

Vernietigingsbeleid Omgevingsdienst Twente 1.0

Kaders en richtlijnen voor digitale vernietiging

Managementsamenvatting

Onderdeel van het beheren van informatie is het tijdig vernietigen van informatie. Het Nationaal Archief geeft duidelijke richtlijnen over hoe openbare lichamen digitale vernietiging kunnen inbedden in de eigen organisatie en geeft aan met welke elementen we rekening moeten houden. Maar waarom vernietigen we eigenlijk informatie? Ten eerste zijn we daartoe verplicht vanuit regelgeving en hebben we ons te houden aan de Archiefwet, de Algemene verordening gegevensbescherming, de Wet open overheid en de Baseline Informatiebeveiliging Overheid. Ten tweede zijn er voordelen aan verbonden. Informatie kan sneller gevonden worden, systemen en daarmee ook het milieu worden minder belast en de kosten voor beheer zijn lager. Maar wat betekent digitaal vernietigen nou eigenlijk? Digitaal vernietigen wil zeggen dat informatie niet meer vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar is. Enkel moet te herleiden zijn dat de informatie ooit heeft bestaan. Om (digitale) vernietiging te bewerkstelligen heeft de OD Twente maatregelen genomen. Zo hanteren we landelijke selectielijsten voor gemeenten en de provincie. Bewaartermijnen zijn gekoppeld aan de zaaktypecatalogus waarin een doorvertaling is gemaakt op productniveau. Zodoende is een bewaartermijn gekoppeld aan het gekozen resultaat van een afgesloten zaak/dossier. Binnen de OD Twente volgen we daarnaast regels en uitgangspunten voor vernietiging. Daarin wordt duidelijk gemaakt wie welke verantwoordelijkheden heeft binnen het vernietigingsproces en wanneer, waar en hoe digitaal vernietigd moet worden. In het vernietigingsprotocol zijn de rollen, verantwoordelijkheden en activiteiten nader uitgeschreven, waarbij tot in detail beschreven is welke stappen doorlopen moet worden. Om te toetsen of de vernietiging volgens beleid en protocol zijn uitgevoerd worden periodiek kwaliteitscontroles uitgevoerd op het vernietigingsproces. In dit vernietigingsbeleid is verder gespecificeerd welke informatie voor vernietiging in aanmerking komt. Daarin zijn bepalingen opgenomen wat betreft reikwijdte, type informatie, vernietigingswijze, wanneer vernietiging plaatsvindt, de wijze van verantwoording en de verwijzing naar het vernietigingsprotocol. Bij het vernietigen van informatie is ook rekening gehouden met het vernietigen van kopiëstukken, back-ups en recovery's.

2 Inleiding

2.1 Handreiking digitaal vernietigen Nationaal Archief

De handreiking digitaal vernietigen van het Nationaal Archief is de basis voor dit document. Op meerdere plaatsen hebben we citaten opgenomen vanuit de handreiking Digitale vernietiging, omdat de tekst duidelijk en verhelderend is en een goede basis geeft voor het beleid dat de Omgevingsdienst Twente (OD Twente) wil hanteren.

2.2 Waarom digitaal vernietigen

Vernietiging van (digitale) archiefbescheiden (lees ook: informatieobjecten) is enerzijds een verplichting vanuit de Archiefwet en heeft raakvlakken met andere wettelijke verplichtingen die geschetst zijn in de Wet open overheid (Woo), Wet algemene verordening persoonsgegevens (AVG) en Baseline Informatiebeveiliging Overheid (BIO). Naast wettelijke verplichtingen, worden de voordelen benoemd die (digitale) vernietiging met zich meebrengt.

2.3 Wet- en regelgeving

Vanuit verschillende wet- en regelgeving wordt gesproken over vernietiging van informatie in informatieobjecten, over vernietiging van informatieobjecten en vernietiging van dragers van informatieobjecten.

2.3.1 Archiefwet- en Archiefbesluit 1995

De Archiefwet is van toepassing op alle overheidsorganisaties. De wet stelt eisen aan het beheer en de toegang van overheidsinformatie. Het verplicht alle overheidsorganisaties om hun (digitale) overheidsinformatie, in de vorm van archiefbescheiden, waarvan de bewaartermijn is verstreken en die niet van vernietiging is uitgezonderd, te vernietigen.

AW Art. 3: Verplicht overheidsorganen zorg te dragen voor vernietiging van 'onder hen berustende' en 'daarvoor in aanmerking komende' archiefbescheiden.

AW Art 5. lid 1: De zorgdrager is verplicht tot het ontwerpen van selectielijsten waarin tenminste wordt aangegeven welke archiefbescheiden voor vernietiging in aanmerking komen.

AW Art. 7: De zorgdrager is bevoegd archiefbescheiden te vervangen door reproducties, teneinde de aldus vervangen bescheiden te vernietigen.

Het bovenstaande wetsartikel wordt geregeld met het vaststellen van het vervangingsbesluit. Met het nemen van het vervangingsbesluit is de OD Twente voornemens 100% digitaal te werken en daarmee enkel digitale vernietiging te regelen.

AB Art. 8: De zorgdrager maakt een verklaring op van de vernietiging, die ten minste een specificatie van de vernietigde archiefbescheiden bevat, alsmede aangeeft op grond waarvan en op welke wijze de vernietiging is geschied. Een exemplaar van deze verklaring wordt bewaard door het overheidsorgaan waaronder de archiefbescheiden zouden berusten, indien deze niet waren vernietigd.

Voor blijvend te bewaren digitale overheidsinformatie geldt dat de Archiefwet impliceert dat bij overbrenging naar een archiefbewaarplaats, ook de kopieën bij de archiefvormer worden vernietigd.

