Bespreekstuk DUTO-functionaliteiten, implementatiepatronen en modeleisen

*NB: Dit document is nog een concept. De Archimate-platen en de modeleisen zijn nog aan veranderingen onderhevig. Op dit moment vragen we om die reden met name feedback op de hooflijnen en structuur.*

# Inleiding

Dit document bevat de beoogde onderdelen voor het beschrijven van de DUTO-functionaliteiten, de implementatiepatronen en de modeleisen. Het stuk heeft een generiek deel en een specifiek deel, met een uitwerking van de DUTO-functionaliteit vernietigen.

Deel 1 begint met een visueel overzicht van DUTO-functionaliteiten in een functiemodel dat uitgaat van de datalifecycle.

Allereerst is het voornemen om een visueel overzicht van DUTO-functionaliteiten te maken. Het basisfunctiemodel. In dit document is een voorbeeld opgenomen van hoe dat eruit zou kunnen zien. Dit voorbeeld gaat uit van de datalifecycle. De vraag aan de redactiegroep is of dit een geschikte basis is om de functionaliteiten te structureren.

Vervolgens beschrijven we drie generieke implementatiepatronen. Deze zijn ontleend aan de ISO 16175 en voorzien van een toelichting hoe deze patronen gelezen moeten worden binnen de context van DUTO. Het idee is dat deze generieke implementatiepatronen voor alle DUTO-functionaliteiten gebruikt kunnen worden.

In deel 2 hebben we de DUTO-functionaliteit vernietigen uitgewerkt. De bedoeling is dat alle DUTO-functionaliteiten volgens hetzelfde stramien worden beschreven. De voorgestelde structuur is als volgt:

* Definitie (wat) – beschrijving van de functionaliteit
  + Gerelateerde termen – overzicht van gerelateerde begrippen en definities
  + Functionele processtappen – beschrijving van welke processtappen door de functionaliteit worden ondersteund
* Rationale (waarom) – koppeling met de waarde(n) van DUTO
* Randvoorwaarden (waarmee) – overzicht van zaken die vooraf geregeld moeten zijn
* Toepassing (wanneer) – beschrijving wanneer de functionaliteit van toepassing is
* Beheerregimes – verschillende beheerregimes, afhankelijk van de informatiewaarde en risico’s
  + Variant zwaar – de meest aangeklede variant
  + Variant licht – de absolute minimumvariant
* Implementatiepatronen – vertaling van de generieke patronen naar de specifieke functionaliteit
* Modeleisen – overzicht van modeleisen, gekoppeld aan de beschreven patronen
* DUTO-relaties – koppeling met de DUTO-waarde(n) en DUTO-kenmerken.

Deel 1: generiek deel

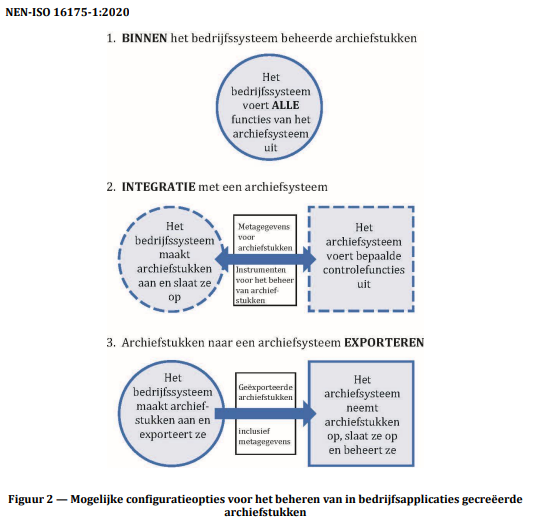
# Basisfunctiemodel

*NB: Onderstaande plaat is niet vastgesteld en is bedoeld als voorbeeld van hoe een basisfunctiemodel er uit zou kunnen zien.*



# Implementatiepatronen

De implementatiepatronen zijn gebaseerd op de ISO 16175. Deze beschrijft de volgende hoofdpatronen:



## Algemene toelichting op de hoofdpatronen

Het doel van de patronen, is om te kunnen bepalen wanneer welke modeleisen van toepassing zijn. De patronen hebben betrekking op een specifieke functionaliteit. Dat betekent dat voor één informatiesysteem voor verschillende functionaliteiten verschillende patronen van toepassing kunnen zijn.

