingen op de openbaarheid van bestuur, ongeacht of hij/zij het stuk in kwestie zelf bijhoudt of reeds in een archief deponeerde. De archivaris moet vragen tot inzage doorspelen aan de archiefvormer. Indien de archiefvormer toestemt in de inzage moet de archivaris toegang verlenen tot de stukken in kwestie. Voor alle duidelijkheid, het gaat hier niet om het Algemeen Rijksarchief of het Rijksarchief in de Provinciën, maar enkel om andere overheidsarchieven[63].

Vrijwillig gedeponeerde stukken

Stukken jonger dan honderd jaar mogen vrijwillig gedeponeerd worden bij het rijksarchief. Deze situatie is in het kader van digitale archivering uiteraard veel interessanter, maar jammer genoeg ook complexer.

De archiefwetgeving legt zelf geen regels vast in verband met de openbaarheid van deze stukken, maar verwijst hiervoor naar een 'reglement van orde' dat door de Minister van Openbaar Onderwijs vastgesteld moet worden. Zo'n reglement van orde is er nooit gekomen. Sinds de invoering van de openbaarheid van bestuur in de grondwet, is zo'n reglement niet meer voldoende om de openbaarheid van archiefstukken in te perken. Zoals gezegd kunnen uitzonderingen op de openbaarheid enkel door de respectievelijke parlementen van ons land ingevoerd worden. Dit is op alle bestuurlijke niveau's gebeurd.
Beide federale wetten op openbaarheid van bestuur sluiten het Algemeen Rijksarchief en het Rijksarchief in de Provinciën uit van hun toepassingsgebied[64]. Op het eerste zicht lijken stukken gedeponeerd in het Rijksarchief dus niet onder de wetten op de openbaarheid van bestuur te vallen, maar enkel onder de archiefwet. Bij gebrek aan expliciete regeling in de archiefwet zou dit betekenen dat we terugvallen op de algemene regel uit de grondwet: bestuursdocumenten zijn openbaar. Volgens Frankie Schram moet dit anders geïnterpreteerd worden. De archiefwet kent enkel een afwijkende openbaarheidsregeling voor verplicht neergelegde archiefdocumenten. Bijgevolg is het logisch om de openbaarheidswetten op vrijwillige neergelegde archiefdocumenten toe te passen. De administratieve overheid zou anders zijn verantwoordelijkheid onder de openbaarheidswetgeving kunnen ontlopen door zoveel mogelijk documenten vrijwillig in het Rijksarchief te deponeren.
Het Vlaamse decreet bepaalt dat de archiefvormer bevoegd blijft om te oordelen over de toegang tot archiefstukken die in een archief gedeponeerd werden. De archivaris moet verzoeken tot inzage dus doorsturen naar de archiefvormer. Voor stukken gedeponeerd bij het rijksarchief wordt geen afwijkende regeling bepaald, het decreet is hierop dus gewoon van toepassing. Het toekomstige Vlaamse decreet herneemt deze regeling.

Meer informatie:
F. SCHRAM, 'Openbaarheid en Archiefwetgeving' *in A.-M. Draye (ed.)*, Openbaarheid van bestuur in Vlaanderen, België en de Europese instellingen, *Leuven, Instituut voor administratief recht, 1996, 153-207.*
F. SCHRAM, Begrenzingen aan de openbaarheid van bestuur, *Proefschrift, Leuven, 2002, p. 1207-1208.*

5. Verhouding met het privacyrecht

Administratieve overheden verwerken veel persoonsgegevens in hun dagelijkse praktijk. Bestuursdocumenten zullen dus regelmatig persoonsgegevens bevatten en de overheid moet zich dus afvragen of zomaar inzage verlenen in deze documenten wel geoorloofd is. De verschillende openbaarheidsreglementeringen houden hier rekening mee.

5.1. Documenten van persoonlijke aard

De meeste openbaarheidsreglementeringen[65] definiëren een bestuursdocument van persoonlijke aard als een document dat:
- een beoordeling of een waardeoordeel bevat van een met naam genoemd of gemakkelijk identificeerbaar natuurlijk persoon, of
- de beschrijving van een gedrag bevat waarvan het ruchtbaar maken aan die persoon kennelijk nadeel kan berokkenen.

In Vlaanderen is een document van persoonlijke aard een document dat een beoordeling, een waardeoordeel of de b*eschrijving van een gedrag* bevat van een bij naam genoemd of een gemakkelijk identificeerbaar natuurlijk persoon[66]. De categorie documenten van persoonlijke aard is dus veel ruimer gedefiniëerd. Om het even welke beschrijving van een gedraging van een gemakkelijk identificeerbare persoon volstaat immers. Een bestuursdocument kan gedeeltelijk bekendgemaakt worden, als slechts een deel ervan persoonlijke informatie bevat[67].
Het toekomstige Vlaamse decreet vervangt document van persoonlijke aard door informatie van persoonlijke aard, maar behoudt dezelfde omschrijving. Het gaat om informatie die betrekking

heeft op een beoordeling of een waardeoordeel, of die de beschrijving van een gedrag bevat van een bij name genoemd of een gemakkelijk identificeerbaar natuurlijk persoon[68]. Een bestuursdocument dat zowel informatie van persoonlijke aard als andere informatie bevat kan gedeeltelijk bekendgemaakt worden[69].
De begrippen 'document van persoonlijke aard' en 'informatie van persoonlijke aard' mogen niet verward worden met de notie 'persoonsgegeven' in de zin van de privacywet.
De verzoeker die een document van persoonlijke aard wil raadplegen moet zijn belang daarbij aantonen[70]. Dit belang is in beginsel hetzelfde belang dat vereist is om naar de Raad van State te stappen, namelijk een belang dat persoonlijk, rechtmatig, actueel, direct en vaststaand is. Als het document over de verzoeker zelf gaat, wordt zijn belang automatisch aanvaard.
Het huidige Vlaamse openbaarheidsdecreet perkt de toegang tot documenten van persoonlijke aard nog verder in. Alleen diegene die door het document of de beslissing ter voorbereiding waarvan het document werd opgesteld of waarop het betrekking heeft, rechtstreeks, persoonlijk en ongunstig in zijn rechtssituatie kan worden geraakt, kan het vereiste belang hebben. Degene waarover het document handelt, moet zijn belang niet bewijzen[71]. Buitenstaanders krijgen dus niet eens de kans om hun belang aan te tonen. Het gaat hier om een algemene en absolute beperking op het recht op toegang tot bestuursdocumenten. Vroeger al heeft het Arbitragehof dergelijke algemene en absolute beperkingen verworpen, het is dus maar de vraag of deze bepaling zou standhouden voor het hof[72].
Het toekomstige Vlaamse decreet bepaalt dat de aanvrager belang heeft bij de openbaarmaking van informatie van persoonlijke aard wanneer hij rechtstreeks en persoonlijk in zijn rechtssituatie kan worden geraakt door ofwel de informatie zelf, de beslissing waarop de informatie betrekking heeft of de beslissing ter voorbereiding waarvan het document dat de informatie bevat, werd opgesteld[73]. Degene waarover het document handelt, moet zijn belang niet bewijzen. Buitenstaanders worden nog steeds op absolute wijze uitgesloten. Milieu-informatie waarin informatie van persoonlijk aard voorkomt, mag toch openbaar gemaakt worden zonder dat de aanvrager een belang aantoont.

5.2. Privacy als uitzonderingsgrond

Zowel bij 'gewone' bestuursdocumenten als bij documenten/informatie van persoonlijke aard moet de overheid nagaan of de openbaarheid niet in strijd is met de bescherming van de persoonlijke levenssfeer. De wet op de privacy dient hier als leidraad. De mededeling van persoonsgegevens is immers eveneens een verwerking ervan.
Deze problematiek is bijzonder prangend wat de archivering en de openbaarheid van e-mail betreft. De privacy-belangen van de ambtenaar en zijn correspondenten staan haaks op de plicht van de overheid om een archiefstukken te bewaren en inzage te verlenen in bestuursdocumenten. Dit thema werd grondig uitgespit in het DAVID-rapport Archiveren van e-mail.

Meer informatie:
F. BOUDREZ, H. DEKEYSER, en S. VAN DEN EYNDE, Archiveren van e-mail http://www.antwerpen.be /david/website/nl/text_rapporten.htm, 2de herwerkte editie, Antwerpen-Leuven, Stadsarchief Antwerpen - ICRI K.U.Leuven, 2003, 96 p.
C. DE TERWANGNE, 'Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles: regards croisés sur deux voies d'accès à l'information' *in CUP, mei 2002, vol. 55, 85-129.*

6. Verhouding met het auteursrecht

Sommige bestuursdocumenten omvatten een auteursrechtelijk beschermd werk. De titularis van het auteursrecht kan zowel een derde zijn als de overheid zelf.
De federale wetten[74] op de openbaarheid van bestuur stellen dat de toestemming van de auteur niet vereist is om ter plaatse inzage in een document te verlenen of uitleg erover te verstrekken. Een kopie afleveren van een beschermd werk kan uitsluitend met de toestemming van de auteur, behalve wanneer de overheid zelf de auteur is. Wanneer de overheid zelf de titularis van het auteursrecht is, mag zij dit volgens de Commissie voor de Toegang tot Bestuursdocumenten niet inroepen om de toegang tot bestuursdocumenten te beperken[75].
Het huidige Vlaamse decreet betreffende de openbaarheid van bestuursdocumenten kent een analoge bepaling[76]. Het toekomstige Vlaamse decreet stelt enkel dat wanneer de aanvraag tot openbaarmaking betrekking heeft op een bestuursdocument dat door een intellectueel recht beschermd wordt, de instantie in haar beslissing hierop moet wijzen[77]. Noch het auteursrecht, noch het octrooirecht verbieden de overheid om inzage en uitleg in een document te geven. Een kopie maken van een auteursrechtelijk beschermd werk is op grond van het auteursrecht enkel toegelaten met de toestemming van de auteur. Deze regel moet niet herhaald worden in het openbaarheidsdecreet.

7. Conclusie

De eindverantwoordelijkheid voor de openbaarheid van bestuursdocumenten ligt bij de archiefvormer, tenminste tot aan de verplichte deponering bij het rijksarchief. Eerst en vooral moet de archiefvormer zijn bestuursdocumenten zo ordenen dat het verlenen van inzage in de praktijk mogelijk is. Zo moet de archiefvormer niet alleen zijn documenten in een systeem organiseren, maar onder meer ook het e-mail systeem zo opzetten dat professionele e-mail toegankelijk is voor iedereen.
In principe beslist de archiefvormer over de inwilliging of afwijzing van elke verzoek tot inzage, zelfs wanneer de documenten in het archief werden gedeponeerd. De archivaris moet verzoeken tot inzage doorverwijzen naar de bevoegde overheid.

E. Privacy

Het recht op privacy omhelst het recht om relaties aan te knopen met anderen en te onderhouden zonder inmenging door derden. Dit fundamenteel recht heeft verregaande implicaties en kent vele incarnaties in ons recht.
Historisch is dit recht ontstaan als een afweerrecht tegen inmengingen van de overheid. Meer en meer wordt duidelijk dat we niet enkel van de overheid schendingen te vrezen hebben, maar eveneens van onze medemensen. De opkomst van de informatietechnologie heeft de privacyproblematiek enkel nog verscherpt.
De privacyregels hebben een verregaande impact op alle aspecten van archiefbeheer:
– Archiefvorming: met de bescherming van de persoonlijke levenssfeer van alle betrokkenen moet rekening gehouden worden vanaf de creatie van archiefstukken.
– Archiefbeheer: persoonsgegevens moeten met de nodige omzichtigheid behandeld worden. De confidentialiteit van de gegevens moet gegarandeerd zijn en ongerechtvaardigde wijzigingen moeten uitgesloten zijn.
– Disseminatie van het archief: de toegang tot persoonsgegevens is strikt gereglementeerd.

1. Toepasselijke wetgeving

Dat de bescherming van de persoonlijke levenssfeer van eenieder een fundamentele waarde in onze maatschappij blijkt uit de overvloed aan rechtsnormen die deze materie beheersen. De voornaamste zijn:
– Artikel 12 van de Universele Verklaring van de Rechten van de Mens (10 december 1948)
– Artikel 8 van het Europese Verdrag van de Rechten van de Mens (4 november 1950, Rome)
– Artikel 17 van het verdrag inzake burgerrechten en politieke rechten (19 december 1966, New York)
– Artikel 7 van het Handvest van de Grondrechten van de Europese Unie (2000/C 364/01, P.B. C 364 18 december 2000, p. 1)
– Artikel 22 en 29 van de Belgische Grondwet
– De Europese richtlijn over de verwerking van persoonsgegevens (1995/46/EG) en de richtlijn betreffende privacy en telecommunicatie/elektronische communicatie (1997/66/EG en 2000/58/EG)
– De wet op de bescherming van de persoonlijke levenssfeer van 8 december 1992, http://privacy.fgov.be/normatieve_teksten.htm.
– Het telecommunicatiegeheim, art. 314bis SW en art. 109terD Telecomwet, http://www.bipt.be/Legislation/telecoms/M41_N.htm.
– C.A.O. nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens (B.S. 29 juni 2002), http://privacy.fgov.be/normatieve_teksten.htm.

De wet op de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens legt het algemene kader vast in ons land en zal hierna besproken worden. Alleen de aspecten die van belang zijn voor digitale archivering worden belicht. Voor een gedetailleerde bespreking van de wet zie D. De Bot, V*erwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, 403 p.
Voor meer informatie over het internationale kader zie het DAVID-rapport Archiveren van e-mail, http://www.antwerpen.be/david/website/nl/text_rapporten.htm.

2. Toepassingsgebied van de privacywet

2.1. Wie?

Elke verwerking van persoonsgegevens die wordt verricht op het Belgische grondgebied, voor zover de verantwoordelijke voor de verwerking hier reëel gevestigd is, moet voldoen aan de voorwaarden opgelegd door de wet[78]. De privacywet is van toepassing op iedereen: de overheid, organisaties en gewone burgers.

De verplichtingen van de wet zijn gericht aan de 'verantwoordelijke voor de verwerking'. Dit is degene die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt[79]. Indien het doel en de middelen voor de verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verantwoordelijke voor de verwerking degene die deze norm aanwijst. In de regel is de archiefvormer de verantwoordelijke voor de verwerking en als zodanig draagt hij de eindverantwoordelijkheid voor de naleving van de privacyregels.

De rol die de archivaris speelt in termen van de privacywet verschilt naar gelang de omstandigheden. Indien de archiefdienst een zelfstandige instantie is die 'ten behoeve van' de archiefvormer werkt, is de archiefdienst een 'verwerker'. Met verwerker wordt bedoeld degene die in opdracht en onder toezicht van de eigenlijke verantwoordelijke voor de verwerking persoonsgegevens verwerkt[80]. De werknemers of ondergeschikten van de verantwoordelijke voor de verwerking zijn geen 'verwerker' in de zin van de privacywet. Dus, een archivaris of records manager in dienst bij de archiefvormer heeft geen zelfstandige plichten op grond van de privacywet. Het Algemeen Rijksarchief heeft een eigen wettelijk mandaat om documenten te archiveren en bijgevolg om persoonsgegevens te verwerken. Het Algemeen Rijksarchief is dus een verantwoordelijke voor de verwerking en geen verwerker.

2.2. Wat?

De wet regelt de verwerking van persoonsgegevens. Een persoonsgegeven is iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Identificeerbaar is een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit[81].

Het begrip persoonsgegeven moet erg ruim geïnterpreteerd worden. Het is niet vereist dat degene die de gegevens in zijn bezit heeft de betrokkene kan identificeren. Van zodra iemand in staat is om de betrokkene te identificeren aan de hand van redelijke middelen, is er sprake van een persoonsgegeven. Zo verklapt een e-mailadres met een pseudoniem (bijvoorbeeld incognito@provider.be) niet meteen wie erachter schuil gaat, de dienstverlener weet waarschijnlijk wel om welke klant het precies gaat. Dit e-mailadres is dus een persoonsgegeven over die klant.

Onder "verwerking" wordt verstaan elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens[82]. Ook dit begrip moet ruim ingevuld worden. De wet is van toepassing op elke verwerking die geheel of gedeeltelijk automatisch gebeurt, en op sommige manuele verwerkingen[83].

De wet is slechts in beperkte mate van toepassing op verwerkingen uitgevoerd door de veiligheids-, politie- en inlichtingendiensten[84]. Ook het Europese centrum voor vermiste en seksueel uitgebuitte kinderen kreeg enkele uitzonderingen[85]. Bijkomende vrijstellingen kunnen verleend worden bij koninklijk besluit Deze vrijstellingen hebben voornamelijk een impact bij de archiefvorming, en slechts in beperkte mate op het archiefbeheer door de archivaris.

3. Basisbeginselen van de privacywet

Aan de privacywet liggen drie belangrijke beginselen ten grondslag: legaliteit of transparantie, finaliteit en proportionaliteit. Deze beginselen worden telkens in concreto uitgewerkt door de bepalingen van de wet.

3.1. Legaliteit of transparantie

Het legaliteits- of transparantiebeginsel houdt in dat elke betrokkene redelijkerwijze moet kunnen weten welke gegevens over hem verwerkt worden, waarom en door wie. Wanneer de overheid gegevens verwerkt moet zij zich kunnen baseren op een rechtsnorm die voldoende duidelijk is en die toegankelijk is voor alle burgers. Tussen privé-personen onderling (zowel natuurlijke personen als rechtspersonen) wordt dit vertaald in het transparantiebeginsel, met andere woorden er moet duidelijke informatie verstrekt worden zodat alle betrokkenen redelijkerwijze weten welke privacyverwachtingen ze mogen koesteren.

De wet leg in eerste instantie vast onder welke omstandigheden de verwerking van persoonsgegevens toelaatbaar is. Voor de publieke sector zijn de volgende situaties van belang:

- wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verantwoordelijke voor de verwerking is onderworpen door of krachtens een wet, een decreet of een ordonnantie[86]
- wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verantwoordelijke voor de verwerking of aan de derde aan wie de gegevens worden verstrekt[87]
- wanneer de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor de verwerking of van de derde aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van deze wet, niet zwaarder doorwegen[88]. De koning is gemachtigd om deze regel in bepaalde gevallen uit te sluiten.

3.2. Finaliteit

Het finaliteitsbeginsel houdt in dat persoonsgegevens enkel voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel verwerkt mogen worden. Daarna de gegevens voor een ander doel gebruiken mag enkel indien dit nieuwe doel verenigbaar is met het oorspronkelijk doel. De verenigbaarheid moet beoordeeld worden rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen[89]. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet als onverenigbaar beschouwd, onder de voorwaarden vastgelegd bij koninklijk besluit[90]. Gegevens verzamelen omdat ze ooit nog eens van pas kunnen komen is uit den boze.

3.3. Proportionaliteit

Ten slotte mogen niet meer gegevens verwerkt worden dan noodzakelijk om het doel te bereiken: gegevens moeten toereikend, terzake dienend en niet overmatig zijn[91]. Daarenboven moeten gegevens nauwkeurig zijn en zo nodig worden bijgewerkt[92]. Aanpassingen moeten niet noodzakelijk in het oorspronkelijke document gebeuren, maar mogen in bijlage toegevoegd worden.

Persoonsgegevens mogen in een vorm die het mogelijk maakt de betrokkenen te identificeren niet langer bewaard worden dan noodzakelijk[93]. Voor historische, statistische of wetenschappelijke doeleinden geldt een bijzonder regime vastgelegd in het privacy-KB.

Bij de selectie van de archiefstukken zal het proportionaliteitsprincipe een rol moeten spelen.

4. De rechten van de betrokkene

4.1. Recht op kennisgeving

De verantwoordelijke voor de verwerking moet alle betrokkenen in beginsel inlichten over de verwerking van persoonsgegevens. De wet maakt een onderscheid naargelang de gegevens bij de betrokkene zelf verkregen worden of uit een andere bron.

Gegevens verkregen bij de betrokkene

Alleen de archiefvormer zal geregeld rechtstreeks bij de betrokkene gegevens opvragen. Bij de archivaris zal deze situatie slechts sporadisch voorkomen.

Uiterlijk op het moment dat de gegevens worden verkregen moet onder meer de hierna volgende informatie aan de betrokkene verstrekt worden, behalve indien hij daarvan reeds op de hoogte is[94] :

- de naam en het adres van de verantwoordelijke voor de verwerking en, in voorkomend geval, van diens vertegenwoordiger
- de doeleinden van de verwerking
- de ontvangers of de categorieën ontvangers van de gegevens
- het al dan niet verplichte karakter van het antwoord en de eventuele gevolgen van niet-beantwoording
- het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem/haar betrekking hebben

Dit lijstje kan aangevuld worden bij koninklijk besluit voor specifieke gevallen.

De archiefvormer vermeldt bij deze gelegenheid best meteen de archief- en openbaarheidsverplichtingen waaraan hij/zij onderworpen is. Archivering en openbaarheid zijn eveneens doelstellingen voor verwerking van persoonsgegevens.

De uitzonderingen op deze regel worden verder besproken.

Gegevens verkregen uit een andere bron

Wanneer de gegevens niet bij de betrokkene zelf verkregen worden, is er geen onmiddellijke gelegenheid om de nodige informatie te verstrekken. De wet geeft de verantwoordelijke voor de verwerking enkele opties: ofwel neemt hij onmiddelijk na ontvangst van de gegevens contact op met de betrokkene, ofwel doet hij dit vooraleer hij gegevens meedeelt aan een derde. Indien de betrokkene reeds op de hoogte is van de nodige informatie, moet de verantwoordelijke voor de verwerking niet opnieuw informeren.

Het gaat om de volgende gegevens:

- de naam en het adres van de verantwoordelijke voor de verwerking en, in voorkomend geval, van diens vertegenwoordiger
- de doeleinden van de verwerking
- het bestaan van een recht om zich op verzoek en kosteloos tegen de voorgenomen verwerking van hem betreffende persoonsgegevens te verzetten, indien de verwerking verricht wordt met het oog op direct marketing. In dit geval dient de betrokkene in kennis te worden gesteld vooraleer de persoonsgegevens voor de eerste keer aan een derde worden verstrekt of voor rekening van derden worden gebruikt voor direct marketing
- de betrokken gegevenscategorieën
- de ontvangers of de categorieën ontvangers
- het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem/haar betrekking hebben.

Opnieuw kan dit lijstje aangevuld worden voor specifieke gevallen bij koninklijk besluit.

Ook op deze regel bestaan verschillende uitzonderingen.

Uitzonderingen op de kennisgevingsplicht

Verwerkingen door bepaalde personen/instanties
Zoals eerder vermeld, geldt de privacywet slechts in beperkte mate voor bepaalde verwerkingen[95]. Onder meer de veiligheids-, politie- en inlichtingendiensten zijn van de kennisgevingsplicht vrijgesteld. Ook verwerkingen voor uitsluitend journalistieke, artistieke of literaire doeleinden zijn vrijgesteld.

De betrokkene is reeds op de hoogte
Wanneer de betrokkene reeds beschikt over de nodige informatie betreffende de verwerking van zijn gegevens, hoeft de verantwoordelijke voor de verwerking niet opnieuw te informeren[96].

De registratie of mededeling is voorgeschreven door een wettelijke bepaling
Wanneer de registratie of de verstrekking van de persoonsgegevens verricht wordt met het oog op de toepassing van een bepaling voorgeschreven door een wettelijke norm[97], moet er geen kennisgeving gebeuren. Deze uitzondering is enkel van toepassing wanneer de gegevens *niet* bij de betrokkene zelf verzameld worden[98].
De overheid zal zich in de regel op deze vrijstelling kunnen beroepen bij de verwerking of de mededeling van persoonsgegevens. Ook voor de overdracht van documenten aan de archiefdienst is deze vrijstelling van belang.
Disseminatie van archiefstukken houdt soms een mededeling van persoonsgegevens aan buitenstaanders in. Dit is een verwerking van persoonsgegevens waarvan de betrokkene in principe op de hoogte gebracht moet worden. Voor zover een wettelijke bepaling, bijvoorbeeld de openbaarheidsregels, een recht op toegang tot archiefdocumenten verleent, is een kennisgeving niet nodig.

Informeren is onmogelijk of kost onevenredig veel moeite
De verantwoordelijke voor de verwerking is van de kennisgevingsplicht vrijgesteld wanneer de kennisgeving aan de betrokkene onmogelijk blijkt of onevenredig veel moeite kost. Deze vrijstelling geldt om evidente redenen enkel wanneer de gegevens *niet* bij de betrokkene zelf verkregen worden[99]. Bijkomende voorwaarden werden opgelegd in het privacy-KB[100].
De wet geeft als voorbeelden de verwerking voor statistische doeleinde, voor historisch of wetenschappelijk onderzoek of voor bevolkingsonderzoek met het oog op de bescherming en de bevordering van de volksgezondheid.
De archivaris kan zich onder bepaalde omstandigheden op deze uitzondering beroepen, bijvoorbeeld bij de terbeschikkingstelling van archiefstukken aan buitenstaanders. In elk concreet geval moet worden onderzocht of kennisgeving in werkelijkheid onmogelijk is of onevenredig veel moeite kost.

4.2. Recht op mededeling
De privacywet geeft iedereen het recht controle uit te oefenen over het gebruik van zijn persoonsgegevens.
Eerst en vooral mag elke betrokkene vragen of er al dan niet gegevens over hem verwerkt worden. Is dit het geval, dan moet de verantwoordelijke ook informatie verstrekken over de doeleinden van deze verwerkingen, van de categorieën gegevens in kwestie en van de categorieën ontvangers aan wie de gegevens worden verstrekt[101].
Bovendien mag de betrokkene vragen dat de verwerkte gegevens in een begrijpelijke vorm aan hem worden verstrekt. Alle beschikbare informatie over de oorsprong van die gegevens moet hieraan worden toegevoegd[102]. Deze bepaling stelt de archiefdiensten voor een loodzware opgave. Het begrip persoonsgegevens wordt erg breed opgevat zodat erg veel mensen deze bepaling kunnen inroepen. Een voorbeeld kan dit illustreren. Een personeelsdossier bevat in eerste instantie persoonsgegevens over de werknemer of ambtenaar in kwestie. Het dossier kan eventueel ook gegevens over zijn gezinsleden, evaluties afkomstig van zijn overste, gegevens over de dossier-

beheerder en correspondentie met allerlei instanties van de sociale zekerheid bevatten. Eén personeelsdossier kan dus persoonsgegevens bevatten over allerlei verschillende mensen.
Idealiter zouden de metadata van elk archiefstuk een lijstje bevatten van betrokken personen. De archiefvormer is het best geplaatst om deze informatie toe te voegen bij de creatie van het stuk. Dit is in zijn eigen belang, aangezien de archiefvormer in principe zelf onderworpen is aan de mededelingsplicht.
Wat het verstrekken van de verwerkte gegevens betreft, pleit men in de rechtsleer voor een pragmatische aanpak. Indien het onevenredig veel moeite kost om van alle gegevens een kopie te maken, zou een overzicht moeten volstaan[103].

Procedure
De procedure wordt omschreven in artikel 10 van de privacywet en artikel 32 privacy-KB.

Uitzonderingen
Op het recht op mededeling bestaan erg weinig uitzonderingen[104]. In sommige gevallen bestaat er geen rechtstreeks recht op mededeling, maar moet de betrokkene zich wenden tot de Commissie voor de Bescherming van de Persoonlijke Levenssfeer[105].

4.3. Recht op verbetering
Iedereen heeft het recht alle onjuiste persoonsgegevens die op hem/haar betrekking hebben kosteloos te doen verbeteren. Naast het verbeteren van onjuiste gegevens, mag de betrokkene ook gegevens aanvullen. Wanneer gegevens in strijd met de wet worden verwerkt, mag hij eisen dat ze worden geschrapt of minstens niet verder worden gebruikt[106].
Subjectieve beoordelingen kan de betrokkene niet zomaar vervangen door zijn/haar eigen visie, maar de verantwoordelijke voor de verwerking moet eventueel wel vermelden dat er betwisting bestaat[107]. Ook in andere gevallen kan het verantwoord zijn om verbeteringen en aanvullingen niet in het originele stuk maar in bijlage aan te brengen.

Procedure
De procedure wordt omschreven in artikel 12 van de privacywet en artikel 32-33 privacy-KB.

Uitzonderingen
Op het recht op verbetering bestaan slechts enkele uitzonderingen[108]. In sommige gevallen moet het recht onrechtstreeks uitgeoefend worden via de Commissie voor de Bescherming van de Persoonlijke Levenssfeer[109].