2.3.2 Wet open overheid

De Wet open overheid (Woo) is van toepassing op overheidsinformatie die niet is overgebracht. Informatie die op grond van een vastgestelde selectielijst is vernietigd, kan op grond van de Woo niet opgevraagd of actief openbaar worden gemaakt. Het tegenovergestelde geldt ook: informatie die op grond van de Archiefwet zou moeten zijn vernietigd of overgebracht, maar desondanks nog bij de overheidsorganisatie berust, moet bij een Woo-verzoek gewoon (al dan niet gelakt) openbaar worden gemaakt aan de indiener. Dat kan in sommige gevallen leiden tot imago- en financiële schade. Wanneer je kunt aantonen dat bepaalde informatie rechtmatig is vernietigd, dan valt dit niet onder de plicht tot openbaarmaking.

2.3.3 Algemene verordening gegevensbescherming

De Algemene verordening gegevensbescherming stelt verplichtingen aan organisaties bij het verwerken van persoonsgegevens. Het vernietigen van informatie is één van de verplichtingen om te voorkomen dat persoonsgegevens onrechtmatig worden gebruikt. Daarbij is het uitgangspunt dat een organisatie persoonsgegevens vernietigt wanneer deze niet meer nodig zijn voor het doel waarvoor ze zijn verzameld of worden gebruikt. Het is mogelijk om bepaalde persoonsgegevens uit te zonderen van vernietiging, bijvoorbeeld voor historische, statistische of wetenschappelijke doeleinden. Het niet naleven van de AVG kan leiden tot een boete.

2.3.4 Baseline Informatiebeveiliging Overheid

Sinds 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht voor het Rijk, gemeenten, waterschappen en provincies. De BIO heeft onder andere tot doel om het onbevoegd openbaar maken, wijzigen, verwijderen of vernietigen van informatie die op media is opgeslagen te voorkomen. Het tijdig en juist vernietigen van informatie die daarvoor in aanmerking komt verkleint de risico's ten aanzien van informatiebeveiliging, omdat het dan niet meer in de verkeerde handen kan vallen. Security incidenten, zoals datalekken, kunnen optreden doordat digitaal vernietigen van vertrouwelijke informatie niet (goed) is uitgevoerd.

2.4 Voordelen van vernietiging

In het artikel 'Alles bewaren? Beter van niet'¹ wordt een opsomming gemaakt van redenen om wel te vernietigen, naast de al geldende wet- en regelgeving: • De kans neemt toe dat de juiste informatie naar voren komt bij een zoekvraag. Bij een Woo-verzoek betekent dit bijvoorbeeld lagere administratieve lasten. Er wordt minder doorzocht, minder beschikbaar gesteld en daarmee ook minder geanonimiseerd.

- Doordat de volumes niet meer zo groot zijn, draaien back-ups sneller en efficiënter. Hier zijn lagere kosten mee gemoeid.
- Kleinere rapportages zorgen voor minder kans dat het informatiesysteem vastloopt of langzaam draait voor de zaakbehandelaren tijdens het opvragen van een rapportage.
- (Toekomstige) conversie- en migratietrajecten zijn minder complex en minder kostbaar.
- Kostenbesparing en milieu. De enorme toename aan digitale overheidsinformatie die organisaties verzamelen leidt tot een steeds groter wordende vraag naar opslag. Wanneer digitaal vernietigen niet is geïmplementeerd, wordt de opslagcapaciteit deels besteed aan informatie die je niet meer nodig hebt.

Onderzoek wijst uit dat de ICT sector qua CO₂-uitstoot in 2020 al even vervuilend was als de mondiale jaarlijkse brandstofgebruik van alle vliegtuigen bij elkaar. Dit is evenveel als 1,4% van de wereldwijde CO₂-uitstoot. Sinds 2020 heeft ICT niet stilgestaan². Naast CO₂-uitstoot is recentelijk ook meer aandacht gekomen over het watergebruik van datacentrales, om onder andere de koeling van servers te waarborgen. Met de klimaatcrisis ontstaat steeds meer schade (in Nederland) door onnatuurlijke hoog- en

1) Artikel Bewaren beter van niet - Od special vernietigen_0.pdf (nationaalarchief.nl)

2) De tweesnijdende rol van ICT in de transitie naar een duurzame samenleving | M&I/Partners (mxl.nl)

laagwaterstanden. Koeling van datacentrales gebeurt door water en het gebruik is hoog in de zomer op het moment dat waterstanden laag zijn.

3 Wat is digitaal vernietigen?

Vernietigen van informatie is het blijvend ontoegankelijk maken van die informatie, waardoor deze niet meer vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar is. Digitaal vernietigen betreft digitale overheidsinformatie, ongeacht de vorm en met behoud van metagegevens over de vernietiging.

NEN-ISO 15489-1:2016 over vernietigen: ISO 15489-1 beschrijft vernietigen als een ‘proces van verwijderen of wissen van een archiefstuk zonder dat deze gereconstrueerd kan worden’.

Digitale overheidsinformatie is er in vele vormen zoals tekstdocumenten, presentaties, spreadsheets, video's, foto's, (chat) berichten, e-mails, gegevenssets in databases, etc. Deze vormen van overheidsinformatie, die samengesteld zijn uit een verzameling van aan elkaar gerelateerde data of gegevens die als eenheid worden behandeld, noemen we informatieobjecten³.