We kennen een aantal varianten waarbinnen DUTO-functies zich kunnen bevinden of worden ondersteund:

1. Binnen een specifieke (vak)applicatie die een stuk specifieke bedrijfsvoeringsfunctie of specifiek uitvoeringproces ondersteunt. Meestal is dat binnen een specifieke afdeling of specifiek domein.



1. Binnen een gemeenschappelijk component die een generieke DUTO-functionaliteit ondersteunt. Meestal is dit op basis van “open” API’s die elke organisatie kan gebruiken.



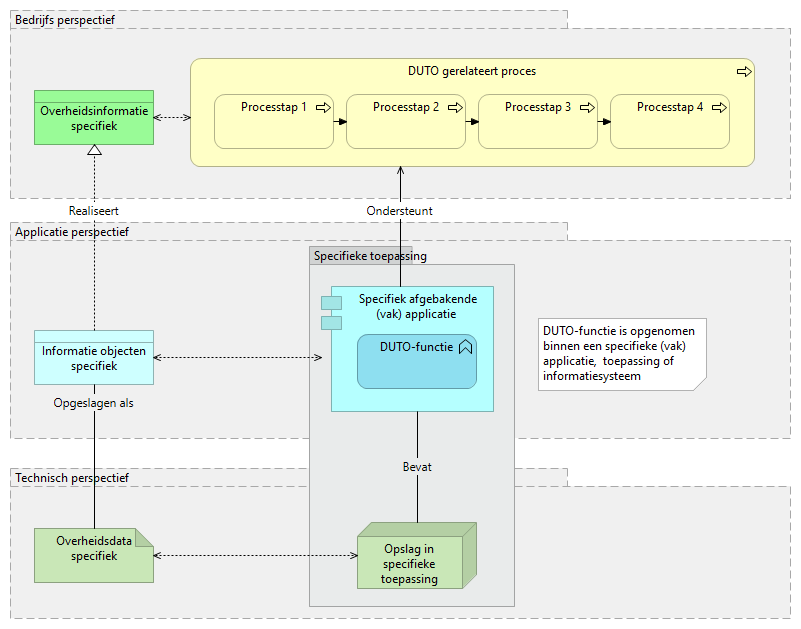
1. Binnen een generieke (concern)applicatie die een generieke functie of domein ondersteunt. Meestal is dit binnen een concern.



## Nadere toelichting op de hoofdpatronen

**Patroon 1:** Een specifiek afgebakende (vak)applicatie, toepassing of systeem dat zowel de bedrijfsfunctie als de DUTO-functionaliteit ondersteunt. Dit kan bijvoorbeeld een zaaksysteem, een vergunningenapplicatie of een personeelssysteem zijn.

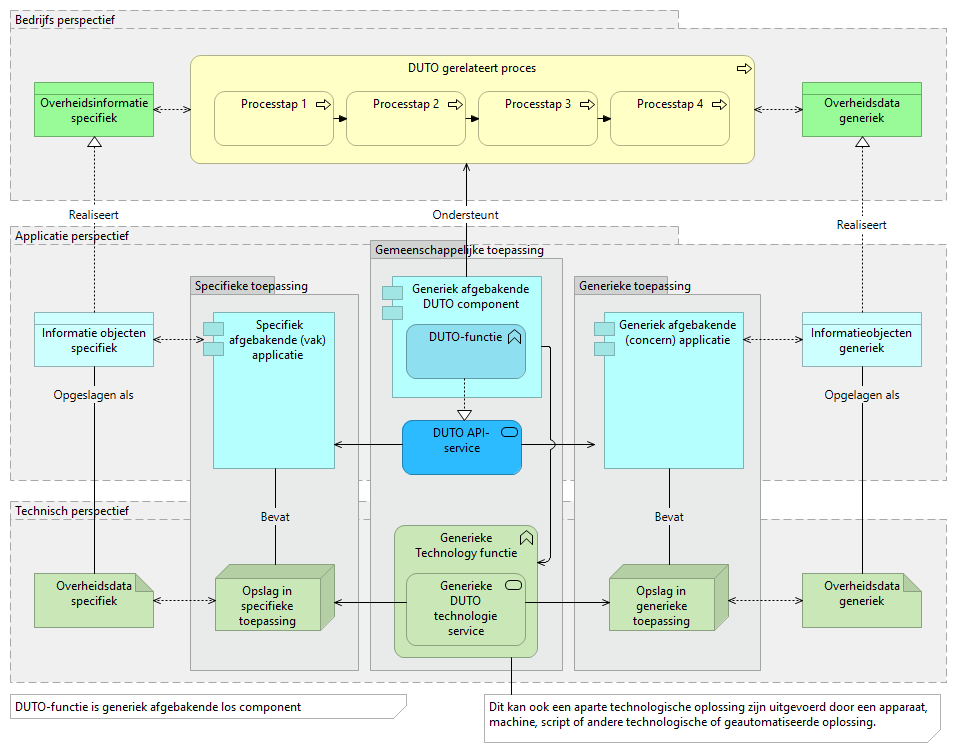
Bij keuze voor dit implementatiepatroon, worden de modeleisen voor de DUTO-functionaliteit dus meegenomen in de aanschaf en/of bouw van de specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt.



