Stuurgroep Rijk aan Informatie

Programma Rijk aan Informatie

Rijnstraat 50
2515XP Den Haag
T +31-70-331 5400

Contact
J.J. Boerties
Projectleider Di-Stroy

T +31 6 11 45 91 69
jos.boerties@nationaalarchief.nl

Datum
19 januari 2018

Onze referentie
1300855

Auteur
J.J. Boerties

memo Whitepaper digitale vernietiging Rijk

1. Aanleiding

Diverse projecten binnen het programma Rijk aan Informatie dragen reeds bij aan verbeteren van uitvoeringskaders voor het permanent bewaren van overheidsinformatie, denk hierbij aan emailarchivering en webarchivering. Het overgrote deel van de overheidsinformatie (om en nabij 85% tot 90%) komt op basis van de huidige selectiecriteria echter niet in aanmerking voor permanente bewaring en moet dientengevolge op termijn vernietigd worden. De digitalisering van de werkprocessen bij de overheid die de afgelopen jaren heeft plaatsgevonden, zet de uitvoerbaarheid van de vernietigingsplicht echter in toenemende mate onder druk. Recent onderzoek van de Erfgoedinspectie toont bijvoorbeeld aan dat vrijwel geen enkel departement momenteel uitvoering geeft aan vernietiging in DMS-systemen.[1] De behoefte aan een betere afbakening, betere handvatten en meer flexibiliteit bij de uitvoering van digitale vernietiging is tevens kenbaar gemaakt door deelnemers aan de netwerkbijeenkomst RAI op 20 juli 2017 en is een actueel vraagstuk in de uitvoeringspraktijk. Doelstelling van het project Di-stroy is dan ook om voor het Rijk tot een beter werkbaar, gemoderniseerd uitvoeringsbeleid voor digitale vernietiging te komen. Deze whitepaper bevat een gedetailleerde probleemanalyse en gaat in op de daarbij voorziene interventies.

2. Samenvatting voorziene interventies

Als voornaamste verbetermaatregel wordt voorgesteld om de vernietigingsplicht veel beter af te bakenen, zodat duidelijker is voor archiefvormers in welke gevallen de vernietigingsplicht hard van toepassing is en in welke gevallen handelingsruimte bestaat. Dit komt compliance en flexibiliteit van het informatiebeheer over de gehele linie ten goede. Tevens zal onderzocht worden of de toevoeging van een authenticiteitskenmerk aan documenten het systeem-overstijgend vernietigen van duplicaten op verschillende schijven kan faciliteren.
In het verlengde hiervan wordt voorgesteld om een ruimere bandbreedte aan te brengen in de termijnen waarop vernietiging plaats kan vinden. Het bestaande uitgangspunt, waarbij vernietiging zo snel mogelijk na vervallen van het primaire gebruiksbelang plaatsvindt, is in een digitale omgeving niet alleen lastig uitvoerbaar, maar negeert tevens de secundaire gebruikswaarde en de daaraan gekoppelde verwachting van burgers en politiek dat overheidsinformatie langdurig beschikbaar is. Met het oog hierop wordt voorgesteld om (waar mogelijk en wenselijk) langere vernietigingstermijnen te hanteren dan nu het geval is.
Omdat deze beleidswijziging mede tot gevolg kan hebben dat persoonsgegevens in voorkomende gevallen pas op langere termijn vernietigd zullen worden, zal tevens een handreiking worden opgeleverd met een overzicht van alternatieve privacy-waarborgen (zoals verwijdering, afscherming, pseudonimisering van gegevens) en de wijze waarop deze effectief kunnen worden ingezet binnen het eigen informatiebeheer.

[1] Erfgoedinspectie: concept-rapport 'Wel digitaal, nog niet duurzaam.'

Visie Rijk aan Informatie

"De informatiehuishouding van het Rijk is gebruiksvriendelijk, toegankelijk, transparant en ontzorgt de medewerker, door in het primaire proces zoveel als mogelijk by design in de automatisering te ondersteunen. Er wordt gewerkt met een slanke ambtelijke organisatie en processen zijn efficiënt ingericht. Door vereenvoudiging van de informatiehuishouding kan beter worden voorzien in rijksbrede samenwerking, delen, archiveren en actieve openbaarmaking waar mogelijk. We zijn gericht op zo min mogelijk regeldruk en informatiediensten -en producten worden zo veel mogelijk integraal aangeboden."