4.4. Recht op verzet
Elke betrokkene mag zich verzetten tegen de verwerking van zijn gegevens indien hij zwaarwegende en gerechtvaardigde redenen heeft[110].
Dit recht van verzet bestaat niet wanneer de verwerking noodzakelijk is:
- om een reglementaire verplichting na te komen waaraan de verantwoordelijke voor de verwerking onderworpen is, of
- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen[111].

In de meerderheid van de gevallen zal een betrokkene zich niet kunnen verzetten tegen de verwerking van persoonsgegevens door de overheid. In de metadata kan de archiefvormer de wettelijke grondslag voor de verwerking van persoonsgegevens vermelden. Op die manier kan men nadien eenvoudig vaststellen of er een recht van verzet bestaat of niet

Procedure
De procedure wordt omschreven in artikel 12 van de privacywet en artikel 32-35 privacy-KB.

Uitzonderingen
Naast de reeds genoemde beperkingen, bestaan nog enkele andere uitzonderingen voor sommige instanties[112]. Soms wordt een onrechtstreeks recht op verzet via de Commissie voor de Bescherming van de Persoonlijke Levenssfeer voorzien[113].

4.5. Recht op verhaal
De privacywet geeft de betrokkene twee bijzondere remedies tegen schendingen van de privacy. De betrokkene kan naar de voorzitter van de rechtbank van eerste aanleg stappen of een klacht neerleggen bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer[114]. Daarnaast kan de betrokkene uiteraard ook de normale juridische remedies gebruiken, zoals een klacht bij het parket neerleggen, zich burgerlijke partij stellen bij de onderzoeksrechter of bij de burgerlijke rechtbank een schadevergoeding eisen.

Meer informatie:
D. DE BOT, Verwerking van persoonsgegevens, *Antwerpen, Kluwer, 2001, 240-243, 339-341 en 352-361.*

5. De verwerking van bijzondere categoriën persoonsgegevens

Bovenop de reeds besproken regels, geldt een strenger regime voor enkele bijzondere categoriën persoonsgegevens[115]. Dergelijke gegevens verwerken is in principe volledig verboden, behalve in de gevallen die de wet omschrijft. Hierna worden enkel de grote lijnen toegelicht.

5.1. Wat?

Gevoelige gegevens
Persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook persoonsgegevens die het seksuele leven betreffen, vallen in de categorie 'gevoelige gegevens'[116].

Gezondheidsgegevens
Deze categorie omvat alle gegevens die de gezondheid betreffen[117.] De wet legt dit begrip niet verder uit, maar het gaat om "alle persoonsgegevens die de vroegere, huidige of toekomstige fysieke of psychische gezondheidstoestand van de betrokkene betreffen"[118.]

Gerechtelijke gegevens
Persoonsgegevens inzake geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten, inzake verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of inzake administratieve sancties of veiligheidsmaatregelen zijn gerechtelijke gegevens[119].

5.2. Regime
In principe is het verboden om deze bijzondere categoriën persoonsgegevens te verwerken. Omdat een absoluut verbod in de praktijk niet haalbaar is, stelt de wet voor elke categorië enkele uitzonderingsgronden in.

In eerste instantie moet de archiefvormer kunnen steunen op een wettelijke grondslag voor de verwerking van bijzondere gegevens. Wat de overheid betreft, verleent de wet verschillende specifieke mogelijkheden[120]. Daarnaast kan de overheid zich beroepen op een open grondslag: met name wanneer de verwerking in een wet, decreet of ordonnantie wordt toegelaten. De precieze modaliteiten verschillen per categorie bijzondere gegevens:

- Gevoelige gegevens mogen verwerkt worden wanneer een wet, een decreet of een ordonnantie dit toelaat om een andere belangrijke reden van publiek belang (art. 6 §2 l) privacywet). Een koninklijk besluit of een ministrieel besluit volstaat in dit geval niet.
- Gezondheidsgegevens mogen verwerkt worden wanneer dit om redenen van zwaarwegend algemeen belang verplicht wordt door een wet, een decreet, een ordonnantie, een koninklijk besluit of een ministrieel besluit (art. 7 §2 e) privacywet). Elke verwerking moet evenwel onder toezicht van een beroepsbeoefenaar in de gezondheidszorg gebeuren[121].
- Gerechtelijke gegevens mogen verwerkt worden indien dit noodzakelijk is voor de verwezenlijking van doeleinden die door een wet, een decreet of een ordonnantie, een koninklijk besluit of een ministrieel besluit zijn vastgesteld (art. 8 §2 b) privacywet).

De koning mag voor elke bijzondere categorie nog bijkomende voorwaarden opleggen en heeft dit ook gedaan[122]:

- De verantwoordelijke voor de verwerking moet de categorieën van personen die de persoonsgegevens kunnen raadplegen aanwijzen. Hij moet omschrijven welke taak zij hebben bij de verwerking van gegevens. Dit geldt eveneens voor gevallen waarbij een verwerker wordt ingeschakeld.
- De verantwoordelijke voor de verwerking zorgt ervoor dat de aangewezen personen door een wettelijke, statutaire of contractuele verplichting tot geheimhouding zijn verbonden.
- In de kennisgeving aan de betrokken persoon of in de aangifte aan de commissie moet de grondslag waarop de verantwoordelijke voor de verwerking zich beroept worden vermeld.

De mededeling van bijzondere persoonsgegevens is eveneens een verwerking en is enkel mogelijk wanneer de wettelijke grondslag waarop men zich beroept dit rechtvaardigt. Voor zover de archivering intern gebeurt (door ondergeschikten of door een verwerker), is er geen probleem. In dat geval is er eigenlijk geen sprake van mededeling aan derden. De overdracht van de gegevens aan een zelfstandige archiefdienst (zoals het rijksarchief) ligt gevoeliger. Wellicht zou een rechter aanvaarden dat de archiefwetgeving een 'belangrijk publiek belang' respectievelijk 'zwaarwegend algemeen belang' nastreeft[123].

Toegang verlenen tot de archiefstukken aan buitenstaanders is een ander paar mouwen. Opnieuw moet er voor deze mededeling een wettelijke grondslag voorhanden zijn. De privacywet zelf biedt een grondslag voor wetenschappelijk onderzoek, zij het enkel onder de voorwaarden bepaald door de koning.[124]

Meer informatie:
D. DE BOT, Verwerking van persoonsgegevens, *Antwerpen, Kluwer, 2001, 403 p.*

6. Administratieve bepalingen

6.1. De aangifte

De verantwoordelijke voor de verwerking moet aangifte doen bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer vooraleer hij begint met de verwerking van persoonsgegevens[125]. Op deze regel bestaan een hele reeks uitzonderingen, om de toevloed van aangiften enigzins te beperken[126]. Vrijgesteld zijn onder meer verwerkingen in het kader van de loonadministratie, personeelsadministratie, boekhouding, klanten- en leveranciersbeheer, gemeentelijke registers en verwerkingen door administratieve overheden[127]. Telkens worden bijzondere voorwaarden opgelegd in het privacy-KB.

Administratieve overheden zijn slechts vrijgesteld indien de verwerking al is onderworpen aan specifieke regels waarin de raadpleging, het gebruik en de verkrijging van de verwerkte gegevens worden geregeld[128]. Het rijksarchief moet hoogst waarschijnlijk beschouwd worden als een administratieve overheid[129]. De archiefwet en het archief-KB regelen de verkrijging, het gebruik en de raadpleging van archiefstukken slechts erg summier. Zo zijn er geen duidelijke regels met betrekking tot de toegang tot archiefstukken jonger dan 100 jaar. Het rijksarchief doet daarom best aangifte bij de commissie.

6.2. Machtiging van het bevoegd sectoraal comité

Sinds 2003 kunnen bij wet sectorale comités binnen de commissie opgericht worden. Deze sectorale comités zijn bevoegd om binnen het toepassingsgebied van bijzondere wetgeving alle aanvragen met betrekking tot de verwerking of de mededeling van gegevens te onderzoeken en er uitspraak over te doen[130]. Een bestaand voorbeeld is het sectoraal comité van de sociale zekerheid[131].

In de privacywet zelf wordt een sectoraal comité voor de federale overheid opgericht. Dit comité is bevoegd voor alle federale overheidsdiensten of openbare instellingen met rechtspersoonlijkheid die onder de federale overheid ressorteren, tenzij een ander sectorieel comité al bevoegd is. Elke mededeling van persoonsgegevens vereist een principiële machtiging van het federale sectoraal comité, dat nagaat of de mededeling wel in overeenstemming is met de wettelijke en reglementaire bepalingen. De leidende ambtenaar van de dienst of instelling in kwestie mag advies uitbrengen aan het federale sectoraal comité.

Het rijksarchief is een federale wetenschappelijke instelling die onder de bevoegdheid valt van het federale sectoraal comité, bij gebrek aan een specifiek sectoraal comité. Vooraleer men toegang verleent tot de digitale collectie aan andere overheden of aan particulieren, moet het rijksarchief een principiële machtiging vragen aan het federale sectoraal comité[132]. Tot op heden (31 december 2003) is het federale sectoraal comité nog niet werkzaam.

Archiefvormers die een federale overheidsdienst of federale openbare instelling zijn, zullen eveneens een machtiging moeten vragen vooraleer ze hun digitale collectie kunnen overdragen aan het rijksarchief.

Meer informatie:

D. DE BOT, 'De Commissie voor de Bescherming van de Persoonlijke Levenssfeer: 'Tussen droom en daad staan er niet alleen wetten in de weg, maar vooral praktische problemen', T.B.B.R., *2003, afl. 6, 384-402.*

7. Overige bepalingen

De privacywet regelt verschillende andere aspecten van de verwerking van persoonsgegevens. Deze bepalingen worden hierna aangehaald voor de volledigheid. Alleen aspecten die specifiek van belang zijn voor de digitale archivering in de overheidssector worden belicht. Voor een algemene bespreking wordt verwezen naar de beschikbare rechtslitteratuur.

7.1. De beveiliging en de vertrouwelijkheid van de gegevensverwerking

Artikel 16 §4 luidt als volgt:

"Om de veiligheid van de persoonsgegevens te waarborgen, moeten de verantwoordelijke van de verwerking, en in voorkomend geval zijn vertegenwoordiger in België alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de pesoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.
Op advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer kan de koning voor alle of voor een bepaalde categorie van verwerkingen aangepaste normen inzake informaticaveiligheid uitvaardigen".

De verantwoordelijke voor de verwerking moet met andere woorden de vertrouwelijkheid en de integriteit van de gegevens kunnen garanderen.
Concreet moet de verantwoordelijke voor de verwerking of, in voorkomend geval, zijn/haar vertegenwoordiger in België:

1. er nauwlettend over waken dat de gegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met de artikelen 4 tot 8, worden verbeterd of verwijderd
2. ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de gegevens en de verwerkingsmogelijkheden, beperkt blijven tot hetgeen die personen nodig hebben voor de uitoefening van hun taken of tot hetgeen noodzakelijk is voor de behoeften van de dienst
3. alle personen die onder zijn gezag handelen, kennisgeven van de bepalingen van deze wet en haar uitvoeringsbesluiten, alsmede van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden
4. zich ervan vergewissen of programma's voor de geautomatiseerde verwerking van persoonsgegevens in overeenstemming zijn met de vermeldingen van de aangifte waarvan sprake is in artikel 17 en dat er geen wederrechtelijk gebruik van wordt gemaakt[133].

Wanneer de verantwoordelijke voor de verwerking beroep doet op een verwerker moet hij:

1. een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking
2. toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen
3. de aansprakelijkheid van de verwerker ten aanzien van de verantwoordelijke voor de verwerking vaststellen in de overeenkomst
4. met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verantwoordelijke voor de verwerking en dat de verwerker is gebonden door dezelfde verplichtingen als deze die waartoe de verantwoordelijke is gehouden
5. in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de bescherming van de gegevens en de eisen met betrekking tot de organisatorische en technische maatregelen vaststellen[134].

7.2. Grensoverschrijdend gegevensverkeer

Doorgifte van gegevens naar derde landen wordt door de wet strenger gereglementeerd dan de uitwisseling van gegevens met EU-landen. De bescherming van persoonsgegevens laat in veel landen immers te wensen over[135].

7.3. Strafbepalingen

Artikel 37-43 privacywet bestraft allerlei overtredingen van de wet met een geldboete.
Naast de veroordeling tot een geldboete kan de rechter de verbeurdverklaring uitspreken van de dragers van persoonsgegevens waarop het misdrijf betrekking heeft, zoals manuele bestanden, magneetschijven of magneetbanden, met uitzondering van de computers of enige andere apparatuur, of bevelen de gegevens uit te wissen. De verbeurdverklaring of de uitwissing kunnen bevolen worden, zelfs wanneer de dragers van persoonsgegevens niet aan de veroordeelde toebehoren[136].

8. Conclusie

De archiefvormer moet rekening houden met de bescherming van persoonsgegevens vanaf de creatie van de archiefstukken. De verwerking van persoonsgegevens moet in eerste instantie een wettige grondslag hebben en een gerechtvaardigd doel nastreven. Bovendien moet elke verwerking in een redelijke verhouding staan tot het nagestreerde doel. De archiefvormer moet elke betrokkene in beginsel informeren over het feit dat over hem gegevens verwerkt worden. Elke betrokkene heeft een recht op toegang en verbetering van zijn gegevens, soms mag hij zich zelfs tegen de verwerking er van verzetten. Persoonsgegevens moeten vertrouwelijk behandeld worden en voldoende beveiligd tegen onrechtmatige manipulaties.
De archiefvormer moet zich zo organiseren dat hij persoonsgegevens verwerkt conform de privacywet. Tegelijk moet hij ervoor zorgen dat degene aan wie hij de gegevens meedeelt ook in staat is de wetsbepalingen na te leven. Hieraan kan de archiefvormer voldoen door bepaalde metadata toe te voegen bij de archiefstukken: bijvoorbeeld een lijst van betrokken personen, de aard van de gegevens, welke kennisgeving er gebeurd is,...
De overdracht van persoonsgegevens aan derden, bijvoorbeeld een zelfstandige archiefdienst, is een verwerking in de zin van de wet. De voorwaarden van de wet moeten dus vervuld zijn. Sinds 2003 is hier een nieuwe vereiste aan toegevoegd voor federale diensten en instellingen: aan elke elektronische mededeling moet een principiële machtiging van het federale sectoraal comité voorafgaan.
De privacyregels naleven in de praktijk is een complexe aangelegenheid. Een goed doordacht privacybeleid uitstippelen is onontbeerlijk. Gegevens die in strijd met de wet verwerkt worden moeten in principe vernietigd worden.

F. Auteursrecht

De impact van het auteursrecht op de archiefsector wordt meer in detail besproken in het DAVID-rapport over auteursrecht. Hierna volgt een korte inleiding in de problematiek.

1. Toepasselijk recht

Conventie van Bern voor de bescherming van letterkundige en kunstwerken (26 juni 1948).
Auteurswet: De wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten (B.S. 27 juli 1994).
Softwarewet: De wet van 30 juni 1994 betreffende de bescherming van computerprogramma's (B.S. 27 juli 1994).
Repro-KB: koninklijk besluit van 30 oktober 1997 betreffende de vergoeding verschuldigd voor het kopiëren voor privé-gebruik of didactisch gebruik van werken die op grafische of soortgelijke wijze zijn vastgelegd (B.S. 7 november 1997).
Auteursrichtlijn: Richtlijn 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (P.B. L 167 van 22/06/2001).

2. Toepassingsgebied

2.1. Wat?

Het auteursrecht beschermt originele werken die in een bepaalde vorm gegoten zijn.

Originaliteit

Een origineel werk is het resultaat van de intellectuele activiteit of inspanning van de maker ervan. De inspanning moet niet erg groot zijn, ze moet enkel aantoonbaar zijn. Daarenboven komt de persoonlijkheid van de maker tot uiting in het werk. Met andere woorden, uit de waaier van mogelijkheden heeft de maker gekozen voor een vorm of uidrukking volgens zijn persoonlijke voorkeur en inzicht.
Origineel wil niet noodzakelijk zeggen 'nieuw', verschillende mensen kunnen onafhankelijk van elkaar tot gelijkaardige resultaten komen. Wanneer veel mensen spontaan hetzelfde idee op dezelfde manier uitdrukken, spreekt men van een 'banaal' werk dat geen auteursrechtelijke bescherming geniet.

Vorm

Ideeën worden niet beschermd door het auteursrecht. Ideeën kunnen niet rechtstreeks aan anderen doorgegeven worden, ze moeten uitgedrukt of in een vorm worden gegoten. Enkel deze uitdrukking of vorm kan worden beschermd.
De kunstenaar Christo werd wereldberoemd door het inpakken van grote bouwwerken, zoals de Pont-Neuf in Parijs of de Reichstag te Berlijn. Het idee op zich om bouwwerken in te pakken wordt niet beschermd door het auteursrecht, iedereen mag dit dus gewoon nadoen.
Een vorm betekent niet dat enkel tastbare voorwerpen beschermd worden. Redevoeringen, radiouitzendingen en websites worden ook beschermd.

Bijzondere types werken

Voor sommige types werken gelden bijzondere regels, dit is onder meer het geval voor afgeleide en collaboratieve werken, audiovisuele werken, databanken en computerprogramma's. Deze

bijzondere regimes worden behandeld in het DAVID-rapport over auteursrecht, http://www.antwerpen.be/david/website/nl/text_rapporten.htm.

2.2. Wie?

De auteur van een werk is de persoon die het werk creëerde. Vaak zullen de auteursrechten toch bij iemand anders berusten: de auteur kan zijn rechten contractueel afstaan en bij zijn dood gaan de rechten over op zijn erfgenamen. Het begrip 'auteur' wordt in de wet zowel gebruikt om de oorspronkelijke maker van een werk aan te duiden, als alle personen die dit recht van de oorspronkelijke auteur verkrijgen. Het begrip auteur zal hier ook in deze beide betekenissen gebruikt worden.

Voor een buitenstaander is het erg moeilijk te weten wie nu juist de titularis is van het auteursrecht. De wet bepaalt dat men ervan uit mag gaan dat degene wiens naam of 'letterwoord' op het werk vermeld staan ook effectief de houder van het auteursrecht is. Gaat het om een anoniem werk, dan wordt de 'uitgever' geacht de auteursrechten uit te oefenen. Het begrip uitgever omvat iedere persoon die auteursrechtelijk beschermde werken laat vervaardigen en commercialiseert.

Naast de auteur spelen nog andere tussenpersonen een rol spelen bij de exploitatie van een werk. Sommige van deze tussenpersonen genieten een aan het auteursrecht naburig recht. Meer bepaald gaat het om de uitvoerende kunstenaar, de producent van fonogrammen en films, de omroeporganisaties en de producent van een databank. Het beschermingsregime leunt nauw aan bij die van het auteursrecht en wordt besproken in het DAVID-rapport over auteursrecht (http://www.antwerpen.be/david/website/nl/text_rapporten.htm).

3. Reikwijdte van de bescherming

De auteur krijgt twee soorten rechten op zijn werk: economische rechten en morele rechten. De economische rechten geven de auteur het monopolie op de exploitatie van zijn werk. De morele rechten beschermen de 'intieme band' tussen de auteur en zijn creatie.

3.1. Vermogensrechten

De auteur heeft het exclusieve recht om zijn werk te reproduceren, te distribueren, te verhuren en uit te lenen. Daarnaast heeft de auteur het alleenrecht om afgeleide werken te produceren, (bijvoorbeeld vertalingen, bewerkingen voor een ander medium, merchandising, enz.). Ten slotte moet de auteur voor elke mededeling aan het publiek zijn toestemming verlenen (bijvoorbeeld uitzending op radio of televisie, opvoering van een toneelstuk).

In de traditionele analoge context omvat het monopolie op reproductie en mededeling aan het publiek hoofdzakelijk exploitatiehandelingen. Alleen de auteur mag bijvoorbeeld zijn boek laten drukken en verspreiden voor de verkoop. De eindgebruiker heeft het recht zijn exemplaar te lezen, verder te verkopen en aan vrienden uit te lenen. De archivaris had als eindgebruiker eveneens het recht een exemplaar van een werk te archiveren en dit in de leeszaal ter beschikking te stellen.

Bij digitale werken liggen de zaken anders. De eindgebruiker kan onmogelijk een digitaal werk gebruiken zonder er verschillende kopies van te maken, zij het beperkt tot vluchtige kopies in het werkgeheugen van de computer. In theorie moet de auteur hiervoor zijn toestemming verlenen. Hierdoor verkrijgt de auteur macht over hoe de eindgebruiker met zijn werk kan en mag omgaan. Digitale werken ter beschikking stellen via een netwerk staat in vele gevallen gelijk met een mededeling aan het publiek. Hiervoor is de toestemming van de auteur dus vereist.

De archivering van digitale werken komt op verschillende manieren in het vaarwater van het auteursrecht. De archivaris moet het werk kopiëren om het in zijn archief op te nemen. Eventueel moet het werk aangepast worden zodat het voor de toekomst toegankelijk blijft. Ten slotte is het ook de bedoeling het werk aan het publiek ter beschikking te stellen.

3.2. Morele rechten

De auteur heeft een divulgatierecht: alleen hijzelf beslist wanneer het werk klaar is om aan het publiek bekendgemaakt te worden. Het vaderschapsrecht houdt in dat de auteur beslist onder welke naam het werk uitgebracht wordt. De auteur kan zich verzetten tegen elke wijziging van zijn creatie op grond van zijn recht op integriteit.
De morele rechten zijn persoonlijkheidsrechten, dit wil zeggen dat deze rechten verbonden zijn aan een bepaalde persoon en niet overdraagbaar zijn. De reden hiervoor is dat de persoonlijkheid van de auteur geacht wordt tot uiting te komen in zijn werk.

4. Duur van de bescherming

Het auteursrecht blijft tot 70 jaar na de dood van de auteur gelden. Na zijn dood gaan de rechten van de auteur over op zijn erfgenamen, tenzij hij iemand anders heeft aangewezen.
Wanneer een werk door meerdere personen samen is gemaakt, blijft het auteursrecht bestaan tot 70 jaar na de dood van de langstlevende.
Voor anonieme of pseudonieme werken begint de termijn van 70 jaar te lopen vanaf het tijdstip waarop het werk op geoorloofde wijze voor het publiek toegankelijk gemaakt is. Indien het pseudoniem geen enkele twijfel laat over de identiteit van de auteur, geldt de algemene regel.
Alle termijnen worden berekend vanaf 1 januari van het jaar dat volgt op het feit dat de rechten doet ontstaan.

5. Auteursrecht en digitaal archiveren

Het auteursrecht verleent de auteur een monopolie op de exploitatie van zijn werk. Dit betekent niet dat de archivering van beschermde werken absoluut verboden is, alleen dat dit aan bepaalde voorwaarden onderworpen is. De archivaris heeft drie opties:

- de archivaris kan een licentie afsluiten met de auteur, waarin toestemming verleend wordt om het werk te preserveren en aan het publiek ter beschikking te stellen
- de wet zelf kan de archivaris toestemming verlenen om het werk te archiveren
- in alle overige gevallen, waar een licentie niet tot de mogelijkheden behoort en er geen wettelijke licentie is, kan het archief opteren voor een pragmatische aanpak.

5.1. Licenties

Digitale documenten die commercieel verspreid worden zijn vaak al voorzien van een standaardlicentie. De auteur of de uitgever kiest dan eenzijdig de licentievoorwaarden. De archivaris kan dan in de licentie nagaan of de auteur toestemming verleent om het werk te archiveren. Indien dit niet het geval is, kan de archivaris proberen alsnog een aparte licentie te verkrijgen. In het DAVID-rapport over auteursrecht wordt een model archieflicentie voorgesteld die kan dienen als basis voor onderhandelingen met de titularis van het auteursrecht.
De archiefinstelling kan overwegen de Koninklijke Bibliotheek te betrekken in de onderhandelingen over een licentie. Van elke publicatie moet immers één exemplaar in depot gegeven worden. Deze verplichting kan de rechthebbende bijkomend motiveren om een licentie te verlenen, vooral indien de plicht tot deponering dan als vervuld wordt beschouwd.
Sommige digitale werken worden verdeeld met een licentie die de gebruiker ruime rechten toekent, dit is meer bepaald het geval met verschillende 'Open Source' licenties. Dergelijk werken kunnen in de regel zonder probleem gearchiveerd en aan het publiek ter beschikking worden gesteld via het internet.

5.2. Wettelijke licentie

Reeds bij de invoering van het auteursrecht in 1886 was de wetgever zich ervan bewust dat bepaalde belangen voorrang moesten krijgen op de exclusieve rechten van de auteur. Daarom verleende de wet zelf toestemming om in bepaalde omstandigheden een werk te reproduceren of aan het publiek mede te delen. Deze uitzonderingen worden ook wel dwanglicenties of wettelijk licenties genoemd. Vaak krijgt de titularis van het auteursrecht ter compensatie een vergoeding.
Het Belgisch recht kent slechts voor een fractie van het archiefpatrimonium een expliciete wettelijke licentie, met name voor het cinematografische patrimonium dat bewaard wordt door het Koninklijk Belgisch Filmarchief. Voor zover de voorwaarden vervuld zijn, kunnen archieven zich beroepen op de andere uitzonderingen uit de auteurswet, met name de uitzondering voor wetenschappelijk onderzoek en openbare uitlening. Naargelang de concrete omstandigheden, kan het archief inroepen dat een auteur zich bezondigt aan rechtsmisbruik wanneer hij de archivering van zijn werk verhindert.
Onder impuls van de Europese Unie moeten de lidstaten hun huiding regime van wettelijke licenties harmoniseren. De Europese richtlijn 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappijrichtlijn laat de lidstaten onder strenge voorwaarden toe voor publieke instellingen, waaronder archieven, een uitzondering te maken op het reproductierecht en het recht op mededeling. Deze richtlijn moest vóór 22 december 2002 omgezet zijn in het Belgisch recht. Op het moment van schrijven (31 december 2003) is dit nog steeds niet gebeurd. Hopelijk grijpt de wetgever deze kans aan om een de wettelijke licentie uit te breiden voor de hele openbare archiefsector.

5.3. Overige situaties: een pragmatische aanpak

In sommige gevallen behoort een licentie niet tot de mogelijkheden, bijvoorbeeld omdat de titularis van het recht niet geïdentificeerd kan worden, omdat de titularis onvindbaar is of omdat het werk zelf een schending van andermans auteursrecht inhoudt. Een wettelijke licentie is niet altijd voorhanden of de toepasbaarheid is soms betwist. Moet het archief dan automatisch beslissen een document niet in de collectie op te nemen?
Om deze vraag te beantwoorden moet men een belangenafweging maken tussen enerzijds de belangen van de auteur en de belangen van het archief. De auteur heeft er belang bij om zijn werk ongestoord te kunnen exploiteren. Het archief bewaart documenten in het algemeen belang, onder meer om historisch en wetenschappelijk onderzoek mogelijk te maken.
De loutere opname van een werk in de archiefcollectie zal de exploitatierechten van de auteur in de regel niet schaden. De terbeschikkingstelling ervan aan archiefmedewerkers en/of gebruikers ligt gevoeliger.
Het beleid van het Internet Archive[137] vormt een uitstekend voorbeeld van deze pragmatische aanpak. Het *Internet Archive* verzamelt websites die vrij beschikbaar zijn op het internet tenzij de eigenaar aangeeft dat hij dit niet wenst. De maker van een site kan op voorhand aangeven dat de site niet gearchiveerd mag worden[138] of vragen dat zijn site uit het archief verwijderd wordt. Het archief is toegankelijk via het internet, maar de bezoeker moet zich aan de gebruiksvoorwaarden houden: het archief mag uitsluitend voor eigen studie en wetenschappelijke doeleinden gebruikt worden, bovendien moet de gebruiker alle toepasselijke wetten naleven[139]. Strikt genomen gaat het om illegale kopies en illegale mededeling aan het publiek. Omdat met ieders belangen rekening wordt gehouden, zijn er nog geen grote conflicten onstaan rond de praktijk van het *Internet Archive*.