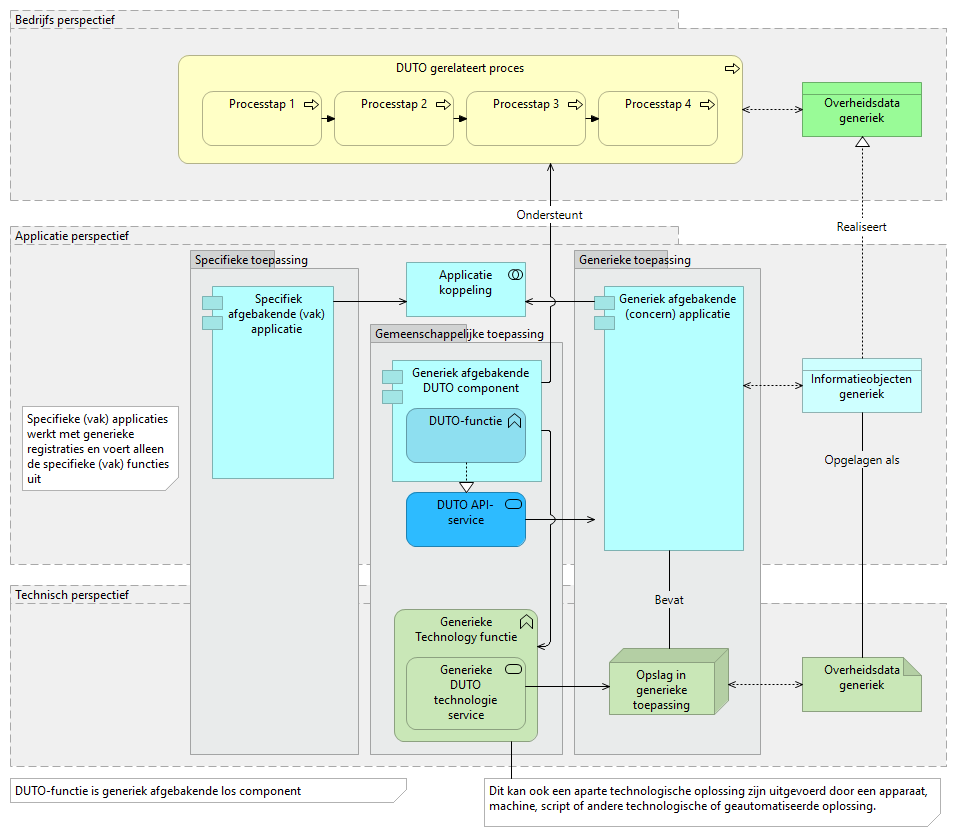
**Patroon 2:** Een specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt, maar niet de DUTO-functionaliteit. De DUTO-functionaliteit bevindt zich in een gemeenschappelijk DUTO-component die de DUTO-functionaliteit generiek ondersteunt. Dit kan bijvoorbeeld een zoek-, anonimisering-, registratie- of vernietigingscomponent zijn.