Bij digitaal vernietigen is soms sprake van het risico dat de vernietigde informatieobjecten toch nog toegankelijk kunnen zijn. In welke mate dit acceptabel is voor een overheidsorganisatie, hangt af van het doel waarmee de informatieobjecten vernietigd zijn. Bijvoorbeeld of het om privacyreglementen of het beperken van ballast gaat. Elk doel vraagt om een andere vorm van vernietiging. Van drastische maatregelen (waarbij ook back-ups en informatiedragers worden vernietigd) tot een lichtere vorm van vernietiging. Met een risicoanalyse⁴ bepaal je wat de passende maatregelen zijn. Zie hiervoor ook hoofdstuk 6.5.

3.1 Gradaties van vernietiging

Gradaties	Uitleg
Administratief vernietigen	Geschikt voor informatieobjecten waar vernietiging weinig tot geen risico's met zich meebrengt. Hierbij verwijder je de verwijzingen naar het te vernietigen informatieobject (uit de indexen) en wordt de ruimte die het informatieobject op de drager inneemt vrijgegeven voor hergebruik.
Eenmalig overschrijven	Indien er sprake is van een risico dat te overzien is, kan worden gekozen voor het eenmalig overschrijven van de informatieobjecten op de drager waarop deze zijn opgeslagen.
Meervoudig overschrijven	Indien er sprake is van grotere risico's (bijvoorbeeld in het kader van de AVG of de BIO) kan worden gekozen voor het meervoudig overschrijven van informatieobjecten op de drager waarop deze zijn opgeslagen.
Fysiek vernietigen	In sommige gevallen (bij een zeer hoog risico, zoals vertrouwelijke en staatsgeheime informatieobjecten) kan worden gekozen om de drager van de informatieobjecten fysiek te vernietigen.

Moreq2010 over vernietigen: De Moreq2010 maakt onderscheid tussen vernietigen en deleten van informatie. Er is sprake van deleten wanneer alle sporen van een informatieobject zijn verwijderd. Bij digitaal vernietigen is er sprake van een overblijfsel van het informatieobject dat bewijst dat dit er ooit was. De inhoud van de informatie is er dan niet meer, maar alleen nog het bewijs van het feit dat de informatie is vernietigd.

Let op: Verwijderen, wissen of deleten valt alleen binnen de werkdefinitie van vernietigen wanneer de informatie overal onherroepelijk wordt vernietigd. Het is daarom belangrijk ook eventuele kopieën op back-ups en in informatiesystemen te vernietigen, zodat de informatie niet kan worden hersteld.

3.2 Alternatieven voor vernietiging?

Het Nationaal Archief beschrijft uitvoerig alternatieve wijzen van vernietiging, maar deze worden hier slechts summier opgesomd, omdat het niet voldoet aan de eisen die de archiefwet voorschrijft en **voor de OD Twente dus geen alternatief zijn**. Door de alternatieven wel te noemen is het makkelijker risico's in kaart te brengen en uitvraag te doen bij leveranciers over wat zij precies onder vernietiging verstaan. Hierover moet geen misvatting bestaan en leveranciers dienen voor hun vernietigingsfunctionaliteit altijd te voldoen aan de eisen zoals geformuleerd in het vernietigingsbeleid van de OD Twente.

3) [Informatieobject | Nationaal Archief](#)

4) [Hoe kun je digitaal vernietigen? | Nationaal Archief](#)

Verbreken van koppelingen: Door de verwijzingen naar informatieobjecten te verwijderen, verliezen deze hun toegankelijkheid, context en informatiewaarde. De losse informatieobjecten zelf blijven bestaan, maar zijn voor geen enkele toepassing meer vindbaar en beschikbaar.

Beëindigen van het beheer: Dit betekent het bewust niet meer actief beheren van informatie in één of meer systemen die deel uitmaken van het applicatielandschap. Bijvoorbeeld omdat de risico's laag zijn en de kosten voor vernietigen hoog zijn. Het gaat hierbij niet om het applicatie- of technische systeembeheer, maar om het informatiebeheer. Dit leidt ertoe dat de duurzame toegankelijkheid niet gegarandeerd kan worden en dat de informatie door de tijd heen steeds minder toegankelijk wordt.

Pseudonimiseren of anonimiseren: In het geval van privacybelang wordt maskeren in de vorm van pseudonimiseren of anonimiseren toegepast bij de beschikbaarstelling van informatieobjecten. Bij pseudonimiseren worden persoonsgegevens gemaskeerd door codering. Alleen als je de juiste sleutel hebt, kun je de gemaskeerde persoonsgegevens achterhalen. Bij anonimiseren worden persoonsgegevens op zodanige wijze gemaskeerd dat ze op geen enkele manier te reconstrueren en met een persoon in verband te brengen zijn.

4 Maatregelen voor digitaal vernietigen

4.1 Selectielijst

De OD Twente hanteert de selectielijst 2020 voor gemeenten en provincies. Er is een doorvertaling gemaakt van zaak- en (sub)producttypes waarbij de OD Twente de landelijke zaaktypecatalogus (ZTC) van de Vereniging Nederlandse Gemeentes (VNG) volgt. De OD Twente is aangesloten bij projectgroep Pleio om actief verbeteringen aan te leveren voor de landelijke doorontwikkeling van de ZTC, de corresponderende naamgeving van resultaten en de bewaartermijnen die daaronder hangen en houdt hier rekening mee in de jaarlijkse producten- en dienstencatalogus (PDC).