3. Wat verstaan we onder vernietiging?

Onder vernietiging moet worden verstaan dat een record (informatieobject) een zodanige bewerking ondergaat dat deze met gangbare technieken en inspanningen nooit meer te reconstrueren is.[2] De verplichting voor overheidsorganen om zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden is vastgelegd in Artikel 3 van de Archiefwet 1995. Hoewel deze verplichting in 1995 voor het eerst in de wet is verankerd bestaat zij voor het Rijk feitelijk al sinds 1980, bij Besluit algemene secretarie-aangelegenheden rijksadministratie (Stb. 1980, 182)

3.1 Hoe werkt vernietiging?

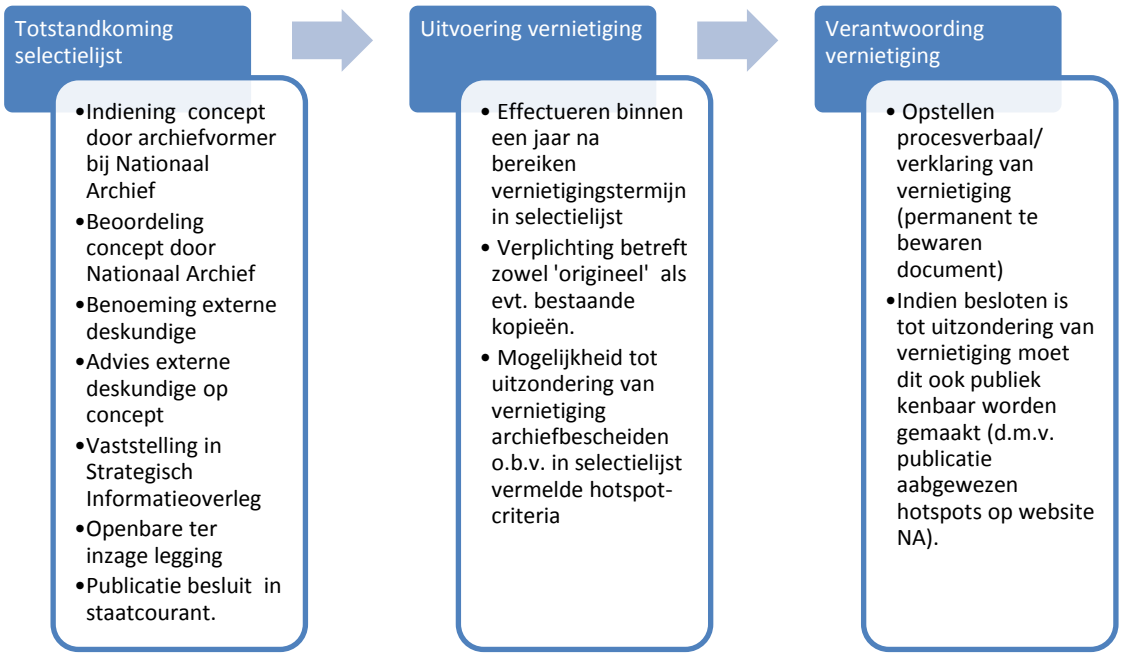
De operationalisering van de vernietigingsplicht is vastgelegd in artikel 5 van de Archiefwet 1995. Daarin is aangegeven dat overheidsorganen verplicht zijn om een selectielijst te maken met een systematisch overzicht van de categorieën archiefbescheiden waarover zij beschikken en vermelding van de daaraan gekoppelde vernietigingstermijnen. Vernietiging moet uiterlijk binnen een jaar na verstrijken van de in de selectielijst opgenomen termijn plaatsvinden[3] en vindt daarom in de praktijk veelal op jaarbasis per informatieproces plaats. In artikel 8 van het Archiefbesluit 1995 is vervolgens vastgelegd dat van elke vernietiging een verklaring (proces-verbaal) beschikbaar moet zijn.
Op grond van artikel 5 van het Archiefbesluit 1995 hebben overheidsorganen de discretionaire bevoegdheid (binnen vooraf vastgestelde criteria) om archiefbescheiden die in de selectielijst als te vernietigen staan aangemerkt uit te zonderen van vernietigen, bijvoorbeeld als er sprake is van zogeheten 'hotspots'.[4] Omgekeerd bestaat deze uitzonderingsmogelijkheid niet; archiefbescheiden die als te bewaren zijn aangemerkt en nog niet zijn overgebracht kunnen slechts vernietigd worden als de status van de bescheiden bij wijziging van de selectielijst wordt omgezet naar 'te vernietigen'.
Zonder vastgestelde selectielijst mogen overheidsorganen archiefbescheiden überhaupt niet vernietigen; De selectielijst is een openbaar besluit van algemene strekking en biedt daarmee

[2] De 'hardheid' van digitale vernietiging is enigszins arbitrair: In uitzonderlijke gevallen, zoals in strafrechtelijk onderzoek en t.b.v. nationale veiligheid, staan de overheid andere middelen ter beschikking zoals geavanceerde data recovery software, die vernietigde digitale bestanden toch weer kunnen reconstrueren. De Archiefwet kent geen grondslag voor deze uitzonderingen.

[3] Memorie van toelichting Archiefwet 1995

[4] Een hotspot is een gebeurtenis die veel maatschappelijke beroering veroorzaakt. Dit kan het noodzakelijk maken om van deze gebeurtenis meer informatie permanent te bewaren t.b.v. een betere reconstructie van het overheidshandelen.