Bij keuze voor dit implementatiepatroon, worden de modeleisen voor de DUTO-functionaliteit meegenomen in de aanschaf en/of bouw van het gemeenschappelijk afgebakende DUTO-component.

**Patroon 2a:** De specifiek afgebakende (vak)applicatie en de generiek afgebakende (concern) applicatie, toepassing of systeem kunnen de DUTO-functionaliteit afnemen via een API-service en/of technologische functie, via het gemeenschappelijke generiek afgebakende DUTO-component



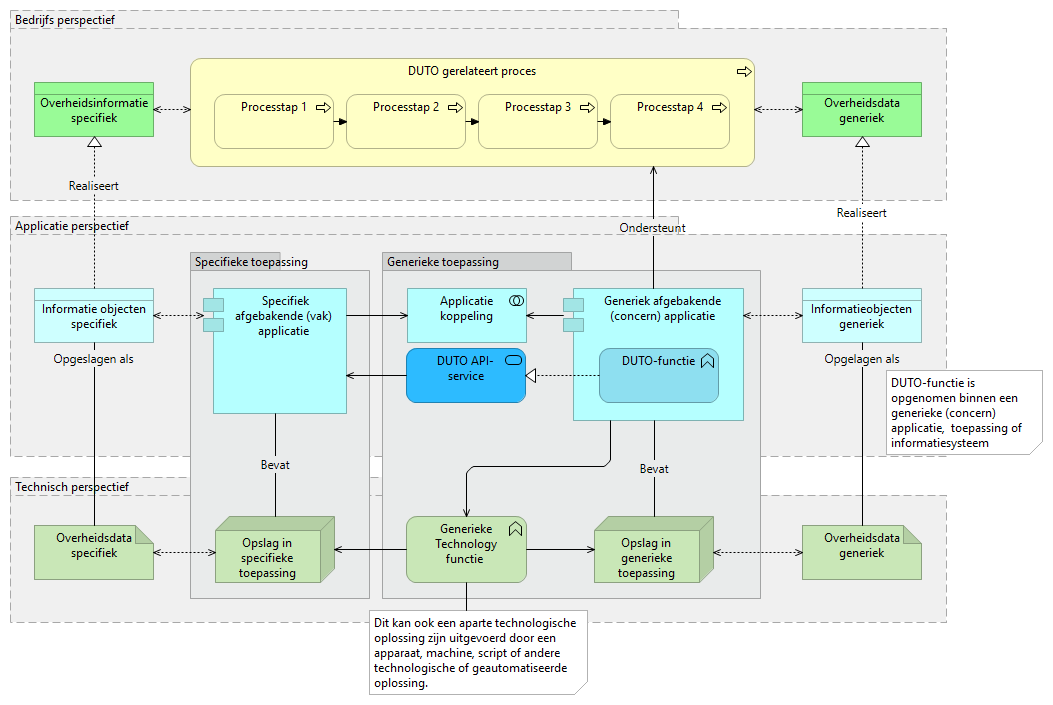
**Patroon 2b:** De specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt gebruikt de generieke opslag van de generiek afgebakende (concern) applicatie. De specifiek afgebakende (vak) applicatie hoeft geen gebruik te maken van de DUTO-functionaliteit. Dit wordt uitgevoerd via de generiek afgebakende (concern) applicatie die de DUTO-functionaliteit afneemt via een API-service en/of technologische functie, van het gemeenschappelijke generiek afgebakende DUTO-component.