6. Conclusie

De regeling met betrekking tot het auteursrecht houdt weinig rekening met de specifieke taken en noden van de archiefsector. Alle twijfels kunnen uit de weg geruimd worden aan de hand van een licentie, voor zover de titularis van het auteursrecht identificeerbaar is en bereid een licentie af te sluiten. Voor zover een licentie niet tot de mogelijkheden behoort, kan het archief zich waarschijnlijk beroepen op de uitzondering voor wetenschappelijk onderzoek om een beschermd werk in de collectie op te nemen.
Het lijkt onwaarschijnlijk dat een archief zich ooit voor een rechtbank zal moeten verantwoorden louter omdat het een werk opneemt in het archief. Het belang van de houder van een auteursrecht om een archief voor de rechter te slepen is vrij beperkt. Welke schade lijdt hij wanneer zijn werk geconserveerd wordt voor de toekomst? In welk opzicht verstoort de archivering de normale exploitatie van een werk?
Het enig teer punt vormt de terbeschikkingstelling aan het publiek, aangezien dit eventueel wel de exploitatie van het werk in het gedrang kan brengen. De manier waarop de terbeschikkingstelling gebeurt is hierbij van groot belang. Consultatie ter plaatse lijkt in elk geval tot de mogelijkheden te behoren, aangezien openbare uitlening expliciet buiten het monopolie van het auteursrecht valt. Terbeschikkingstelling via het internet daarentegen ligt gevoeliger. In bepaalde gevallen kan het archief kiezen voor een pragmatische oplossing die de belangen van de auteur met die van het publiek verzoent.

Meer informatie

M. BUYDENS, Auteursrechten en internet, Problemen en oplossingen voor het creëren van een online databank met beelden en/of tekst, *Brussel, DWTC, 1998, 104 p.*
H. DEKEYSER, Digitale Archivering: een juridische stand van zaken vanuit Belgisch perspectief, Deel 2: Auteursrecht, technische beschermingsmaatregelen en wettelijk depot, *Antwerpen-Leuven, 2003, http://www.antwerpen.be/david/website/nl/text_rapporten.htm*
S. DUSOLLIER, 'Droit d'auteur et bibliothèques dans l'univers numérique', *Revue Ubiquité 2002, afl. 12, 79-89.*
J.-P. TRIAILLE en A. STROWEL, Le droit d'auteur du logiciel au multimédia, *Brussel, Bruylant, 1997, 510 p.*

Eindnoten

[1] Belgische wet- en regelgeving is beschikbaar op Juridat, http://www.juridat.be/cgi_wet/wetgeving.pl.

[2] B.S.12 augustus 1955.

[3] B.S. 12 december 1957.

[4] A.J.M. DEN TEULING, Archiefterminologie voor Nederland en Vlaanderen, Stichting Archiefpublicaties, 's-Gravenhage, 2003, 8.

[5] Onder andere het Ministerie van Landsverdediging, zie art. 4 §1 Archief-KB.

[6] Waals decreet van 6 december 2001 betreffende de openbare archieven.

[7] H. VANDENBERGHE, Voorrechten en Hypotheken, Leuven, Wouters, 1997, 6.

[8] Zie De Kamer, http://www.dekamer.be.

[9] Zie Senaat, http://www.senate.be.

[10] Art. 2 wet 17 juli 1975 met betrekking tot de boekhouding en de jaarrekening van de ondernemingen (B.S. 4 september 1975).

[11] Art. 9 §2 wet 17 juli 1975.

[12] Art. 6 lid 4 wet 17 juli 1975.

[13] Art. 20 wet 16 maart 1803 op het notarisambt (B.S. 6 mei 1980).

[14] Art. 62 Wet Notarisambt.

[15] B.S. 2 december 1978.

[16] Art. 3 en 3bis KB 8 augustus 1980 betreffende het bijhouden van sociale documenten, B.S. 27 augustus 1980.

[17] Art. 195 §1 1° Wetboek van Vennootschappen.

[18] Art. 315 Wetboek Inkomstenbelasting, art. 63 BTW Wetboek.

[19] Antwerpen, 28 september 1992, F.J.F. 1993, 188.

[20] Art. 4 wet 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld (B.S. 28 januari 1993).

[21] W. REYNDERS, "Het bijhouden en bewaren van sociale documenten", T.S.R. 1980, 463.

[22] G. VAN DE WEG, "Archivering als basis voor verantwoording" in G.M. VAN TRIER (ed.), Handboek Informatiewetenschap, Alphen a/d Rijn, Samson, 1996, IV A 210.

[23] Zie boek 3, Titel III, hoofdstuk IV van het burgerlijk wetboek.

[24] M. RENARD-DECLAIRFAYT, "La reconstitution des minutes d'actes notariés perdues ou détruites", Rev.Not.B. 1983, 227.

[25] J. DUMORTIER en S. VYDT, Onderzoek over de modernisering van de burgerlijke stand in opdracht van het Ministerie van Justitie, Eindrapport, Leuven, ICRI, 1998, 4.

[26] G. STESSENS, De nationale en internationale bestrijding van het witwassen, Antwerpen, Intersentia, 1997, 198.

[27] K. VAN HULLE, "Boekhhoud- en jaarrekeningenrecht" in Handels- en economisch recht Deel 1 Ondernemingsrecht Volume A, Brussel, Story-Scientia, 1989, 186.

[28] Parl. St., Senaat, 1974-75, nr. 436/1, 1.

[29] Art. 6 lid 4 Jaarrekeningenwet.

[30] Art. 198 §1 wetboek van vennootschappen.

[31] Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (B.S. 22 december 2000).

[32] Art. 16 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[33] Art. 16 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[34] Art. 3 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[35] Art. 3 en 17 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[36] Memorie van toelichting, Parl. St. Kamer 2002-03, nr. 2100/001, 5596, 14.

[37] Art. 1322 2de lid: "Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont." Ingevoegd door de wet van 20 oktober 2000 betreffende de elektronische handtekening (B.S. 22 december 2000).

[38] Art. 16 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[39] Art. 16 punt 2 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[40] Art. 16 punt 2 van de wet op de elektronische handel van 11 maart 2003 (B.S. 17 maart 2003).

[41] Zie artikel 19 van de wet van 2 mei 1956 op de postcheque (B.S. 13 juni 1956), artikel 103bis van de wet van 4 decem-

ber 1990 op de financiële transacties en de financiële instellingen (B.S. 22 december 1990), artikel 196 van de wet van 17 juni 1991 tot organisatie van de openbare kredietsector (B.S. 9 juli 1991), artikel 18bis van de wet van 27 februari 1987 betreffende de tegemoetkoming aan gehandicapten (B.S. 1 april 1987), artikel 173ter van de wet betreffende de kinderbijslag voor loonarbeiders van 19 december 1939 (ingevoegd bij art. 89 wet 29 december 1990, B.S. 9 januari 1991), artikel 8 van het Koninklijk besluit van 22 maart 1993 betreffende de bewijskracht ter zake van de sociale zekerheid (B.S. 1 april 1993).

[42] Art. 5 van het KB van 12 september 1983

[43] B.S. 30 juni 1994.

[44] B.S. 15 juni 1999.

[45] Parl. St., Vlaamse Parlement, Zitting 2002-2003, nr. 1732/9, http://www.vlaamsparlement.be.

[46] Art. 162 van de Grondwet.

[47] B.S. 19 december 1997.

[48] Art. 14 van de wetten op de Raad van State, gecoördineerd op 12 januari 1973.

[49] Richtlijn 2003/4 inzake de toegang van het publiek tot milieu-informatie (P.B. L 041 van 14/02/2003 blz. 0026 - 0032) en het UNECE- Verdrag 'Verdrag betreffende de toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden' (Verdrag van Aarhuus, 25 juni 1998).

[50] Art. 1 Wet openbaarheid van bestuur.

[51] Art. 4 Vlaams Openbaarheidsdecreet.

[52] Art. 4 §1 toekomstige Vlaamse Openbaarheidsdecreet.

[53] Art. 2 Wet op de openbaarheid van bestuur in gemeenten en provincies.

[54] Gedr. St., Kamer, 1992-93, nr. 839/1, verklarende nota, 5.

[55] C. DE TERWANGNE, "Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles: regards croisés sur deux voies d'accès à l'information" in CUP, mai 2002, vol. 55, p. 94-95.

[56] Art. 8 toekomstige Vlaamse decreet.

[57] Art. 17 §3 2de lid toekomstige Vlaamse decreet.

[58] A.J.M. DEN TEULING, Archiefterminologie voor Nederland en Vlaanderen, Stichting Archiefpublicaties, 's-Gravenhage, 2003, 8.

[59] Art. 1 lid 1 archiefwet.

[60] Art. 3 archiefwet.

[61] Art. 1 lid 1 archiefwet.

[62] Art. 11 Wet openbaarheid van bestuur. Wat de archiefstukken van het Ministerie van Buitenlandse zaken betreft regelt een Ministrieel Besluit van 27 juli 1981 de openbaarheid. Militaire archieven ouder dan 50 jaar vallen onder het KB van 11 juni 1976. Zowel het MB als het KB kunnen de openbaarheid niet verder beperken dan de federale wet bepaalt. De grondwet aanvaardt geen uitzonderingen vastgelegd in een MB of een KB.

[63] Art. 11 Wet openbaarheid van bestuur.

[64] Art. 11 Wet openbaarheid van bestuur bij de federale adminstratie, en art. 12 Wet openbaarheid van bestuur bij lokale administraties.

[65] Art. 1, 2de lid 3° federale openbaarheidswet, art 2 2de lid 3° federale wet op de openbaarheid bij lokale besturen, art. 1 2de lid 3° openbaarheidsdecreet van het Waalse Gewest van 30 maart 1995 (B.S. 28 juni 1995).

[66] Art. 3 4° Vlaams openbaarheidsdecreet.

[67] Art. 11 §3 Vlaams openbaarheidsdecreet.

[68] Art. 3 6° toekomstige Vlaamse openbaarheidsdecreet.

[69] Art. 9 toekomstige Vlaamse openbaarheidsdecreet.

[70] Art. 4 2de lid federale openbaarheidswet. Art. 5 2de lid federale wet op de openbaarheid bij lokale besturen. Art. 7 Vlaams openbaarheidsdecreet.

[71] Art. 7 §1 Vlaams Openbaarheidsdecreet.

[72] C. DE TERWANGNE, "Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles: regards croisés sur deux voies d'accès à l'information" in CUP, mei 2002, vol. 55, 108-111.

[73] Art. 17 §2 2de lid toekomstige Vlaamse openbaarheidsdecreet.

[74] Art. 9 Wet openbaarheid van bestuur bij de federale adminstratie en art. 10 Wet openbaarheid van bestuur bij lokale administraties.

[75] F. SCHRAM, Openbaarheid van bestuur, Brugge, Die Keure, 2003, 69-70; Zie ook 'De auteurswet, de uitzonderingen en de wet openbaarheid van bestuur'. Nota van de Commissie voor de toegang tot bestuursdocumenten, 6 mei 2002.

[76] Art. 13 Vlaams openbaarheidsdecreet.

[77] Art. 20 §2 6de lid toekomstige Vlaamse openbaarheidsdecreet.

[78] Art. 3bis 1° privacywet.

[79] Art. 1 §4 privacywet.

[80] Art. 1 §5 privacywet.

[81] Art. 1 §1 privacywet.

[82] Art. 1 §2 privacywet.

[83] Art. 3 §1 privacywet.

[84] Het gaat onder meer om de Veiligheid van de Staat, de Algemene Dienst inlichting en veiligheid van de Krijgsmacht, de Veiligheidsautoriteit, de veiligheidsofficieren en het Vast Comité van Toezicht op de inlichtingendiensten en de Dienst Enquêtes ervan, voor zover de verwerkingen noodzakelijk zijn voor de uitoefening van hun opdrachten.

[85] Art. 3 §§4-7 privacywet.

[86] Art. 5 c privacywet.

[87] Art. 5 e privacywet.

[88] Art. 5 f privacywet.

[89] Art. 4 §1 2° privacywet.

[90] K.B. van 13 februari 2001 ter uitvoering van de privacywet, hierna privacy-KB, (B.S. 13 maart 2001), http://privacy.fgov.be/normatieve_teksten.htm.

[91] Art. 4 §1 3° privacywet.

[92] Art. 4 §1 4° privacywet.

[93] Art. 4 §1 5° privacywet.

[94] Art. 9 §1 privacywet.

[95] Art. 3 privacywet.

[96] Art. 9 §1 lid 1 en §2 lid 1 privacywet.

[97] Het gaat met name om een wet, een decreet, een ordonnantie, een K.B. of een ministrieel besluit.

[98] Art. 9 §2 lid 2 b) privacywet.

[99] Art. 9 §2 lid 2 a) privacywet.

[100] Art. 30 privacy-KB.

[101] Art. 10 §1 a) privacywet.

[102] Art. 10 §1 b) privacywet.

[103] Het algemene leerstuk van rechtsmisbruik kan hier toegepast worden. Zie D. DE BOT, Verwerking van persoonsgegevens, Antwerpen, Kluwer, 2001, 227-228.

[104] Art. 3 privacywet.

[105] Art. 13 privacywet.

[106] Art. 12 §1 lid 1 en 5 privacywet.

[107] Zie D. DE BOT, Verwerking van persoonsgegevens, Antwerpen, Kluwer, 2001, 227-228.

[108] Art. 3 privacywet.

[109] Art. 13 privacywet.

[110] Art. 12 privacywet.

[111] Art. 5 b) en c) privacywet.

[112] Art. 3 privacywet.

[113] Art. 13 privacywet.

[114] Art. 14 en 31 privacywet.

[115] Art. 6-8 privacywet.

[116] Art. 6 §1 privacywet.

[117] Art. 7 §1 privacywet.

[118] D. DE BOT, Verwerking van persoonsgegevens, Antwerpen, Kluwer, 2001, p. 154.

[119] Art. 8 §1 privacywet.

[120] Gevoelige gegevens en gezondheidsgegevens mogen onder meer verwerkt worden indien dit verplicht wordt door het arbeidsrecht of de sociale zekerheid. Zie art. 6 §2 b) en h) en art 7 §2 b) en c) privacywet. Gerechtelijke gegevens mogen onder meer verwerkt worden onder toezicht van een openbare overheid of van een ministeriële ambtenaar in de zin van het Gerechtelijk Wetboek, indien de verwerking noodzakelijk is voor de uitoefening van hun taken. Art. 8 §2 a) privacywet.

[121] Art. 7 §4 privacywet.

[122] Art. 25-27 privacy-KB.

[123] De CBPL heeft zich hierover nog niet uitdrukkelijk uitgesproken, maar erkent wel de waarde van archieven onder meer voor wetenschappelijk onderzoek. Advies CBPL van 11 september 1997, nr. 7.

[124] Hoofdstuk II van het privacy-KB.

[125] Art. 17 privacywet.

[126] Art. 17 §8 privacywet.

[127] Art. 51-62 privacy-KB.

[128] Art. 61 privacy-KB.

[129] De Raad van State heeft enkele criteria uitgewerkt om vast te stellen of een instantie een adminstratieve overheid is of niet. Een administratieve overheid:
– maakt geen deel uit van de wetgevende of rechterlijke macht
– heeft een beslissingsbevoegdheid
– is opgericht of erkend door de overheid
– voert een opdracht van algemeen belang of algemeen nut uit
– heeft het beheer van een openbare dienst
– staat onder toezicht van de overheid.
Zie W. LAMBRECHTS, "De evolutie van het begrip administratieve overheid", T.B.P. 1987, 357-366.

[130] Art. 31bis privacywet.

[131] Art. 37 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (B.S. 22 februari 1990).

[132] Men kan zich de vraag stellen in hoeverre deze regels stroken met de openbaarheid van bestuur.

[133] Art. 16 §2 privacywet.

[134] Art. 16 §1 privacywet.

[135] Art. 21-22 privacywet.

[136] Art. 41 privacywet.

[137] http://www.archive.org.

[138] Dit kan door een robot.txt bestand op de server te plaatsen waarin het verbod opgenomen is.

[139] Zie de pagina van het Internet Archive over de algemene voorwaarden, privacy en copyright.

DEEL 2

ARCHIEFLUIK

A. Inleiding

Het DAVID-project onderzocht hoe digitale archiefdocumenten op een duurzame en betrouwbare wijze worden gearchiveerd. De lange termijnarchivering van digitale archiefdocumenten is omwille van diverse redenen een uitdaging met veel drempels. Deze worden hieronder één voor één opgesomd zodat duidelijk is welke oplossingen nodig zijn. Aangezien DAVID zich in de eerste plaats richt op digitale archiefdocumenten is het nuttig om ons onderzoeksobject van naderbij te belichten. Vanuit dit uitgangspunt wordt immers de brede problematiek van digitaal archiveren in het algemeen benaderd.

1. Problematiek?

Administratieve medewerkers, ambtenaren, IT-verantwoordelijken, documentbeheerders en archivarissen worden alsmaar meer geconfronteerd met het bewaren en het archiveren van digitale archiefdocumenten. Digitaal archiveren is niet vanzelfsprekend, maar vraagt bijzondere oplossingen voor:

- 1.1. de technologische veroudering
- 1.2. de grote hoeveelheid documenten
- 1.3. de archiefwaardering en selectie
- 1.4. de verscheidenheid
- 1.5. de authenticiteit en betrouwbaarheid
- 1.6. de archivering van de context
- 1.7. de ontsluiting en het toegankelijk maken

1.1. De technologische veroudering

Digitale archiefdocumenten zijn per definitie digitaal. Voor het bekijken van digitale documenten is echter een bepaalde hard- en softwareconfiguratie nodig. Aangezien men dient uit te gaan van het principe dat archiefdocumenten een langere levensduur hebben dan de hard- en software omgeving waarbinnen ze werden gecreëerd of beheerd, dient men een oplossing te hebben voor de technologische veroudering. Een digitaal archiefdocument kan immers een lange of zelfs permanente bewaartermijn hebben terwijl de gemiddelde IT-infrastructuur slechts een levensduur van gemiddeld 5 tot 10 jaar heeft. De technologische veroudering is ook van toepassing op de dragers van digitale informatie. Digitale media zoals harde schijven, CR-R's en tapes hebben een kortere levenstermijn dan traditionele dragers zoals perkament, papier en microfilm.

1.2. De grote hoeveelheid documenten

De administraties maken volop gebruik van IT voor het aanmaken en uitwisselen van documenten. De hoeveelheid digitale documenten neemt elke dag toe. Zelfs wanneer archiefdiensten archiefwaardering en selectie goed toepassen, zullen zij met een grote toestroom aan digitale documenten worden geconfronteerd. Hiervoor zullen passende oplossingen zoals geautomatiseerde archiefbewerkingen en bulkverwerkingen nodig zijn. Deze processen dienen echter nauwlettend gecontroleerd te worden. Strenge kwaliteitscontroles en foutopsporings- en foutverbeteringsmechanismen zullen noodzakelijk zijn.

1.3. De archiefwaardering en selectie

Digitale archiefdocumenten nemen fysiek nauwelijks plaats in. Men kan zich bijgevolg de vraag stellen of archiefwaardering en selectie nog wel nodig zijn en of niet alle digitale documenten

kunnen gearchiveerd worden. Opslag wordt immers almaar goedkoper. Toch blijven archiefwaardering en selectie noodzakelijk. Goed archiefbeheer vraagt dat documenten die geen waarde meer hebben, worden vernietigd. Digitaal archiveren is immers een complex probleem dat veel onderzoek, tijd en middelen vraagt. Die worden bij voorkeur aangewend voor documenten met de status van archiefdocument. Het is zinloos om documenten zonder archiefwaarde te bewaren, bijkomende handelingen van gebruikers te vragen of om bijzondere vereisten te stellen aan informatiesystemen waarbinnen geen archiefdocumenten worden geproduceerd. Immers, het creëren van goed archiveerbare digitale documenten van een hoge kwaliteit, het intellectuele beheer en het leesbaar houden vragen, in tegenstelling tot de opslag, wel veel middelen en inspanningen. Archiefwaardering is de sleutel om de archiefdocumenten van complexe en technologie-afhankelijke systemen te archiveren. Archiefwaardering speelt ook mee in de keuze van een bepaald bestandsformaat als archiveringsformaat. Door de documenten zonder archiefwaarde te vernietigen, verhoogt men de toegankelijkheid van de documenten met archiefwaarde. Archiefwaardering en selectie maken efficiënter beheer mogelijk. Tenslotte houdt selectie ook de functionele vereisten voor de infrastructuur van het archiveringssysteem in de hand.

1.4. De verscheidenheid

De digitale documenten die momenteel gecreëerd en ontvangen worden zijn van een heel verscheiden aard. Er zijn niet alleen de diverse types digitale objecten (tekstverwerkingsbestanden, spreadsheets, e-mails, databanken, afbeeldingen, audiovisuele materialen, websites, GIS, CAD, virtuele modellen, enz.) ook de hard- en softwareconfiguraties zijn heel verscheiden. Voor elk digitaal archiefdocument is een passende archiveringsoplossing nodig. Rekening houdend met de grote verscheidenheid aan besturingssystemen en applicaties is dit geen evidentie.

1.5. De authenticiteit en betrouwbaarheid

Digitale documenten bieden het voordeel dat ze na vastlegging nog steeds bewerkt kunnen worden. Digitale documenten kunnen snel worden aangepast. De inhoud van archiefdocumenten moet vast en ongewijzigd zijn. In veel gevallen kan de wijziging achteraf niet waargenomen worden. Hierdoor kunnen twijfels rond de betrouwbaarheid rijzen zodat passende maatregelen vereist zijn. De archivaris dient ervoor te zorgen dat de digitale archiefdocumenten niet onrechtmatig worden gewijzigd en dat eventuele manipulaties opgespoord en ongedaan worden gemaakt. Alleen zo is hij/zij in staat om de geloofwaardigheid van de archiefdocumenten te verzekeren.

1.6. De archivering van de context

Digitale documenten zijn in de toekomst slechts bruikbaar wanneer ze door de gebruiker geïnterpreteerd kunnen worden. Met andere woorden, de gebruiker van het archiefdocument moet weten binnen welke context de documenten werden gecreëerd of ontvangen, wat de functie van het archiefdocument was en welke betekenis het document inhoudt. Hij/zij moet daarvoor minimaal weten binnen welk werkproces het document werd gecreëerd, op welk dossier of onderwerp het document betrekking heeft en wat het verband is met andere documenten. In de papieren wereld zijn documentbeheer en werkprocessen sterker met elkaar verweven. Dit contact dreigt in de digitale omgeving verloren te gaan.

1.7. De ontsluiting en het toegankelijk maken

Archiefdocumenten moeten in een geordende en toegankelijke staat bewaard worden om hun functie te vervullen. Deze verplichting is dus ook van toepassing op digitale archiefdocumenten. Digitale archiefdocumenten moeten op een logische, overzichtelijke en gestructureerde wijze bewaard worden zodat ze snel opspoorbaar zijn. Hierbij moet informatie over de context aan de archiefgebruiker worden gecommuniceerd zodat hij de archiefdocumenten ten volle kan begrij-

pen. Interpretatie van de digitale archiefdocumenten is slechts mogelijk wanneer ze leesbaar zijn en er bijgevolg een oplossing is voor het digitale duurzaamheidsprobleem.

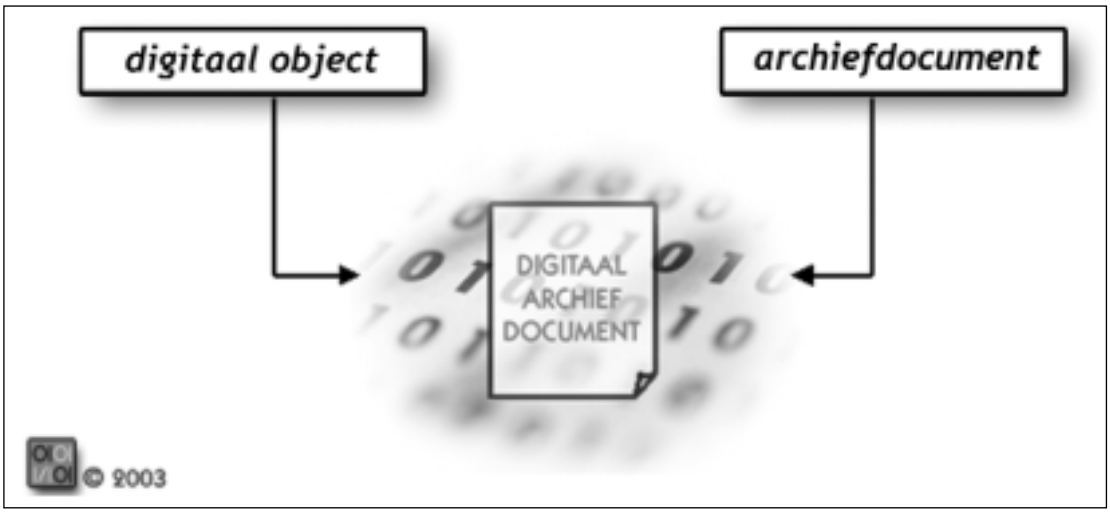
2. Het digitale archiefdocument

Digitale archiefdocumenten verschillen in meerdere opzichten van papieren archiefdocumenten. Een aantal belangrijke verschillen vloeien voort uit het feit dat digitale archiefdocumenten digitale objecten zijn[1]:

- de opslagwijze en de verschijningsvorm van een digitaal object zijn niet dezelfde: op de digitale drager wordt informatie als bits (reeksen nullen en enen) opgeslagen, terwijl op het scherm een document in zijn intellectuele vorm wordt gepresenteerd. Een meer expliciete identificatie en beschrijving van het digitale archiefdocument wordt noodzakelijk.
- drager en archiefdocument vormen geen eenheid meer: wijzigingen zijn niet meer visueel waarneembaar.
- voor de weergave van digitale objecten is hard- en software vereist: er is software nodig om de digitale representatie van een digitaal archiefdocument (bits) om te zetten naar de documentaire vorm van het archiefdocument. Digitale objecten kunnen slechts geraadpleegd worden mits de vereiste computerapparatuur en -programmatuur voorhanden is.
- de originele bitstream kan niet onderscheiden worden van de gekopieerde bitstream.
- digitale objecten hebben verschillende verschijningsvormen: de weergave op scherm van een digitaal document is afhankelijk van de computer- en gebruikersinstellingen.
- één digitaal archiefdocument kan verschillende bitrepresentaties hebben: hetzelfde archiefdocument (bijvoorbeeld een e-mail) kan in verschillende formaten (bijvoorbeeld MSG, ASCII/Unicode, TIFF, PDF, XML, enz.) en dus in verschillende bitstreams worden opgeslagen.
- er is geen vaste relatie tussen digitale archiefdocumenten en computerbestanden waardoor duidelijke identificatie nodig is. De relatie tussen archiefdocumenten en computerbestanden varieert immers van:
  - 1 op 1: 1 archiefdocument wordt in 1 computerbestand opgeslagen
  - 1 op veel: 1 archiefdocument bestaat uit meerdere computerbestanden
  - veel op 1: meerdere archiefdocumenten worden in 1 computerbestand bewaard.

Deze kenmerken zijn inherent aan het 'digitaal-zijn'. Het 'digitaal-zijn' is een essentiële karakteristiek van het archiefdocument die niet verloren mag gaan, maar die mee in tijd moet worden overgebracht. Archivarissen vertrekken immers vanuit het archiefwetenschappelijke principe dat archiefdocumenten in hun primaire vorm worden gearchiveerd: wat digitaal ontstaat, wordt digitaal gearchiveerd.

Door haar digitale eigenschap komt het concept van 'het' originele document onder druk te staan. In de digitale wereld overleeft het origineel immers niet. Door de technologische veroudering is het origineel gedoemd te verdwijnen. Telkens wanneer men een digitaal document reconstrueert, wordt als het ware een nieuwe kopie van het origineel gecreëerd. De uitvoering van eenzelfde bitstream resulteert immers in een nieuwe uitvoering of verschijning, afhankelijk van de gebruikte computer- en gebruikersinstellingen. Bovendien kan het originele digitale document niet altijd even gemakkelijk gedefinieerd worden. Digitale documenten hebben immers geen vaste verschijningsvorm. Dit maakt het extra moeilijk om de originele 'look and feel' van een document vast te leggen. Daarenboven kunnen originele bitstreams en hun kopieën niet van elkaar worden onderscheiden.



Digitale archiefdocumenten zijn anderzijds ook meer dan louter digitale objecten. Digitale archiefdocumenten onderscheiden zich van digitale objecten en digitale informatie door hun[2] :
– vaste documentaire vorm[3]: de samenstelling en de weergave van het document vastleggen
– statische of gefixeerde inhoud ('capture')
– context: archivalische band met de archiefvormer, met het werkproces waarbinnen ze werden gecreëerd of ontvangen, met gerelateerde papieren en digitale documenten.