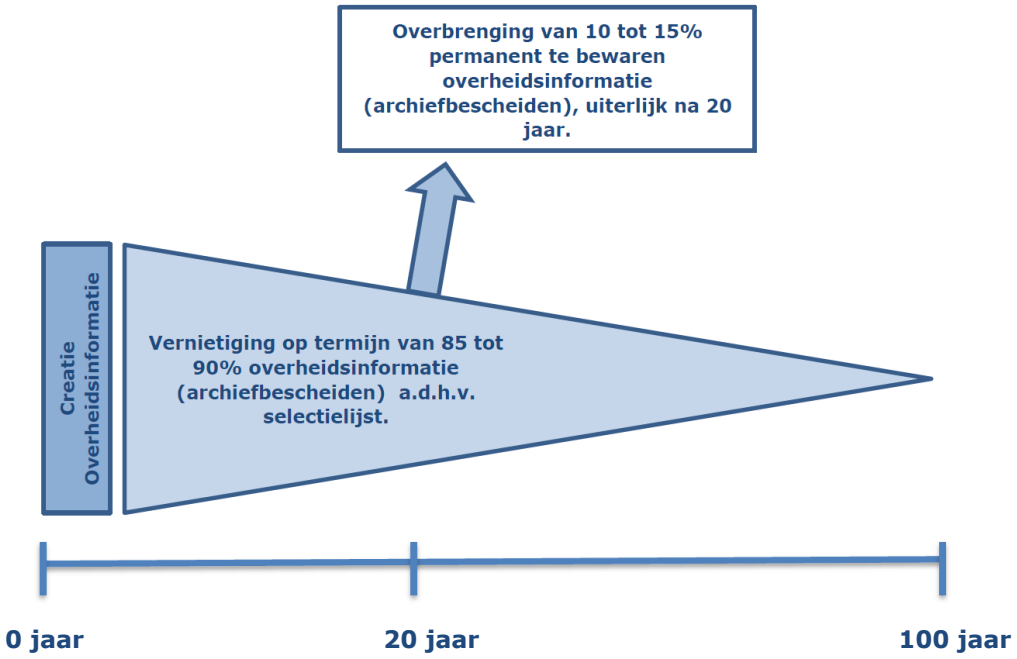
essentiële waarborgen voor burgers in het licht van het legaliteitsbeginsel en het rechtszekerheidsbeginsel.



Figuur 1: vernietigingsprocedure

3.2. Wat wordt met vernietiging beoogd?

Vernietigen van archiefbescheiden dient binnen het huidige wettelijke kader voornamelijk twee doelen; de uitvoerbaarheid van het informatiebeheer en tijdsbegrenzing van informatieverstrekking. In de eerste plaats ontlast vernietiging de archiefvormer van het beheren van een omvangrijke hoeveelheid informatie die hij niet meer actief nodig heeft. In de tweede plaats wordt door toekennen van een vernietigingstermijn de periode waarbinnen een archiefvormer over informatie behoort te beschikken en desgevraagd moet kunnen verstrekken, formeel en transparant afgebakend. Tevens zijn in sommige sectorale wetten, zoals de Jeugdwet, de Wet op de Inlichtingen- en Veiligheidsdiensten, de Wet Politiegegevens en de Wet op de Geneeskundige Behandelingsovereenkomst harde vernietigingstermijnen opgenomen om te voorkomen dat burgers nog lange tijd met gevoelige informatie kunnen worden achtervolgd.



Figuur 2: huidige situatie vernietiging

3.3. Vernietiging t.b.v. informatiebeheer

In de memorie van toelichting op de Archiefwet 1995 staat over de meerwaarde van vernietiging voor informatiebeheer het volgende: "Door archieven zo spoedig mogelijk te ontdoen van niet meer relevante stukken nemen de toegankelijkheid en beschikbaarheid toe en dalen de beheerskosten."[5] Het beoogde effect hiervan was dat in combinatie met scherpe selectiecriteria uiteindelijk een vernietigingspercentage van 90 tot 95 procent gerealiseerd zou kunnen worden voor het totaal aan archiefbescheiden dat sinds 1945 gecreëerd is. In de praktijk wordt dit percentage nu geschat op 85 tot 90 procent.

3.4. Vernietiging t.b.v. afbakening informatieverstrekking

Bestuurlijke verantwoording, aan parlement en aan de burger, is een basisbeginsel van onze democratische rechtsstaat. Echter, verantwoording kent ook een tijdsverloop. In de memorie van toelichting op de Wet Openbaarheid van Bestuur wordt erkend dat het exacte moment waarop het bestuurlijk belang van documenten ophoudt te bestaan moeilijk te begrenzen is, omdat de situatie van aangelegenheid tot aangelegenheid verschilt.[6]
De harde koppeling tussen de termijn van informatieverstrekking t.b.v. openbaarheid van bestuur en vernietiging als archivistische verplichting, biedt de facto die begrenzing en bestaat daarom (impliciet) al sinds de inwerkingtreding van de Wob in 1980.