4.2 Beleid

Het beleid voor digitaal vernietigen is onderdeel van het beleid voor informatiebeheer, zoals vastgelegd in de bewaar- en beheerstrategie. In dit vernietigingsbeleid zijn de uitgangspunten voor digitaal vernietigen vastgelegd:

1. Er zijn 'By-design-maatregelen' voor digitale vernietiging. Door de principes van 'archiving by design' in een aanbesteding te integreren, kan de OD Twente de eisen voor duurzame toegankelijkheid meegeven aan potentiële leveranciers⁵. (Een aanbesteding is dus een mooie kans om ook de functionele eisen ten aanzien van digitaal vernietigen mee te nemen in de selectie van een nieuwe applicatie⁶;
2. Bij het vernietigen wordt het vernietigingsprotocol toegepast, zie hoofdstuk 5.6;
3. Het is duidelijk welke wijze van vernietigen wordt gehanteerd. De OD Twente leunt hiervoor op de afspraken over vernietiging zoals vastgesteld door de leverancier. De leverancier verantwoordt zich hierover door middel van de NEN-ISO certificering. Zie ook fig. 7.1. 'Flowchart afvoer ICT middelen';
4. Het doel van digitaal vernietigen is te voldoen aan wetgeving. Daarnaast benut de OD Twente voordelen voor beheer, milieu, gebruik en overbrenging, zie hoofdstuk 3;
5. Welke middelen voor digitaal vernietigen beschikbaar zijn, zie hoofdstuk 5.3;
6. Het beoogde tijdspad voor de implementatie en uitvoering van digitaal vernietigen, zie hoofdstuk 5.6;
7. De teammanager is verantwoordelijk voor een juiste en zorgvuldige vernietiging van informatie binnen zijn of haar team/proces en/of informatiedragers en/of informatieomgeving;
8. De eigenaar van informatiedragers en informatieomgevingen is verantwoordelijk voor een juiste en zorgvuldige vernietiging of uitfasering daarvan;
9. Het team Informatiebeheer heeft een bewakende, signalerende en toetsende rol bij het uitvoeren van de jaarlijkse vernietiging;
10. Het team Informatiebeheer geeft advies over de vernietigingsprocedure en de implementatie ervan;
11. Voor vernietiging worden altijd de generieke procedures gehanteerd;
12. Alle activiteiten in het vernietigingsproces worden bijgehouden in het daarvoor opgestelde logboek;
13. De vernietigingslijsten dienen te voldoen aan het principe van 'dataminimalisatie' waarbij het doel is te bewijzen dat informatie is vernietigd;
14. Voorafgaand aan de vernietiging hebben de noodzakelijke/verplichte toetsingen en controles plaatsgevonden en heeft de archivaris toestemming gegeven voor de vernietiging, in de vorm van een opgestelde akkoordverklaring;

5) Zie ook de [werkgroep Archiving by design](#)

6) Lees meer over [requirements voor vernietiging](#)

15. Van de vernietigde informatie wordt een samengestelde vernietigingslijst opgesteld en gearchi-veerd;
16. Het uitgangspunt is dat informatie tijdig wordt vernietigd, dat wil zeggen binnen een jaar na het verstrijken van de vernietigingstermijn.

4.3 Mensen, middelen en verantwoordelijkheden

4.3.1 Mensen en hun verantwoordelijkheden in het proces

Om in kaart te brengen welke actoren (medewerkers en teams) op welk verantwoordelijkheidsniveau betrokken zijn in het vernietigingsproces maken we gebruik van het RACI- model. Het RACI-model beantwoordt de vraag: wie doet wat? Door gebruik te maken van het RACI-model wordt duidelijk wie verantwoordelijk is voor welke taak, wie bij de taakuitoefening geïnformeerd dienen worden, aan wie vragen kunnen worden gesteld voor de uitoefening van de taak en wie eindverantwoordelijk is voor het proces. De letters in het RACI-model staan dus voor:

- Responsible: Verantwoordelijk voor de taakuitvoering.
- Accountable: Eindverantwoordelijke, zorgt dat de taak uit is gevoerd.
- Consulted: Ter consultering bij het uitoefenen van de taak.
- Informed: Deze actoren dienen geïnformeerd te worden dat de taak is uitgevoerd.

In sommige modellen komt de 'S' van 'support' voor, maar dat is niet specifiek relevant in het vernietigingsproces waar een consult ook een bevraging kan zijn. Binnen het RACI-model is altijd één eindverantwoordelijke (A) en een verantwoordelijke voor het uitvoeren van de taak (R). Het is niet verplicht om de te consulteren actoren (C) om een consult te vragen, maar deze actoren staan hier wel altijd voor klaar. Alle te informeren actoren (I) moeten daadwerkelijk geïnformeerd worden. Dit is niet optioneel, zoals bij de te consulteren rol. Onderstaand het verantwoordelijkheidsschema volgens het RACI- model:

