Sint-Michielsgestel
geeft ruimte

GEMEENTEBLAD

Officiële uitgave van de gemeente Sint-Michielsgestel

Nr. 229735
20 mei
2022

Analoge en digitale vernietiging archiefbescheiden

0. Managementsamenvatting

0.1. Inleiding

Overheidsinformatie wordt conform de Selectielijst gemeenten en intergemeentelijke organen opgenomen in een archief. De duur van opslag in het archief is afhankelijk van de inhoud van de archiefbescheiden, sommige stukken kunnen na een jaar na afhandeling al worden verwijderd uit het archief, andere stukken zijn voor altijd te bewaren. De juiste bewaartermijnen zijn uitgewerkt in de selectielijst.

Archiefbescheiden die blijvend te bewaren zijn, worden na 20 jaar overgedragen naar de archiefbewaarplaats. Dit is een statisch archief, vaak ondergebracht bij een regionale archiefdienst. Voor de gemeenten Boxtel en Sint-Michielsgestel en GR MijnGemeenteDichtbij is dat het Brabants Historisch Informatie Centrum (BHIC) in Den Bosch. Deze informatie wordt dan openbaar.

Archiefbescheiden met een vernietigingstermijn korter dan 20 jaar worden opgeslagen in het semi-statisch archief, (vaak) op locatie van de zorgdrager. Deze draagt dan ook zorg voor vernietiging. Vernietigen van informatie is het blijvend ontoegankelijk maken van die informatie, waardoor deze niet meer vindbaar, beschikbaar, leesbaar, te interpreteren en betrouwbaar is. Vernietigen betreft overheidsinformatie, ongeacht de vorm, en met behoud van metagegevens over de vernietiging, zowel analoog als digitaal. Achteraf moet te herleiden zijn wat wanneer is vernietigd.

Er zijn twee soorten archief binnen MGD:
- Analoog (papieren) archief, dat zich in de archiefkluizen bevindt in de gemeentehuizen
- Digitaal archief, dat is opgeslagen in applicaties

Het wettelijke kader wordt gevormd door:
- Archiefwet
- Wet Algemene verordening Gegevensbescherming (privacy)
- Wet openbaarheid van bestuur (Wob)
- Baseline Informatiebeveiliging Overheid (informatiebeveiliging)
- En sectorale wetgeving

0.2. Huidige situatie

Binnen MGD (en daarvoor bij de afzonderlijke gemeenten) wordt vernietiging van het analoge archief reeds uitgevoerd. Met betrekking tot het digitale archief is bij de migratie van Corsa en Verseon naar het zaaksysteem alles wat vernietigd had moeten zijn vóór 2019 niet gemigreerd naar het zaaksysteem en daarmee vernietigd. Alle digitale informatie die zich in andere systemen bevindt, zoals vak-applicaties, schijven en/of Outlook is niet meegenomen.

0.3. Gewenste situatie

Binnen MGD is nog niet eerder beleid voor Vernietiging geformuleerd. Omdat we inmiddels over een module Vernietiging in het zaaksysteem beschikken, hebben we nu beleid opgesteld dat geldt voor zowel analoog als digitaal archief.

0.4. Risicoanalyse

Met betrekking tot informatie wordt onderscheid gemaakt tussen gestructureerde informatie en ongestructureerde informatie. Gestructureerde informatie is data opgeslagen en geordend in databases met aanvullende metadata (lees zaaktypen, bewaartermijnen, resultaten), die beheer van de data mogelijk maakt. Ongestructureerde informatie is alle informatie die ongeordend is opgeslagen in willekeurige opslagsystemen, waardoor beheer praktisch onmogelijk is.

Risico MGD
Binnen MGD bevindt zich momenteel veel informatie op schijven, in Outlook en in vak-applicaties, die niet over een (goedwerkende) archieffunctie beschikken. Deze informatie valt allemaal onder ongestructureerde informatie. Op deze informatie is selectie- en vernietiging niet uitvoerbaar waardoor niet wordt voldaan aan de Archiefwet. Daarnaast zit veel informatie ook (dus dubbel) in het zaaksysteem Onegov.

In het zaaksysteem wordt zaakgericht gewerkt en is het beheer van de informatie conform de selectielijst gestructureerd ingeregeld. Hier is sprake van gestructureerde informatie.

0.5. Reikwijdte

De reikwijdte van de vernietiging bij MGD heeft betrekking op vernietiging van archiefbescheiden van drie archiefvormende organen, namelijk:
- Archief MGD.
- Archief gemeente Boxtel.
- Archief gemeente Sint-Michielsgestel.

Daarbij dient aangemerkt te worden dat de vernietiging zich alleen richt archiefbescheiden die op een gestructureerde manier zijn opgeslagen. Dit betekent dat aan de archiefbescheiden voor zowel analoog als digitaal metadata is toegevoegd, bijvoorbeeld in de vorm van bewaartermijnen conform de geldende selectielijst van gemeenten en gemeentelijke organen. Alle andere informatie, analoog of digitaal, die hier niet onder valt, wordt niet meegenomen in de vernietiging. Dit betekent dat informatie van de organisatie, die niet gestructureerd is opgeslagen, buiten de vernietiging en overbrenging naar archiefbewaarplaats valt.

0.6. Vernietigingsprotocol

Op basis van de handreiking, zoals hierboven beschreven is voor MijnGemeenteDichtbij een twee sporen protocol ontwikkeld. Namelijk het spoor van doorlopende machtiging en het spoor van de reguliere vernietiging.

Doorlopende machtiging:
1. Op basis van de met BHIC afgestemde lijst van zaaktypen die in aanmerking komen voor doorlopende machtiging wordt door de DIV A-medewerker een vernietigingszaak aangemaakt en wordt de vernietiging doorgevoerd.
2. Vervolgens wordt een verklaring van vernietiging opgesteld welke wordt getekend door de gemeentesecretaris, deze wordt toegestuurd aan de gemeentearchivaris BHIC.
3. De vernietigingslijst, het akkoord van de gemeentearchivaris, de verklaring van vernietiging en vernietigingsbewijs vernietigingsbedrijf of uitdraai van de vernietigingsmodule in het zaaksysteem wordt opgeslagen in een te bewaren zaak in het zaaksysteem.