[5] Memorie van toelichting wetsvoorstel Archiefwet 1995

[6] Tweede Kamer, vergaderjaar 1986-1987, 19 859, nr. 3, p.11

Toen is aanvullend op de Archiefwet 1962 in het Besluit algemene secretarie-aangelegenheden rijksadministratie (Stb. 1980, 182) een vernietigingsplicht voor rijksorganen opgenomen. Bij inwerkingtreding van de Archiefwet 1995 is dit besluit komen te vervallen omdat de vernietigingsplicht vanaf dat moment in de wet zelf is verankerd.
De facto is daarmee de vernietigingstermijn van archiefbescheiden de formele demarcatielijn voor Wob-informatieverstrekking. Dit is onder meer terug te zien in diverse rechterlijke uitspraken, zoals in ECLI:NL:RVS:2015:3894, waar de RvS aangeeft dat het niet kunnen verstrekken door een bestuursorgaan van bij Wob-verzoek gevraagde stukken, gebaseerd moet zijn op de in een selectielijst opgenomen vernietigingstermijn en daaruit volgende verklaring van vernietiging.
Consequentie van dit beginsel in de uitvoeringspraktijk is dat zolang geen vernietiging heeft plaatsgevonden, de voor vernietiging in aanmerking komende archiefbescheiden aangemerkt blijven als archiefbescheiden in de zin van de wet. Daarmee zijn archiefbescheiden gedurende hun bestaansduur dus ook altijd onderhevig aan een wettelijk openbaarheidsregime (Wob dan wel AW).

3.5. Vernietiging i.r.t. bescherming persoonsgegevens

Aanvullend op bovengenoemde wettelijke doelen wordt vernietiging ook vaak als maatregel ingezet t.b.v. bescherming van persoonsgegevens, nadat deze gegevens niet meer noodzakelijk zijn voor het primaire verwerkingsdoel. Maar in tegenstelling tot wat vaak gedacht wordt bevat zowel de Wbp als de AVG geen algemene verplichting tot vernietiging.[7]
Naast vernietiging zijn er immers meer mogelijkheden om inbreuk op privacy bij verzameling, verwerking en publicatie van persoonsgegevens te voorkomen.
Denk hierbij aan verwijdering (buiten de actieve administratie plaatsen) van gegevens, dat op basis van jurisprudentie en advisering door de Autoriteit Persoonsgegevens als volwaardig alternatief voor vernietiging mag worden beschouwd.[8,9] Bijvoorbeeld door de aan de gegevens gekoppelde metadata niet meer vindbaar te maken in de reguliere zoekfunctionaliteit en daarmee toegang te beperken tot functioneel beheer.

4. Uitvoeringsproblematiek digitale vernietiging anno 2018

Sinds 1995 hebben de digitale ontwikkelingen een ongekende en destijds onvoorziene vlucht genomen. Overheidsinformatie is exponentieel in volume gegroeid. Het aantal bestandsformaten, de dupliceerbaarheid en uitwisselbaarheid van informatie zijn enorm toegenomen. De keuze tussen vernietigen of bewaren is in dat licht ook minder zwart-wit geworden. De uitvoering van de vernietigingsplicht begint hierdoor te knellen. In de hier volgende paragrafen zal nader op deze problematiek worden ingegaan.

---

[7] Uitzondering hierop bij de AVG is de bepaling in artikel 17 dat de betrokkene het recht heeft van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen in bepaalde gevallen en op individuele basis. Dit wordt ook wel aangeduid als 'het recht om vergeten te worden'.

[8] "Als u de persoonsgegevens niet meer nodig heeft of de bewaartermijn is verlopen, dan moet u de gegevens verwijderen. Dit betekent niet dat u de gegevens altijd moet vernietigen. Het is al voldoende dat u de gegevens buiten het bereik van de actieve administratie brengt en in een archiefdepot of op een aparte schijf opslaat." - College bescherming persoonsgegevens, Informatieblad Bewaartermijnen in uw bestanden, nummer 11A, juli 2012

[9] Jurisprudentie: Gerechtshof Den Bosch 27 mei 2009, ECLI:NL:GHSHE:2009:BI6357, rov. 3.2.5 en Rechtbank Gelderland, 25 april 2016, ECLI:NL:RBGEL:2016:3350, rov. 2.7

4.1. Problematiek i.r.t. informatiebeheer

In de uitvoeringspraktijk zien we aanwijzingen dat de oorspronkelijke business case voor vernietiging, als kostenbesparende maatregel voor informatiebeheer, mogelijk niet langer valide is. Dit heeft enerzijds te maken met de trend dat door schaalvergroting en de snelheid van digitale ontwikkelingen de kosten van storage per TB de afgelopen jaren sterk zijn afgenomen.[10]
Anderzijds kwantificeren informatie-gedreven organisaties steeds vaker hun informatie als activa op hun balans (infonomics), waarbij het goed is om te beseffen dat het business model van techgiganten als Apple, Google en Facebook inmiddels volledig op het toekennen van waarde aan informatie is gestoeld. Bij overheden is de commerciële waarde van informatie uiteraard niet leidend maar moet de kwantificering gezien worden in het licht van maatschappelijke baten (social return on investment) die met langdurige beschikbaarheid van informatie beter gediend kunnen worden.
Aandachtspunt hierbij is dat in het huidige selectiebeleid van het Rijk juist de bulk aan uitvoeringsinformatie die op lange termijn relevant kan zijn voor secundair gebruik (herbruikbare open data, big data – en trendanalyses) en voor de recht- en bewijszoekende burger, gewaardeerd wordt met kortlopende vernietigingstermijnen.[11] Oftewel, de bestaande uitvoeringspraktijk van digitale vernietiging kan in dit licht gezien worden als een vorm van grootschalige kapitaalvernietiging.