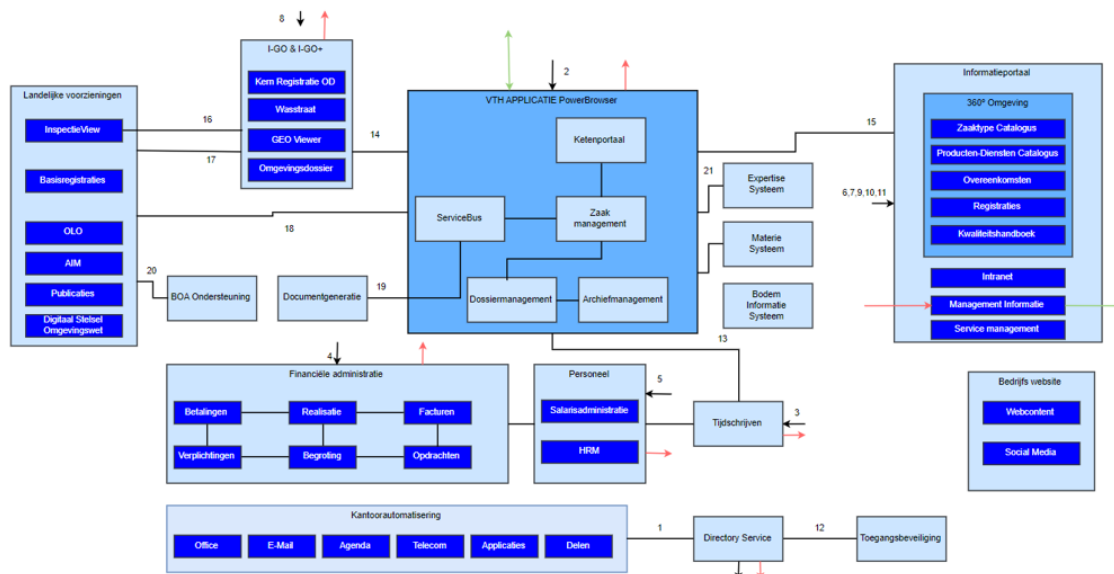
RACI- model	Di-rec-teur	Teamma-nager Bedrijfs-voering	Re-cord-mana-ger	Infor-matie-adviseur	Kwali-teits- en gege-vensbe-heerder	Team Infor-matie-beheer	Team-ma-gers/pro-ceseige-naren	Ar-chi-varis	Functi-oneel Be-heer	Gehele organi-satie
Vernietigingsplan	-	A/I	R	C	C	R	I	I	I	-
Vernietigingslijsten	-	A	R	C	C	R	-	-	-	-
Lijsten controleren	-	A	C	C	C	C	R	R	-	-
Akkoord op lijst	I	A/I	R	I	I	R	I	I	I	I
Vernietiging	-	A	R	I	I	I	-	-	I	-
Verklaring opstellen	-	A	R	C	C	R	-	-	-	-
Verklaring tekenen	R	A	I	I	I	I	-	-	-	-
Archiveren	I	A	C	C	R	R	I	I	I	I
Eindcontrole	-	A	I	C	R	R	-	-	-	-

4.3.2 Middelen

Ieder jaar worden de verwachte kosten voor het vernietigen opgenomen in de jaarlijkse begroting. Ook in de meerjarenbegroting wordt vernietiging meegenomen als onderdeel van opgenomen lasten onder het onderdeel 'informatiebeheer'. Het vernietigingsproces wordt zodoende opgenomen in de planning- en controlcyclus.

4.4 Overzicht van informatieobjecten, processen, informatiesystemen en hun samenhang

Bij de OD Twente is met name voor het primaire proces een overzicht gecreëerd door het maken van een referentiearchitectuur, zie het onderstaande figuur 1.1.



Figuur 1.1. Referentiearchitectuur

Echter is de architectuurplaat voor de bedrijfsondersteuning niet in detail beschreven. In de online handleiding van de OD Twente, de WIKI, staat het volgende over applicaties in het secundaire proces.

Procesondersteuning van het secundaire werk

Functionaliteit: Dit zijn meerdere applicaties die veelal geordend zijn naar bedrijfsfuncties als Inkoop, Financiën, Personeel, Facilitaire Zaken. Daarnaast is er vaak een aparte applicatie die de ondersteuning levert voor het opmaken van de begroting, het bijstellen van de begroting, het rapporteren van de voortgang van de uitvoering en het verantwoorden middels een jaarrekening en jaarverslag. Kortom: deze applicatie ondersteunt de uitvoering van Planning & Control cyclus. In deze applicatie hoort ook thuis: het productgericht plannen en verantwoorden van het ingezette volume aan personeel (tijdregistratie) en financiën (budgetregistratie en financiële administratie van de realisatie).

Naast de opslag van informatie(objecten) in zaakdossiers binnen het zaakstelsel PowerBrowser (ODie) moeten we ook denken aan opslag van (kopieën van) informatieobjecten op onder andere:

- E-mail
- Schijf
- Website
- Ibabs
- Microsoft Teams
- AFAS
- NAZCA

4.5 Risicoanalyse

De OD Twente voert voor het opstellen van een vernietigingslijst een risicoanalyse uit op basis van kwaliteit van het ingevulde resultaatveld. Bij zaaktypes en producttypes waarbij onvoldoende zeker is of het juiste resultaattype is meegegeven zondert de OD Twente deze zaken uit van vernietiging. Daarnaast draagt de organisatie er zorg voor dat maatregelen genomen worden om de kwaliteit te verbeteren en zo voldoende zekerheid te geven voor het opnemen van de records voor opvolgende vernietigingslijsten.

Zoals beschreven in hoofdstuk 3.2. hanteert de OD Twente geen alternatieve wijzen voor vernietiging en daarvoor wordt de risicoanalyse dan ook niet ingezet.

4.6 Vernietigingsprotocol

Bij het daadwerkelijk overgaan tot digitaal vernietigen volgt de OD Twente haar vernietigingsprotocol. Daarin zijn belangrijke en heldere afspraken gemaakt. Welke activiteiten moeten op welk moment worden uitgevoerd? En door wie? In het vernietigingsprotocol verantwoordt de OD Twente hoe ze informatie vernietigen. Het vernietigingsprotocol beschrijft een vaste en rigide werkwijze. Het biedt weinig

flexibiliteit, zodat meer duidelijkheid bestaat over de te volgen stappen en de werkwijze ook beter gecontroleerd kan worden middels audits. De OD Twente gaat dus uit van een 'strikte aanpak'.