Algemeen worden in een digitaal archiefdocument vijf componenten onderscheiden[4]:
– inhoud
– structuur
– context
– opmaak, 'look and feel'
– gedrag.

De identificatie van de archiefdocumenten en de archiefwaardering resulteert in het vastleggen van de essentiële en incidentele eigenschappen of componenten van een archiefdocument. De inhoud, de structuur en de context van een archiefdocument zijn essentiële componenten[5]. De 'look and feel' en het gedrag daarentegen zijn dit niet altijd. Deze componenten zijn overigens niet altijd even gemakkelijk te archiveren. De 'look and feel' en het gedrag zijn dikwijls zodanig afhankelijk van specifieke computerprogramma's dat ze zonder die programma's nauwelijks of niet kunnen worden bewaard.

De essentiële eigenschappen worden gearchiveerd, terwijl de incidentele eigenschappen mogen verloren gaan of gewijzigd worden. Uit InterPARES onderzoek blijkt immers dat digitaal archiveren niet betekent dat het archiefstuk geen wijzigingen mag ondergaan, maar wel dat de finaliteit van het document niet mag gewijzigd zijn en dat de essentiële componenten volledig en correct moeten zijn[6].

3. Digitaal archiveren

Digitaal archiveren heeft tot doel *interpreteerbare* digitale archiefdocumenten in tijd over te brengen. Men gaat er best van uit dat de ontvanger van het digitale archiefdocument toegang moet hebben tot het intellectuele archiefdocument en dat het document begrijpbaar moet zijn. Dit houdt in dat in de toekomst zowel computer als mens in staat moet zijn om de digitale archiefdocu-

menten te verwerken en te begrijpen. Dit stelt drie eisen aan de digitale archiefdocumenten. Zij moeten uitvoerbaar, visualiseerbaar en begrijpbaar zijn:
– uitvoerbaar: de digitale dragers moeten intacte bitstreams bevatten die naar het computergeheugen kunnen overgebracht worden
– visualiseerbaar: de bitstreams moeten door computers correct verwerkt worden zodat op het scherm het archiefdocument wordt getoond
– begrijpbaar: de gebruiker kent de functie, de betekenis en de context van het archiefdocument zodat de archiefdocumenten herbruikbaar zijn.

Uit het voorgaande blijkt dat opslag van bitstreams onvoldoende is om toegang te hebben tot de inhoud van een digitaal archiefdocument. Het raadplegen van een interpreteerbaar archiefdocument is maar mogelijk wanneer een aaneenschakeling van opeenvolgende afhankelijkheden correct kan worden uitgevoerd:
1 de digitale drager bevat intacte bitstreams
2 de bitstreams worden in het computergeheugen ingeladen. Hiervoor zijn goed functionerende randapparaten, poorten, kabels en stuurprogramma's nodig en moet het besturingssysteem van de computer compatibel zijn met het bestandssysteem van de drager
3 de ingeladen bits worden omgezet in het intellectuele archiefdocument en worden als zodanig op het scherm gepresenteerd. Dit is enkel mogelijk wanneer men over de nodige applicatiesoftware beschikt die het bestandsformaat van het digitale archiefdocument ondersteunt
4 de gebruiker heeft informatie over de context waarbinnen het document werd gemaakt of gebruikt zodat hij/zij de functie en de betekenis ervan ten volle kan inschatten.

Van zodra één van deze schakels ontbreekt is het archiefdocument niet meer interpreteerbaar en dient het als verloren of niet meer bruikbaar te worden beschouwd. Hoe groter het aantal afhankelijkheden, hoe groter het risico op verlies van archiefdocumenten. Vanwege deze reden worden elementen zoals back-upformaten, compressie en encryptie zoveel mogelijk vermeden.

Uit de karakteristieken van een digitaal archiefdocument volgt dat digitaal archiveren niet hetzelfde is als het maken van back-ups. Back-ups hebben als doel op korte termijn verloren of gewiste digitale bestanden te herstellen, terwijl veel digitale archiefdocumenten op lange termijn herbruikbaar moeten zijn. Gezien het korte termijnperspectief kan men bij back-ups er vanuit gaan dat de oorspronkelijke IT-configuraties nog aanwezig zijn, wat voor digitale archiefdocumenten met een lange bewaartermijn niet het geval is. De gebruikers van back-ups zijn doorgaans de auteurs van de documenten zelf die de documenten kunnen gebruiken zonder contextuele of administratieve metadata. De gebruikers van digitale archiefdocumenten zijn in veel gevallen niet de auteurs of één van de dossierbehandelaars.

4. Besluit

Digitaal archiveren is:
– de digitale eigenschap van digitale archiefdocumenten bewaren
– de mogelijkheid tot reconstructie bewaren: ervoor zorgen dat digitale archiefdocumenten in de toekomst gereconstrueerd kunnen worden
– een interactie tussen bitstreams enerzijds en hard- en software anderzijds mogelijk maken: maatregelen nemen zodat bruikbare en toegankelijke digitale archiefdocumenten worden gearchiveerd
– (externe) afhankelijkheden tot een minimum beperken
– risk assessment: inschatten en beperken van de risico's, inbouwen van zekerheden

- meer dan het bewaren van digitale objecten, en dus ook:
  - vastleggen van de essentiële eigenschappen of componenten van een digitaal archiefdocument door identificatie van de archiefdocumenten en archiefwaardering
  - informatie over de archivalische band en de context expliciet registreren en archiveren: ervoor zorgen dat digitale archiefdocumenten begrepen kunnen worden
  - kennis in tijd overbrengen: de intellectuele inhoud en de betekenis van digitale archiefdocumenten toegankelijk maken
- bewaren met een visie op lange termijn: digitale archiefdocumenten kunnen in aanmerking komen voor permanente bewaring
- digitale documenten onder intellectueel beheer en controle brengen
- vanaf de creatie of bij de ontvangst van digitale archiefdocumenten met archivering rekening houden: procedures inbedden in de volledige levenscyclus van documenten, pro-actief optreden zodat kwaliteitsvolle digitale archiefdocumenten worden gecreëerd en beheerd.

B. Bewaarstrategieën

Digitale archiefdocumenten zijn digitale objecten. Voor de lange termijnarchivering van digitale objecten kunnen verschillende bewaarstrategieën worden toegepast. Hieronder worden de meest courante bewaarstrategieën besproken en wordt nagegaan in welke mate deze geschikt zijn voor de bewaring van digitale archiefdocumenten[7]. Volgende bewaarstrategieën worden besproken:

1. Hard copy
2. Bewaren van de technologie
3. Conversie
4. Migratie
5. DAVID-bewaarstrategie

1. Hard copy

In de hard copy strategie wordt het digitale archiefdocument overgezet naar microfilm of afgedrukt op papier.

De archiefwetenschap gaat echter uit van de archivering van archiefdocumenten in hun oorspronkelijke, primaire vorm: wat digitaal (op papier) ontstaat, wordt digitaal (op papier) gearchiveerd. Bij omzetting naar papier of microfilm gaat een essentiële karakteristiek van het archiefdocument ("het digitaal-zijn") verloren. Alleen al vanwege deze reden wordt de hard copy strategie beter niet toegepast. Bovendien spelen bij overzetting naar papier of microfilm nog andere factoren mee:

– de archiefdocumenten verliezen hun 'digitale voordelen' zoals herbruikbaarheid, centrale bewaring en decentrale terbeschikkingstelling, geautomatiseerde archiefbeschrijvingen en zoekopdrachten, enz.
– functionaliteiten of bepaald gedrag van het digitale archiefdocument gaan verloren
– voor de vernietiging en de vervanging van archiefdocumenten is de goedkeuring van de Algemene Rijksarchivaris of diens gemachtigde vereist (art. 5 Archiefwet 24 juni 1955)
– moeilijk te vermijden dat de digitale versies nog worden gebruikt als basis voor de handelingen: de vertrouwdheid met digitale informatie groeit en de digitale versies zal men in werkprocessen als de primaire kopie blijven beschouwen én gebruiken
– niet alle essentiële informatie wordt altijd afgedrukt
– niet alle digitale archiefdocumenten kunnen gemakkelijk naar papier of microfilm worden overgezet (bijvoorbeeld GIS, CAD, multimedia objecten, databanken)
– hogere kostprijs: overzetten naar papier en microfilm is duurder dan digitale archivering.

Afdrukken op papier of overzetten op microfilm kan in principe enkel als tijdelijke archiveringsoplossing worden toegepast, in afwachting van een volwaardige digitale archiveringsprocedure. Deze optie is overigens niet toepasbaar voor alle types digitale documenten; enkel digitale archiefdocumenten met een papieren equivalent kunnen gemakkelijk afgedrukt worden. Een belangrijke vereiste is dat alle essentiële informatie mee wordt afgedrukt op papier of microfilm.

2. Bewaren van de technologie

2.1. Computermuseumstrategie

Deze piste bestaat uit het bewaren van de originele hard- en software waarmee de digitale archiefdocumenten werden gecreëerd. Op die wijze wordt een oude computerconfiguratie in stand gehouden zodat de computerbestanden in hun oorspronkelijke vorm raadpleegbaar blijven.

Voor middellange- en langetermijnbewaring is deze oplossing niet praktisch of haalbaar:
- alle verschillende configuraties moeten bewaard worden
- hard- en software hebben een beperkte levensduur
- oude hardware onderdelen worden almaar schaarser
- IT-kennis die nodig is voor het werken met oude hard- en software verdwijnt
- productondersteuning is niet meer mogelijk na verloop van tijd
- overzetten van digitale archiefdocumenten naar nieuwe dragers is noodzakelijk vanwege de degradatie van de dragers. De kans is klein dat nieuwe apparaten en bijhorende stuurprogramma's op oude computers kunnen worden geïnstalleerd.

Deze piste is slechts haalbaar voor de korte termijnbewaring (5 à 10 jaar) van digitale archiefdocumenten. De museumstrategie is bijgevolg maar bruikbaar voor de bewaring van archiefdocumenten waarvan de bewaartermijn niet langer is dan die van de levensduur van de technologie of als tijdelijke oplossing in afwachting van een duurzamere archiveringsoplossing. Oude computerconfiguraties kunnen soms nog gebruikt worden voor het recupereren van archiefdocumenten in verouderde formaten.

2.2. Emulatie

Bij emulatie wordt niet de originele hard- en software bewaard maar wordt het vereiste platform op een toekomstige computerconfiguratie gereconstrueerd zodat de computerbestanden in hun oorspronkelijk formaat raadpleegbaar zijn.

Emulatie kan op diverse niveaus worden toegepast. Men kan computerhardware, besturingssystemen, specifieke software of een combinatie van dit alles nabootsen. Emulatie is mogelijk op basis van configureerbare chips (emulatie door hardware) of op basis van computerprogramma's (emulatie door software).

Inmiddels bestaan verschillende visies op de wijze waarop emulatie voor digitale archivering kan worden toegepast:
- Jeff Rothenberg: Emulation Virtual Machine[8]
- Steve Gilheany: Turing Machine[9]
- Raymond Lorie: Universal Virtual Machine (data preservatie, programma preservatie)[10]
- Cedars & Camileon project: Migration on request[11].

Emulatie heeft een aantal interessante voordelen:
- in theorie kunnen de documenten in hun oorspronkelijke formaat gearchiveerd worden:
  - alle originele eigenschappen en functionaliteiten blijven behouden
  - er gaan geen elementen verloren ten gevolge van omzettingen
  - de authenticiteit van de digitale archiefdocumenten is gemakkelijker te garanderen
- de formaten waarin de documenten zijn opgeslagen, hoeven niet omgezet te worden telkens de formaten in onbruik raken
- de kostprijs is niet afhankelijk van het aantal gearchiveerde digitale documenten.

Anderzijds zijn er ook een aantal nadelen aan emulatie verbonden:
- emulatie is technisch complex: de nodige know-how en expertise voor ontwikkeling en onder-

houd zijn in archieven niet aanwezig. Archieven zijn bijgevolg afhankelijk van externe diensten en partners. Dit botst met de doelstelling om een zelfvoorzienend digitaal archief te bouwen.
- emulatie heeft hoge ontwikkelings- en onderhoudskosten: kunnen archieven die nu voor deze benadering kiezen de financiële inspanningen in de toekomst blijven leveren?
- de platformen waarop emulatieprogramma's draaien, evolueren, wat op termijn omzettingen van of aanpassingen aan emulatieprogramma's zal vergen
- overkill: bepaalde emulatiebenaderingen gaan uit van de volledige reconstructie van de oorspronkelijke applicaties met alle functionaliteiten, terwijl in principe een viewer volstaat om het (statisch) archiefdocument weer te geven. Emulatie richt zich hoofdzakelijk op de lange termijn bewaring van systemen en software, terwijl de archivaris in eerste plaats de archivering van het digitale archiefdocument beoogt
- de bescherming van het auteursrecht op hard- en software houdt restricties in voor reverse engineering, decompileren en disassembleren en het bouwen van emulatoren
- archiefvormers maken gebruik van tal van verschillende informatiesystemen, waarvan een aantal op maat van de organisatie zijn gesneden of ad hoc ontwikkeld zijn: archieven dienen over tal van emulatoren te beschikken en kunnen bepaalde kosten niet delen met andere archieven
- emulatie van viewers voor gesloten of niet-gedocumenteerde bestandsformaten op basis van reverse engineering is risicovol, zoniet onmogelijk. Emulatie van viewers voor gestandaardiseerde en gedocumenteerde formaten is gemakkelijker en veiliger. Wordt emulatie dan toch voorafgegaan door een migratie naar een gedocumenteerd archiveringsformaat?
- gebruikers werken met oude software en kunnen geen gebruik maken van technologische vernieuwingen
- archieven moeten niet alleen digitale archiefdocumenten beheren, maar ook emulatiehardware en -software en bijhorende documentatie
- de haalbaarheid van bepaalde emulatiepistes zal pas in de toekomst blijken.

De promotoren van emulatie als digitale bewaarstrategie schuiven voornamelijk het behoud van het oorspronkelijk computerbestand met alle originele eigenschappen als belangrijkste argument naar voor. Men beklemtoont in het bijzonder de mogelijkheid tot bewaring van de 'look and feel' en de functionaliteiten, terwijl deze eigenschappen bij migratie veelal gewijzigd worden of verloren gaan. Ze stellen niet de vraag of alle 'originele' eigenschappen wel bijdragen tot de archiefstatus van een digitaal object en bijgevolg wel dienen gearchiveerd te worden, hoe de originele 'look and feel' kan gedefinieerd worden en of het behouden van de oorspronkelijke functionaliteiten wel noodzakelijk is. Ze beschouwen digitale archiefdocumenten louter als digitale artefacten waarvan alle eigenschappen behouden dienen te worden. Het is niet toevallig dat de grote emulatievoorstanders in de eerste plaats computerwetenschappers zijn. Men mag niet uit het oog verliezen dat archieven andere taken en doelstellingen hebben dan musea en dat archiefwaardering en contextualisering een essentiële taak van archivarissen is.

Niettegenstaande dit alles, blijft emulatie een potentiële strategie die zijn nut voor de archivering van digitale archiefdocumenten kan hebben. In ieder geval heeft men nog maar beperkte ervaringen met emulatie als digitale bewaarstrategie. Er zijn bovendien nog maar weinig praktische en grootschalige emulatietoepassingen voor digitale archivering operationeel.

3. Conversie

Bij conversie worden digitale documenten overgezet van een lagere versie naar een hogere versie van hetzelfde bestandsformaat. Een voorbeeld is de conversie van een document van MS Word97 naar MS Word2000.

Voordelen:
– documenten blijven uitvoerbaar en functioneel.

Nadelen:
– digitale archiefdocumenten moeten met een hoge frequentie geconverteerd worden (bijvoorbeeld MS Word 6.0 ⇨ MS Word97 ⇨ MS Word2000 ⇨ MS Word2002 ⇨ MS Word2003)
– eigenschappen worden gewijzigd of gaan verloren waardoor de authenticiteit moeilijker kan worden gegarandeerd
– digitale documenten blijven in veel gevallen in een producent-, software- of versiegebonden formaat bewaard: men heeft geen enkele garantie over de lange termijnondersteuning van producent- of softwaregebonden formaten.

Conversie is geen praktische lange termijnbewaarstrategie voor digitale documenten. Conversie wordt bijgevolg zoveel mogelijk vermeden, tenzij er geen andere mogelijkheden zijn. Bijvoorbeeld wanneer er geen geschikt archiveringsformaat bestaat of er verlies dreigt van essentiële componenten van het archiefdocument.

4. Migratie

Migratie is de bewaarstrategie waarbij digitale documenten naar een geschikt archiveringsformaat worden omgezet. Dit wordt momenteel het meest toegepast bij de archivering van digitale archiefdocumenten.

Aangezien geschikte archiveringsformaten bij voorkeur standaardformaten zijn, is dit de bewaarstrategie waarbij de digitale documenten naar een standaardformaat worden omgezet. Standaarden zijn in principe gedocumenteerd, stabiel en niet afhankelijk van één producent. Migratie wordt soms ook wel aangeduid met ‘transformatie’ of ‘normalisatie’ wanneer standaarden als doelformaat worden gebruikt.

Voordelen van migratie als bewaarstrategie:
– digitale archiefdocumenten worden niet in een producent-, software- of versiegebonden formaat bewaard
– de specificatie van het bestandsformaat is beschikbaar: op basis van deze documentatie kan ten allen tijd een nieuwe viewer geprogrammeerd worden
– beschikbaarheid van omzettingstools: er zijn niet alleen veel omzettingstools op de markt, migraties zijn ook gemakkelijk te realiseren met behulp van wijdverspreide computerprogramma’s.

Nadelen:
– deze bewaarstrategie is sterk gebonden aan standaarden. Standaarden hebben echter een aantal nadelen:
  • hun ontwikkelingsproces neemt veel tijd in beslag: standaarden kunnen de marktevolutie niet even snel volgen
  • standaarden worden niet altijd nauwgezet toegepast of geïmplementeerd: standaarden worden soms uitgebreid om extra functionaliteiten mogelijk te maken waardoor de documenten niet meer ten volle uitwisselbaar zijn
  • standaarden ondersteunen nagenoeg geen applicatie-eigen functionaliteiten
  • niet alle standaarden zijn wijdverspreid of hebben voldoende marktpenetratie
  • standaarden hebben geen onbeperkte levensduur
– voor bepaalde bestandsformaten zijn geen geschikte archiveringsformaten beschikbaar
– de oorspronkelijke eigenschappen of functionaliteiten van het bronformaat kunnen maar

zelden integraal worden overgezet naar het doelformaat: migratie gaat in veel gevallen met verlies gepaard
– bij elk omzettingsmoment is de authenticiteit van de archiefdocumenten bedreigd.

Migratie is momenteel de meest toegepaste bewaarstrategie voor digitale archiefdocumenten. Bij migratie dient men er wel over te waken dat er geen essentiële informatie verloren gaat of de authenticiteit van de digitale archiefdocumenten wordt geschonden. Dit is op zich geen belemmering voor de toepassing van de migratiestrategie. Mits een grondige analyse van bron- en doelformaat kan men risico's vermijden en het verlies tot een minimum beperken. Gekoppeld aan archiefwaardering moet dit tot overname van alle essentiële en zoveel mogelijk incidentele eigenschappen leiden.

Rekening houdende met de grote hoeveelheid digitale archiefdocumenten dient een migratiestap geautomatiseerd uitgevoerd te worden. Manuele omzettingen zijn arbeidsintensief en niet altijd even accuraat. Geautomatiseerde migraties stellen een aantal bijzondere eisen aan het omzettingsproces:
– uitgebreide testfase van de procedure en omzettingsoperatie alvorens tot effectieve toepassing over te gaan
– omzettingstool:
  • uitgebreid testen en controleren zodat men zeker is dat in alle scenario's de omzetting correct wordt toegepast
  • voorzien van een foutenopsporingsmechanisme en error-handling
  • kwaliteitscontrole en validatie van de omgezette bestanden
  • registreren van de documenten die niet correct kunnen omgezet worden zodat deze achteraf manueel gemigreerd kunnen worden.

5. Besluit: Bewaren van originele en gemigreerde bitstreams

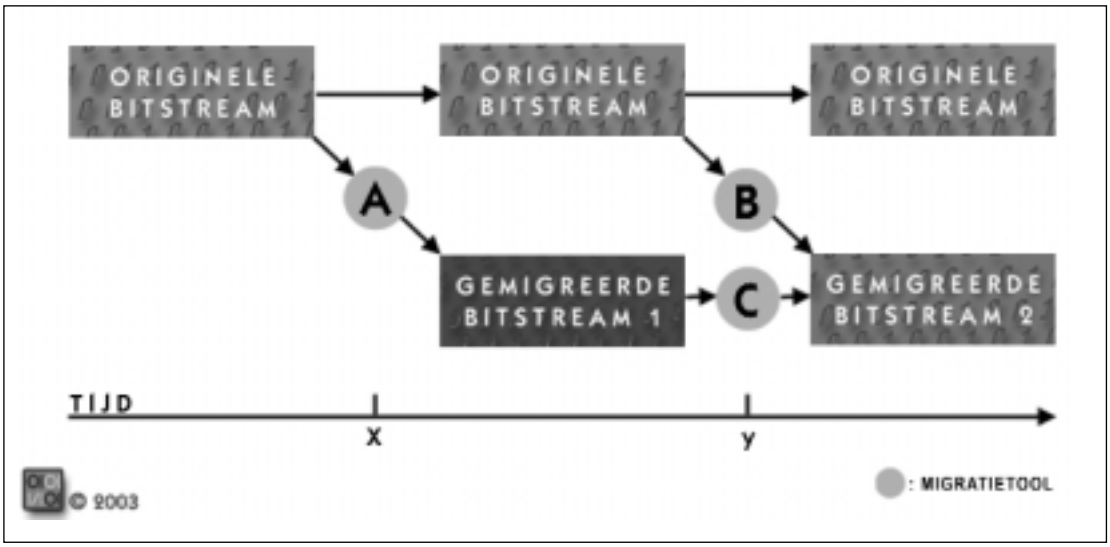
Uit de evaluatie van de mogelijke digitale bewaarstrategieën blijkt dat er momenteel nog geen definitieve oplossing voor het bewaarprobleem van digitale archiefdocumenten is. Geen enkele bewaarstrategie is risicovrij.

De zoektocht naar een passende bewaarstrategie werd jarenlang toegespitst op de vraag of emulatie van de originele software-omgeving dan wel migratie van de digitale archiefdocumenten de beste oplossing was. Beide oplossingen hebben met elkaar gemeen dat ze een bitstream vertalen naar een leesbaar document. Migratie en emulatie doen dit wel op een verschillend tijdstip. Bij migratie gebeurt dit in het heden, terwijl emulatie deze actie naar de toekomst verschuift. Migratie biedt een oplossing aan documentenzijde, terwijl emulatie voor het leesbaarheidsprobleem aan de hard- en/of softwarezijde een oplossing zoekt.

Inmiddels is het inzicht gegroeid dat beide benaderingen elkaar niet uitsluiten. Beide oplossingen zijn complementair in de levenscyclus van een digitaal archiefdocument of zijn meer geschikt voor een welbepaald type digitaal archiefdocument. In het algemeen is emulatie meer geschikt wanneer de 'look and feel' en het gedrag van een document van belang is, terwijl migratie volstaat wanneer inhoud en structuur de essentiële componenten van een archiefdocument zijn. Voor een succesvolle emulatie moet de specificatie van de technologie beschikbaar zijn. Ondertussen bestaan ook tal van tussenoplossingen die elementen van de migratie- en emulatieoplossing combineren.

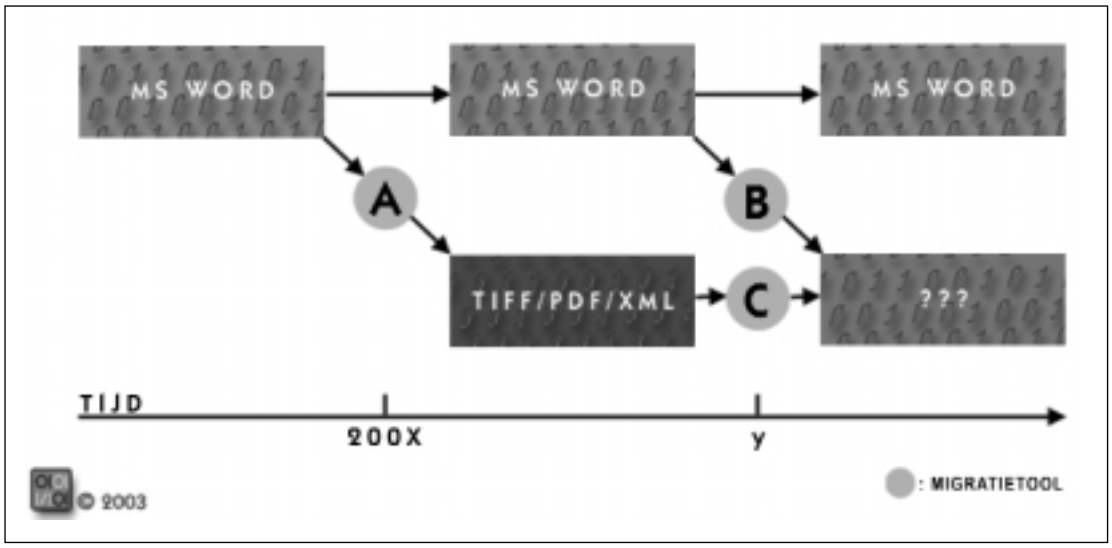
De bewaarstrategie die DAVID voorstelt[12], is een middenweg tussen emulatie en migratie, houdt naar de toekomst nog alle opties open en biedt een directe oplossing voor het leesbaarheidspro-

bleem. Dit kan door het bewaren van de originele bitstreams te combineren met het creëren en bijhouden van gemigreerde versies in een bestandsformaat die meer garanties inzake leesbaarheid biedt. Digitale archiefdocumenten die niet in een geschikt archiveringsformaat zijn opgeslagen, worden voor opname in het digitaal archief gemigreerd naar een archiveringsformaat. Het archiefdocument in zijn oorspronkelijk bestandsformaat wordt niet vernietigd, maar wordt eveneens in het digitaal depot opgenomen. Van deze archiefdocumenten worden dus twee bitrepresentaties bijgehouden: één in het oorspronkelijke bestandsformaat, één in het gemigreerde bestandsformaat. Men kan deze bitrepresentaties in afzonderlijke computerbestanden bewaren of in een XML-container inkapselen. Dit biedt het voordeel dat in de toekomst zowel emulatie als migratie van het oorspronkelijk of het gemigreerde bestandsformaat mogelijk zijn. Voor digitale archiefdocumenten die van bij hun creatie in een geschikt archiveringsformaat worden bijgehouden, is geen migratie nodig zodat slechts één bitrepresentatie wordt bewaard.



Toegepast op een tekstdocument dat werd opgeslagen in MS Wordformaat houdt deze bewaarstrategie de volgende stappen in. Ten laatste op het moment van opname in het digitaal archief wordt het tekstdocument in MS Word gemigreerd naar een geschikt archiveringsformaat (migratietool A). Afhankelijk van de identificatie van de essentiële componenten en de archiefwaardering wordt een keuze gemaakt uit de archiveringsformaten XML, TIFF en PDF. MS Word is immers een ongedocumenteerd producent- en applicatiegebonden bestandsformaat met in tijd beperkte ondersteuning[13], dat helemaal niet geschikt is voor lange termijnarchivering. Zo is er na 30 juni 2008 in principe geen ondersteuning meer voor MS Word 2002. In het digitaal depot worden het MS Wordbestand en het gemigreerde bestand opgeslagen. Wanneer het archiveringsformaat XML, TIFF of PDF in onbruik dreigt te geraken, heeft men de keuze tussen verschillende opties:

– gebruiken van een emulator voor het MS Wordformaat
– gebruiken van een emulator voor het gemigreerde formaat
– migratie naar een nieuw archiveringsformaat (gemigreerde bitstream 2) op basis van het MS Wordbestand met migratietool B
– migratie naar een nieuw archiveringsformaat (gemigreerde bitstream 2) op basis van het gemigreerde formaat (gemigreerde bitstream 1) met migratietool C.



Zelfs al lijkt emulatie in het geval van MS Word een weinig waarschijnlijke mogelijkheid, deze bewaarstrategie zou kunnen betekenen dat in het tweede archiveringsformaat meer originele eigenschappen van het archiefdocument aanwezig zijn dan in het eerste archiveringsformaat. Een ander voordeel is het vermijden van accumulerende omzettingsfouten. Dit kan allemaal doordat het archiefdocument in zijn oorspronkelijk bestandsformaat als bronbestand voor migraties beschikbaar blijft.