Naast het kostenargument kunnen ook vraagtekens gezet worden bij de mate waarin het vernietigingsbeleid momenteel bijdraagt aan het beoogde 'in control' zijn op de eigen informatiehuishouding. Veel compliance-issues worden juist veroorzaakt door de inflexibiliteit van de vernietigingsplicht. De multichannel-dienstverlening en diversiteit van het applicatielandschap maken dat het beheer van archiefbescheiden systeem-overstijgend moet worden gemanaged. Hoewel document management systemen binnen het Rijk inmiddels veelal zijn voorzien van 'by design'-oplossingen die selectie aan de bron regelen, is het bijzonder complex om vernietiging in alle aanpalende informatiesystemen uniform te realiseren. Temeer omdat het voorkomt dat een document in processen met verschillende vernietigingstermijnen gebruikt wordt. De volumes van digitale informatie maken tevens dat handmatige controles om dit probleem te ondervangen volstrekt onuitvoerbaar zijn.
De bevindingen van de Erfgoedinspectie in haar recente onderzoeksrapport 'Wel digitaal, nog niet duurzaam.' bevestigen dit beeld en onderstrepen de urgentie om tot werkbare oplossingen te komen.

Een ander veel voorkomend probleem is dat kopieën van formeel vernietigde archiefbescheiden blijven bestaan buiten het bereik van de actieve beheeromgeving, op persoonlijke schijven en in back-ups. Dat roept de vraag op welke status deze kopieën hebben en in welke mate nog rechten kunnen worden ontleend aan formeel vernietigde archiefbescheiden. Deze helderheid is er op dit moment simpelweg niet.
Ook ontbreekt het overzicht van in sectorale wetgeving vastgelegde vernietigingstermijnen.

---

[10] PWC Eindrapportage Financiële doorlichting DTR 2015, p.11

[11] Zie Generiek Waarderingsmodel Rijksdienst Categorie 10: Uitvoering. Alle uitvoeringsprocessen krijgen default waarderingen minimaal V1 tot maximaal V20 jaar.

Denk hier bijvoorbeeld aan de Wet op de Geneeskundige Behandelovereenkomst (WGBO),de Wet op de Inlichtingen –en Veiligheidsdiensten (WIV) en de Wet Politiegegevens die specifieke termijnen voorschrijven. Een archiefvormer kan hier in zijn selectielijst niet eigenstandig van afwijken, maar het gebrek aan overzicht van toepasselijke wet- en regelgeving maakt het risico op het onrechtmatig toekennen van een andere termijn onnodig groot.

4.2. Problematiek i.r.t. informatieverstrekking

Het gebrek aan 'control' op digitale vernietiging maakt dat ook de bestuurlijke verantwoording onder druk komt te staan; Op het moment dat niet duidelijk is of informatie vernietigd had moeten worden of dat opgedoken duplicaten van formeel vernietigde informatie verstrekt moeten worden, ontstaat het risico van willekeur. Dit doet afbreuk aan het kenbaarheidsbeginsel van selectiebesluiten; De samenleving moet erop kunnen vertrouwen dat de informatie die de overheid over burgers verzameld gebonden is aan kenbare termijnen in een openbaar gepubliceerd en gemotiveerd selectiebesluit, en dat afwijkingen daarvan (zoals t.b.v. hotspots) ook gemotiveerd en gepubliceerd worden. Dat principe staat door de uitvoerbaarheidsproblematiek rond digitale archiefbescheiden in toenemende mate onder druk.

Een goed voorbeeld hiervan is de informatievoorziening i.r.t de zaak Cees H., waar de Minister van VenJ toezegde om een ultieme poging te doen de door de Kamer gevraagde betaalgegevens behorende bij een ontnemingsschikking te achterhalen. Deze informatie bleek in een back-up nog aanwezig te zijn en is uiteindelijk aan de Kamer verstrekt. Omdat in deze specifieke casus de betaalgegevens niet gevonden konden worden in het betreffende ontnemingsdossier, maar daar wel onderdeel van behoorden uit te maken, kon redelijkerwijs gesteld worden dat de informatie onterecht verloren was gegaan. Dat rechtvaardigde de inzet van een back-up, aangezien het doel van een back-up is om bij verlies of beschadiging van gegevens een herstel te kunnen doorvoeren.[12]
Dit roept echter wel de vraag op wat VenJ had moeten doen als de betaalgegevens op de back-up een V-termijn zouden hebben gehad en conform Archiefwet vernietigd waren i.p.v. verloren. Had dan alsnog tot verstrekking moeten worden overgegaan? Back-ups dienen geen archiveringsdoel en bevinden zich dus in een grijs gebied als het gaat om informatieverstrekking. De trend dat back-ups de laatste jaren steeds vaker in zoekvragen op grond van de Wob (t.b.v. de burger) en art. 68 Grondwet (t.b.v. de Kamer) betrokken worden maakt het gebrek aan een helder antwoord erg pregnant.