In het vernietigingsprotocol is vastgelegd:

1. Wat de rollen en verantwoordelijkheden zijn;
2. Wat de beslismomenten zijn en hoeveel tijd er is om te beslissen;
3. Welke activiteiten in welke volgorde dienen te worden uitgevoerd;
4. Welke controlemomenten er zijn;
5. De wijze waarop verantwoording over de digitale vernietiging wordt afgelegd;
6. Dat een review plaatsvindt van te vernietigen informatie.

4.7 Vernietigingsfunctionaliteit

Het uitgangspunt voor vernietiging is dat een vernietigingsfunctionaliteit aanwezig moet zijn en het moet helder zijn wat dit inhoudt. De leverancier toont dit aan doormiddel van de certificering NEN-ISO 16175:2020.

4.8 Kwaliteitsmanagement en toezicht

Beleid, procedures en protocollen met betrekking tot digitaal vernietigen moeten zijn vastgelegd in een systeem, waarin de kwaliteitszorg voor deze instrumenten is geborgd. Met audits en intern toezicht, in de vorm van monitoring en rapportage, wordt nagegaan of beleid, procedures en protocollen correct worden toegepast. Ook wordt gecontroleerd of deze periodiek geactualiseerd worden, actueel zijn in de uitvoering en op de agenda worden gehouden. De rapportages met betrekking tot digitaal vernietigen dienen te worden geagendeerd in het strategisch informatieoverleg (SIO). Ook dienen de rapportages opgenomen te worden in de plan – do – check – act (PDCA)-cyclus zoals beschreven in het kwaliteits-handboek.

5 Stappenplan digitaal vernietigen

5.1 Reikwijdte en plaats van vernietiging

Digitale vernietiging vindt plaats in de bronapplicatie waar de 'originale exemplaren' zijn opgeslagen. Voor de OD Twente betekent dit alle zaken met een bewaartermijn, waarvan de bewaartermijn overschreden is. Bij het vernietigen worden ook alle kopieën en back-ups vernietigt.

Voor het bepalen van waar kopieën zich kunnen bevinden wordt gekeken naar de procesbeschrijvingen zoals die in de WIKI staan. Behandelaren en teammanagers zijn verantwoordelijk voor de goede naleving van de beschreven procedures en zien erop toe dat iedereen alle kopieën vernietigt van de bestanden die op de vernietigingslijst staan. Dit betekent voor behandelaren een handmatige actie op de eigen schijf, e-mailbox, Teams omgeving en/of andere applicaties die gebruikt worden voor de (niet daarvoor bestemde) opslag van informatieobjecten.

5.2 Bepaling object van vernietiging

Er wordt te allen tijde vernietigt op dossier/zaakniveau. Dit betekent dat alle documenten en de daarbij horende metadata die in een zaak opgeslagen zijn gelijktijdig worden vernietigd. Het gekozen zaak- en producttype genereren resultaatmogelijkheden waar een bewaartermijn voor geldt, deze is op basis van de classificatie en op basis van de gemeentelijke en provinciale selectielijst(en) die gelden voor de te vernietigen zaken.

5.3 Bepaling van de wijze waarop vernietiging plaatsvindt

Bij het vernietigen maakt de OD Twente gebruik van de vernietigingsfunctionaliteit die geïntegreerd is in PowerBrowser.

5.4 Bepaling van het moment waarop vernietiging plaatsvindt

Ieder kwartaal wordt een vernietigingsronde doorlopen, waarbij de vernietiging van informatieobjecten plaatsvindt aan het eind van ieder kwartaal. Dit moment wordt tevens gecommuniceerd met alle deelnemers middels een communicatiekanaal. Bij de bepaling van het moment van vernietiging wordt rekening gehouden met beleidsregel 16 onder hoofdstuk 4.2 'tijdsige vernietiging'.

5.5 Bepaling wijze van verantwoording

Door vast te leggen welke informatie vernietigd is en welke processtappen doorlopen zijn kan de OD Twente zich verantwoorden. De OD Twente legt ter verantwoording het volgende vast:

- Een logboek;
- Een samengestelde vernietigingslijst van alle bedrijfsonderdelen;
- Een vernietigingsbewijs uit het zaaksysteem/DMS;
- Een verklaring van vernietiging.

5.5.1 Logboek

Welke verwijderingshandelingen worden verricht, door wie, op welk moment en hoe worden die gedocumenteerd?

Om dit inzichtelijk te maken wordt een logboek gemaakt. Team Informatiebeheer houdt het logboek bij waarin alle 'verwijderingshandelingen' beschreven worden. Het logboek wordt aan het eind van het proces als bijlage bij de vernietigingsverklaring gearcheveerd.

5.5.2 Samengesteld vernietigingslijst

Welk type informatieobjecten worden vernietigd?

Het type informatieobject is te vinden in de vernietigingslijst. Veelal zal vernietiging uitgevoerd worden op zaak- en dossierniveau, maar het vernietigingsbeleid- en protocol voorzien ook in de mogelijke vernietiging op documentniveau. Voor het vernietigen van gegevensdragers zal een uitbreiding van het vernietigingsbeleid- en protocol nodig zijn.

Hoeveel informatieobjecten zijn vernietigd?

De hoeveelheid verwijderde informatieobjecten is terug te vinden in de samengestelde vernietigingslijst.

Welke metagegevens zijn behouden ter verantwoording van de vernietiging?