C. Archiveringsstandaarden

1. Belang

IT-standaarden spelen een belangrijke rol in elke bewaarstrategie. Bij migratie worden de archiefdocumenten bij voorkeur naar een gestandaardiseerd bestandsformaat omgezet. Hierdoor dienen de archiefdocumenten minder frequent omgezet te worden. Aangezien de technische specificatie van gestandaardiseerde formaten beschikbaar is, biedt dit het voordeel dat ten allen tijde nieuwe viewers voor het verouderd formaat kunnen worden geprogrammeerd. Emulatie van software voor het visualiseren van documenten in gestandaardiseerde formaten is eenvoudiger en realistischer dan het bouwen van emulatieprogramma's voor ongedocumenteerde formaten. Tenslotte zijn standaarden ook belangrijk bij de opslag van archiefdocumenten op dragers. Digitale dragers zijn immers ook onderhevig aan technologische veroudering. Bij opslag op een drager wordt bij voorkeur een fysieke (type drager) en logische (bestandssysteem) standaard toegepast zodat de digitale archiefdocumenten uitwisselbaar zijn.

Standaarden kunnen worden toegepast op:
– de dragers waarop de digitale archiefdocumenten worden bewaard
– de bestandsformaten waarin de digitale archiefdocumenten zijn opgeslagen.

2. Dragers

2.1. Duurzame dragers

Of digitale archiefdocumenten in de toekomst nog raadpleegbaar zijn, is in de eerste plaats afhankelijk van de drager waarop ze zijn opgeslagen. De digitale archiefdocumenten worden best op een duurzame drager opgeslagen. De drager moet in staat zijn om voor een lange termijn gegevens te bevatten en mag niet snel fysiek aftakelen.

De levensduur van dragers wordt in de regel onderzocht op basis van tests waarbij het verouderingsproces wordt versneld terwijl het aantal fouten op de drager wordt gemeten. Op basis van die tests voorspelt men vervolgens de levensduur van de drager wanneer deze in goede materiële omstandigheden wordt bewaard. Hierbij wordt rekening gehouden met het foutopsporings- en verbeteringssysteem. Voor elk type opslagmedium bestaat immers een foutopsporings- en verbeteringssysteem. Deze mechanismen kunnen tot op zekere hoogte fouten op de drager corrigeren zodat de digitale bestanden leesbaar blijven. Het aantal verbeterbare fouten heeft echter een bovengrens. Als die grens wordt overschreden, zijn de computerbestanden onleesbaar. De levensduurtests geven een goede indicatie van de verwachte levensduur van de drager maar zijn op zich geen garantie voor de leesbaarheid van de archiefdocumenten op lange termijn.

Een duurzame drager en de goede materiële bewaring zorgen er enkel voor dat de drager nog de gegevens bevat die er ooit werden opgeplaatst. Of de informatie op de drager nog effectief kan ingelezen worden, is afhankelijk van de beschikbare technologie.

2.2. Levensduur van de technologie

In de toekomst dient men immers over de nodige hard- en software te beschikken om de informatie op een bepaalde drager in het computergeheugen te laden (o.a. apparaten, stuurprogram-

ma's). Deze technologie veroudert snel en heeft doorgaans een kortere levensduur dan de dragers die digitale archiefdocumenten bevatten. In die zin is het irrelevant of een CD-R al dan niet een levensduur van 100 jaar heeft. De kans is heel groot dat binnen 10 of 20 jaar de apparatuur en/of programmatuur om CD-R's in te lezen, niet meer voorhanden is[14]. Voor verschillende diskette- en tapeformaten is dit nu al het geval. Dit geldt overigens voor alle types dragers, zowel optische als magnetische. De keuze van een drager wordt bijgevolg mee bepaald door de beschikbare technologie. Overzettingen naar andere dragers zullen zich bijgevolg opdringen van zodra een bepaalde technologie niet meer beschikbaar dreigt te worden. Door zorgvuldig een stabiele drager en duurzame technologie te kiezen kan men de overzettingsfrequentie tot een minimum herleiden.

2.3. Algemene aanbevelingen

In de praktijk worden zowel magnetische als optische dragers als opslagmedium voor digitale archiefdocumenten gebruikt. Voor beide type dragers gelden de volgende aanbevelingen:

- spreid het risico: bewaar indien mogelijk de archiefdocumenten op verschillende types digitale dragers. Hou de verschillende soorten optische en magnetische dragers van digitale archiefdocumenten wel in de hand zodat het aantal ondersteunde systemen beperkt kan blijven.
- kies dragers met een technologie die zijn betrouwbaarheid en bedrijfszekerheid inmiddels bewezen heeft; vermijd de allernieuwste technologieën die op dit vlak nog niets bewezen hebben
- bewaar archiefdocumenten op dragers die niet snel degraderen: kies dragers met een lange levensduur en een robuust foutopsporings- en verbeteringssysteem
- zorg ervoor dat de nodige apparatuur en programmatuur beschikbaar is:
  - fysiek formaat: gebruik gestandaardiseerde dragers die met meerdere types apparaten van verschillende producenten kunnen gelezen worden
  - logisch formaat: beschrijf de drager volgens een standaard bestandssysteem
- maak veiligheidskopieën en bewaar die op afzonderlijke en veilige locaties: hoe groter de capaciteit of densiteit van de drager, des te meer veiligheidskopieën nodig zijn
- bewaar de opslagmedia in goede materiële omstandigheden
- voer regelmatig kwaliteitscontroles uit
- zet de digitale archiefdocumenten naar een andere drager over, wanneer:
  - het aantal verbeterbare fouten op de drager sterk stijgt
  - de technologie in onbruik dreigt te raken
- controleer bij het refreshen de integriteit van de overgezette bytestreams (bijvoorbeeld door checksums te vergelijken)
- zorg voor elk type drager van digitale archiefdocumenten voor een rampen- en herstelplan
- voeg bij elke drager een overzicht van de mappenstructuur en de bestanden (papier/digitaal)
- plaats de archiefdocumenten in een gestandaardiseerd bestandssysteem en een open, gedocumenteerd en ongecomprimeerd bestandsformaat op de drager.

2.4. Magnetische dragers

Informatie en praktische aanbevelingen zijn beschikbaar op de DAVID-website:

- *Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 6:* Duurzame magnetische dragers
- *F. BOUDREZ,* Magnetische dragers voor het archief, *Stadsarchief Antwerpen, Antwerpen, 2002.*

Aandachtspunt: gebruik geen harde schijven als medium voor lange termijnbewaring!
– harde schijven zijn niet duurzaam, want hebben een relatief korte levensduur (slijtage, warmte)
– de mappen en bestanden zijn in een bestandssysteem van een bepaald besturingssysteem opgeslagen.

Aandachtspunt: gebruik geen back-uptapes voor archiveringsdoeleinden!
Back-uptapes zijn in de regel gecomprimeerde kopieën van platformafhankelijke computerbestanden. Back-uptapes zijn waardeloos zonder de originele back-upsoftware en het computerbesturingssysteem en de applicatiesoftware waarmee de digitale archiefdocumenten werden gemaakt:
– back-upformaten zijn meestal ongedocumenteerde of gesloten formaten eigen aan één bepaalde producent of back-upprogramma
– back-upbestanden zijn doorgaans gecomprimeerd. Voor de decompressie is specifieke software nodig
– niet alle informatie voor de reconstructie van de computerbestanden is noodzakelijk op de drager opgeslagen. Bepaalde essentiële informatie wordt op de back-upcomputer bijgehouden.

2.5. Optische dragers

Informatie en praktische aanbevelingen zijn beschikbaar op de DAVID-website:
– *Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 2:* Duurzame CD's
– *F. BOUDREZ,* CD's voor het archief, *Stadsarchief Antwerpen, Antwerpen, 2001.*

Aandachtspunt: gebruik geen DVD's als lange termijndrager!
– de standaardisatie van DVD is nog niet voltooid
– beschrijfbare DVD's zijn niet gemakkelijk uitwisselbaar.

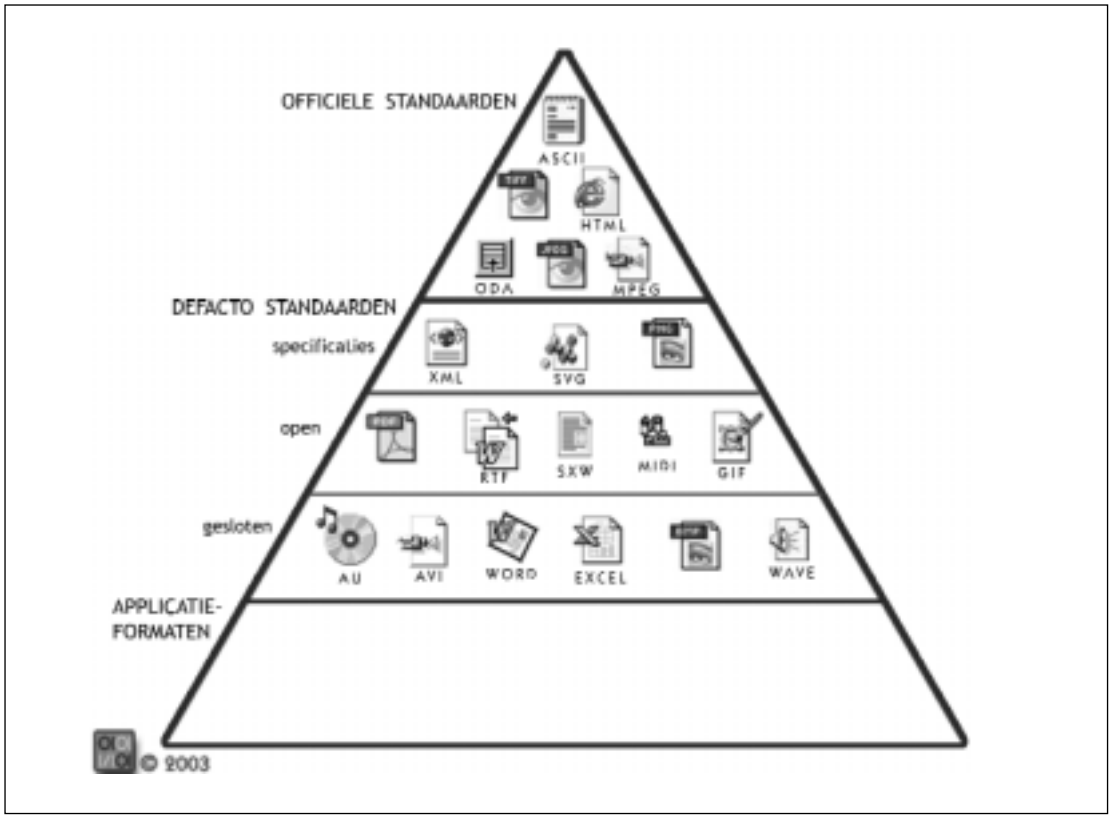
3. Bestandsformaten

Digitale archiefdocumenten worden bij voorkeur in een gestandaardiseerd bestandsformaat opgeslagen. Gestandaardiseerde bestandsformaten zijn in de regel:
– open en gedocumenteerd: hun technische specificatie is beschikbaar. Men gaat ervan uit dat viewers gemakkelijk te programmeren zijn wanneer men over de technische specificatie van het formaat beschikt
– stabiel: standaarden kunnen pas gewijzigd worden na het doorlopen van een procedure
– software-onafhankelijk: standaarden worden ondersteund door software van meerdere producenten en open source initiatieven
– producent-onafhankelijk.

3.1. Hiërarchie
In de IT-wereld bestaan tal van standaarden. Om het overzicht te behouden en als uitgangspunt in de keuze van een bepaald bestandsformaat kan men een hiërarchische indeling hanteren.

Bovenaan in de hiërarchie staan de officiële standaarden. Deze standaarden zijn vastgelegd door officiële standaardiseringsorganisaties en danken hun officiële status aan de participatie van een (inter-)gouvernementele organisatie. Bekende voorbeelden hiervan zijn *ISO* (International Organisation for Standardisation), *IEC* (International Electrotechnical Commission), *ITU* (International Telecommunications Union). Daarnaast zijn er veel officiële regionale en nationale standaardiseringsorganisaties.

Onder deze groep standaarden situeren zich de defacto standaarden. De defacto standaarden kunnen in drie subgroepen worden onderverdeeld. De specificaties zijn het resultaat van niet-officiële standaardiseringsinitiatieven (bijvoorbeeld W3C). Hun beheer is niet in handen van één producent maar van een standaardiseringsinstantie. De open formaten zijn net zoals de specificaties publiek gedocumenteerd, maar hun beheer is in handen van één bepaalde producent. Tenslotte zijn er de gesloten formaten. Deze formaten danken hun status van defacto standaard aan hun wijdverspreidheid maar hun technische specificatie wordt niet vrijgegeven en ze zijn afhankelijk van één producent.



Bij het kiezen van een geschikt archiveringsformaat richt men zich bij voorkeur op de officiële standaarden en de specificaties. Enig pragmatisme is hierbij aanbevolen. De hiërarchie is een belangrijke leidraad maar is niet zaligmakend. De status van officiële standaard garandeert niets op zich. Zo kennen bepaalde specificaties een grotere toepassing dan hun officiële equivalenten (cf. Unicode vs. ISO-10646; XML vs. SGML). Naast de mate van standaardisatie gelden immers nog andere criteria voor geschikte archiveringsformaten.

3.2. Geschikte archiveringsformaten

Een geschikt archiveringsformaat beantwoordt bij voorkeur aan volgende criteria:

- gestandaardiseerd: gedocumenteerd, stabiel en niet afhankelijk van één producent
- wijdverspreid en voldoende marktpenetratie
- uitwisselbaar: onafhankelijk van bepaalde besturingssystemen, netwerkprotocollen en applicaties
- voorziet een robuust foutopsporing- en verbeteringsmechanisme: fouten in bitopslag zijn herstelbaar
- mogelijkheid tot systematische en geautomatiseerde validatie
- goed gestructureerde opslag van informatie
- opslag zonder informatieverlies (geen lossy compressie)

– mogelijkheid tot insluiten van (zelfgedefineerde) metadatavelden
– in staat om de essentiële eigenschappen van het archiefdocument in tijd over te brengen
– bewaren van de authenticiteit van de archiefdocumenten
– autonoom en zelfvoorzienend
– drager en apparaat onafhankelijke opslag mogelijk
– gebruiksvriendelijk.

Deze criteria zijn belangrijk in de keuze van een bepaald bestandsformaat als archiveringsformaat. Ook bij het toepassen van archiveringsstandaarden houdt men best deze kwaliteitsvereisten voor ogen. Standaarden kunnen immers op diverse wijzen worden toegepast. De meeste archiveringsformaten laten de gebruiker toe om een aantal instellingen en parameters te definiëren. Zo kan men diverse soorten TIFF-, XML- en PDF-bestanden produceren maar niet elk TIFF-, XML- of PDF-document is geschikt om op lange termijn te archiveren. Bij afbeeldingen die als TIFF-bestand worden bewaard, kan JPEG-compressie worden toegepast. Er gaan hierbij niet alleen gegevens verloren, maar voor de reconstructie is men afhankelijk van de overeenstemmende decompressie. De kwaliteit van XML-documenten is afhankelijk van de nesting en semantiek van de XML-tags. PDF-documenten bestemd voor lange termijnbewaring zijn bij voorkeur getagd of op zijn minst gestructureerd.

De gearchiveerde digitale archiefdocumenten zijn best zo autonoom mogelijk. De afhankelijkheden voor reconstructie worden best tot een absoluut minimum beperkt. Het ontbreken van één noodzakelijke schakel in het reconstructieproces kan immers tot verlies van het archiefdocument leiden. Omwille deze reden worden compressie, encryptie, paswoorden of andere beveiligingsinstellingen zoveel mogelijk vermeden.

Meer informatie over geschikte archiveringsformaten is beschikbaar op de DAVID-website:
– *Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 4:* Standaarden voor bestandsformaten
– *F. BOUDREZ,* Standaarden voor digitale archiefdocumenten, *Stadsarchief Antwerpen, Antwerpen, 2003*
– *F. BOUDREZ,* <XML/> en digitaal archiveren, *Stadsarchief Antwerpen, Antwerpen, 2002.*

Voor bepaalde types digitale informatie zijn (nog) geen geschikte archiveringsformaten beschikbaar. Deze digitale documenten zijn nauw verbonden met de hard- en softwareomgeving waarbinnen ze werden gecreëerd en kunnen nauwelijks of niet daar buiten worden gebruikt. Dit is momenteel het geval voor bepaalde multimedia-objecten. In dit geval is het aanbevolen om een bestandsformaat te zoeken dat aan zoveel mogelijk criteria van een geschikt archiveringsformaat beantwoordt en waarbij afhankelijkheden maximaal worden vermeden.

Aandachtspunt: archiveer geen gecomprimeerde digitale documenten!
Het toepassen van compressie wordt vermeden vanwege volgende redenen:
– decompressie is een extra reconstructieschakel die botst met het principe om afhankelijkheden zoveel mogelijk te vermijden
– bij lossy compressie gaat informatie en kwaliteit verloren. Voor audiovisuele archiefdocumenten wordt het kwaliteitsverlies, de ruis en/of de vervormingen gemakkelijk auditief of visueel waarneembaar wanneer verschillende compressie-algoritmes opeenvolgend worden toegepast
– het verwerken van gecomprimeerde bitstreams is complexer
– gecomprimeerde digitale documenten zijn kwetsbaarder dan ongecomprimeerde documenten. Een fout in een gecomprimeerd bestand leidt sneller tot onherstelbaar verlies
– de compressienoodzaak vloeit meestal voort uit technologische beperkingen (verwerking, opslag, transmissie). Deze restricties zullen ten gevolge van de technologische vooruitgang de komende jaren soepeler worden of zelfs helemaal verdwijnen.

Als compressie onvermijdelijk is, opteer dan voor een lossless compressiemethode (zonder informatieverlies) en kies een compressie met een open, gedocumenteerde en gestandaardiseerde decompressie-algoritme.

3.3. Voorbeelden van geschikte archiveringsformaten

TYPE DOCUMENT	**ARCHIVERINGSFORMAAT**
Tekst:	ASCII/UNICODE, TIFF, PDF, XML
Afbeeldingen:	
Raster	TIFF, PNG
Vector	SVG
Raster en vector	CGM
Geluid:	WAV (ongecomprimeerde PCM)
CAD:	DXF
GIS:	GML
Video:	MXF

Tips en aanbevelingen:

- beperk het aantal bestandsformaten die binnen de organisatie als archiveringsformaat worden gebruikt
- bewaar archiefdocumenten indien mogelijk vanaf de creatie in een geschikt archiveringsformaat
- bewaar archiefdocumenten niet in een gesloten of ongedocumenteerd formaat
- vermijd het gebruik van compressie (bijvoorbeeld LZW, JPEG, ZIP in een TIFF-bestand; ZIP in een PDF-bestand)
- verpak de archiefdocumenten niet in gecomprimeerde formaten (.zip; .tar)
- wanneer de originele formaten niet bewaard worden: vernietig de originele computerbestanden pas na de controle van de omzettingen
- ga na of standaarden wel correct worden toegepast en/of de gearchiveerde digitale documenten wel beantwoorden aan de formele definitie van de standaard.

D. Beleid en Procedures

1. Archiveringsbeleid

Elke organisatie heeft nood aan een algemeen beleid dat de basisopties en de richting van de archiveringspolitiek vastlegt. Dit beleid moet een coherent document- en archiefbeheer mogelijk maken en heeft als finaliteit dat de archiefdocumenten in een goede, geordende en toegankelijke staat bewaard zijn zolang dit nodig is. Het archiveringsbeleid is het platform voor de uitvoerende acties en concrete procedures.

De archiveringspolitiek binnen de organisatie wordt bij voorkeur vastgelegd in een beleidsdocument dat formeel is bekrachtigd en dat betrekking heeft op zowel het papieren als digitaal archief. In dit document wordt onder meer vastgelegd:
- wat de algemene doelstellingen en uitgangspunten van het archiveringsbeleid van de organisatie zijn
- welke wettelijke verplichtingen van toepassing zijn op het document- en archiefbeheer binnen de organisatie
- welke documenten voor de organisatie de status van archiefdocument hebben
- welke documenten op papier of digitaal worden bewaard
- welke bewaarstrategie voor digitale archiefdocumenten wordt gevolgd
- hoe en in welke mate de betrouwbaarheid van de digitale archiefdocumenten wordt gewaarborgd
- welk organisatie-onderdeel gemandateerd is voor het uitwerken van archiveringsprocedures
- hoe de bevoegdheden en de verantwoordelijkheden worden verdeeld tussen de administratie, IT-verantwoordelijken en de archiefdienst
- wat de algemene richtlijnen zijn voor de creatie, het gebruik, het beheer, de archivering en de vernietiging van (digitale) archiefdocumenten
- hoe de kosten worden gedragen
- wat de archiefvormer en de archiefgebruikers mogen verwachten.

2. Het Open Archival Information System (OAIS) model

Het Open Archival Information System (OAIS) model kan een gids zijn bij de ontwikkeling van een informatiebeheer- en archiveringssysteem. OAIS werd ontwikkeld door Nasa's Consultative Committee for Space Data Systems en werd inmiddels als ISO-standaard vastgelegd (ISO-14721: 2002)[15]. Alhoewel het OAIS-model toepasbaar is op zowel papieren als digitale documenten, is het model voornamelijk op deze tweede categorie gericht.

Het OAIS-model is geen model archiveringssysteem dat onmiddellijk kan geïmplementeerd worden maar een conceptueel referentiemodel. Het biedt een kader waarbinnen procedures voor de lange termijnarchivering van digitale informatie worden uitgewerkt. Voor het uittekenen van een archiveringsprocedure zijn onder meer de processen en de metadata van belang die binnen OAIS worden geïdentificeerd. De functies, activiteiten en workflow zijn primaire onderdelen van elk archiveringssysteem en geven gestalte aan de archieffunctie van een archiefdienst of archiefinstelling:
- inname: kwaliteitscontrole, registratie, beschrijving, extractie metadata, transformatie archiefdocumenten, enz.

– lange termijn opslag (fysiek beheer): goede materiële omstandigheden voorzien, vervangen dragers, foutopsporing (checksums), rampenplan, back-ups maken, leesbaar houden, enz.
– toegankelijk maken (intellectueel beheer): beheren en bijwerken beschrijvingen en metadata, zoekmogelijkheden voorzien
– beheer: formuleren beleid, overleggen met archiefvormers, standaarden vastleggen, beheer digitaal depot, bijhouden documentatie, opvolgen technologische veranderingen, enz.
– ter beschikking stelling: archieftoegangen en archiefdocumenten beschikbaar stellen.

Deze vijf functies vormen de sleutelprocessen in elke archiveringsprocedure voor digitale archiefdocumenten en overbruggen de documentenstroom tussen archiefvormer en archiefgebruiker. Hoe deze processen vorm krijgen is afhankelijk van de concrete invulling van de archiveringsprocedures.

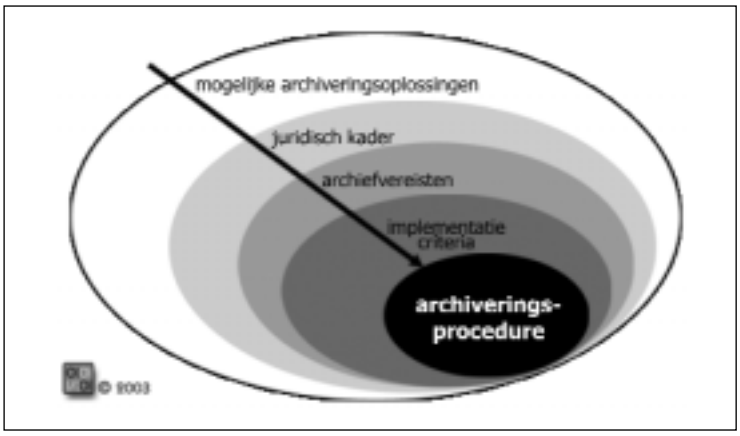
3. Naar een concrete archiveringsprocedure

Het archiveringsbeleid en de archieffunctie binnen een organisatie wordt in de praktijk gebracht door concrete archiveringsprocedures.

Voor de archivering van digitale archiefdocumenten zijn in principe diverse archiveringsprocedures toepasbaar. Voor de archiefvormer is het van belang om de archiveringsprocedure te kiezen die het meest effectief is voor de organisatie en haar archiefdocumenten. Het uittekenen van een goede archiveringsprocedure is een proces dat globaal gezien in twee stappen opsplitsbaar is:
– het definiëren van de algemene criteria waaraan een archiveringsprocedure moet beantwoorden
– het concreet invullen van de archiveringsprocedure op basis van een beslissingsmodel.

3.1. Algemene criteria voor een archiveringsprocedure

Algemeen zijn er drie soorten criteria waaraan elke archiveringsprocedure moet beantwoorden:
– juridisch: het juridische kader waarbinnen de archiveringsprocedure plaatsvindt, houdt doorgaans een aantal beperkingen en/of verplichtingen in waaraan moet worden voldaan. In het algemeen dient rekening te worden gehouden met de bescherming van de persoonlijke levenssfeer, de openbaarheidsverplichtingen, de bescherming van het auteursrecht. Bovendien kan voor elk type archiefdocument nog andere specifieke wet- en regelgeving gelden.
– archiefwetenschappelijk: de digitale archiefdocumenten dienen te beantwoorden aan een aantal archivistische kwaliteitsvereisten zoals digitale duurzaamheid, zo autonoom en zelfvoorzienend mogelijk, voorzien van de nodige metadata, gecontextualiseerd, enz.
– implementatie: technologische infrastructuur, schaalbaarheid, gebruiksvriendelijkheid, medewerking en bereidwilligheid gebruikers, enz.

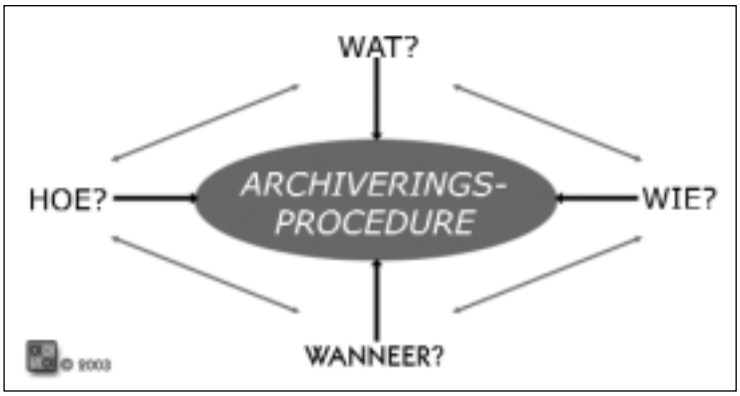


Een voorstudie levert de criteria waaraan de archiveringsprocedure dient te beantwoorden. Elke groep criteria bakent de mogelijke archiveringsoplossingen verder af zodat in een volgende stap de archiveringsprocedure verder praktisch kan worden ingevuld.

3.2. Het DAVID-beslissingsmodel

Eens de algemene criteria gedefinieerd zijn, legt men in een volgende stap de bouwstenen van de eigenlijke archiveringsprocedure vast. Het DAVID-beslissingsmodel kan hierbij als leidraad dienen. Dit beslissingsmodel kan worden toegepast voor de archivering van allerlei soorten digitale archiefdocumenten.

Op basis van het beslissingsmodel worden concrete keuzes gemaakt en wordt een antwoord geformuleerd op vier vragen:
- WAT archiveren?
- WIE archiveert?
- HOE archiveren?
- WANNEER archiveren?



De vertrekbasis voor het beantwoorden van deze vier vragen is het informatiesysteem waarbinnen de archiefdocumenten worden opgemaakt, ontvangen of beheerd. Typisch voor het beslissingsmodel is dat het antwoord op één van de deelvragen mee het antwoord van de andere deelvragen zal/kan bepalen. Als bijvoorbeeld het antwoord op de HOE-vraag emulatie is, dan zal dit mee vastleggen WAT wordt gearchiveerd.