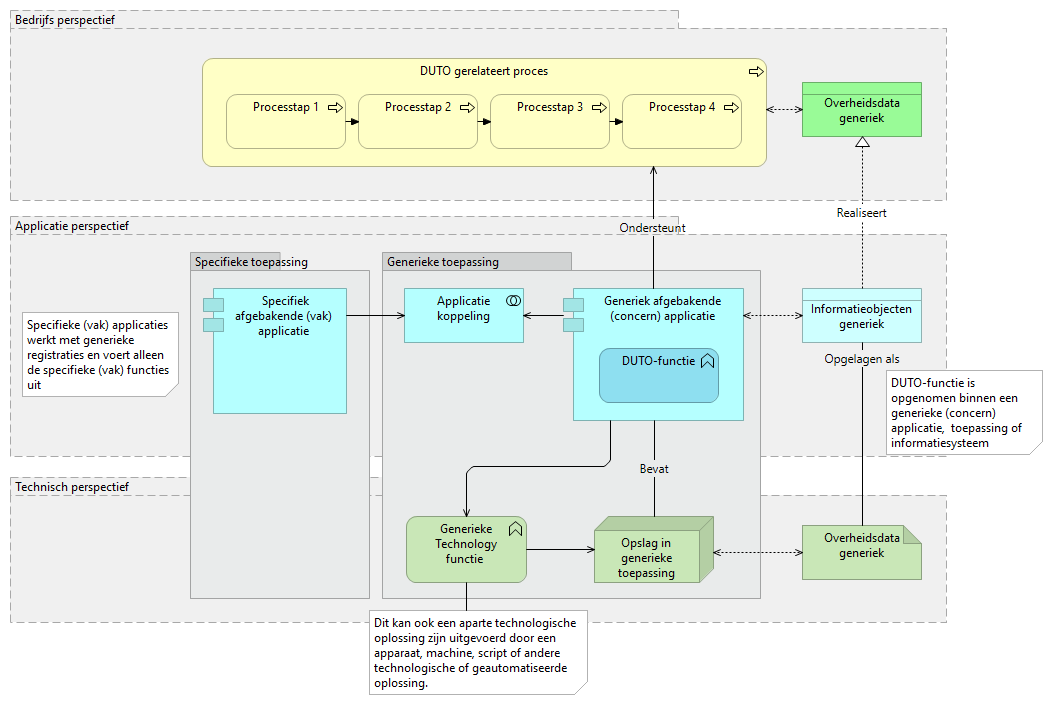
**Patroon 3:** Een specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt, maar niet de DUTO-functionaliteit. De DUTO-functionaliteit bevindt zich in een generiek afgebakende applicatie, toepassing of systeem die de DUTO-functionaliteit generiek ondersteunt. Dit kan bijvoorbeeld een e-depot, DMS of RMA-systeem zijn.

Bij keuze voor dit implementatiepatroon, worden de modeleisen voor de DUTO-functionaliteit dus meegenomen in de aanschaf en/of bouw van de generiek afgebakende (concern) applicatie, toepassing of systeem.

**Patroon 3a:** De specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt kan de DUTO-functionaliteit via een koppeling, API-service en/of technologische functie, van de generiek afgebakende (concern) applicatie afnemen.



**Patroon 3b:** De specifiek afgebakende (vak)applicatie, toepassing of systeem die de bedrijfsfunctie ondersteunt gebruikt de generieke opslag van de generiek afgebakende (concern) applicatie. De specifiek afgebakende (vak) applicatie hoeft geen gebruik te maken van de DUTO-functionaliteit. Dit wordt uitgevoerd via de generiek afgebakende (concern) applicatie

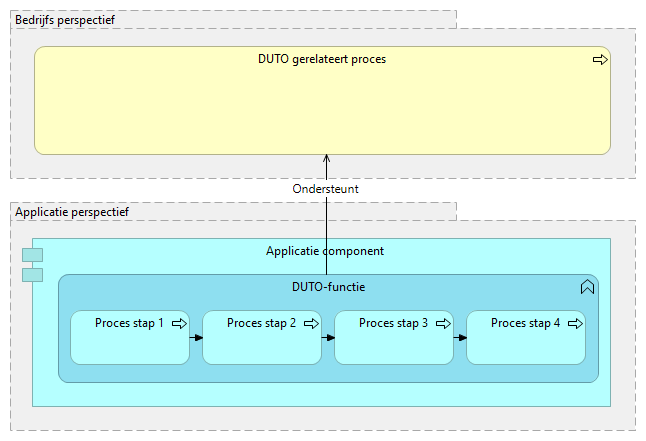


Beheerregimes

In deze opzet zijn twee beheerregimes beschreven: een maximumvariant (zwaar) en een minimumvariant (licht). In de praktijk zijn tussenvarianten mogelijk. Organisaties kunnen dergelijke tussenvarianten vormgeven door het voorgestelde gewicht van de modeleisen aan te passen.