Reguliere vernietiging:
1. De DIV A-medewerkers stelt een vernietigingslijst (voordracht tot vernietiging) op waarin alle te vernietigen archiefbescheiden staan vermeld.
2. De vernietigingslijst wordt ter toetsing doorgestuurd naar de teammanagers van de vak-afdelingen waar de te vernietigende zaken betrekking op hebben.
3. Toetsing of onderbouwing van verlenging moet voldoende beargumenteerd zijn voordat deze wordt doorgevoerd.
4. De vernietigingslijst wordt toegezonden naar het BHIC, t.a.v. de gemeentearchivaris.
5. De inspecteur controleert de lijst en maakt eventueel opmerkingen.
6. Als er aanpassingen zijn doorgevoerd in de selectielijst wordt de aangepaste lijst nogmaals naar de gemeentearchivaris gestuurd.
7. De gemeentearchivaris brengt positief advies uit over de vernietiging (machtiging voor vernietiging) van de in de vernietigingslijst genoemde archiefbescheiden.
8. Op basis van het advies is akkoord voor de uitvoering van vernietiging plaats van de archiefbescheiden
9. Gemeentesecretaris/directeur MGD (afhankelijk van archief) accordeert de verklaring van vernietiging.
10. Ondertekende verklaring van vernietiging wordt toegezonden naar het BHIC.
11. De vernietigingslijst, het akkoord van de gemeentearchivaris, de verklaring van vernietiging en vernietigingsbewijs vernietigingsbedrijf of uitdraai van de vernietigingsmodule in het zaaksysteem wordt opgeslagen in een te bewaren zaak in het zaaksysteem.

1. Achtergrond

1.1. Inleiding

Overheidsinformatie wordt conform de Selectielijst gemeenten en intergemeentelijke organen opgenomen in een archief. De duur van opslag in het archief is afhankelijk van de inhoud van de archiefbescheiden, sommige stukken kunnen na een jaar na afhandeling al worden verwijderd uit het archief, andere stukken zijn voor altijd te bewaren. De juiste bewaartermijnen zijn uitgewerkt in de selectielijst.

Archiefbescheiden die blijvend te bewaren zijn, worden na 20 jaar overgedragen naar de archiefbewaarplaats. Dit is een statisch archief, vaak ondergebracht bij een regionale archiefdienst. Voor de gemeenten Boxtel en Sint-Michielsgestel en GR MijnGemeenteDichtbij is dat het Brabants Historisch Informatie Centrum (BHIC) in Den Bosch. Deze informatie wordt dan openbaar.

Archiefbescheiden met een vernietigingstermijn korter dan 20 jaar worden opgeslagen in het semi-statisch archief, (vaak) op locatie van de zorgdrager. Deze draagt dan ook zorg voor vernietiging. Vernietigen van informatie is het blijvend ontoegankelijk maken van die informatie, waardoor deze niet meer vindbaar, beschikbaar, leesbaar, te interpreteren en betrouwbaar is. Vernietigen betreft overheidsinformatie, ongeacht de vorm, en met behoud van metagegevens over de vernietiging, zowel analoog als digitaal. Achteraf moet te herleiden zijn wat wanneer is vernietigd.

1.1.1. Soorten archieven

Overheidsinformatie zit opgeslagen in een archief. We onderscheiden twee soorten archieven.

- Analoog (papieren) archief: De papieren worden doorgaans opgeslagen in dozen. Deze worden voorzien van de inhoud en vernietigingsjaar. Deze dozen worden in een logische volgorde opgeslagen, doorgaans in stalen, brandvrije of -vertragende archiefkasten of archiefkluizen.
- Digitaal archief: archief in applicaties. Digitale informatie is er in vele vormen zoals tekstdocumenten, presentaties, spreadsheets, video's, foto's, (chat) berichten, e-mails, gegevenssets in databases, etc.

1.1.2. Definities archiefbescheiden/archiefstuk en informatieobject

- Archiefstuk: een informatieobject, ongeacht zijn vorm, met bijbehorende metadata ontvangen of opgemaakt door een natuurlijke en/of rechtspersoon bij uitvoering van taken en bewaard om te voldoen aan wettelijke en/of administratieve eisen en/of maatschappelijke behoeften. Dit omvat in bepalingen van Nederlands archiefrecht ook synoniemen als archiefbescheiden, gegevens, informatie, documenten en (gegevens)bestanden.
- Archiefbescheiden: synoniem voor archiefstukken.
- Informatieobject: een geheel van gegevens met een eigen identiteit.

1.2. Wettelijk kader

Vernietigen van archiefbescheiden/informatieobjecten is wettelijk verplicht, zowel voor analoge als voor digitale archiefbescheiden. Het draagt bij aan het voldoen aan wet- en regelgeving, informatiebeveiliging, privacy, de beheersbaarheid van informatie, kostenbesparing en milieu. Uitgangspunt is dat vernietigen van archiefbescheiden integraal deel uitmaakt van het informatiebeheer. Dus een terugkerend proces is.

1.2.1. De Archiefwet

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 analoge en digitale overheidsinformatie, in de vorm van archiefbescheiden, waarvan de bewaartermijn is verstreken en die niet van vernietiging is uitgezonderd, te vernietigen. De Archiefwet gaat over het vernietigen van informatieobjecten en diens kopieën.

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.

Het wettelijk kader wordt bepaald door de Selectielijst gemeenten en intergemeentelijke organen 2020. De VNG ontwerpt, gemachtigd door vrijwel alle gemeenten, een ontwerpselectielijst voor archiefbescheiden die door de minister van OCW wordt vastgesteld. In de selectielijst zijn de bewaartermijnen van archiefbescheiden van gemeentelijke en intergemeentelijke organen vastgelegd. De selectielijst bevat, op basis van artikel 5 lid 1 sub e Archiefbesluit 1995, ook een opsomming van criteria op basis waarvan archiefbescheiden, die voor vernietiging in aanmerking komen, van vernietiging kunnen worden uitgezonderd, voorbeeld Hotspots. Zie hiervoor het Beleid Hotspot-monitor.

1.2.2. Algemene verordening Gegevensbescherming (privacy)

De Algemene verordening gegevensbescherming (AVG) stelt verplichtingen aan (overheids)organisaties bij het verwerken van persoonsgegevens. Het vernietigen van informatie is één van de verplichtingen om te voorkomen dat persoonsgegevens onrechtmatig worden gebruikt. Het uitgangspunt daarbij is

dat een organisatie persoonsgegevens vernietigt wanneer deze niet meer nodig zijn voor het doel waarvoor ze zijn verzameld of worden gebruikt. Het is mogelijk 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. De AVG gaat over het vernietigen van (persoons)gegevens die onderdeel zijn van informatieobjecten.