3.2.1. Wat archiveren?

– identificeren van de archiefdocumenten:
  • wat zijn de archiefdocumenten?
  • welke digitale componenten identificeren de documenten met permanente archiefwaarde? Wat identificeert de archiefdocumenten: bestandsnamen, unieke ID's, enz.?
  • welke componenten van de archiefdocumenten worden (permanent) gearchiveerd: inhoud, structuur, context, opmaak, gedrag, functionaliteiten?
    ⇨ wat zijn de essentiële en incidentele eigenschappen van een digitaal archiefdocument?
    ⇨ welke componenten geven een document de status van archiefdocument?
– worden de archiefdocumenten in hun origineel bestandsformaat bijgehouden of worden ze enkel in hun archiveringsformaat bewaard?
– zijn er specifieke computerprogramma's nodig voor het reconstrueren van de archiefdocumenten (bijvoorbeeld emulatieprogramma's)?
– welke beschrijvende en technische metadata van de archiefdocumenten worden gearchiveerd?
– welke beschrijvende en technische metadata over het informatiesysteem waarbinnen de archiefdocumenten werden gecreëerd en/of beheerd, worden gearchiveerd?

3.2.2. Wie archiveert?

– wie vormt de digitale dossiers?
– wie registreert de beschrijvende metadata?
– wie registreert de technische metadata?
– wie zet de documenten om naar een archiveringsformaat?
– wie legt de archiefdocumenten neer bij de archiefdienst?

Parameters:
  • houdt de bescherming van de persoonlijke levenssfeer beperkingen in?
  • is er bijzondere hardware en software nodig?
  • wie beschikt over de vereiste technische kennis?

3.2.3. Hoe archiveren?

– welke bewaarstrategie voor digitale objecten wordt toegepast:
  • migratie?
  • emulatie?
  • een combinatie van migratie en emulatie?
– in welk archiveringsformaat worden de archiefdocumenten bewaard?
– hoe worden de metadata gearchiveerd:
  • in een afzonderlijk computerbestand?
  • ingekapseld in hetzelfde computerbestand als het archiefdocument?
  • in een databank?
– welke instrumenten/tools worden gebruikt voor het registreren van de metadata en de omzetting naar archiveringsformaten?
– hoe worden de oude digitale archiefdocumenten gearchiveerd? Welke tools zijn hiervoor nodig?
– hoe worden de archiefdocumenten en hun metadata neergelegd bij de archiefdienst?
– op welke drager worden de archiefdocumenten en hun metadata opgeslagen?
– hoe wordt de authenticiteit en integriteit van gearchiveerde digitale documenten gewaarborgd?
– hoe zorg je ervoor dat archiefdocumenten na hun vastlegging niet meer worden gewijzigd?

3.2.4. Wanneer archiveren?

– wanneer wordt het archiefdocument vastgelegd? Wanneer is het archiefdocument gevormd? Wanneer heeft het document de status en de functie van archiefdocument?

– wanneer worden welke stappen in de archiveringsprocedure uitgevoerd?
  - wanneer vindt de 'capture' plaats?
  - wanneer worden de archiefdocumenten naar de archiefdienst overgebracht?

Parameters:
- capaciteit van het opslagsysteem
- de administratieve bewaartermijn van de documenten
- performantie van het informatiesysteem
- producentenondersteuning van het informatiesysteem
- vervanging van het informatiesysteem waarmee de documenten werden gecreëerd of beheerd.

E. Archiveringsprocedures

1. Uitgangspunten

Ter uitvoering van het archiveringsbeleid worden concrete archiveringsprocedures ontwikkeld en toegepast. De archiveringsprocedures vertalen het algemene beleid naar de praktijk en worden op maat gesneden van de organisatie en haar documenten.

Binnen het DAVID-project zijn twee archiveringsprocedures uitgewerkt: één voor voor kantoordocumenten en één voor informatiesystemen. Beide archiveringsprocedures vallen terug op de algemene criteria voor een archiveringsprocedure en op het DAVID-beslissingsmodel. In de procedure voor kantoordocumenten is het digitale klassement met zijn digitale dossiers het uitgangspunt, terwijl de procedure voor informatiesystemen vanuit elk informatiesysteem zelf vertrekt. In de loop van het DAVID-project werden tools en instrumenten ontwikkeld om beide procedures in de praktijk om te zetten. Ondanks hun verschillende uitgangspunten delen beide procedures ook een aantal gelijkaardige processtappen en instrumenten zoals kwaliteitscontroles, registratie en ontsluiting, toepassing van archiveringsstandaarden, enz.

Bij het uitwerken van de archiveringsprocedures zijn volgende uitgangspunten gehanteerd:
- toepassen van het records continuumprincipe: de archiveringsprocedure start bij de creatie of ontvangst van digitale documenten en loopt tot het archiefbeheer en terbeschikkingstellen. De archivaris begeeft zich op het terrein van records management.
- zoveel mogelijk handelingen uit het 'papieren documentbeheer' overnemen waarmee de gebruiker al vertrouwd is
- zoveel mogelijk handelingen automatiseren:
  - automatisering verhoogt de gebruiksvriendelijkheid
  - door automatisering verzekert men zich ervan dat de handelingen correct worden uitgevoerd
- in eerste instantie de archiveringsprocedure zoveel mogelijk inpassen in de bestaande IT-infrastructuur.

Het toepassen van deze archiveringsprocedure is afhankelijk van een aantal factoren, niet in het minst van de IT-infrastructuur waarbinnen de procedure wordt ingepast. In een eerste fase zal de archiveringsprocedure zoveel mogelijk binnen de bestaande IT-omgeving worden toegepast. Computerconfiguraties kunnen immers niet zomaar worden vervangen. In de praktijk zal dit veelal betekenen dat een aantal (geautomatiseerde) documentbeheersfunctionaliteiten in de bestaande configuraties worden ingebouwd. In welke mate dit allemaal mogelijk is, zal onder meer afhangen van de flexibiliteit en mogelijke customisaties van de geïnstalleerde besturingssystemen en applicaties. De courante computerprogramma's hebben op dit vlak hun beperkingen, maar dit hoeft op zich geen nadeel te zijn. Het is zelfs aan te raden om het documentbeheer in eerste instantie binnen de bestaande IT-omgeving te organiseren alvorens over te gaan tot het aankopen en implementeren van meer geavanceerde document- of recordsmanagementsystemen. De gebruikers kunnen op die manier binnen de vertrouwde softwareomgeving blijven werken en raken vertrouwd met handelingen zoals digitale dossiervorming en registratie in een digitale context. Ondertussen doen alle betrokken partijen ervaring op en krijgt men een beter zicht op de specifieke vereisten die aan nieuwe software wordt gesteld. Bij de keuze van nieuwe software kan men dan beter definiëren wat de functionele vereisten zijn die vanuit documentbeheer worden gesteld zodat men vanaf de tweede fase de volledige procedure kan toepassen.

2. Kantoordocumenten

De DAVID-archiveringsprocedure voor kantoordocumenten bestaat uit 6 stappen:
1. Digitaal klassement uitbouwen
2. Kwaliteitsdocumenten creëren en beheren
3. Digitale dossiervorming
4. Archiefwaardering en selectie
5. Omzetting naar archiveringsformaten
6. Opname in het archief en opzoeken

De basishandelingen van de DAVID-archiveringsprocedure voor kantoordocumenten zijn toepasbaar binnen elke IT-omgeving. De implementatie van een archiveringsprocedure kan stapsgewijs gebeuren. Niet alle stappen hoeven noodzakelijk van bij de start operationeel te zijn. Stap 1 tot en met 3 zijn prioritair. Eens de digitale dossiervorming loopt, is er opnieuw tijd om de implementatie van de resterende stappen voor te bereiden en om de oude digitale documenten met terugwerkende kracht in de archiveringsprocedure op te nemen. De eerste stappen zijn voornamelijk gericht op het creëren van kwaliteitsdocumenten binnen een gestructureerde en gecontroleerde omgeving. Digitale documenten die niet in een georganiseerde omgeving worden gecreëerd en beheerd, kunnen achteraf maar moeilijk onder intellectueel archiefbeheer worden gebracht en kunnen maar moeilijk kwaliteitsvolle archiefdocumenten worden. Optreden vanaf de creatie is dus een noodzaak. Indien mogelijk worden deze eerste stappen zoveel mogelijk gekoppeld aan archiefwaardering, zodat de essentiële componenten van de archiefdocumenten gestructureerd worden vastgelegd.

2.1. Digitaal klassement uitbouwen

Het uitbouwen van een digitaal klassement waarbinnen digitale documenten worden beheerd, is een eerste stap om digitale documenten onder intellectuele controle te brengen.

Een digitaal klassement maakt het structureren van de digitale dossiers en het ordenen van de digitale documenten mogelijk. Op die manier kan de archiefcontext van de dossiers en de stukken worden vastgelegd. Door het digitale klassement te baseren op de bedrijfsprocessen en de handelingen van de archiefvormer, kan de samenhang aangegeven worden tussen de dossiers- of onderwerpsmappen en de werkprocessen waarbinnen ze ontstaan zijn. Archief is immers procesgerelateerde informatie en heeft als doel werkprocessen te documenteren. Het klassement bereikt dit doel het best wanneer het een weerspiegeling is van de werkprocessen die aan de basis van de archiefvorming liggen. Indien mogelijk, is het ook wenselijk het digitale en papieren klassement aan elkaar te koppelen. Dit kan door dezelfde structuur te hanteren of door een gemeenschappelijke dossier- of registratiecode te gebruiken. Zo kan de relatie tussen digitale en papieren dossiers- of onderwerpsmappen worden aangeduid[16].

Door de digitale dossiers te klasseren, wordt de structuur van het archief zichtbaar gemaakt. Voor elk dossier of onderwerp wordt een map aangemaakt. Binnen het klassement ordent men de dossiers- of onderwerpsmappen zodat hun onderlinge relaties aangegeven worden. Door semantische mapnamen toe te kennen, kan men verder betekenis toekennen aan de digitale stukken die binnen deze structuur worden bijgehouden. Op deze wijze ontstaat een logische en overzichtelijke mappenstructuur die informatie over de context communiceert. De dossiers en documenten zijn hierdoor ook gemakkelijker opspoorbaar en bruikbaar door derden en niet enkel door de behandelende administratieve medewerkers.

Het digitale klassement vormt niet alleen de structuur waarbinnen digitale archiefdocumenten worden gearchiveerd maar levert ook een belangrijk metadatagegeven voor de digitale archiefdocumenten op. In combinatie met de namen van de bovenliggende mappen verschaft de map-

naam informatie over de archiefcontext en geeft de vindplaats van de documenten aan. De klassementsstructuur moet niet alleen mee gearchiveerd worden; men voorziet zelfs best de mogelijkheid tot reconstructie van de mappenstructuur.

Kortom, een digitaal klassement is vanuit archiveringsstandpunt om meerdere redenen belangrijk:
- digitale documenten worden in een gestructureerde en gecontroleerde omgeving gevormd
- de band tussen dossier- of onderwerpsmappen enerzijds en het werkproces anderzijds wordt aangegeven: documenten kunnen begrepen en geïnterpreteerd worden, documenten worden binnen hun archiefcontext beheerd
- digitale en papieren dossiers worden aan elkaar gerelateerd
- het klassement biedt een overzicht van de digitale documenten waar de organisatie over beschikt: de mappenstructuur versterkt het concept van digitale informatie als gemeenschappelijk bedrijfsmiddel
- de structuur van het archief wordt zichtbaar gemaakt: documenten zijn toegankelijker
- digitale dossiers- of onderwerpsmappen worden gevormd: vastleggen van de band tussen digitale archiefdocumenten; gerelateerde digitale documenten kunnen als groep beheerd worden
- een klassement maakt archiefwaardering en selectie mogelijk zodat het te lang bijhouden van dossiers wordt vermeden: tijdig archiveren of vernietigen
- toegankelijk maken op basis van consistente beschrijvingen en de structuur van het archief wordt mogelijk.

Het organiseren van een goede mappenstructuur is niet alleen vanuit archiveringsstandpunt belangrijk, maar biedt ook een aantal praktische voordelen:
- documenten worden sneller teruggevonden, en bijgevolg meer herbruikt
- dezelfde documenten worden niet meer in veelvoud op verschillende locaties opgeslagen: fileservers worden ontlast en hebben minder te leiden onder capaciteitsproblemen
- grotere duidelijkheid over waarde en belang van documenten
- gemakkelijker om een versiebeheer te hanteren.

De digitale klassementsstructuur is idealiter het resultaat van overleg tussen archiefvormer, IT-verantwoordelijken en de archivaris. Voor het uitbouwen van een gemeenschappelijke mappenstructuur wordt best de nodige tijd voorzien want de mappenstructuur is het kader waarbinnen digitale documenten worden gecreëerd en beheerd. De eindgebruiker moet gemakkelijk zijn weg vinden in de structuur, zo niet zal de dossiervorming in een later stadium mank lopen. Van bij het vastleggen van de structuur worden best ook afspraken gemaakt over het beheren en controleren van de structuur.

Deze eerste stap heeft voornamelijk betrekking op het organiseren van de digitale mappen, en is toepasbaar binnen elk besturingssysteem. De courante besturingssystemen laten de creatie van een hiërarchische mappenstructuur toe (Windows, Unix-Linux, Apple). Een digitaal klassement kan men met behulp van zeer eenvoudige bestandsbeheersapplicaties maken en beheren (Windows Verkenner, Nautilus File Manager, Mac Finder). Natuurlijk hebben deze applicaties hun beperkingen: geen versiebeheer, beperkte toegangscontrole, geen mogelijkheid tot registratie van zelf gedefinieerde metadata op dossierniveau, enz. Binnen meer geavanceerde documentbeheers- of records managementssystemen zijn dergelijke functionaliteiten wel aanwezig[17]

Praktische tips en aanbevelingen voor het aanmaken van een digitaal klassement zijn beschikbaar op de DAVID-website:
- *Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 3:* Mappenstructuur en bestandsnamen voor digitale documenten.

2.2. Kwaliteitsdocumenten creëren en beheren

Om uiteindelijk goede digitale documenten te archiveren, is het belangrijk om van bij het ontstaan kwaliteitsdocumenten te creëren. Deze stap is gericht op het creëren en beheren van authentieke, (her)bruikbare en goed archiveerbare digitale documenten. Aangezien de authenticiteit van een archiefdocument betrekking heeft op zijn identiteit en zijn integriteit[18], wordt in deze stap aan deze aspecten de nodige aandacht besteed.

De kwaliteit van een digitaal document is afhankelijk van:
- de structuur
- de metadata
- het bestandsformaat
- de betrouwbaarheid
- de gebruiker.

De specifieke kwaliteitsvereisten van een bepaald type document zijn afhankelijk van de functie van de digitale documenten binnen het werkproces waarbinnen ze worden gecreëerd en beheerd. Goede archiefdocumenten moeten ook gekoppeld blijven aan het werkproces waarbinnen ze tot stand kwamen (zie 2.1 en 2.3).

De creatie en het beheer van kwaliteitsvolle archiefdocumenten zorgen er niet alleen voor dat de archivering gemakkelijker en efficiënter verloopt, maar ook dat meer incidentele documenteigenschappen op lange termijn worden bewaard.

2.2.1. De structuur

De interne structuur van een document is niet alleen belangrijk omdat het in de meeste gevallen een essentieel component van een digitaal archiefdocument is, maar ook omdat succesvolle migraties slechts mogelijk zijn wanneer de documenten goed zijn gestructureerd.

Samen met de inhoud is de structuur van een digitaal archiefdocument van belang om de kennis en betekenis die in het document vervat zit, in tijd over te brengen. De structuur is bijgevolg in de meeste gevallen een essentieel component van het archiefdocument. Het structureren van digitale documenten hangt nauw samen met documentmodellering. Dit is één van de geijkte methoden om kennis op een digitale wijze te communiceren. Het documentmodel weerspiegelt de kennis die ontstaat na definiëren, identificeren en relateren van computerdata. Immers, computerdata hebben op zich geen betekenis, maar krijgen betekenis door hun verbanden vast te leggen en duidelijk te maken. De interne structuur geeft ook aan hoe de onderdelen van een document met elkaar verbonden zijn. Hoe beter de logische relatie tussen de elementen wordt aangegeven, des te beter een document zijn functie kan vervullen.

Het welslagen van een omzetting is in belangrijke mate afhankelijk van de structuur van het brondocument. Digitale documenten met een goede structuur zijn gemakkelijker en beter te migreren dan ongestructureerde documenten. Deze laatste documenten zijn overigens altijd moeilijker te herbruiken buiten hun oorspronkelijke software-omgeving. Goed gestructureerde documenten zullen gemakkelijker de tand des tijds overleven en zijn gemakkelijker automatisch te verwerken.

Het is bijgevolg van belang dat digitale documenten intern op een expliciete wijze worden gestructureerd. De structuur van een document louter en alleen op basis van opmaak aangeven, houdt een risico in want opmaak gaat in veel gevallen verloren. Beter is om opmaakstijlen en koptekst te gebruiken waaraan eventueel opmaak kan worden gekoppeld.

De gedetailleerdheid van de structuur is afhankelijk van de documentmodellering en van de mate waarin onderdelen van het document (afzonderlijk) herbruikbaar of opspoorbaar moeten zijn.

2.2.2. De metadata

Digitale documenten kunnen hun functie van archiefdocument pas ten volle vervullen wanneer in de toekomst metadata over het document en zijn context beschikbaar zijn. De kwaliteit van een archiefdocument is mede afhankelijk van de kwaliteit van de metadata. Metadata vervullen verschillende functies zoals identificatie van het archiefdocument, informatie verstrekken over de archiefcontext van digitale documenten, lange termijn leesbaarheid helpen garanderen, de betrouwbaarheid mee waarborgen, enz.

Metadata moeten net zoals de digitale archiefdocumenten vast, stabiel en leesbaar zijn. Metadata hebben dezelfde bewaartermijn als de digitale documenten waarop ze betrekking hebben. Idealiter kunnen de metadata van digitale archiefdocumenten automatisch worden verwerkt. Ook voor metadata gelden een aantal kwaliteitsvereisten:

– statisch
– expliciet
– gestructureerd
– digitaal
– leesbaar op lange termijn
– gekoppeld aan archiefdocumenten.

Met betrekking tot de metadata van een archiefdocument dient men als onderdeel van het DAVID-beslissingsmodel af te vragen welke metadata, op welk niveau, en waar ze worden opgeslagen, en door wie ze worden geregistreerd.

Welke metadatavelden noodzakelijk zijn, is mede afhankelijk van het type digitaal archiefdocumenten en hun functie. Van bepaalde types documenten zijn metadata zoals auteur, versie, titel, datum, enz. belangrijk terwijl dit voor andere documenten niet het geval is. De metadata voor een e-mail verschillen van de metadata voor een gearchiveerde website.

De metadata kunnen betrekking hebben op verschillende niveaus:

– het individuele archiefdocument: bijvoorbeeld titel, auteur, versie, datum, verwijzing naar het dossier of het onderwerp, omschrijving, trefwoorden, betrouwbaarheidswaarborgen, bestandsnaam, software, enz.
– de dossier- of onderwerpsmap: bijvoorbeeld vindplaats, ID, bewaartermijn, gerelateerde (papieren) dossiers, enz.
– de serie/reeks: bijvoorbeeld archiefvormer, functie, handeling, wijze van ordenen, gerelateerde stukken, omvang, uiterste data, historiek archivering, enz.
– het archief: bijvoorbeeld archiefvormer, mandaat, functie, handeling, uiterste data, enz.

De metadata over digitale archiefdocumenten kunnen op verschillende plaatsen worden opgeslagen. Metadata kunnen:

– in het digitale archiefdocument worden ingekapseld (bijvoorbeeld het documentprofiel van een tekstbestand)
– in een afzonderlijk computerbestand worden opgeslagen
– in een databank worden opgenomen.

In de praktijk zal veelal een combinatie van deze drie mogelijkheden worden toegepast en is veel afhankelijk van de wijze waarop toegang wordt verschaft tot de gearchiveerde dossiers en documenten. Inkapseling heeft als voordeel dat de metadata onlosmakelijk verbonden zijn met het archiefdocument maar een dergelijke decentrale bewaring heeft nadelen bij automatische zoekopdrachten. Opslag in een centrale databank is daarom beter, maar vraagt een bijzondere zorg voor de koppeling met archiefdocumenten. Ongeacht de opslagplaats dient ook rekening gehouden te worden met de lange termijnbewaring van de metadata. Ingekapselde metadata moeten bijvoorbeeld mee overgezet worden naar het doelformaat (bijvoorbeeld documentprofiel MS

Word omzetten naar XML, TIFF of PDF) en mogen geen leesbaarheidsproblemen opleveren. Databanken waarbinnen de metadata worden opgeslagen, zijn eveneens onderhevig aan technologische veroudering.

Waar mogelijk worden metadata bij voorkeur op een automatische wijze geregistreerd. Veel metadata zijn immers in de informatiesystemen aanwezig. In veel gevallen komt het erop aan de metadata op een statische en expliciete wijze vast te leggen en te linken aan het document of het dossier waarop ze betrekking hebben. Een andere mogelijkheid is de metadata automatisch te laten samenstellen. Niet alle metadata kunnen echter op een automatische wijze geregistreerd worden. Metadata over de archiefcontext zijn hier een typisch voorbeeld van. Deze metadata kunnen best geregistreerd worden door diegenen die de context van de documenten of dossiers het best kennen, in concreto de administratieve medewerkers. Als op dit punt van de gebruiker enige actie wordt verwacht, dan is het aangewezen om een heel gebruiksvriendelijke oplossing aan te reiken. Anders is de kans groot dat er geen metadata worden toegekend.

Metadata worden best bij creatie of zo snel mogelijk na ontvangst geregistreerd. Aangezien het toekennen van metadata een incrementeel proces is, dient hier rekening mee te worden gehouden.

2.2.3. Het bestandsformaat

De keuze van het bestandsformaat waarin digitale informatie wordt opgeslagen, heeft rechtstreekse gevolgen voor de levensduur en de duurzaamheid van digitale documenten. Het verdient aanbeveling om vanaf de creatie digitale documenten in een geschikt archiveringsformaat op te slagen. Hierdoor worden omzettingen en verlies van incidentele componenten vermeden.

In de praktijk zal dit echter niet altijd mogelijk of wenselijk zijn. Zo kan beslist worden om ten behoeve van de functionaliteit, de herbruikbaarheid of de gebruiksvriendelijkheid, digitale documenten tijdelijk in een niet-uitwisselbaar producent- of applicatiegebonden formaat te bewaren. In dit geval dient vanaf de creatie het migratiepad (doelformaat, omzettingstool) voor dit type document bekend te zijn zodat indien nodig nog bijzondere maatregelen in het creatieproces kunnen worden getroffen. Aangezien de eindgebruiker bij de opslag van digitale kantoordocumenten zelf het bestandsformaat en een aantal instellingen kan kiezen, is het van belang om hierover duidelijke richtlijnen en afspraken te communiceren. Indien mogelijk wordt het aangewezen bestandsformaat voorgeprogrammeerd zodat fouten worden vermeden.

Bij opslag in een archiveringsformaat dient men erover te waken dat de digitale documenten worden weggeschreven conform de instellingen die belangrijk zijn vanuit archiveringsstandpunt. De meeste archiveringsformaten kunnen immers op diverse wijzen samengesteld worden. De gebruiker kan vrij een aantal instellingen opgeven, maar lang niet alle instellingen zijn even interessant voor lange termijnarchivering. Zo is het niet aangewezen om PDF-documenten met een PDF-writer samen te stellen of JPEG-compressie toe te passen bij het bewaren van een TIFF-document.

Meer informatie is beschikbaar op de DAVID-website:
- *F. BOUDREZ*, Standaarden voor digitale archiefdocumenten, *Antwerpen, 2003*
- *Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 4:* Standaarden voor bestandsformaten.

2.2.4. De betrouwbaarheid

Hoe de betrouwbaarheid op lange termijn en op sluitende wijze kan gewaarborgd worden, is vooralsnog geen uitgemaakte zaak. In ieder geval is het archiveren van betrouwbare archiefdocumenten slechts mogelijk wanneer vanaf de creatie of de ontvangst een procedure loopt die de betrouwbaarheid waarborgt. De betrouwbaarheid moet immers voor de hele levenscyclus worden verzekerd. De procedure moet er in eerste instantie voor zorgen dat digitale documenten niet onrechtmatig worden gewijzigd en dat wijzigingen opspoorbaar zijn. De klemtoon ligt hierbij op

het beschermen van de integriteit van het archiefdocument. De archiefvormer kan hiervoor verschillende eenvoudige of meer complexe maatregelen combineren:
- toegangscontrole en -rechten: alleen geautoriseerde gebruikers hebben toegang tot mappen en bestanden (bijvoorbeeld gebruikersID's, paswoorden, biometrie, PKI)
- 'read-only'-toegang: digitale documenten zijn na hun vastlegging niet meer wijzigbaar (beveiligde mappen en/of bestanden, enkel raadpleging met viewersoftware)
- versiecontrole: wijzigingen kunnen enkel als nieuwe versie worden opgeslagen
- audit-trail bijhouden: registreren van bepaalde acties met documenten (bijvoorbeeld wie wijzigde wat op welk tijdstip?). Aangezien het bijna onmogelijk is om alle acties te loggen, dient men op voorhand te bepalen welke acties en wat van die acties wordt geregistreerd. De logbestanden die worden gebruikt voor het systeembeheer zullen maar zelden deze functie kunnen vervullen, zodat de creatie van afzonderlijke audit-trails noodzakelijk zal zijn.
- hashing: bijhouden van de hash-codes berekend op de bits van digitale documenten zodat achteraf controles mogelijk zijn
- time-stamping: registratie van datum en tijdstip
- encryptie: transformatie van digitale documenten zodat ze onleesbaar zijn voor wie niet over de overeenstemmende decryptiesleutel beschikt.

De betrouwbaarheid van digitale archiefdocumenten wordt verzekerd door een combinatie van procedure en technologie. Hierbij mag men niet uit het oog verliezen dat technologie onderhevig is aan veroudering en dat voor een doeltreffende toepassing van technologieën opnieuw procedures vereist zijn. De technologieën worden bij voorkeur ook ingebed in een algemene procedure die op lange termijn de betrouwbaarheid garandeert. De (technologische) onderdelen van deze procedure moeten vervangbaar zijn wanneer de technologie wijzigt.

Aangezien de betrouwbaarheid een belangrijke factor is in de archiefwaardering, en vanwege de noodzaak om de betrouwbaarheid aan te tonen, is het belangrijk dat de archiefvormer zijn procedure documenteert en die op een gegeven tijdstip ter beschikking stelt van de archivaris.

2.2.5. De gebruiker

De kwaliteit van digitale documenten wordt ten slotte ook mee bepaald door de gebruiker en de wijze waarop hij digitale documenten creëert, metadata registreert en zijn documenten organiseert.

De creatie van kwaliteitsvolle digitale documenten en in een volgende stap de dossiervorming, zijn afhankelijk van de vertrouwdheid van de gebruikers met IT en hun zorgvuldigheid. Bewustmaking, opleiding en het aanleren van procedures zijn bijgevolg onmisbaar. De integratie van de basisvaardigheden voor goed documentbeheer in standaard IT-opleidingen voor administratieve medewerkers is aan te bevelen. Aangezien de creatie van goede digitale documenten in een aantal gevallen beperkingen oplegt aan de gebruiker, is het ook belangrijk om het hoe en het waarom te motiveren.

2.2.6. Toepassing en voorbeelden

De creatie van digitale kwaliteitsdocumenten is sterk afhankelijk van de wijze waarop de gebruiker zijn documenten samenstelt en bewaart. Men kan dit proces sturen door te voorzien in de nodige training en door bij de creatie van standaarddocumenten of sjablonen gebruik te maken. Met sjablonen kan men de structuur van een document op voorhand vast leggen en eventueel al anticiperen op toekomstige migraties door bijvoorbeeld dynamische gegevens op een statische en expliciete wijze te registreren. Met sjablonen kan ook de mogelijkheid voorzien worden tot automatische of gebruiksvriendelijke toekenning van metadata.

Met sjablonen kunnen bepaalde handelingen op een volledig geautomatiseerde of gebruiksvriendelijke wijze worden uitgevoerd. Kantoortoepassingen zoals MS Office en OpenOffice laten toe dat macro's en scripts aan sjablonen worden gekoppeld.