Op de vernietigingslijsten staan de te behouden metadata. De gearcheveerde lijsten dienen ter verantwoording van de vernietigde informatie. In het zaakstelsel zijn enkel de volgende gegevens te zien:

Metadata veld	Invulling
Zaaknummer	ZJJJJ-ODT-XXXXXX
Record Identifier	XXX.XXX
Datum aanmaak	DD-MM-JJJJ UU:MM
Datum wijziging	'datum vernietiging'
Formulier status	'inactief'
Datum in Archief	DD-MM-JJJJ UU:MM
Bewaartermijn	VJ
Ingangsdatum vernietiging	DD-MM-JJJJ
Medewerker	Naam
Entiteit	'zaak'
Activiteit	'vernietigen'
Opmerking	'zaak vernietigd'

Welke niet te openbaren informatie wordt verwijderd of verborgen?

Informatie die niet openbaar gemaakt dient te worden, bijvoorbeeld in het kader van de AVG, dient ook niet vindbaar te zijn op de vernietigingslijsten. Het kan zijn dat een dossier- of zaaktitel en/of andere metadata niet te openbaren informatie bevatten. Deze informatie dient dan geanonimiseerd, gepseudonimiseerd of verwijderd te worden.

5.5.3 Vernietigingsbewijs

Het vernietigingsbewijs dient als bewijs dat de informatie daadwerkelijk vernietigd is uit het zaakstelsel/DMS. Het vernietigingsbewijs staat synoniem aan het bewijs dat een geaccrediteerd vernietigingsbedrijf in de analoge situatie zou overhandigen ter bewijs dat de informatie vernietigd is.

5.5.4 Verklaring van vernietiging

De handtekening van de directeur bezegelt dat de procedure volgens de daarvoor gestelde kaders en richtlijnen is doorlopen. In het RACI-model is de teammanager bedrijfsvoering steeds eindverantwoordelijk voor de controle dat het proces goed doorlopen is. Met de getekende verklaring wordt toezicht gehouden dat de teammanager Bedrijfsvoering zijn gemandateerde rol als 'toezichthouder' over het proces goed heeft uitgevoerd. Met de verklaring door de directeur is dus nog een extra stap ingebouwd om toe te zien dat de teammanager Bedrijfsvoering tevens gehouden is en wordt aan het uitvoeren van de toezichthoudende rol.

5.6 Uitvoering vernietiging volgens vernietigingsprotocol

Zie hiervoor het document vernietigingsprotocol.

6 Back-ups en kopiestukken

De OD Twente wil zo compleet mogelijk zijn in de vernietiging van informatieobjecten, omdat dit bedrijfsrisico's vermindert en dit overeenkomt met verschillende wettelijke eisen, zoals de Archiefwet en de AVG. Voor kopiestukken geldt dat binnen de verschillende bedrijfsonderdelen aandacht moet zijn voor het zo minimaal creëren van kopiestukken en het opslaan daarvan in verschillende vormen/bestandsformaten op verschillende opslaglocaties. Daarnaast zullen teams er zelf voor moeten zorgen dat kopieën van te vernietigen informatieobjecten tijdig worden opgespoord en verwijderd/vernietigd. De OD Twente leunt voor haar IT faciliteiten grotendeels op afspraken die de gemeente Almelo maakt met leveranciers op gebied van back-ups, recovery, beveiliging, toegang, bewaring en vernietiging. Voor de back-ups in het zaaksysteem PowerBrowser leunt de OD Twente op de back-up strategieën van haar leverancier Genetics. De leverancier toont, aan de hand van certificering, aan dat ze betrouwbaar omgaan met het bewaren, beveiligen, afschermen en vernietigen van informatieobjecten en het terugzetten daarvan. Leveranciers worden hierop gemonitord door auditors die toetsen of de leverancier zich houdt aan de certificeringseisen van onder andere ISO-NEN 27001:2017 en ISO-NEN 16715-1.

6.1 Kopiestukken

De teams hebben zelf de verantwoordelijkheid voor de informatieobjecten die ze onder zich hebben en houden. Er moet meer aandacht komen voor de gevaren die het creëren en opslaan van kopieën met zich meebrengen, omdat het beheer niet in alle applicaties/systemen actief gevoerd wordt. Daardoor bestaat de mogelijkheid dat een deel van de informatie niet in zicht is van informatiebeheer en worden de bedrijfsrisico's groter. Het credo 'eenmalige opslag, meervoudig gebruik' zou dus in het DNA van de teams moeten komen en daar ondersteunen de informatiebeheerders bij. Bij de kwartaalvernietiging zullen teams ook actief moeten zoeken naar de kopiestukken van te vernietigen zaken/dossiers op onder andere persoonlijke schijven, Teams omgevingen, taak specifieke applicaties en e-mail. Per proces zal geïnventariseerd worden waar het origineel gearchiveerd is en waar zich mogelijke kopieën bevinden. Op alle plaatsen waar zich te vernietigen kopieën van informatieobjecten bevinden zijn afspraken gemaakt over:

- Het vernietigingsbeleid van back-ups;
- De frequentie van het back-uppen;
- Het soort back-up.

6.2 Back-ups en Recovery

Originele informatieobjecten horen thuis in de centraal daarvoor aangewezen archiefruimten. Voor alle VTH-zaken geldt dat PowerBrowser het daarvoor aangewezen zaaksysteem is en vanuit deze applicatie vernietiging uitgevoerd zal worden. Voor de back-up strategie leunt de OD Twente op het beheer dat door Genetics, de leverancier van PowerBrowser, wordt uitgevoerd.