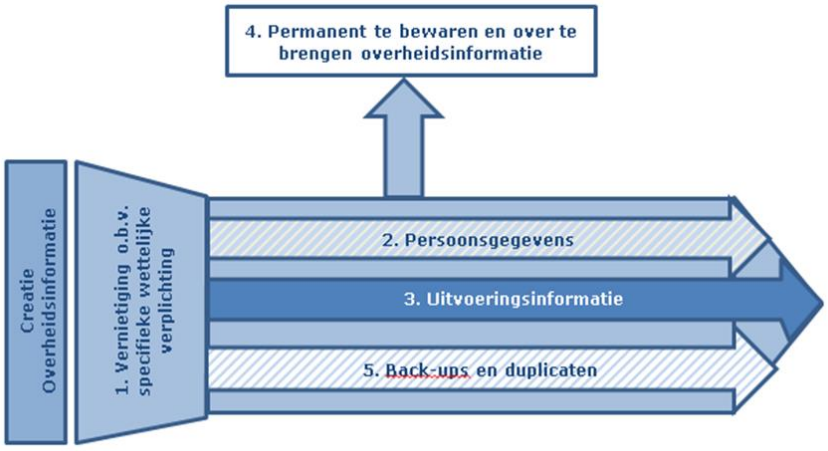
De noodzaak die archiefvormers zien om back-ups te betrekken bij Wob-verzoeken en Kamervragen (als alternatief voor of aanvullend op de primaire informatiesystemen) hangt ook samen met de manco's van het huidige vernietigingsbeleid, dat gericht is op het zo snel mogelijk vernietigen na vervallen van het primaire gebruiksdoel. Secundair gebruik (o.a. t.b.v. bestuurlijke verantwoording) wordt met het huidige beleid slecht gefaciliteerd.
Vernietiging van informatie staat haaks op de verwachtingen van burgers en parlement, die de informatiepositie van de overheid veelal grof overschatten. Het antwoord dat de overheid niet meer over de gevraagde informatie beschikt is in toenemende mate ontoereikend en krijgt snel het stempel 'doofpot' toebedeeld.
In de informatiesamenleving is het immers vanzelfsprekend dat informatie altijd en overal beschikbaar is. Dit leidt ertoe dat de kloof tussen heersende maatschappelijke verwachtingen

[12] Rapport Commissie Oosting deel II, 2016 p.36/37

en de praktijk van de digitale overheid bij een gelijkblijvende toepassing van de vernietigingsplicht, steeds verder zal groeien. Dit erodeert het vertrouwen van burgers en parlement in de informatievoorziening van de overheid.

5. Voorstel verbetermaatregelen

Binnen de door RAI op te leveren uitvoeringskaders kan de vernietigingsplicht *an sich* niet buiten werking worden gesteld, mede gelet op de verankering van het principe in de Archiefwet en de verstrekkende implicaties voor bestuurlijke verantwoording.
Mogelijkheden om binnen de bestaande wettelijke kaders de uitvoeringspraktijk te verbeteren zijn er echter zeker.
In het hier volgende figuur zijn vijf categorieën overheidsinformatie weergegeven. De verbetermaatregelen binnen project Di-stroy zullen met name op deze categorieën gericht zijn. Hierna volgt een toelichting van de interventies per categorie.



Figuur 3: categorieën overheidsinformatie waar interventies Di-Stroy op gericht zijn.

5.1. Informatie met wettelijk bepaalde vernietigingstermijn

Zoals aangegeven bevatten sectorale wetten zoals de WIV, WGBO en Wet Politiegegevens regelmatig harde termijnen voor bewaring en vernietiging van gegevens. Zo staat in artikel 14 van de Wet Politiegegevens de volgende bepaling:

"Politiegegevens verzameld met het oog op de uitvoering van de dagelijkse politietaak (…)worden gedurende een termijn van vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd."

Momenteel ontbreekt echter ieder overzicht van de mate waarin dergelijke expliciete vernietigingstermijnen in wet- en regelgeving voorkomen. Dat maakt het risico op compliance-issues bij vernietiging onnodig groot.

Voorgesteld wordt daarom om een Rijksbrede of overheidsbrede inventarisatie uit te voeren en deze specifieke gevallen vast te leggen in een centraal register. Bij totstandkoming van selectielijsten en de uitvoering van vernietiging kan vervolgens een beroep worden gedaan op dit centrale overzicht.
Als aanvullende maatregel is vereist dat in het Integraal Afwegingskader voor beleid en regelgeving (IAK) de proceswaarborg wordt opgenomen dat bij voorstellen voor het opnemen van nieuwe (of wijziging van bestaande) vernietigingstermijnen in wet- en regelgeving eerst afstemming wordt gezocht met de eigen CIO en de ARA (t.b.v. bewaking van de eenheid van selectiebeleid). Hiermee kan de noodzaak en uitvoerbaarheid van de voorstellen getoetst worden en kunnen nieuwe wettelijke termijnen meteen worden vastgelegd in het register.