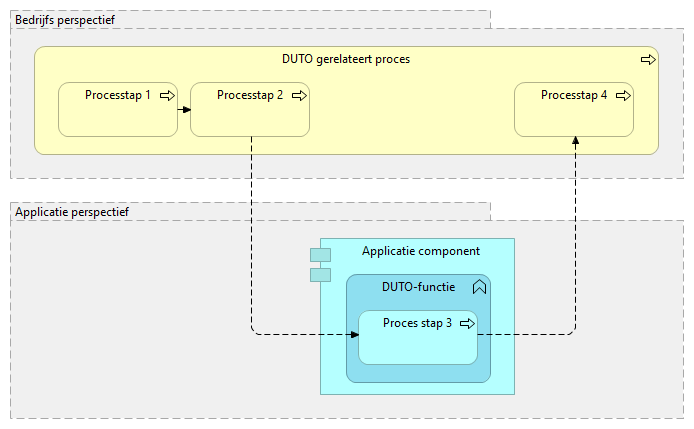
Beheerregime zwaar

In het beheerregime zwaar, worden alle functionele processtappen die een relatie hebben met de DUTO-functionaliteit applicatief ondersteund.



Beheerregime licht

In het beheerregime licht, worden niet alle processtappen die een relatie hebben met de DUTO-functionaliteit applicatief ondersteund.



Modeleisen

Per patroon kan het beheersregime worden toegepast en hiermee kan de zwaarte van de modeleisen worden bepaalt. In de modeleisen die per functie worden/zijn uitgewerkt is in een kolom de relatie naar het patroon en beheerregime aangegeven.



Deel 2: DUTO-functionaliteit vernietigen

# Definitie (wat)

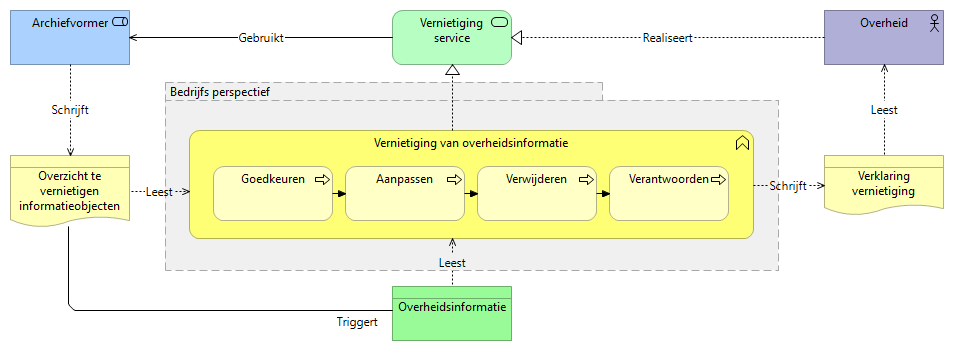
De DUTO-functionaliteit vernietigen gaat over de activiteiten die nodig zijn om informatieobjecten, zoals (combinaties van) bestanden, gegevens, datasets, links en verwijzingen, aan het einde van de vastgestelde bewaartermijn te vernietigen op de plek waar deze zich bevinden zodat deze voor niemand meer kenbaar en/of vindbaar en/of reconstrueerbaar zijn.

## Gerelateerde termen:

* Verwijderen: dit is de meest eenvoudige methode waarbij het volstaat om de gegevensdrager eenmalig te overschrijven met een willekeurig bitpatroon. Opgemerkt wordt dat informatieobjecten die op deze manier zijn vernietigd op een eenvoudige manier teruggehaald kunnen worden. (Bron: BIO)
* Overschrijven: hierbij wordt de gegevensdrager meervoudig (minimaal drie keer) overschreven doormiddel van een ‘nul’ character, een ‘één’ character gevolgd door een willekeurig character of teken (niet binair). Bij deze vorm van vernietigen is het terughalen van de vernietigde informatieobjecten praktisch onmogelijk. (Bron: BIO)
* Deleten: hierbij wordt de drager (het apparaat) van de informatieobjecten versnipperd, of fysiek vernietigd of verbrand. Deze vorm is nodig wanneer het soort informatie extra gevoelig is of als andere methoden om gegevens te verwijderen niet kunnen worden gebruikt (bv. CD/DVD). (Bron: BIO)
* Digitaal 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. (Bron: Moreq2010)

## Functionele processtappen

Vernietigen kent vier functionele processtappen.