1.2.3. Wet openbaarheid van bestuur (Wob)

Op overheidsinformatie die niet is overgebracht naar de archiefbewaarplaats , is de Wet openbaarheid van bestuur (Wob) van toepassing. Informatie die op grond van een vastgestelde selectielijst is vernietigd, kan op grond van de Wob 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 Wob-verzoek gewoon (al dan niet geanonimiseerd) openbaar worden gemaakt aan de indiener. Dat kan in sommige gevallen leiden tot financiële- en imagoschade. Wanneer de organisatie kan aantonen dat bepaalde informatie rechtmatig is vernietigd, dan valt dit niet onder de plicht tot openbaarmaking.

1.2.4. Baseline Informatiebeveiliging Overheid (informatiebeveiliging)

Sinds 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht voor 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.

1.2.5. Sectorale wetgeving

Dit is wet- en regelgeving dat van toepassing in een specifieke sector waarbij publieke belangen geborgd zijn. Denk hierbij aan het Burgerlijk Wetboek of Omgevingswet.

1.3. Voordelen van vernietiging

Een groot gedeelte van alle overheidsinformatie komt voor vernietiging in aanmerking. Nadat de bewaartermijn volgens de selectielijst is verstreken, vormt deze informatie ballast voor de informatiehuishouding. Door die te vernietigen behaalt de organisatie een aantal voordelen.

Mogelijke voordelen	Uitleg
Lager kosten hosten en beheren	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. Alhoewel de kosten van terabytes opslag aan digitale informatie steeds verder afnemen, zijn er aan het hosten en beheren van data desalniettemin kosten verbonden. Dit zijn kosten die een organisatie niet hoeft te maken voor informatie waarvan de vernietigingstermijn al is verstreken.
Lagere kosten licenties en onderhoud	Je maakt kosten voor licenties en onderhoud van informatiesystemen en back-ups waarop digitale overheidsinformatie staat die vernietigd had moeten zijn. Doordat volumes na vernietiging niet meer zo groot zijn, draaien back-ups sneller en efficiënter. Ook hier zijn lagere kosten mee gemoeid.
Verminderen administratieve last	Bij een grotere hoeveelheid informatie kost het een medewerker veel meer moeite en tijd om de juiste informatie te vinden. Onder andere bij Wob-verzoeken. Deze grotere administratieve last leidt tot hogere overheidsuitgaven.
Eisen duurzame toegankelijkheid	Het voldoen aan de eisen van duurzame toegankelijkheid brengt kosten met zich mee. Een overheidsorganisatie is verantwoordelijk voor het vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar maken én houden van alle informatie die deze in beheer heeft. Ook daarvoor geldt dat je die bespaart wanneer je je ontdoet van ballast.
Voorkomen imagoschade	Het nog beschikken over informatie die al vernietigd had moeten zijn kan leiden tot imagoschade. Vaak komt het voor dat binnen een organisatie niet goed in beeld is welke informatie zich in onder andere back-ups of andere schaduwarchieven bevindt. Een verminderde beheersbaarheid van informatie leidt zo mogelijk tot imago-

	schade. In sommige gevallen vloeien daar politiek-bestuurlijke consequenties uit voort.
Eenvoudiger conversie of migratietrajecten	(Toekomstige) conversie- en migratietrajecten zijn minder complex en minder kostbaar ballast is verdwenen.
Milieuvoordelen	Digitale opslag belast het milieu door de CO_2-uitstoot van de servers en datacenters. Het bewaren van digitale informatie die op grond van wet- en regelgeving vernietigd had moeten worden, brengt een onnodige milieubelasting met zich mee.

2. Vernietigen volgens handreiking Nationaal Archief

2.1. Selectielijst

De selectielijst Nederlandse gemeenten en intergemeentelijke organen speelt een belangrijke rol bij het vernietigen van archiefbescheiden/informatieobjecten. In de selectielijst is opgenomen welke categorieën archiefbescheiden blijvend moeten worden bewaard en welke categorieën archiefbescheiden na een bepaalde termijn moeten worden vernietigd. De selectielijst is daarmee een belangrijk beleidsdocument voor vernietiging.

2.2. Beleid

Beleid voor vernietigen dient onderdeel uit te maken van het beleid voor informatiebeheer. In dit beleid horen de beleidsuitgangspunten voor vernietigen te zijn vastgelegd, zoals:
- Dat er altijd verplicht een risicoanalyse gemaakt moet worden.
- Dat er een vernietigingsprotocol moet worden toegepast.
- Welke wijze van vernietigen wordt gehanteerd.
- Welke doelen vernietigen nastreeft.
- Welke middelen voor vernietigen beschikbaar zijn.
- Het beoogde tijdspad voor de implementatie en uitvoering van vernietigen.

Voor digitaal vernietigen zijn tevens de volgende uitgangspunten in het beleid bepaald:
- Dat by-design-maatregelen nodig en wenselijk zijn voor digitale vernietiging.
- De keuze tussen het inrichten van centrale vernietigingsfunctionaliteit of juist vernietiging bij de bron.

2.3. Middelen en mensen

Voor het succesvol implementeren van vernietigen zijn de volgende aspecten van belang met betrekking tot middelen en mensen:
- Duidelijk is wie welke rol en verantwoordelijkheid heeft in het proces van vernietigen.
- De benodigde middelen voor vernietiging beschikbaar worden gesteld. Dit kan door ervoor te zorgen dat deze middelen expliciet worden opgenomen in de meerjarenbegroting.

2.3.1. Onduidelijkheid over verantwoordelijkheden

Vernietigen van archiefbescheiden/informatieobjecten is niet alleen een taak van team DIV. Het is belangrijk dat medewerkers in zowel de business (zoals proceseigenaren), ICT (zoals applicatiebeheerders) als het informatiemanagement (zoals architecten) betrokken zijn bij vernietigen. En dat zij weten wat er van hen wordt verwacht, wat hun verantwoordelijkheden zijn en daarbij voldoende mandaat hebben. In de praktijk bestaan hierover vaak onduidelijkheden. Waardoor het vernietigen niet, nauwelijks, onvolledig of niet goed gebeurt.

Onder andere de volgende functionarissen kunnen een rol spelen (verantwoordelijkheid hebben) bij vernietigen: gemeentesecretaris, managers of proceseigenaren, CIO, FG, CISO, Archivaris, Directeur ICT, Adviseur of specialist informatiemanagement, recordmanager, (informatie)architect, projectleider, Beleidsmedewerker (DIV), functioneel beheerder, applicatiebeheerder, applicatieontwikkelaar, beheerder infrastructuur, etc.