6.2.1 Back-up beleid PowerBrowser

1. Elke nacht wordt een volledige database back-up gemaakt van de PowerBrowser omgeving en opgeslagen op een beveiligde en versleutelde opslag. Hierbij wordt ervoor gezorgd dat de back-ups op minstens twee fysieke locaties aanwezig zijn en dat deze alleen toegankelijk zijn voor enkele specifiek geautoriseerde medewerkers van Genetics.
2. Naast een volledige database back-up vindt ook nachtelijk een incrementele back-up plaats van de complete infrastructuur op virtualisatie-niveau.
3. Een klant van Genetics kan via het helpdesksysteem PowerReport een verzoek indienen voor het herstellen van (data uit) een back-up. Een geautoriseerde medewerker voert vervolgens deze opdracht uit en herstelt de gegevens in overleg met en na akkoord van de klant.
4. De dagelijkse back-up wordt voor 30 dagen bewaard en de maandelijkse back-up voor 12 maanden. Binnen 30 dagen kan je dus terug naar een back-up per dag en als het langer geleden is kan je terug naar de back-up van begin van elke maand.
5. Minstens één keer per jaar vindt een data-recovery test plaats waarin wordt getest of de gemaakte back-ups ook daadwerkelijk terug te zetten zijn. Hier wordt ook een rapport van opgesteld als bewijs in onze jaarlijkse ISO 27001 audits.

6. Na een jaar worden automatisch de oude back-ups verwijderd van de back-up-opslag.

6.2.2 Omgang gegevensdragers

1. Bij de afvoer van ICT middelen, bijvoorbeeld servers of harde schijven die niet meer gebruikt zijn bij vervanging van apparatuur, wordt de onderstaande flowchart (fig 7.1.) gevolgd om te bepalen welke wijze van vernietiging plaats dient te vinden.

2. Omdat in PowerBrowser ook vertrouwelijke gegevens zijn opgeslagen, is bij deze gegevensdragers altijd de 'Overschrijven' of 'Vernietigen' methode van toepassing afhankelijk van de exacte gegevensdragers waar het om gaat.

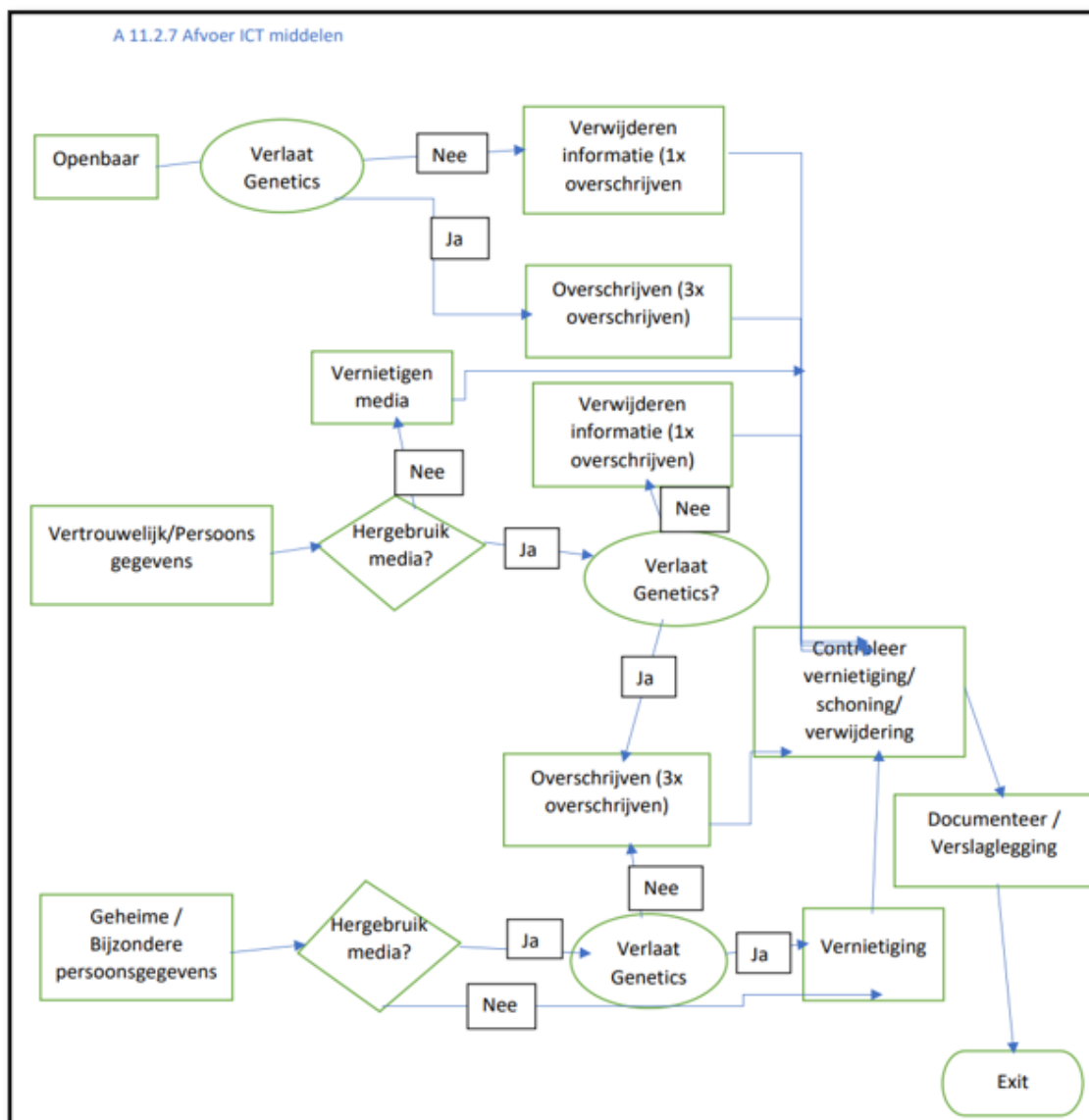


Fig. 7.1. Flowchart afvoer ICT middelen door Genetics