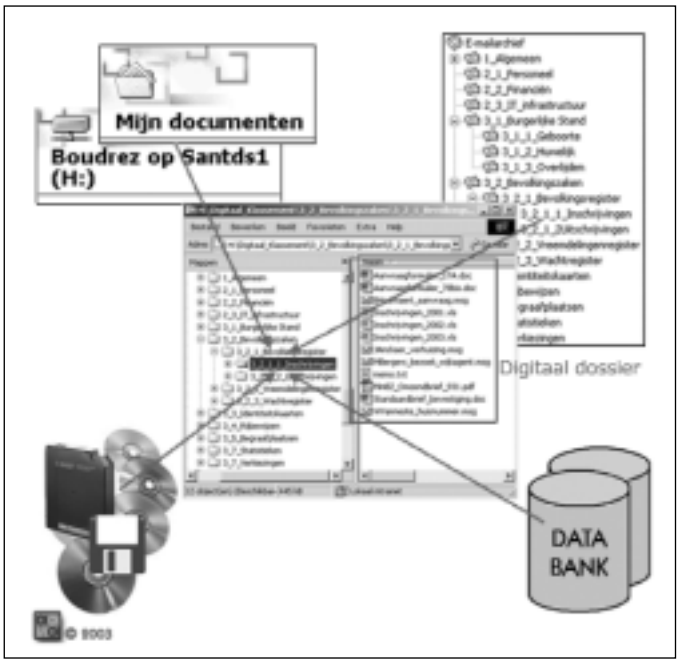
Op de DAVID-website zijn twee voorbeelden van dergelijke sjablonen beschikbaar:
- e-mailsjabloon met script:
  - automatische registratie van metadata: e-mailadres van de afzender, datum en tijdstip van verzending en ontvangst, bestandsnamen van de bijlagen
  - gebruiksvriendelijk toekennen van de klassementscode en doelmap door afzender en ontvanger
  - exportfunctionaliteit: bewaren in een voorgedefinieerd bestandsformaat, scheiden e-mail en bijlagen, vervangen niet toegelaten karakters in de bestandsnamen
- wordsjabloon met macro: automatisch en gebruiksvriendelijk verplicht invullen van voorgeprogrammeerde en gecustomiseerde metadata op documentniveau door de gebruiker bij openen en afsluiten van een tekstverwerkingsdocument.

Tips en aanbevelingen voor goede digitale documenten:
- geef kantoordocumenten een duidelijk identificatiekenmerk
- leg de interne structuur van documenten op een expliciete wijze vast: duid de structuur aan met behulp van opmaakstijlen in plaats van louter en alleen opmaak.
- zorg ervoor dat de inhoud van dynamische velden (bijvoorbeeld automatisch datumveld) is gefixeerd van zodra het document is gefinaliseerd
- maak afspraken voor het herbruiken van documenten en voor het maken van nieuwe versies na het definitief vastleggen van de originele versie.

2.3. Digitale dossiervorming

Binnen het digitale klassement worden digitale dossiers gevormd. Alle digitale documenten die betrekking hebben op een taak, een dossier of een onderwerp worden in dezelfde map samen bewaard. Op deze wijze wordt de band tussen gerelateerde documenten vastgelegd.

Het vormen van digitale dossiers biedt het voordeel dat binnen de organisatie de mogelijke vindplaatsen van digitale documenten worden herleid tot één centrale opslagplaats. In plaats van documenten te verspreiden over lokale harde schijven, fileservers, e-mailsystemen, databanksystemen, externe dragers, enz. worden de digitale documenten in één centraal dossier samengebracht. Op die manier verwerft men op een snelle manier een overzicht van alle beschikbare informatie binnen de organisatie en van alle digitale documenten met betrekking tot één zaak of één dossier: tekstdocumenten, spreadsheets, e-mails, presentaties, enz.



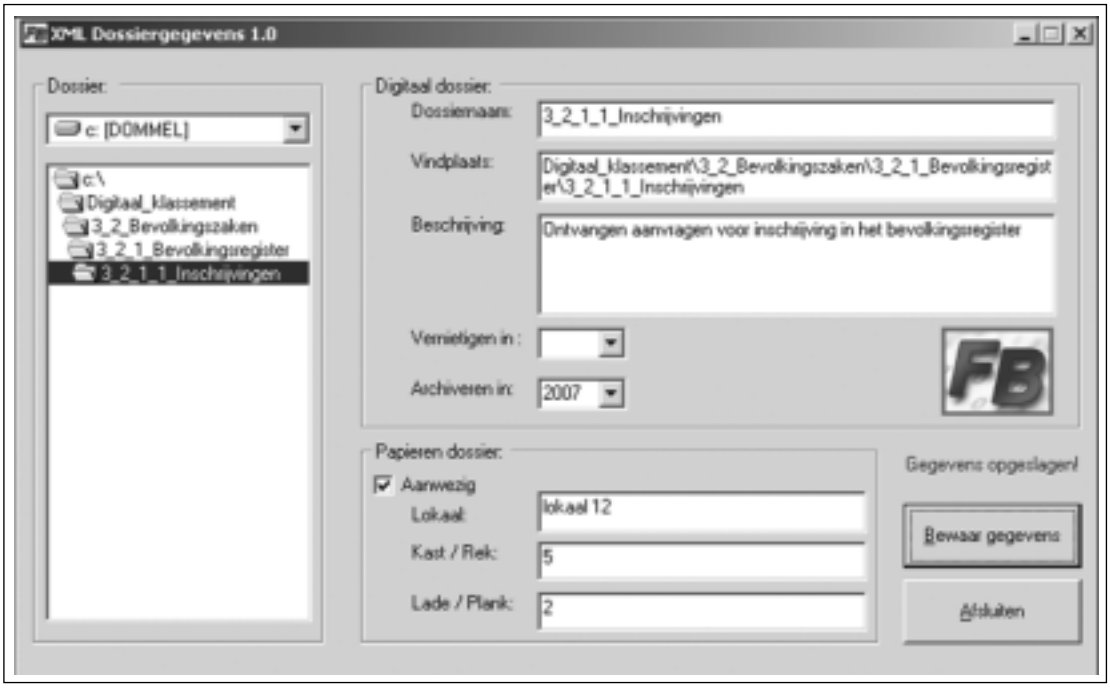
Het ordenen van de digitale documenten per dossier of per onderwerp laat de administratie en archivaris toe de digitale documenten in groep te bewerken. Archiefwaardering en selectie kunnen dan bijvoorbeeld op dossier- of onderwerpsniveau gebeuren. Dit heeft echter voor gevolg dat een document in een bepaalde map plaatsen een beslissing is die gevolgen heeft voor bewaring of vernietiging. Enige controle hierop is aangewezen maar in de praktijk niet altijd even gemakkelijk te realiseren.

Een essentieel onderdeel van de digitale dossiervorming is het registreren van metadata over de digitale dossiers. Belangrijke gegevens over de digitale dossiers zijn ondermeer: situering binnen een bepaald werkproces, beschrijving, relatie met en vindplaats van een verwant papieren dossier, documenten in het dossier, en bewaartermijn. Deze metadata zijn gemeenschappelijk voor alle documenten binnen het dossier en dienen op één of andere wijze aan het digitale dossier gekoppeld te worden. Op die manier stelt men een dossierprofiel samen. De courante besturingssystemen bieden niet de mogelijkheid om zelf gekozen metadata op mapniveau te registreren. Met WebDAV-toepassingen of meer geavanceerde documentbeheerssystemen is dit wel mogelijk. Een tussenoplossing is de ad hoc applicatie die door DAVID werd ontworpen. Deze applicatie biedt de gebruiker een invulscherm aan en het ingevulde documentprofiel wordt als een XML-document weggeschreven in de map waarop de metadata betrekking hebben[19].

De digitale dossier- of onderwerpsmappen vormen de bouwstenen van het digitale klassement. Aangezien de volgende stappen in de archiveringsprocedure vertrekken vanuit dit klassement, kan het opnemen van een document in een bepaalde map beschouwd worden als het formele punt waarop een document effectief een archiefdocument voor de organisatie wordt. Digitale documenten die geen deel uitmaken van het klassement ontsnappen defacto aan het archiveringssysteem en worden niet in het digitaal archief opgenomen.

De mappenstructuur en de plaats van de digitale documenten zijn een belangrijk metadatagegeven. De mappenstructuur weerspiegelt de context waarbinnen documenten worden beheerd en geeft de relatie tussen de documenten onderling en met het werkproces aan. De mappenstructuur dient bijgevolg gearchiveerd te worden en wordt bij voorkeur zelfs uitgebreid gedocumenteerd. Verlies van de mappenstructuur betekent immers verlies van de archiefcontext. Dit is één van de essentiële componenten van een archiefdocument. Een mogelijke oplossing hiervoor is het

maken van XML-Dossierlijsten. In zo'n dossierlijst wordt een hiërarchisch overzicht van de mappen aangelegd met vermelding van de documenten die in de mappen worden bewaard[20].



2.4. Archiefwaardering en selectie

Binnen de digitale wereld situeert de problematiek inzake archiefwaardering en selectie zich op twee niveaus: het dossier en het document. Op dossierniveau spitst de selectievraag zich vooral toe op welke dossiers gearchiveerd dan wel vernietigd worden. Op documentniveau wordt op basis van archiefwaardering beslist welke componenten essentieel en incidenteel zijn. Bij papieren documenten stelt deze laatste vraag zich niet.

In principe gelden voor digitale dossiers geen andere bewaartermijnen dan voor papieren dossiers. De selectielijsten die betrekking hebben op de papieren dossiers, gelden even goed voor de digitale dossiers. Vertaald naar de werkvloer betekent dit dat op een gegeven tijdstip dossiers die voor lange termijnarchivering in aanmerking komen, geselecteerd worden en uit de actieve klassementsstructuur worden verwijderd. Die selectie kan gebeuren op basis van een manuele en/of automatische selectie. Deze laatste methode vraagt wel dat de bewaartermijn op één of andere manier aangegeven wordt. Een mogelijkheid is bijvoorbeeld de bewaartermijn opnemen in de dossiermetadata.

Met het oog op archiefwaardering en selectie is het geen overbodige luxe om metadata op dossierniveau te registreren. Deze metadata verschaffen informatie over de context en de waarde die de archiefvormer toekent aan de dossier- of onderwerpsmappen in het digitale klassement. De administratieve medewerkers bewaartermijnen laten toekennen, vervangt de selectielijsten niet. Integendeel, het toekennen van bewaartermijnen is gebaseerd op de selectielijsten of archiefbeheersplannen. Deze worden in overleg tussen archiefvormer en archivaris opgesteld en geven onmiddellijk aan welk belang de archiefvormer aan bepaalde dossiers hecht.

Op documentniveau is de archiefwaarderings- en selectieproblematiek eigenlijk constant aanwezig in de archiveringsprocedure. Vanaf de creatie moet eigenlijk al bekend zijn welke componenten van het document essentieel zijn en gearchiveerd worden zodat eventueel de nodige maatre-

gelen kunnen genomen worden. Dezelfde vraag stelt zich vooraleer wordt overgegaan tot migratie naar een geschikt archiveringsformaat en telkenmale wanneer in de toekomst opnieuw wordt gemigreerd. De uitkomst van de archiefwaardering zal immers mee beslissen welk bestandsformaat als archiveringsformaat wordt gebruikt. De essentiële eigenschappen worden mee opgenomen in het archiveringsformaat. Het archiveringsformaat moet deze eigenschappen dus ondersteunen en in tijd kunnen overbrengen. De incidentele eigenschappen mogen bij omzettingen verloren gaan of gewijzigd worden.

2.5. Omzetting naar archiveringsformaten

Na de selectie en alvorens de digitale documenten in het digitaal archief op te nemen, worden de digitale documenten indien nodig naar een geschikt archiveringsformaat omgezet. Dit biedt twee voordelen:

– ten eerste worden enkel de digitale documenten met archiefwaarde omgezet, wat kosten en tijd bespaart
– ten tweede kan de omzetting onder verantwoordelijkheid van de archiefvormer gebeuren en kan hij de omgezette documenten authentiek verklaren.

De digitale documenten die vanaf de creatie in een archiveringsformaat werden opgeslagen, hoeven niet omgezet te worden. Een controle op de toepassing van de goede instellingen vanuit archiveringsstandpunt is echter aangewezen. Indien nodig moeten compressie, encryptie, paswoorden, enz. nog worden verwijderd.

De omzetting naar een geschikt archiveringsformaat gebeurt met omzettingstools die bij voorkeur grote hoeveelheden digitale documenten automatisch kunnen migreren. De kwaliteit van de omgezette documenten is sterk afhankelijk van het computerprogramma dat voor de omzetting wordt gebruikt. Voor de omzettingstool gelden dan ook bijzondere vereisten:

– 100 % correct toepassen van de standaard of de specificatie
– mogelijkheid tot instellen welk profiel van het archiveringsformaat wordt toegepast
– betrouwbaar en foutenvrij migreren: uitgebreid testen!
– foutenopsporing- en signalering: registreren welke documenten niet succesvol werden omgezet, zodat ze achteraf nog handmatig kunnen worden gemigreerd
– kwaliteitscontrole op de omgezette documenten.

Voor de omzetting kunnen commerciële of open source tools worden gebruikt, bestaande computerapplicaties aangepast, of eigen software worden ontwikkeld. Zelf bestaande applicaties aanpassen of software (laten) creëren biedt het voordeel dat men zelf de functionele vereisten van de omzettingstool bepaalt en dat men beter kan inschatten welke operaties achter de schermen worden uitgevoerd. Beschikken over, controleren en documenteren van de broncode van de omzettingstool is bijna een must om de betrouwbaarheid van de omzetting te verifiëren en aan te tonen.

Tips en aanbevelingen:

– stoot oude hard- en software pas af na kwaliteitscontrole op de gemigreerde documenten. Verwijder bepaalde hard- en software pas als je zeker bent dat alle data met archiefwaarde en gemaakt met die hard- en software nog raadpleegbaar zijn met hun plaatsvervangers.
– controleer en documenteer de broncode van de omzettingsapplicaties. Leg contractueel vast dat de broncode van ad hoc gecreëerde software wordt gedocumenteerd door de programmeur en wordt overgedragen aan de opdrachtgever.

2.6. Opname in het archief en opzoeken

2.6.1. Controle en registratie

Bij opname in het archief worden in eerste instantie de overgedragen documenten gecontroleerd en geregistreerd.

De controle van de digitale archiefdocumenten heeft betrekking op:
- de volledigheid van de overdracht: bevatten de dragers alle documenten (bijvoorbeeld controle op basis van XML-Dossierlijst die als overdrachtslijst wordt gebruikt)
- de kwaliteit van de digitale archiefdocumenten: opgeslagen in een geschikt archiveringsformaat (identificatie van de bestandsformaten), correct archiveringsprofiel toegepast (validatie van de bestandsformaten), voorzien van metadata?
- de kwaliteit van de overbrengingsdragers wanneer deze ook als lange termijndrager worden gebruikt
- computervirussen.

Wanneer bij de controle problemen aan het licht komen of de vooropgezette kwaliteitsvereisten niet werden nageleefd, moet de archiefvormer gecontacteerd worden om de problemen op te lossen.

Na positieve evaluatie van de kwaliteit krijgt de archiefvormer de toelating om de documenten te verwijderen en worden de aanwinsten geregistreerd. De archiefdocumenten worden geïnventariseerd en hun metadata worden verder aangevuld. Hierbij dient aandacht besteed te worden aan een uniek ID voor de digitale documenten. Bij de registratie kunnen ook de metadata op dossier- en/of documentniveau geïndexeerd worden en opgenomen worden in een databank zodat centrale bevraging mogelijk is.

2.6.2. Gearchiveerde dossiers en documenten opzoeken

Men kan de gebruiker op diverse niveaus toegang geven tot de gearchiveerde digitale dossiers en archiefdocumenten:
1. reeks
2. dossier
3. document

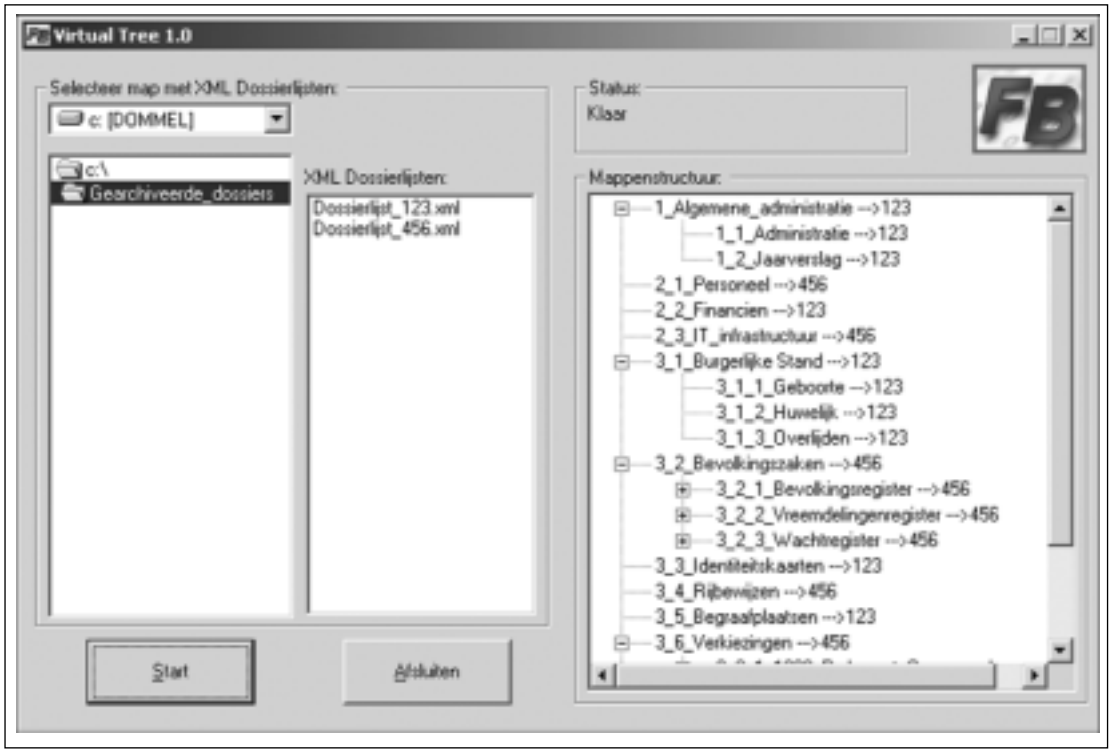
Enkel toegang geven op reeksniveau (bijvoorbeeld 'personeelsdossiers') is te algemeen om gearchiveerde dossiers en documenten op een efficiënte wijze op te zoeken. Opzoekingen op dossier- en documentniveau zijn interessanter en maken meer gerichte zoekacties mogelijk. Hieronder wordt verder besproken hoe gearchiveerde documenten op beide niveaus kunnen worden opgezocht. Hiervoor worden twee methoden aangereikt:
1. via de opslag van metadata in een databank
2. via XML-Dossierlijsten

Het niveau en de wijze waarop de digitale dossiers en documenten worden opgezocht, is in hoofdzaak afhankelijk van de beschikbaarheid en de opslagplaats van hun metadata. Een performante bevraging van alle metadata is slechts mogelijk wanneer die centraal in een databank zijn opgeslagen. Voor ontsluiting op dossierniveau houdt dit in dat de dossiermetadata van alle digitale dossiers bekend zijn en worden ingevoerd. Wanneer deze metadata digitaal, expliciet en gestructureerd zijn opgeslagen, kunnen deze gegevens volledig automatisch in de databank worden opgenomen.

Met betrekking tot ontsluiting op documentniveau is men opnieuw afhankelijk van de beschikbaarheid van metadata (bijvoorbeeld de bestandsnaam, de onderwerpsomschrijving, trefwoorden, enz.). Meer gedetailleerd zoeken op woorden die in documenten voorkomen, is een optie. Dit

houdt in dat de archiefdocumenten worden geïndexeerd en dat een full-text index aan de databank met metadata wordt toegevoegd.

Dossiers en documenten opzoeken is ook mogelijk op basis van de XML-Dossierlijsten die werden gecreëerd ter documentering van het digitale klassement en die ook als overdrachtslijst worden gebruikt (zie 2.3 en 2.6.1). Deze methode maakt geen gebruik van een databank waarin alle dossier- en/of documentmetadata worden opgenomen, maar biedt de archiefgebruiker een zoekmechanisme op basis van de gegevens die in de XML-Dossierlijsten zijn opgenomen. De functie van de XML-Dossierlijsten wordt op die manier uitgebreid.



Op basis van de XML-Dossierlijsten kan het digitale klassement van een archiefvormer gereconstrueerd worden zodat zoekopdrachten tegen de klassementsstructuur mogelijk blijven, ook al zijn de gearchiveerde dossiers uit de actieve klassementsstructuur weggenomen en staan ze verspreid op meerdere dragers. Het zoeken naar gearchiveerde documenten gebeurt hierbij in twee stappen. Via de werkprocessen en de taken zoekt de archiefgebruiker eerst de relevante dossiers- en onderwerpsmappen. Vervolgens wordt binnen de gevonden map het document gezocht. Deze zoekactie gebeurt hoofdzakelijk op basis van de bestandsnaam van de documenten. Aangezien de bestandsnamen van de documenten in de XML-Dossierlijsten zijn opgenomen, kunnen ze indien gewenst in de resultaatscherm aan de mapnamen worden weergegeven. Ook het bestandstype kan een leidraad zijn bij de opzoeking. Aangezien de zoekactie nu al verfijnd wordt tot zoeken binnen één bepaalde map kan een 'on the fly query' op de inhoud van de documenten sneller en doeltreffender verlopen. Voor heel grote hoeveelheden documenten blijft dit echter geen aangewezen of performante werkwijze, want de documenten worden hierbij één voor één doorlopen.

Het zoekpad bij ontsluiting op basis van XML-Dossierlijsten blijft hoofdzakelijk beperkt tot de structuur van het archief die gebaseerd is op de werkprocessen, taken en activiteiten van de archiefvormer. Voor gebruikers die vertrouwd zijn met de handelingen van de archiefvormer, zoals de administratieve medewerkers en ambtenaren, kan dit volstaan. Voor externe archiefgebruikers geldt dit minder. Voor hen dienen de gearchiveerde dossiers en documenten nog explicieter ont-

sloten en gecontextualiseerd te worden zodat zij andere zoekpaden kunnen volgen. XML Topic Maps kunnen aan deze nood beantwoorden. Op basis van een topic map kan een externe archiefgebruiker via zijn eigen associaties en zoekpaden gearchiveerde dossiers en documenten terugvinden. De XML-Dossierlijsten kunnen als bouwsteen voor de XML Topic Map worden gebruikt.

Meer informatie
- *F. BOUDREZ, H. DEKEYSER en S. VAN DEN EYNDE*, Archiveren van e-mail, *Antwerpen-Leuven, 2003. (DAVID-rapport nr. 5)*.
- *F. BOUDREZ*, E-mails: hoe bewaren en goed archiveren?, *Technisch Rapport Stadsarchief Antwerpen, Antwerpen, 2003.*
- *F. BOUDREZ*, Hoe archiveer je digitale kantoordocumenten, *in: Lokaal, nr. 7*
- *F. BOUDREZ*, XML Topic Maps voor digitale archivering, *Stadsarchief Antwerpen, Antwerpen, 2002.*
- *DAVID praktijkcasussen: e-mail.*

3. Informatiesystemen

3.1. Kenmerken

Naast digitale kantoordocumenten beheren organisaties grote digitale informatiesystemen waarmee digitale informatie en documenten worden gecreëerd, beheerd en verspreid. Voorbeelden van dergelijke informatiesystemen zijn websites, geografische informatiesystemen, toepassingen voor het beheren van allerhande registers, het verlenen van vergunningen, postregistratie, dossieropvolging, enz.

Deze informatiesystemen hebben een aantal typische eigenschappen waardoor een afzonderlijke archiveringsprocedure noodzakelijk is. Deze eigenschappen zijn onder meer:
- de informatiesystemen worden meestal aangestuurd door databanken. De data en/of de documenten zijn opgeslagen in databanksystemen die op hun beurt deel uitmaken van een geïntegreerd geheel van interactieve applicaties.
- de gegevens die in deze systemen worden gecreëerd en beheerd hebben niet altijd één vastgelegde documentaire vorm. Dit is een gevolg van het gebruik van nieuwe technologieën en van het feit dat data en niet langer documenten als basis dienen.
- de documenten worden meestal op het moment zelf samengesteld en zijn niet als zodanig statisch opgeslagen. De inhoud van de documenten is afhankelijk van de beschikbare informatie op dat tijdstip en van de interactie met de gebruikers.
- de gegevens/documenten worden volledig centraal op mainframes en servers beheerd en kunnen niet dossiergewijs worden geordend.

Uit deze kenmerken volgt alvast dat 'capture' (identificeren, vastleggen en registreren) van de archiefdocumenten een essentieel onderdeel van de archiveringsprocedure voor informatiesystemen is. Op basis van archiefwaardering worden de archiefdocumenten in deze data-centrische informatiesystemen geïdentificeerd. Het dynamisch en interactief karakter van de informatiesystemen en de weinig vaste documentaire vorm van veel documenten maakt dit echter niet vanzelfsprekend.

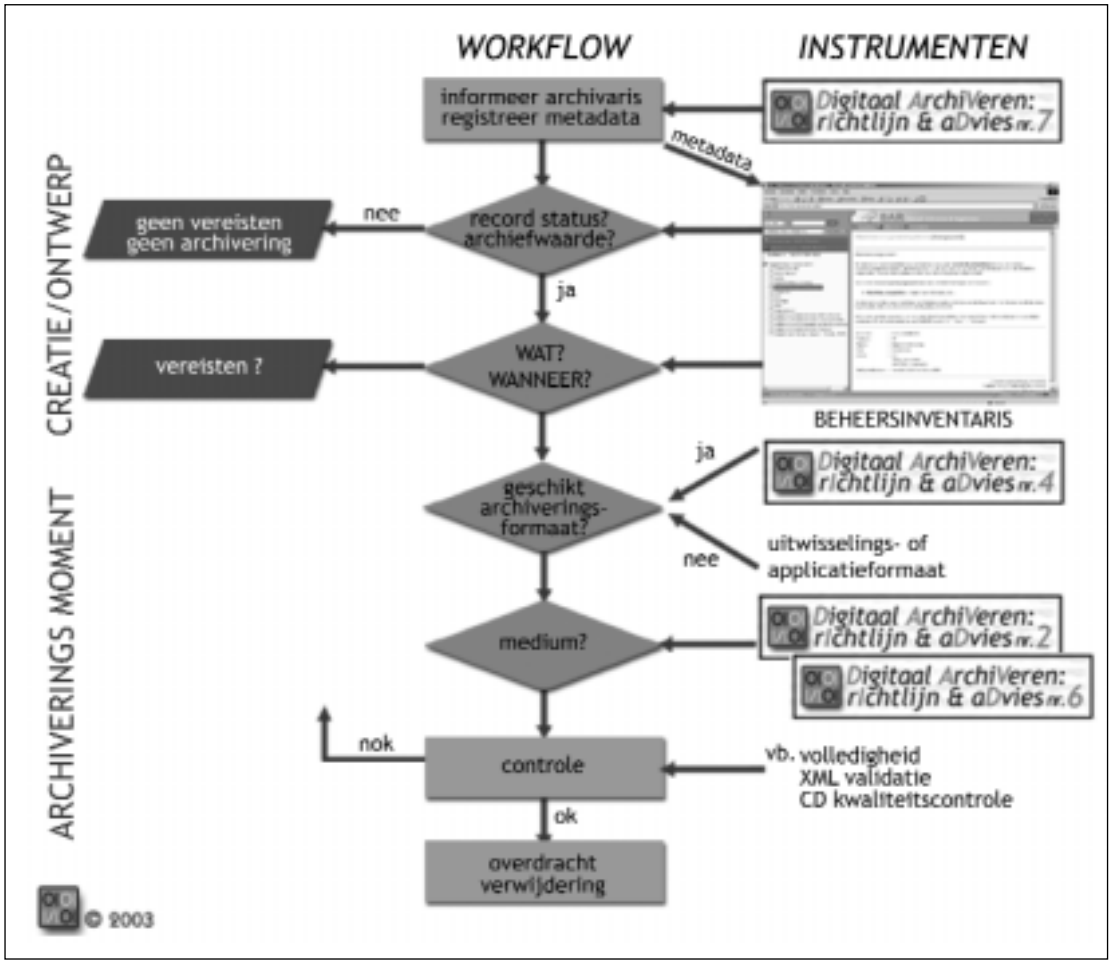
3.2. Informatiesysteem als vertrekpunt

Het uitgangspunt in de archiveringsprocedure is het informatiesysteem waarbinnen de documenten worden gecreëerd en beheerd. Er is een grote variëteit en complexiteit aan informatiesystemen zodat er nood is aan analyse van elk informatiesysteem en zijn specifieke eigenschappen. De architectuur, de functionaliteiten, de afhankelijkheden, de workflow, de interacties, enz. verschillen immers van systeem tot systeem zodat de archiveringsprocedure vanuit elk informa-

tiesysteem zelf moet vertrekken om te achterhalen WAT, HOE en WANNEER wordt gearchiveerd. Aangezien de informatiesystemen doorgaans volledig centraal beheerd worden, is het antwoord op de WIE-vraag de systeemverantwoordelijke, al zijn hierop uitzonderingen mogelijk.