2.3.2. Onduidelijkheid over middelen

Aan vernietigen zijn kosten verbonden. Deze zijn afhankelijk van hoe vernietigen wordt gerealiseerd. Naast de kosten voor de inzet van mensen, moet er bij digitaal vernietigen ook rekening gehouden worden met bijvoorbeeld aanschafkosten of ontwikkelkosten voor de vervanging of aanpassing van informatiesystemen. Ook de investering in de benodigde kennis bij zowel analoge als digitale vernietiging kan kosten met zich meebrengen.

2.3.3. Informatie-overleggen

Veel overheidsorganisaties hebben binnen de eigen organisatie een strategisch informatieoverleg ingericht. Sommige overheidsorganisaties hebben ook een tactisch informatieoverleg intern georganiseerd. In deze informatie-overleggen worden vraagstukken belegd over het functioneren en de kwaliteit van de informatiehuishouding. Ook op operationeel niveau vindt er overleg plaats, onder andere over de uitvoering van het vernietigen van archiefbescheiden/informatieobjecten.

In de informatie-overleggen vindt er een afweging plaats, waarbij alle relevante kennis en expertise bijeen wordt gebracht door besluitvormers. Dit zijn onder andere de CIO en archivaris en hun adviseurs in de business, ICT en het informatiemanagement. Zo kan het informatiebeheer, inclusief vernietigen, in samenhang worden georganiseerd. De informatie-overleggen van de organisatie vormen op die manier een plek waar vernietigen kan worden geagendeerd en besluitvorming kan plaatsvinden. Het mandaat voor de implementatie van vernietigen van archiefbescheiden/informatieobjecten wordt hier gelegd.

2.4. Protocol vernietigen

Om daadwerkelijk tot vernietigen over te gaan is het belangrijk dat er heldere afspraken zijn gemaakt. Welke activiteiten moeten op welk moment worden uitgevoerd? En door wie? Dit wordt in een vernietigingsprotocol of -procedure vastgelegd waarmee je verantwoordt hoe je analoog of digitaal vernietigt. Het startpunt is de selectielijst en een lijst met de voor vernietiging in aanmerking komende informatie (vernietigingslijst). Ook de verplicht op te stellen verklaring van vernietiging bij iedere vernietigingsactie is onderdeel hiervan. Om informatieobjecten te kunnen vernietigen, is er vernietigingsfunctionaliteit nodig.

In het protocol kan vastgesteld zijn dat vernietiging altijd volgens een strikte aanpak wordt uitgevoerd. Maar je kunt ook besluiten om in het vernietigingsprotocol ruimte te laten voor een meer flexibele aanpak, rekening houdend met het risico op informatieverlies en -behoud. Een andere mogelijkheid is om bij het in beheer nemen van een informatiesysteem als eis op te stellen dat er een vernietigingsprotocol is voor de informatieobjecten in dat systeem.
In een vernietigingsprotocol is tenminste vastgelegd:

- Wat de rollen en verantwoordelijkheden zijn.
- De beslismomenten.
- Welke activiteiten in welke volgorde dienen te worden uitgevoerd.
- De controlemomenten.
- De wijze waarop verantwoording over de vernietiging wordt afgelegd.
- Dat er een review plaatsvindt van te vernietigen informatie.

2.5. Kwaliteitsmanagement en toezicht

Beleid, procedures en protocollen met betrekking tot vernietigen moeten zijn vastgelegd in een systeem, waarin de kwaliteitszorg voor deze instrumenten is geborgd. Met 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.

2.6. Overzicht informatieobjecten, processen en informatiesystemen

Om te kunnen vernietigen is het belangrijk om een goed overzicht te hebben van de processen, en eventueel de informatiesystemen en de informatieobjecten binnen een organisatie. Informatieobjecten kunnen zich namelijk in meerdere informatiesystemen bevinden, door meerdere informatiesystemen worden gebruikt en in verschillende processen worden toegepast. Wanneer je niet in beeld hebt welke processen of informatiesystemen de informatieobjecten gebruiken of creëren, is het praktisch onmogelijk om deze te selecteren en te vernietigen. Ook is het belangrijk dat kopieën van de informatieobjecten op back-ups in beeld zijn. De meeste overheidsorganisaties beschikken inmiddels over een Enterprise Architectuur waarin de informatieobjecten, processen en informatiesystemen al aan elkaar zijn gerelateerd.

2.7. Gradaties van digitale vernietiging

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. De risicoanalyse bepaalt wat passende maatregelen zijn. Op basis van de uitkomst van de risicoanalyse kan vervolgens worden gekozen voor verschillende gradaties van vernietigen.

2.7.1. 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.

2.7.2. 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.

2.7.3. 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.

2.7.4. 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.

2.8. Alternatieven voor vernietigen

2.8.1. 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. Het vernietigen van alle verwijzingen naar een informatieobject kan consequenties hebben voor de toegankelijkheid van dat informatieobject vanuit een andere context (dossier). Het kan zijn dat een ander dossier waarin hetzelfde informatieobject voorkomt, nog wel moet worden bewaard. Door bij het informatieobject alleen de link met het te vernietigen dossier te vernietigen, kan het langer te bewaren dossier intact blijven.

Vernietigingsperspectief	**Mogelijke nadelen en risico's**
Voldoen aan wet- en regelgeving	• Omdat de informatieobjecten zelf niet – maar alleen de verwijzingen er naartoe – vernietigd worden, is er nog steeds een risico op een datalek. • Door het verbreken van de koppeling maak je de informatieobjecten niet direct blijvend ontoegankelijk. De koppeling kan, theoretisch en technisch gezien, namelijk weer worden hersteld.
Beheersbaarheid van informatie	• Geen besparing op kosten voor licenties en onderhoud, omdat de opslagcapaciteit niet afneemt in het systeem waarin de informatie is opgeslagen. • (Toekomstige) migratietrajecten zijn niet minder complex en niet minder kostbaar, en back-ups niet sneller; er is geen vermindering van ballast, omdat verbreken van koppelingen niet leidt tot kleinere volumes.
Kostenbesparing en milieu	Omdat de informatieobjecten zelf niet vernietigd worden, is er sprake van een toename aan kosten voor benodigde opslag en een grotere milieubelasting.