5.2. Vernietiging persoonsgegevens

De beschikbaarheid van aan vernietiging gelijkwaardige privacy-waarborgen zoals verwijderen (buiten de actieve administratie plaatsen) en afschermen (onvindbaar maken in centrale zoekfunctionaliteit, pseudonimiseren) van persoonsgegevens, maakt dat de ruimte bestaat om langere vernietigingstermijnen te hanteren die secundair gebruik van deze gegevens beter faciliteren.[13] Deze actielijn lijkt op voorhand kansrijk o.b.v. jurisprudentie, maar met de komst van de AVG zal de juridische haalbaarheid van dit voornemen uitputtend onderzocht moeten worden. Daaruit volgend zal een handreiking digitale vernietiging moeten worden opgesteld die onder meer ingaat op de inzet van beschikbare alternatieve privacy-strategieën, de consequenties voor secundair gebruik en de verantwoording van langere vernietigingstermijnen voor persoonsgegevens in selectielijsten.

Hierbij wordt overigens de advieslijn gevolgd die reeds in 2015 is geschetst door de Raad voor het Openbaar Bestuur en de Raad voor Cultuur in het rapport 'Het Puberbrein van de Overheid':

"Als het systeem aangeeft dat er een gebruikstermijn is verlopen, dan worden de betreffende gegevens ontoegankelijk en onbruikbaar voor de betreffende gebruiker. Pas als alle gebruikstermijnen verlopen zijn en er geen sprake is van een toekomstig (onderzoeks)belang, wordt informatie daadwerkelijk verwijderd en vernietigd."[14]

5.3. Vernietiging uitvoeringsinformatie

Deze categorie overlapt in zoverre met de vorige dat uitvoeringsinformatie ook vaak persoonsgegevens bevat. Reden om deze categorie toch apart te benoemen is dat uitvoeringsinformatie op basis van het huidige selectiebeleid veelal als te vernietigen wordt aangemerkt, ook als er géén privacy-implicaties mee gemoeid zijn[15]. Het is echter specifiek deze categorie informatie die in toenemende mate als open data en ten behoeve van big data-analyses aan langdurige (her)gebruikswaarde wint.

---

[13] Secundair gebruik betreft o.a. gebruik t.b.v. bestuurlijke verantwoording in de zin van de Wob en Art. 68 Grondwet, open data in de zin van de Wet Hergebruik Overheidsinformatie en big data-toepassingen.

[14] Het Puberbrein van de overheid – Raad voor Cultuur & Raad voor het Openbaar Bestuur, 2015, p.43

[15] De selectiedoelstelling van het Nationaal Archief is met name gericht op het kunnen reconstrueren van het overheidshandelen op hoofdlijnen en het reconstrueren van bijzondere gebeurtenissen. Uitvoeringsinformatie wordt slechts beperkt als permanent te bewaren aangemerkt, waarbij het dan vaak gaat om representatieve steekproeven.

Voorgesteld wordt daarom om het Generiek Waarderingsmodel Rijksdienst uit 2012 te herijken, waarbij de default vernietigingstermijnen van uitvoeringsinformatie met secundaire gebruikswaarde worden verlengd van 1 tot 20 naar 50 tot 100 jaar.[16] Dit komt feitelijk neer op semi-permanente bewaring, zonder overbrenging, binnen de eigen beheeromgeving. Uiteraard hebben archiefvormers de flexibiliteit om naar behoefte van deze default-waarderingen af te wijken in hun eigen selectielijst. De maatregel biedt dus sowieso meer flexibiliteit maar moet ook nadrukkelijk worden gezien als een principiële beleidswijziging, waarbij het uitgangspunt verschuift van 'vernietigen, tenzij' naar 'niet vernietigen, tenzij'.
Implementatie van dit voornemen vereist een goede kosten-batenanalyse, waarbij de meerwaarde van langdurige beschikbaarheid van informatie moet worden afgezet tegen de extra beheer- en storagekosten. In dit verband zal ook gekeken moeten worden naar de kostenimplicaties i.r.t. duurzame toegankelijkheid van de informatie.

5.4. Permanent te bewaren/ over te brengen informatie

Aandachtspunt bij permanent te bewaren informatie is dat de Archiefwet impliceert dat informatie niet op twee plekken onder twee zorgdragers (lees: de archiefvormer en de archiefinstelling) tegelijkertijd kan bestaan. In het licht van de eerste digitale overbrengingen die momenteel plaatsvinden worden de ketenpartners echter wel voor dit vraagstuk geplaatst. Nadere afspraken en waarborgen t.b.v. authenticiteit en control zijn in dit verband noodzakelijk. Nationaal Archief en IND voeren hiertoe inmiddels ook al een onderzoek uit waarvan de resultaten mogelijk generiek toepasbaar kunnen worden gemaakt.[17]
De kansen die 'hashing'[18] biedt om de integriteit van documenten te valideren maken hier prominent onderdeel van uit; Elk in DMS aangemaakt document beschikt namelijk conform Toepassingsprofiel Metagegevens Rijksoverheid over een checksum als onderdeel van de technische metadata.
Dit is de digitale equivalent van een vingerafdruk; Een identiek duplicaat van een document zal exact dezelfde checksum-code hebben, maar bij wijziging van slechts één letter verandert de code ook. Dit biedt (vooralsnog onbenutte) mogelijkheden om integriteit en authenticiteit van stukken op verschillende plaatsen (bij archiefvormer en archiefinstelling) te waarborgen.