3.3 Workflow en instrumenten

De archiveringsprocedure voor informatiesystemen loopt net zoals die voor kantoordocumenten van creatie tot en met ontsluiting. Al heel vroeg worden de eerste stappen in de archiveringsprocedure gezet. De archiveringsprocedure start bij het ontwerpen en het ontwikkelen van het informatiesysteem waarbinnen de documenten worden gecreëerd en beheerd, dus nog vóór de eigenlijke creatie van de documenten zelf.



informeer archivaris registreer metadata

De procedure start bij het informeren van de archivaris en het registreren van metadata over het informatiesysteem.

De archiefvormer brengt de archivaris op de hoogte van de ontwikkeling van een nieuw informatiesysteem, de aanpassing van een bestaand informatiesysteem of de afbouw van een oud informatiesysteem. Deze meldingsverplichting wordt binnen de organisatie best als een formele stap in de algemene IT-procedure opgenomen. Het tijdstip van de melding is bij voorkeur zo vroeg mogelijk, zodat de archivaris de nodige tijd voor onderzoek heeft en nog kan anticiperen zonder achter de feiten te moet aanhollen. De essentie van de melding is dat de archivaris weet voor welk informatiesysteem een archiveringsoplossing nodig is en dat hij betrokken wordt bij de ontwikkeling, de aanpassing of de afbouw van informatiesystemen.

Aangezien de archivaris voor de volgende stappen in de archiveringsprocedure informatie nodig heeft over het informatiesysteem is het belangrijk dat zo vroeg mogelijk op een gestructureerde en georganiseerde wijze documentatie over het informatiesysteem wordt geregistreerd en bijgehouden. Metadata over informatiesystemen worden echter in zeer weinig administraties of IT-afdelingen systematisch bijgehouden. Op het ogenblik van archivering beschikken archivarissen bijgevolg enkel over het informatiesysteem zelf, in het beste geval aangevuld met mondeling verstrekte informatie. Het spreekt voor zich dat dit een onvoldoende basis is voor belangrijke beslissingen zoals de identificatie van archiefdocumenten, de archiefwaardering en het uitstippelen van de archiveringsstrategie.

De metadata over informatiesystemen worden geregistreerd en bijgehouden in een nieuw archiefinstrument: de beheersinventaris van digitale informatiesystemen. In deze beheersinventaris houden de archiefvormer, de systeemverantwoordelijke(n) en de archivaris vanaf de creatie metadata bij over het digitale informatiesysteem. Het basisdatamodel voor deze beheersinventaris zijn de gegevensvelden die vanuit archiefstandpunt noodzakelijk zijn. Deze hebben betrekking op de ontstaanscontext, de technische context en de beheerscontext. Een dergelijke beheersinventaris kan echter ook andere doeleinden dienen zoals de helpdeskfunctie of het beheer van de IT-infrastructuur. Op die manier biedt de beheersinventaris een meerwaarde voor de hele organisatie en zijn de archiefvormer en de archivaris niet de enige belanghebbende partijen voor het up-to-date houden van de beheersinventaris. De beheersinventaris kan diverse vormen aannemen. Dit kan evolueren van een eenvoudig tekstbestand tot een meer geavanceerde databanktoepassing. De beheersinventaris van de stad Antwerpen bijvoorbeeld is een relationele databank met webinterface en dynamisch datamodel.

Op basis van de informatie in de beheersinventaris - eventueel aangevuld met bijkomende documentatie - identificeert de archivaris de archiefdocumenten binnen het systeem en onderzoekt hij of er documenten met archiefwaarde worden gecreëerd. De archivaris kan zich voor het onderzoek naar nieuwe systemen ook baseren op demo-versies of technische fiches van het informatiesysteem. Aangezien er in dit geval nog geen documenten gecreëerd zijn, is het zeer belangrijk om de archiefwaardering te koppelen aan de werkprocessen waarbinnen de documenten worden gevormd en aan hun functie die ze daarbinnen vervullen. In het geval van aanpassingen aan of het afbouwen van bestaande systemen is het informatiesysteem zelf een belangrijke bron.

Met betrekking tot databanken dient de archivaris na te gaan of:
– de databank op zich één archiefdocument is
– de databank een aggregaat van archiefdocumenten is
– de output van de databank de archiefdocumenten zijn.

Bij het identificeren van het archiefdocument bakent de archivaris ook de grenzen van het archiefdocument af. Veel informatiesystemen zijn immers aan elkaar gekoppeld en halen informatie op uit externe bronnen. Op basis van identificatie van de archiefbescheiden en archiefwaardering bepaalt de archivaris of de externe informatie als onderdeel van dit informatiesysteem, of afzonderlijk wordt gearchiveerd.

Als er binnen het informatiesysteem geen archiefdocumenten worden gevormd, dan spreekt het voor zich dat er geen archiveringsprocedure wordt uitgewerkt en dat er vanuit archiveringsstandpunt ook geen bijzondere vereisten aan het informatiesysteem worden opgelegd.

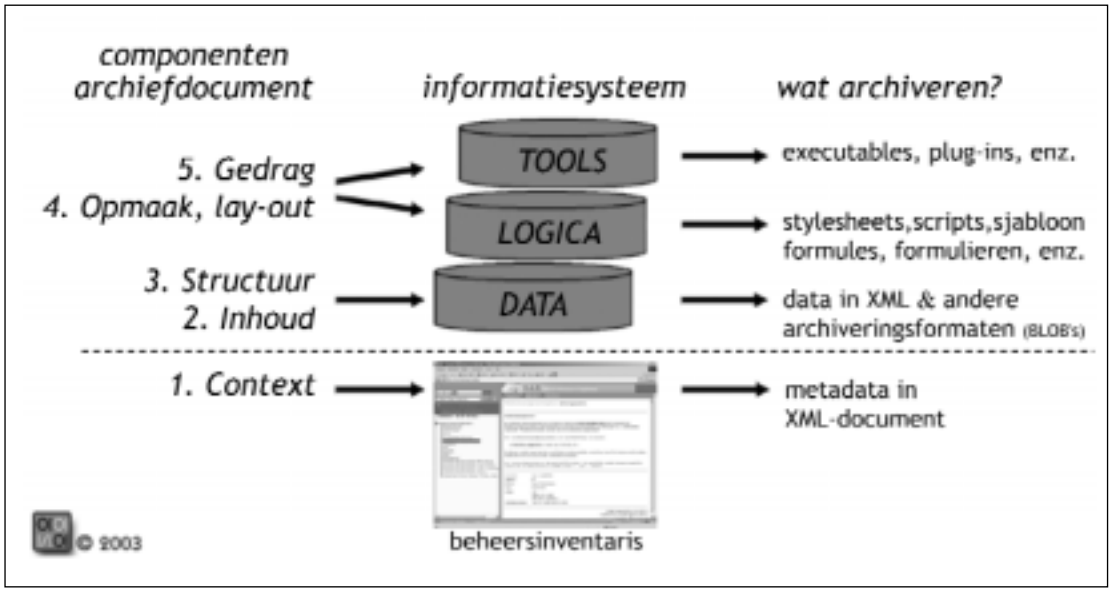
Worden er binnen het informatiesysteem wel archiefdocumenten gecreëerd en beheerd, dan beantwoordt de archivaris de WAT- en WANNEER-vragen van het DAVID-beslissingsmodel. Het is van belang om

deze vragen onmiddellijk te koppelen aan de bewaartermijn van de archiefdocumenten en aan de vereiste om stabiele en vaste documenten te archiveren.

Archiefdocumenten met een beperkte bewaartermijn of waarvan de levensduur niet langer is dan die van de informatiesystemen zelf kunnen meer dan waarschijnlijk binnen de actieve informatiesystemen worden bewaard, terwijl voor documenten met een lange bewaartermijn een lange termijnoplossing buiten het informatiesysteem nodig is.
– in het eerste geval ziet de archivaris er op toe dat de archiefdocumenten binnen de informatiesystemen worden bijgehouden en raadpleegbaar zijn
– in het tweede geval zorgt de archivaris ervoor dat de archiefdocumenten als conceptuele objecten worden vastgelegd zodat in de toekomst weergave en interpretatie mogelijk is zonder het oorspronkelijk informatiesysteem.

Op basis van de identificatie van de archiefdocumenten en hun bewaartermijn gaat de archivaris na welke onderdelen van het informatiesysteem op lange termijn worden gearchiveerd. De keuze van de componenten van het informatiesysteem die al dan niet worden gearchiveerd is niet alleen afhankelijk van de klassieke archiefcriteria, maar ook van de technische vereisten om in de toekomst de archiefdocumenten op een getrouwe wijze te reconstrueren.

Een hulpmiddel bij het beantwoorden van de WAT-vraag is de voorstelling van een informatiesysteem als een samenstelling van drie interactieve lagen:
– de data: de volledige databank, een deel van de databank of een bepaalde output
– de logica: de elementen die de input behandelen en de output genereren
– de tools: de programma's voor input, output en weergave.



Deze drie lagen kunnen gekoppeld worden aan de componenten van het archiefdocument. Vanuit de identificatie van de essentiële en incidentele componenten van de archiefdocumenten komt vast te liggen welke laag of welke onderdelen van die laag worden gearchiveerd. Op die manier wordt bijvoorbeeld in de datalaag een onderscheid gemaakt tussen computerdata en archiefdocumenten wanneer niet de volledige databank het archiefdocument is. In dit geval zal op basis van de archiefwaardering een query worden gemaakt op basis waarvan de archiefdocumenten worden samengesteld. Dit resultaat wordt vervolgens buiten het databanksysteem geëxporteerd en gearchiveerd. Wanneer daarentegen de databank zelf het archiefdocument is, dient veel aandacht besteed te worden aan de structuur. Voor hiërarchische databanken is de parent-child relatie van

belang, terwijl bij relationele databanken de relaties tussen de tabellen en de structuur van de records mee gearchiveerd moeten worden.
De context van het archiefdocument vormt hierop enigszins een uitzondering want de context zit meestal niet in het informatiesysteem zelf vervat. Aangezien de context en de metadata van het informatiesysteem gedocumenteerd worden in de beheersinventaris van de digitale informatiesystemen, kunnen beide hieruit worden gedistilleerd.

Voor archiefdocumenten die in aanmerking komen voor lange termijnarchivering wordt best vastgelegd WANNEER ze buiten het informatiesysteem worden gebracht. Het antwoord op de WANNEER-vraag kan van meerdere factoren afhankelijk zijn:
– beperkingen van het opslagsysteem
– performantie van het informatiesysteem
– ondersteuning van leveranciers
– vervanging of upgrade door een nieuw informatiesysteem.

Ongeacht de bewaartermijn en op basis van de WAT- en WANNEER-vragen wordt in deze stap nagegaan of er bijzondere vereisten gelden voor het informatiesysteem met het oog op het creëren, bijhouden en gemakkelijk archiveren van goede digitale archiefdocumenten. Deze vereisten kunnen betrekking hebben op:
– de encoding van de data: toepassen van standaarden, bijhouden documentatie
– het bestandsformaat waarin de documenten worden opgeslagen en de kwaliteitsvereisten
– de registratie van metadata
– het bijhouden van wijzigingen of aanleggen van een historiek
– het bijhouden van documentatie
– het inbouwen van betrouwbaarheidswaarborgen en -maatregelen
– voorzien van een archiveringsmodule zodat de documenten op een geautomatiseerde en eenvoudige wijze periodiek kunnen worden gearchiveerd.

Het vluchtige en interactieve karakter van informatiesystemen staat dikwijls haaks op de stabiele eigenschap van archiefdocumenten. De gegevens in databanken worden continu aangevuld of gewijzigd terwijl archiefdocumenten per definitie een vaste documentaire vorm met gefixeerde inhoud hebben. Vanwege de noodzaak om de gegevens te reconstrueren is het dikwijls aangewezen om een historiek van de gegevens bij te houden. Deze historiek kan zowel binnen de databank zelf, als buiten de databank in een logbestand worden bijgehouden. Als men deze laatste oplossing toepast, gebruikt men best niet zomaar de logbestanden die databankmanagementsystemen automatisch aanmaken. Deze logbestanden hebben hoofdzakelijk algemeen databankbeheer en recovery als doel, en zijn bijgevolg niet zo geschikt voor archiveringsdoeleinden. De standaard logbestanden bevatten ook te veel informatie die niet van belang is voor archivering, waardoor ze heel groot worden en niet gemakkelijk te ontcijferen zijn. Voor archivering is het beter om afzonderlijke logbestanden aan te leggen en op voorhand te bepalen welke acties worden geregistreerd en wat van die acties in het logbestand wordt bijgehouden. Op die manier beperkt men de omvang van de logbestanden en zorgt men ervoor dat ze het archiveringsdoel beter bereiken. Beide vragen worden best beantwoord vanuit de identificatie en de waardering van de archiefdocumenten. Het spreekt voor zich dat men vanaf de creatie van databanken hier al rekening mee houdt. Dit geldt overigens ook voor de audit-trails die worden aangelegd en bijgehouden.

Ten laatste op het archiveringsmoment worden de archiefdocumenten omgezet naar een archiveringsformaat. Voor een aantal types digitale documenten zijn geschikte archiveringsformaten beschikbaar. De archiveringsformaten die een archiefdienst hanteert worden bij voorkeur op een formele wijze vastgelegd. Hierbij wordt voor elk formaat het formaatprofiel met de ideale archiveringsinstellingen gedefinieerd. Bij ontstentenis aan een geschikt archiveringsfor-

maat worden de archiefdocumenten opgeslagen in een uitwisselingsformaat. Als het echt niet anders kan, is een applicatieformaat een (tijdelijke) oplossing.

Welk archiveringsformaat wordt gebruikt is hoofdzakelijk afhankelijk van WAT wordt gearchiveerd. Aangezien databanksystemen niet als dusdanig worden gearchiveerd, maar enkel de inhoud (of beter de documenten) kunnen dezelfde archiveringsformaten als voor kantoordocumenten gebruikt worden. Toegepast in de praktijk kan dit betekenen dat de gegevens van een GIS-applicatie als GML-documenten worden bijgehouden of dat de kaarten en plattegronden als GeoTIFF- of SVG-bestanden worden gearchiveerd. XML is samen met ASCII of Unicode het aangewezen archiveringsformaat voor puur tekstuele databanken. Binaire objecten die in een databank werden opgeslagen of de gegenereerde output kunnen best naar het archiveringsformaat worden omgezet dat het best aansluit bij hun type.

In de meeste gevallen is het aangewezen om bij het uitstippelen van de archiveringsprocedure een archiveringsformaat vast te leggen. In de praktijk is dit niet altijd mogelijk en wacht men beter af wat de opties zijn op het tijdstip van archivering. De informatietechnologie en de standaardisatie zijn immers voortdurend in evolutie.

Een volgende deelvraag in het HOE-aspect van het beslissingsmodel betreft het medium dat dient als overbrengings- en/of lange termijndrager. De archiefdienst bepaalt welke dragers als overbrengingsmedium worden gebruikt. In principe komt elk type drager die de archiefdienst kan inlezen hiervoor in aanmerking. Overbrenging via netwerk is mogelijk, maar is geen evidentie wanneer grote hoeveelheden computerbestanden getransfereerd moeten worden. De archiefdienst zet de overgedragen bestanden over naar een geschikte lange termijndrager.

De zaken liggen complexer wanneer de archiefdienst de overbrengingsdrager ook als lange termijndrager wil gebruiken. In dit geval gelden strenge kwaliteitsvereisten voor het beschrijven en het manipuleren van deze dragers.

In de voorlaatste stap van de procedure worden de overgedragen documenten gecontroleerd. Net zoals bij de archivering van kantoordocumenten worden zowel de digitale archiefdocumenten als hun dragers gecontroleerd op hun volledigheid, kwaliteit en bijgeleverde metadata. Voorbeelden zijn validatie van de XML-documenten, steekproefgewijze tests op binaire formaten, kwaliteitscontrole van de CD-R's, enz.

Als de overdracht de kwaliteitscontrole niet doorstaat, moeten de fouten of problemen eerst rechtgezet worden en dienen bepaalde acties te worden hernomen. Het is dus van belang dat de gegevens en/of documenten nog niet uit de informatiesystemen zijn verwijderd, maar dat hiermee wordt gewacht tot na een succesvolle kwaliteitscontrole.

Wanneer de overdracht aan alle kwaliteitsvereisten beantwoordt, kunnen de archiefdocumenten worden geregistreerd en ontsloten. De archiefvormer krijgt de toelating om de gearchiveerde documenten uit de informatiesystemen te verwijderen of het hele informatiesysteem af te bouwen.

Meer informatie

- *F. BOUDREZ*, Het digitaal archiveringssysteem: beheersinventaris, informatielagen en beslissingsmodel als uitgangspunt, *Stadsarchief Antwerpen*, *Antwerpen*, *2001 (DAVID-rapport nr. 4)*.
- *F. BOUDREZ*, Een archiveringssysteem voor dynamische en interactieve informatiesystemen, *Stadsarchief Antwerpen*, *Antwerpen*, *2003*.
- *F. BOUDREZ*, Preservation of electronic records from database-driven informationsystems, *ErpaWorkshop: Long-term preservation of databases*, *Bern*, *9 april 2003*.
- *DAVID praktijkcasussen: kiezersregister / bevolkingsregister / websites*.

Eindnoten

[1] INTERPARES 1, *How to preserve authentic electronic records?*, 2001; K. THIBODEAU, R. MOORE EN C. BARU, *Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation,* in: *Proceedings of the DLM-Forum on electronic records. European citizens and electronic information: the memory of the information society*, Brussel 18-19 oktober 1999, Brussel, 2000, p. 113-118. (http://europa.eu.int/ISPO/dlm/fulltext/full_thib_en.htm)

[2] K. THIBODEAU, *Building the Archives of the Future. Advances in Preserving Electronic Records at the National Archives and Records Administration,* in: D-Lib Magazine (February 2001) Volume 7.

[3] The documentary form is the primary means by which the content of a record, its immediate administrative and documentary context, and its authority are communicated. (INTERPARES 1, *The InterPARES Glossary*, p. 3).

[4] J. ROTHENBERG en T. BIKSON, *Digital Preservation. Carrying Authentic, Understandable and Usable Documents Through Time,* Den Haag, 1999, p. 7.

[5] ICA, *Guide for managing electronic records from an archival perspective*, Parijs, 1997, p. 22.

[6] INTERPARES 1, *Authenticity Task Force Report*, p. 2.

[7] F. BOUDREZ, *Het digitaal archiveringssysteem: beheersinventaris, informatielagen en beslissingsmodel als basis*, Antwerpen, 2001; K. THIBODEAU, *Overview of technological approaches to digital preservation and challenges in coming years*, in: The State of Digital Preservation: An International Perspective, 2002, p. 4-31; (http://www.clir.org/pubs/reports/pub107/thibodeau.html); TESTBED DIGITALE BEWARING, *Migratie: context en huidige stand van zaken*, Den Haag, 2001, p. 6-8 (http://www.digitaleduurzaamheid.nl).

[8] J. ROTHENBERG EN T. BIKSON, *Digital preservation: carrying authentic, understandable and usable digital records through time. report to the dutch national archives and ministry of the interior*, 1999 (http://www.digitaleduurzaamheid.nl/bibliotheek/docs/final-report_4.pdf); J. ROTHENBERG, *An experiment in using emulation to preserve digital publications*, Den Haag, 2000 (http://www.kb.nl/coop/nedlib/results/emulationpreservationreport.pdf); J. ROTHENBERG, *Avoiding technological quicksand: finding a viable technical foundation for digital preservation. a report to the council on library and information resources*, Washington, 1999 (http://www.clir.org/pubs/reports/rothenberg/pub77.pdf); J. ROTHENBERG, *Ensuring the longevity of digital information*, Santa Monica, 1999 (http:// www.clir.org/pubs/archives/ensuring.pdf).

[9] http://www.archivebuilders.com/aba010.html.

[10] http://www.rlg.org/preserv/diginews/diginews5-3.html#feature2.

[11] http://www.rlg.org/preserv/diginews/diginews5-4.html#feature2.

[12] Deze zienswijze is geïnspireerd op de "*Migration on request*"-strategie van het CAMiLEON-project en op de benadering van de Nationale Archiefdienst van Australië (P. MELLOR, P. WHEATLEY EN D. SERGEANT, *Migration on Request - a practical technique for preservation*, http://www.si.umich.edu/CAMILEON/reports/mor/index.html; H. HESLOP, S. DAVIS EN A. WILSON, National Archives Green Paper: *An approach to the preservation of digital records*, Canberra, 2002, http://www.naa.gov.au/recordkeeping/er/digital_preservation/summary.html).

[13] Microsoft Corporation hanteert vanaf 15 oktober 2002 een formeel Support Life Cycle beleid. Dit beleid bevat richtlijnen voor de beschikbaarheid van productondersteuning. (http://support.microsoft.com/default.aspx?scid=fh;nl;complifeport).

[14] "The general rule is that the longevity of storage media is greater than the longevity of the storage media drives, and that the longevity of the drives is greater than that of the software". (C. DOLLAR, *Authentic electronic records: strategies for long-term access*, Chicago, 1999, p. 86).

[15] De Blue Book-versie van het OAIS-model is beschikbaar op: http://wwwclassic.ccsds.org/documents/pdf/CCSDS-650.0-B-1.pdf. Informatie over de standaard en zijn toepassing is beschikbaar op: http://www.rlg.org/longterm/oais.html en http://www.erpanet.org (workshop Kopenhagen).

[16] T. THOMASSEN, *Een korte introductie in de archivistiek*, in: P.J. HORSMAN, F.C.J. KETELAAR EN T.H.P.M. THOMASSEN, *Naar een nieuw paradigma in de archivistiek*, p. 11-20; K. THIBOUDEAU, *Building the Archives of the Future, in: D-Lib Magazine*, febr. 2001 (vol. 7, nr. 2).

[17] *Model requirements for the management of electronic records*, Brussel - Luxemburg, 2001, p. 21-25; DOD, *Design criteria standard for electronic records management software applications* (DoD 5015.2-STD), Washington, 2002 (tweede versie).

[18] INTERPARES 1, *Authenticity Task Force Report*, p. 2.

[19] Een voorbeeld XML-document met dossiermetadata is beschikbaar op de DAVID-website (http://www.antwerpen.be/david/website/nl/dossier_metadata.htm).

[20] Een voorbeeld XML-Dossierlijst is beschikbaar op de DAVID-website (http://www.antwerpen.be/david/website/nl/xml.metadata.htm)

DAVID Publicaties

DAVID-rapporten:

1. R. VERHAERT, *De permanente bewaring van digitale overheidsgegevens: de situatie in de Vlaamse instellingen en archiefdiensten,* Antwerpen, Stadsarchief Antwerpen, 2000.
2. F. BOUDREZ en S. VAN DEN EYNDE, *Digitale archivering van het kiezersregister*, Antwerpen – Leuven, Stadsarchief Antwerpen – ICRI, 2001.
3. F. BOUDREZ, *Het digitaal archiveringssysteem: beheersinventaris, informatielagen en beslissingsmodel als uitgangspunt,* Antwerpen, Stadsarchief Antwerpen, 2001.
4. S. VAN DEN EYNDE, *Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1,* Leuven, ICRI, 2001.
5. F. BOUDREZ, H. DEKEYSER en S. VAN DEN EYNDE, Archiveren van e-mail, Antwerpen-Leuven Stadsarchief Antwerpen – ICRI, 2002.
6. S. VAN DEN EYNDE, *Hoe archiveren en Wat? Op zoek naar de rol van PKI voor digitale archieven*, Leuven, ICRI, 2001.
7. F. BOUDREZ, en S. VAN DEN EYNDE, *Archivering van websites*, Antwerpen-Leuven, Stadsarchief Antwerpen – ICRI, 2002.
8. H. DEKEYSER, *Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 2: Auteursrecht, technische beschermingsmaatregelen en wettelijk depot*, Leuven, ICRI, 2004.

Digitaal ArchiVeren. rIchtlijnen en aDvies:

1. Archiveren van e-mail
2. Duurzame cd's
3. Mappenstructuur en bestandsnamen voor digitale documenten
4. Standaarden voor bestandsformaten
5. Websitesbeheer voor archivering
6. Duurzame magnetische dragers
7. Checklist voor IT-verantwoordelijken
8. Checklist voor de digitale archivaris
9. Digitaliseren van analoge archiefdocumenten
10. Migratie naar archiveringsformaten

DAVID-bijdragen

- F. BOUDREZ, *Standaarden voor digitale archiefdocumenten*, Antwerpen, Stadsarchief Antwerpen, 2001-2004.
- F. BOUDREZ, en S. VAN DEN EYNDE, *Woordenlijst van het DAVID-project*, Antwerpen-Leuven, Stadsarchief Antwerpen-ICRI, 2001-2004.
- S. VAN DEN EYNDE, *Archiveren van e-mail. Deel 1: Controlerechten van de records manager*, in: Bibliotheek- & Archiefgids, 77 (2001), 5, p.15-19.
- F. BOUDREZ, *Archiveren van e-mail. Deel 2: een archiveringssysteem voor e-mails*, in: Bibliotheek- & Archiefgids, 77 (2001), 5, p.9-14.
- F. BOUDREZ, *Inventaris van de digitale informatiesystemen van de stadsadministratie, het OCMW en het havenbedrijf van Antwerpen*, Antwerpen, Stadsarchief Antwerpen, 2001.
- F. BOUDREZ, *CD's voor het archief*, Antwerpen, Stadsarchief Antwerpen, 2001.
- J. DUMORTIER, en S. VAN DEN EYNDE, *'Electronic signatures and trusted archival services'*, in: Proceedings of the DLMForum 2002 in Barcelona, Luxemburg, 2002, 520-528.
- J. DUMORTIER, en S. VAN DEN EYNDE, *Op-Slag Bewezen. Juridische mogelijkheden en moeilijkheden bij het opzetten van een elektronisch documentbeheersysteem,* Brussel, 2002.

- F. BOUDREZ, *Van backup tot gearchiveerde website. De archivering van de eerste versies van de Digitale Metropool Antwerpen*, Antwerpen, Stadsarchief Antwerpen, 2002.
- F. BOUDREZ, *Magnetische dragers voor het archief*, Antwerpen, Stadsarchief Antwerpen, 2002.
- F. BOUDREZ, *<XML/> en digitaal archiveren*, Antwerpen, Stadsarchief Antwerpen, 2002.
- F. BOUDREZ, *XML Topic Maps voor digitale archivering*, Antwerpen, Stadsarchief Antwerpen, 2002.
- F. BOUDREZ, *Archief onder controle? De beheersinventaris als instrument bij de archivering van digitale archiefdocumenten*, Antwerpen, Stadsarchief Antwerpen, 2002.
- F. BOUDREZ, *Digitaal archiveren in Vlaanderen*, in: Nederlands Archievenblad, feb. 2003, p. 28-29.
- F. BOUDREZ, *Hoe archiveer je digitale kantoordocumenten?*, in: Lokaal nr. 7, april 2003, p. 17-19.
- F. BOUDREZ, *DAVID-conferentie: e-Archiving for posterity*, in: Nederlands Archievenblad, aug. 2003, p. 14-15.
- F. BOUDREZ, *Een archiveringssysteem voor dynamische en interactieve informatiesystemen*, Antwerpen, Stadsarchief Antwerpen, 2003.
- F. BOUDREZ, *E-mailarchieven. E-mails: hoe bewaren en goed archiveren? Technisch rapport*, Stadsarchief Antwerpen, 2003.
- F. BOUDREZ, *Handleiding archiveren van e-mail*, Antwerpen, Stadsarchief Antwerpen, 2003.
- F. BOUDREZ, *XML in het stadsarchief Antwerpen*, in: Nieuwsbrief Testbed, nr 5, 2003.
- F. BOUDREZ, *Videoarchivering: bruggen bouwen op technologisch drijfzand*, Antwerpen, Stadsarchief Antwerpen, 2004.

DAVID-website: http://www.antwerpen.be/david

DAVID-mailadres: david@stad.antwerpen.be