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

Vernietigingsperspectief	Mogelijke nadelen en risico's
Voldoen aan wet- en regelgeving	De bescherming van persoonsgegevens (die onderdeel zijn van de informatieobjecten) kan niet worden gegarandeerd wanneer deze niet meer worden beheerd.
Beheersbaarheid van informatie	• Het wel behouden, maar niet meer beheren van de informatie zorgt niet voor meer grip en een grotere beheersbaarheid van de informatiehuishouding; • er is nog steeds sprake van ballast, • niet (goed) beheerde informatie kan ertoe leiden dat de informatie verkeerd wordt geïnterpreteerd en gebruikt, en • • de kwaliteit van de informatiehuishouding gaat erop achteruit.
Kostenbesparing en milieu	Het beëindigen van het beheer draagt bij aan een overload aan informatie, veroorzaakt grotere vraag naar servercapaciteit (en bijbehorende (onderhouds)kosten) en zorgt voor meer belasting van het milieu.

2.8.3. 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.

Vernietigingsperspectief	Mogelijke nadelen en risico's
Voldoen aan wet- en regelgeving	• De Archiefwet is ingericht op het dossier of documenten als object van vernietiging. Bij pseudonimiseren of anonimiseren wordt een dossier of document niet integraal vernietigd. • Pseudonimiseren is niet onomkeerbaar. Het voorkomen van een datalek is dan niet 100% waterdicht. • Geen besparing op kosten voor licenties en onderhoud, omdat de opslagcapaciteit niet toeneemt in het systeem waarin de gemaskeerde informatieobjecten worden opgeslagen. • (Toekomstige) migratietrajecten zijn niet minder complex en niet minder kostbaar, en back-ups niet sneller; er is geen vermindering van ballast, omdat de gemaskeerde informatieobjecten leiden tot grotere volumes.
Beheersbaarheid van informatie	Omdat bij het maskeren van persoonsgegevens in een informatieobject een nieuw informatieobject (archiefbescheid) ontstaat dat ook beheerd moet worden, neemt de beheersbaarheid af.
Kostenbesparing en milieu	Omdat er sprake is van nieuwe informatie objecten (met daarin de gemaskeerde gegevens) is er geen sprake van verminderde benodigde opslag en milieubelasting.

2.9. Werkwijze vernietigen archiefbescheiden/informatieobjecten

Vernietigen van overheidsinformatie kan plaatsvinden langs de volgende stappen:

2.9.1. Uitvoeren van een risicoanalyse

Bij het uitvoeren van een risicoanalyse op de te vernietigen overheidsinformatie worden afwegingsfactoren meegenomen, zoals het:
- Bedrijfsbelang.
- Verantwoordingsbelang.
- Maatschappelijk belang.

Ook worden de kansen en risico's bepaald voor:
- Voldoen aan wet- en regelgeving (o.a. informatiebeveiliging, privacy).
- De beheersbaarheid van informatie.
- Kostenbesparing en milieu.

Op basis van de uitkomsten van de uitgevoerde risicoanalyse worden weloverwogen keuzes gemaakt bij het bepalen van:

- De reikwijdte van vernietigen.
- Het object van vernietigen.
- De wijze waarop vernietigen plaatsvindt.
- Waar vernietigen plaatsvindt.
- Het moment van vernietigen.
- Verantwoording en vastlegging van vernietigen.

De uitkomsten van de risicoanalyse zijn belangrijke input om keuzes te kunnen maken bij de vervolgstappen. Op basis van de risicoanalyse kun je besluiten om bepaalde vervolgstappen wel of juist niet uit te voeren. Ook kan een risicoanalyse uitwijzen welke personen op welke momenten betrokken moeten zijn.

2.9.2. Bepalen van de reikwijdte van vernietigen

Archiefbescheiden/informatieobjecten bevinden zich op en in verschillende systemen binnen de organisatie, maar kunnen zich ook buiten de organisatie bevinden. Bijvoorbeeld wanneer deze extern worden opgeslagen of gehost. De informatieobjecten bevinden zich vaak als 'origineel bronexemplaar' in de 'oorspronkelijke bronsystemen', maar ook als kopieën op back-ups of in andere informatiesystemen. Bij vernietigen is het belangrijk dat bewust een keuze wordt gemaakt: óf de informatieobjecten in het bronsysteem (of archiefsysteem) en zoveel mogelijk eventuele digitale kopieën vernietigen óf alleen het originele bronexemplaar. Maak bij het bepalen van de reikwijdte gebruik van het 'overzicht in informatieobjecten, processen en informatiesystemen' uit de Enterprise Architectuur.

2.9.3. Bepalen waar vernietigen plaatsvindt

Bepaal waar de informatieobjecten vernietigd moeten worden. Dit is afhankelijk van de plek (archiefruimte of informatiesysteem) waarin de archiefbescheiden/informatieobjecten zich bevinden. Deze kunnen zijn opgeslagen in:

- Het bronsysteem waarin ze gemaakt zijn en/of beheerd worden.
- In het archief van de organisatie.
- Een centraal informatiesysteem waarin ze worden opgeslagen en beheerd.

Maak bij het bepalen waar vernietiging plaats vindt gebruik van het 'overzicht in informatieobjecten, processen en informatiesystemen' uit de Enterprise Architectuur.

Houd daarbij rekening dat in een service georiënteerde architectuur een informatieobject ('het bronexemplaar') niet per se in één, maar verspreid over meerdere informatiesystemen kan zijn opgeslagen.

2.9.4. Bepalen van het object van vernietigen

Bepaal wat het object van vernietigen is, bijvoorbeeld op het niveau van:

- Document: het informatieobject.
- Dossier: alle informatieobjecten die horen bij een proces of zaak.
- Hardware: de (fysieke en tastbare) drager van de informatieobjecten.

De selectielijst en de Enterprise Architectuur kunnen een startpunt zijn voor de keuze voor het object van digitaal vernietigen.

2.9.5. Bepalen van de wijze van vernietigen

Bepaal op welke wijze je de archiefbescheiden/informatieobjecten gaat vernietigen, bijvoorbeeld door:

- Leegruimen van archiefdozen met informatie die op de vernietigingslijst is opgenomen.
- Op maat gemaakte 'scripts' waarmee informatieobjecten vernietigd worden.
- Specifieke vernietigingsfuncties die worden of zijn ingebouwd in de informatiesystemen.
- Shredders waarmee in fysieke dragers van informatieobjecten vernietigd worden.