5.5. Vernietiging back-ups en duplicaten

Bovengenoemde onderzoekslijn biedt ook kansen voor het technisch faciliteren van vernietiging. De frequentie van back-ups en het gemak van dupliceerbaarheid van informatie maakt dat van de meeste digitale archiefbescheiden binnen de informatiehuishouding meerdere kopieën bestaan. Als een document vervolgens formeel vernietigd wordt binnen het DMS, is de kans reëel dat duplicaten ervan buiten de actieve beheeromgeving, op persoonlijke schijven of in back-ups, nog blijven bestaan. Het is dan ook wenselijk om hier een full-proof systeem-overstijgend controlemechanisme voor in te richten.

---

[16] De implicaties t.a.v. digitaal beheer verschillen per organisatie en per informatiecategorie. De DUTO-eisen bieden hier handvatten voor maar hebben geen algehele verplichtende werking. Bredere adoptie van DUTO-kwaliteitseisen is in het licht van de geschetste beleidswijziging wel zeer aan te bevelen.

[17] Het Nationaal Archief en de IND gaan in 2018 een onderzoek uitvoeren n.a.v. digitale overbrenging van de afgesloten IND-dossiers t/m 2010. Afgesproken is dat gedurende de looptijd afstemming met project Di-Stroy zal plaatvinden om de samenhang in oplossingsvoorstellen te bewaken.

[18] Hashing-techniek wordt gebruikt voor fixity checks, dat zijn handmatige of geautomatiseerde checks om te bepalen of een document bedoeld of onbedoeld gewijzigd is.

D.m.v. geautomatiseerde systeem-overstijgende vergelijkingen van checksums van bestanden zouden de exacte kopieën van documenten buiten het DMS geïdentificeerd kunnen worden en gelijktijdig met het primaire bestand vernietigd kunnen worden. Dit draagt in grote mate bij aan de uitvoerbaarheid van de vernietigingsplicht en AVG-compliance (vooral in gevallen waar sprake is van keten- of netwerksamenwerking en/of het principe van eenvoudige creatie, meervoudig gebruik leidend is). Binnen het project wordt voorzien in oplevering van een proof of concept, als onderdeel van een brede verkenning van technische beheersmaatregelen die digitale vernietiging beter kunnen faciliteren. Denk in dit verband bijvoorbeeld ook aan evt. aanvullende metadata-vereisten en de mogelijkheid om deze geautomatiseerd toe te kennen, by design en achteraf.

De status van back-ups i.r.t. de vernietigingsplicht vereist tevens meer helderheid. Het maken van back-ups is een op zichzelf staande verplichting ten behoeve van informatiebeveiliging en dient als zodanig geen direct archivistisch –en of verantwoordingsbelang.
Het ontbreken van specifieke bepalingen voor back-ups in archiveringsregels maakt dat er momenteel een risicovolle interpretatievrijheid bestaat. Voorgesteld wordt om in de Baseline Informatiebeveiliging Rijksdienst (BIR) t.a.v. het creëren van back-ups de volgende bepalingen op te nemen:

- Houdt bij het bepalen van de bewaarduur van de back-up rekening met de aard van de gegevens die erop worden bewaard en de mate waarin deze onderhevig zijn aan vernietiging zoals bepaald in uw selectielijst.
- Nadat de noodzaak tot behoud t.b.v. informatiebeveiliging is vervallen dient de back-up zo snel mogelijk overschreven te worden.
- Bij terugplaatsing van een back-up valt de daarop bewaarde informatie onder de werkingssfeer van de Archiefwet en moet dientengevolge geïnventariseerd worden of de back-up formeel reeds vernietigde informatie bevat. Als dit het geval is dient deze informatie zo snel mogelijk na terugplaatsing conform selectielijst vernietigd te worden.

In het openbaarheidsbeleid Rijk kan daarnaast worden opgenomen dat back-ups vanuit hun specifieke doelbinding aan informatiebeveiliging in de regel niet betrokken zullen worden in informatieverstrekking. Een duidelijke begrenzing draagt in grote mate bij aan compliance van AVG en Archiefwet.

Dit voorkomt immers dat formeel vernietigde informatie toch weer verstrekt kan worden, waarmee het risico op datalekken wordt beperkt en een harde waarborg wordt geboden voor het kenbaarheidsbeginsel van selectiebeslissingen. De juridische haalbaarheid van deze maatregel i.r.t. het documentbegrip in de Wob vereist nader onderzoek.

6. Eindbeeld

Na oplevering en implementatie van de maatregelen is compliance aan de vernietigingsplicht voor digitale bestanden naar verwachting een stuk beter uitvoerbaar. Het vernietigingsbeleid is gemoderniseerd en toekomstbestendig. Tevens is de informatiehuishouding met deze maatregelen beter ingericht op secundair gebruik van archieven en beter in lijn met maatschappelijke verwachtingen, waardoor belangen als verantwoording, openbaarheid van bestuur, open data en big data-analyse beter kunnen worden gediend.