De wijze van vernietigen die gekozen wordt, is afhankelijk van analoog of digitaal vernietigen. Digitaal vernietigen is afhankelijk van de mogelijkheden die het informatiesysteem biedt. In sommige gevallen kan vernietiging in legacy-systemen of in systemen zonder vernietigingsfunctionaliteit worden gerealiseerd. In sommige gevallen, bij bestaande 'moderne' systemen of bij nieuw te ontwikkelen of aan te schaffen informatiesystemen, kunnen de principes van archiving by design, common ground of volledig geautomatiseerd vernietigen worden toegepast.

De Enterprise Architectuur (waarin ook vernietigingsfunctionaliteit per informatiesysteem in kaart is gebracht) kan een startpunt zijn om te bepalen op welke wijze vernietigd kan en zal worden.

Let op:
- Outsourcing van informatiesystemen.
- Informatiesystemen die extern (in de cloud) worden gehost en waarvoor ook een verwerkingsovereenkomst geldt. Overheidsorganisaties die hun eigen informatiesystemen niet beheren, moeten een overeenkomst sluiten waar digitaal vernietigen onderdeel van is met de beheerder van deze systemen.

2.9.6. Bepalen van het moment
Bepaal op welk moment je de archiefbescheiden/informatieobjecten moet vernietigen, bijvoorbeeld:
- Direct na het verstrijken van de bewaartermijn.
- Op vastgestelde momenten, na het verstrijken bewaartermijn.
- Op het moment dat de applicatie waarin de informatie zich bevindt 'end of life' is en wordt uitgefaseerd.

2.9.7. Bepalen van wijze van verantwoording
Er moet worden bepaald hoe de verantwoording en vastlegging van de te vernietigen archiefbescheiden/informatieobjecten zal plaatsvinden. Dit kan door vast te leggen:
- Welke verwijderingshandelingen er verricht zullen worden: door wie, op welk moment en hoe die worden gedocumenteerd.
- Welk type informatieobjecten vernietigd wordt; zijn dit gegevensets in databases, documenten of hele dossiers?
- De aantallen te vernietigen informatieobjecten.
- Welke metagegevens je bewust níét vernietigt, zodat je over de vernietiging verantwoording af kunt leggen en het niet lijkt alsof de informatieobjecten nooit hebben bestaan.

Metagegevens Het is verstandig c.q. noodzakelijk om bepaalde metagegevens te behouden die bewijzen dat het informatieobject er ooit was én dat dit op juiste wijze is vernietigd. Bijvoorbeeld door de status van het informatieobject vanaf het moment van vernietiging aan te passen in 'vernietigd' en deze status als metadata wel te bewaren na vernietiging van het informatieobject. Dat kan in het bronsysteem, maar bijvoorbeeld ook middels een gedetailleerde verklaring van vernietiging. Daarbij spelen ook de beveiligings- of toegangsbeperkingen voor het informatieobject een rol.

- Wat er niet wordt vastgelegd; denk bijvoorbeeld aan het geanonimiseerd opnemen van persoonsgebonden informatie uit de titel van een dossier in de (concept)vernietigingslijsten en de vernietigingsverklaringen.

Voor sommige informatieobjecten is het niet wenselijk dat op basis van de (concept)vernietigingslijst en vernietigingsverklaring zichtbaar is over wie of wat de informatie ging. Een alternatief hiervoor is dat je bij de te bewaren vernietigingsverklaring een geanonimiseerde of geaggregeerde versie opneemt.

- Wanneer vernietiging heeft plaatsgevonden, kan er een audit gehouden worden waarbij wordt getoetst of dit proces volgens de kwaliteitseisen is verlopen en gedocumenteerd. Bij eventuele onderzoeken van bijvoorbeeld de Auditdienst of de Rekenkamer en bij rechtszaken, kan dan eenvoudig worden aangetoond dat de juiste informatie op de juiste wijze is vernietigd.

2.9.8. Vernietigen conform protocol
Nadat de voorgaande stappen zijn doorlopen, worden de gemaakte keuzes en afspraken eenduidig vastgelegd in een vernietigingsprotocol. Nadat dit vernietigingsprotocol in het juiste gremium formeel is vastgesteld, kan de uitvoering van het protocol beginnen. Het is van belang dat ten minste de volgende activiteiten worden uitgevoerd:
- Vernietigingslijst opstellen met de te vernietigen informatieobjecten.
- Vernietigingslijst vaststellen in juiste gremium.
- Vernietiging uitvoeren conform vastgelegde afspraken.
- Verklaring van vernietiging opstellen en vaststellen.
- De duurzame toegankelijkheid van de verklaring van vernietiging borgen.

3. Vernietigen van archiefbescheiden/informatieobjecten bij MGD

3.1. Risicoanalyse

Met betrekking tot informatie wordt onderscheid gemaakt tussen gestructureerde informatie en ongestructureerde informatie. Gestructureerde informatie is data opgeslagen en geordend in databases met

aanvullende metadata (lees zaaktypen, bewaartermijnen, resultaten), die beheer van de data mogelijk maakt. Ongestructureerde informatie is alle informatie die ongeordend is opgeslagen in willekeurige opslagsystemen, waardoor beheer praktisch niet mogelijk is.

Binnen MGD bevindt zich momenteel veel informatie op schijven, in Outlook en in vak-applicaties, die niet over een (goedwerkende) archieffunctie beschikken. Deze informatie valt allemaal onder ongestructureerde informatie. Daarnaast zit veel informatie ook (dus dubbel) in het zaaksysteem Onegov. In deze applicatie wordt zaakgericht gewerkt en is het beheer van de informatie conform de selectielijst gestructureerd ingeregeld. Hier is sprake van gestructureerde informatie. MGD is momenteel bezig met de doorontwikkeling van Microsoft 365, Teams & Projecten, waarbij zicht komt op een tweede faciliteit om informatie gestructureerd op te slaan. Informatie die zich momenteel op schijven bevindt. Er zal dan ook gekeken worden naar het overzetten van deze informatie (na opschoning) en het beperken van opslag op de schijven. Vooral voor informatie die zich in mindere mate leent voor zaakgericht werken, waar het zaaksysteem zich op richt, is de doorontwikkeling belangrijk.

3.2. Reikwijdte

De reikwijdte van de vernietiging bij MGD heeft betrekking op vernietiging van archiefbescheiden van drie archiefvormende organen, namelijk:
- Archief MGD.
- Archief gemeente Boxtel.
- Archief gemeente Sint-Michielsgestel.

Daarbij dient aangemerkt te worden dat de vernietiging zich alleen richt archiefbescheiden die op een gestructureerde manier zijn opgeslagen. Dit betekent dat aan de archiefbescheiden voor zowel analoog als digitaal metadata is toegevoegd, bijvoorbeeld in de vorm van bewaartermijnen conform de geldende selectielijst van gemeenten en gemeentelijke organen. Alle andere informatie, analoog of digitaal, die hier niet onder valt, wordt niet meegenomen in de vernietiging. Dit betekent dat informatie van de organisatie, die niet gestructureerd is opgeslagen, buiten de vernietiging en overbrenging naar archiefbewaarplaats valt.

Voor de twee gemeenten geldt dat er een analoog archief aanwezig is binnen het betreffende gemeentehuis. Daarnaast is er voor beide gemeenten en voor MGD een digitaal archief, dat is opgenomen in het zaaksysteem en op termijn in MS Teams & Projecten.

3.3. Locatie van vernietiging

De archiefbescheiden van de drie archiefvormende organen zijn op verschillende locaties opgeslagen. De vernietiging zal worden uitgevoerd door medewerkers van de afdeling DIV op de onderstaande locaties.

Gemeente	Locatie	Welk archief	Type archief
Boxtel	Kelder gemeentehuis	Algemeen Boxtel V-serie Sint-Michielsgestel	analoog
Boxtel	Begane grond gemeentehuis, afd. Burgerzaken	Burgerzaken	analoog
Boxtel	Kelder gemeentehuis	Sociaal Domein	analoog
Boxtel	Zaaksysteem (cloud)	Algemeen	digitaal
Sint-Michielsgestel	Begane grond	Bewaren serie Sint-Michielsgestel	analoog
Sint-Michielsgestel	Begane grond, afd. Burgerzaken	Algemeen	analoog
Sint-Michielsgestel	Zaaksysteem (cloud)	Algemeen	digitaal
MijnGemeenteDichtbij	Zaaksysteem (cloud)	Algemeen	digitaal

3.4. Object van vernietiging

Voor het analoge archief van de beide gemeenten geldt dat archiefbescheiden op basis van vernietigingsjaren en bewaarblokken zijn opgeslagen. Alle dossiers, die binnen eenzelfde vernietigingsjaar vallen, zullen gelijktijdig worden vernietigd, mits er tijdens de procedure om tot de juiste vernietigingslijst te komen, bepaald wordt dat er zaken niet vernietigd moeten worden. Object van vernietiging in het analoge archief is een dossier.

Binnen MGD is afgesproken dat in het digitale archiefsysteem, het zaaksysteem, zaakgericht geregistreerd wordt. Dat betekent dat het object van vernietiging een zaak is met de daarbij behorende documenten, en metadata. Op basis van het zaaktype dat aan een zaak is gehangen zijn resultaten met bijbehorende

bewaartermijnen en ander metadata ingeregeld, die uitgangspunt zijn bij de vernietiging. Alle zaken, die binnen eenzelfde vernietigingsjaar vallen, zullen gelijktijdig worden vernietigd, mits er tijdens de procedure om tot de juiste vernietigingslijst te komen, bepaald wordt dat er zaken niet vernietigd moeten worden. Object van vernietiging in het digitale archief is een zaak.

3.5. Wijze van vernietiging

De wijze van vernietiging binnen MGD verschilt tussen het analoge en het digitale archief.
Voor het analoge archief van de beide gemeenten (MGD heeft geen analoog archief) geldt dat de dozen met dossiers, die vallen binnen het betreffende vernietigingsjaar dat moet worden uitgevoerd, worden leeggemaakt in een specifieke container. Deze container wordt door een specialistisch bedrijf op het gebied van archiefvernietiging opgehaald en zij zorgen ervoor dat de archiefbescheiden worden vernietigd. Hier ontvangt MGD een verklaring van. Het hele proces van vernietiging wordt opgeslagen als een zaak in het zaaksysteem. De verklaring wordt hierbij opgenomen.

Voor het digitale archief van alle drie de archiefvormende organisaties geldt dat er binnen het zaaksysteem een aparte vernietigingsmodule is geïmplementeerd. Deze module genereert vernietigingslijsten, voorzien van een vernietigingsbatch. Het gehele proces verloopt digitaal.

Bij beide processen geldt dat een vernietigingslijst opgesteld wordt. Deze lijst worden ter goedkeuring voorgelegd aan teammanagers en de gemeentearchivaris (BHIC). Nadat deze akkoord zijn gegaan, wordt er een definitieve lijst gemaakt en wordt de vernietiging doorgevoerd. Tenslotte wordt er een Verklaring van vernietiging opgesteld, ondertekend door de gemeentesecretaris of de directeur van MGD en toegestuurd aan de gemeentearchivaris. Het proces van vernietiging wordt eveneens vastgelegd in het zaaksysteem.

Naast de bovenstaande procedure van digitale informatie zijn er binnen MGD afspraken gemaakt met BHIC over de doorlopende machtiging van vernietiging. Met een doorlopende machtiging hoeven er geen vernietigingslijsten worden opgemaakt van individuele archiefbescheiden (dossiers/zaken). Hiervoor wordt jaarlijks een formulier ´Aanvragen machtiging vernietiging´ ingevuld en opgestuurd naar het BHIC. Het BHIC controleert en adviseert over vernietiging. Na het ontvangen advies voert de zorgdrager (DIV) de vernietiging uit, vergelijkbaar aan hierboven beschreven procedure bij digitale vernietiging.

Wijze van verantwoorden bij MGD

De door DIV opgestelde vernietigingslijst wordt allereerst voorgelegd aan de teammanager van de vak-afdeling, waar de te vernietigende zaken betrekking op hebben. Na diens akkoord gaat de lijst door naar de gemeentearchivaris van BHIC, die een advies uitbrengt. Na vernietiging wordt een verklaring van vernietiging opgesteld, die door de gemeentesecretaris wordt ondertekend en daarna wordt verzonden naar de gemeentearchivaris van BHIC.

3.6. Vernietigingsprotocol MGD

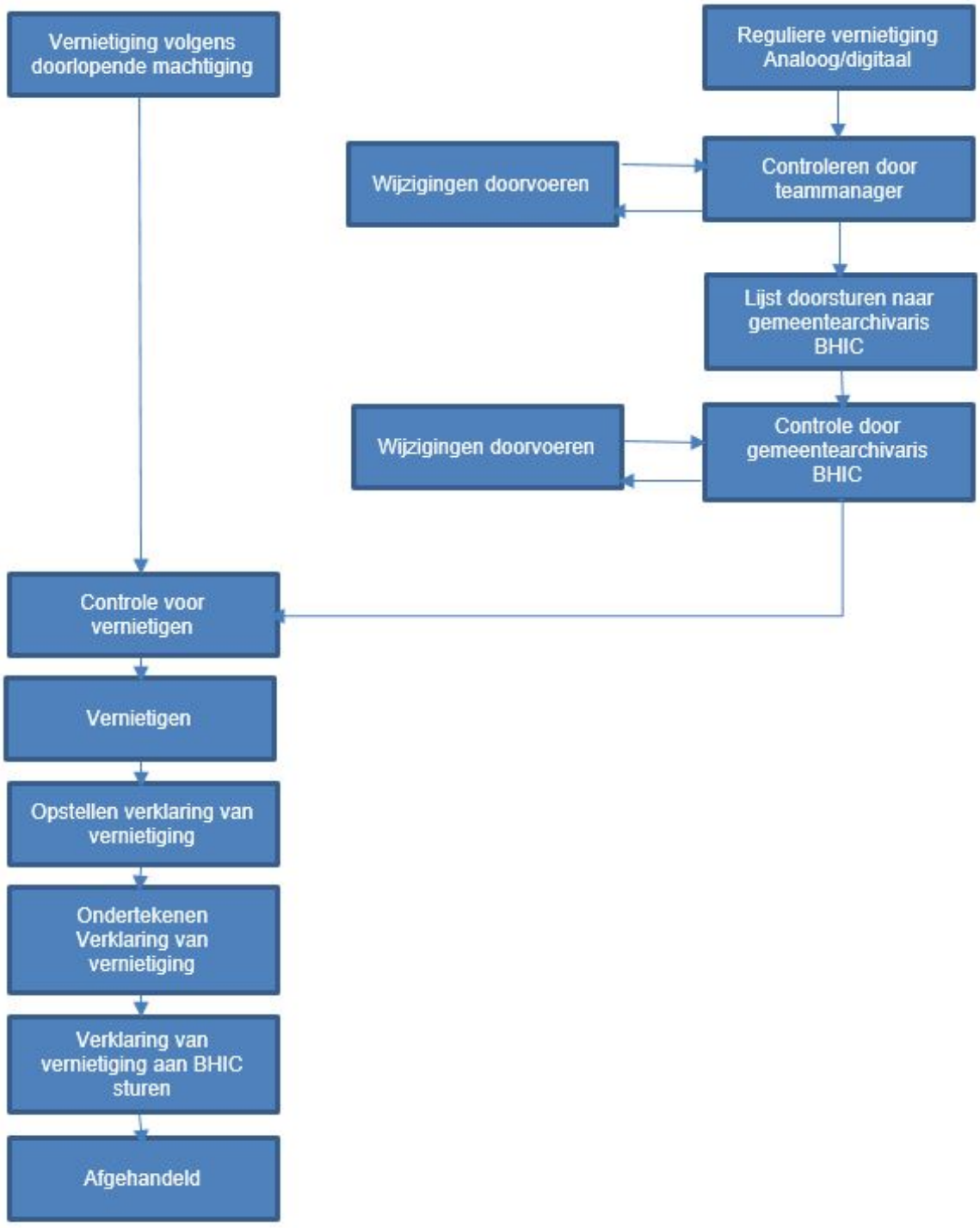
Op basis van de handreiking, zoals hierboven beschreven is voor MijnGemeenteDichtbij een twee sporen protocol ontwikkeld. Namelijk het spoor van doorlopende machtiging en het spoor van de reguliere vernietiging.

Doorlopende machtiging:
1. Op basis van de met BHIC afgestemde lijst van zaaktypen die in aanmerking komen voor doorlopende machtiging wordt door de DIV A-medewerker een vernietigingszaak aangemaakt en wordt de vernietiging doorgevoerd.
2. Vervolgens wordt een verklaring van vernietiging opgesteld welke wordt getekend door de gemeentesecretaris, deze wordt toegestuurd aan de gemeentearchivaris BHIC.
3. De vernietigingslijst, het akkoord van de gemeentearchivaris, de verklaring van vernietiging en vernietigingsbewijs vernietigingsbedrijf of uitdraai van de vernietigingsmodule in het zaaksysteem wordt opgeslagen in een te bewaren zaak in het zaaksysteem.

Reguliere vernietiging:
1. De DIV A-medewerkers stelt een vernietigingslijst (voordracht tot vernietiging) op waarin alle te vernietigen archiefbescheiden staan vermeld.
2. De vernietigingslijst wordt ter toetsing doorgestuurd naar de teammanagers van de vak-afdelingen waar de te vernietigende zaken betrekking op hebben.
3. Toetsing of onderbouwing van verlenging moet voldoende beargumenteerd zijn voordat deze wordt doorgevoerd.
4. De vernietigingslijst wordt toegezonden naar het BHIC, t.a.v. de gemeentearchivaris.

5. De inspecteur controleert de lijst en maakt eventueel opmerkingen.
6. Als er aanpassingen zijn doorgevoerd in de selectielijst wordt de aangepaste lijst nogmaals naar de gemeentearchivaris gestuurd.
7. De gemeentearchivaris brengt positief advies uit over de vernietiging (machtiging voor vernietiging) van de in de vernietigingslijst genoemde archiefbescheiden.
8. Op basis van het advies is akkoord voor de uitvoering van vernietiging plaats van de archiefbescheiden
9. Gemeentesecretaris of directeur MGD accordeert de verklaring van vernietiging.
10. Ondertekende verklaring van vernietiging wordt toegezonden naar het BHIC.
11. De vernietigingslijst, het akkoord van de gemeentearchivaris, de verklaring van vernietiging en vernietigingsbewijs vernietigingsbedrijf of uitdraai van de vernietigingsmodule in het zaaksysteem wordt opgeslagen in een te bewaren zaak in het zaaksysteem.

Een en ander is in navolgend figuur schematisch weergegeven.



3.7. Frequentie van vernietiging

De frequentie van vernietigen wordt bepaald door welke procedure gevolgd moet worden.

Analoge vernietiging	Digitale reguliere vernietiging	Digitale Doorlopende machtiging
1x per jaar alles tegelijk	2x per jaar in blokken van maximaal 1000 zaken	In principe 4x per jaar*

* Op basis van het aanbod van het aantal te vernietigen stukken kan voor de doorlopende machtiging een afwijkende frequentie worden toegepast.