Per processtap is een aantal mogelijke activiteiten beschreven.

1. Goedkeuren
   * Vernietigingsoverzichten genereren per stuk, per kwartaal, per jaar, etc
   * Accorderen van het vernietigingsoverzicht
2. Aanpassen bewaartermijn
   * Uitzonderen van vernietigen
   * Verlengen bewaartermijn
3. Verwijderen informatieobjecten
   * Verwijderen van verwijzingen en indexen
   * Eenmalig of meervoudig overschrijven
   * Deleten met behoud van metadata dat het gegeven er ooit is geweest
   * Onherstelbaar vernietigen
   * Fysieke drager vernietigen
4. Verantwoorden
   * Vernietigingsoverzichten genereren per kwartaal, per jaar etc.

# Rationale (waarom)



De kern ligt bij het hoofddoel *Legitimiteit:* benodigd om bewaartermijnen en risico’s na te leven conform wet- en regelgeving.

Secundair draagt vernietiging bij aan *Organisatie****:*** efficiëntie, beheerlast, kosten, duurzaamheid.

Door het proces van vernietiging goed te documenteren, wordt tot slot bijgedragen aan *Publieke waarde*: open en transparant.

# Randvoorwaarden (waarmee)

* Er is een selectielijst, waarin opgenomen de te vernietigen informatieobjecten of onderdelen daarvan.
* Er is beleid met betrekking tot vernietigen dat is vastgesteld en verankerd binnen de organisatie.
* Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd.
* Er is een (architectuur)overzicht van informatieobjecten, processen, informatiesystemen en hun samenhang.
* Er is een procedure voor vernietiging inclusief protocol voor wijze van vernietigen en wijze van verantwoorden.
* Er kan over vernietiging worden verantwoord, bijvoorbeeld: borging door toezicht in P&C cyclus.

# Toepassing (Wanneer)

Wanneer de functie vernietigen wordt ingezet wordt bepaald door:

* Verplicht op basis van wet- en regelgeving

# Toepassing (waar)

De locatie van de te vernietigen informatieobjecten is afhankelijk van het informatiesysteem waarin de informatieobjecten zich bevinden.

Informatieobjecten kunnen zijn opgeslagen in bijvoorbeeld:

* Het bron(vak)systeem waarin ze gemaakt zijn en/of beheerd worden.
* Een centraal informatiesysteem waarin ze worden opgeslagen en beheerd.
* Een fysieke drager die is aangeleverd

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

# Beheerregimes

In deze opzet zijn twee beheerregimes beschreven: een maximumvariant (zwaar) en een minimumvariant (licht). In de praktijk zijn tussenvarianten mogelijk. Organisaties kunnen dergelijke tussenvarianten vormgeven door het voorgestelde gewicht van de modeleisen aan te passen.

## Beheerregime zwaar

In het beheerregime zwaar, worden alle functionele processtappen applicatief ondersteund.

Dit beheerregime is van toepassing op informatiecategorieën waarvoor het op basis van de uitzonderingsgronden in de selectielijst mogelijk is om af te wijken van de standaardbewaartermijn.

Bijvoorbeeld: De selectielijst voor gemeentelijke en intergemeentelijke organen 2020 noemt een zestal uitzonderingscriteria, zoals: ‘Archiefbescheiden over zaken of gebeurtenissen met een voor het eigen orgaan uniek of bijzonder karakter, of archiefbescheiden die door hun vorm of aard op zichzelf of voor de gemeente beeldbepalend, representatief, karakteristiek of bijzonder zijn’. Dit zou bijvoorbeeld van toepassing kunnen zijn op informatiecategorieën als vergunningen of subsidies.

## Beheerregime licht

In het beheerregime licht, worden niet alle processtappen applicatief ondersteund.

Dit beheerregime is van toepassing op informatiecategorieën met gegevens die nooit gedeeld wordt in een keten en die een standaardbewaartermijn kent die niet afhankelijk is van variabelen, zoals het resultaat van het proces. In deze gevallen is een bewaartermijn al vóór de start van het proces bekend. De processtappen “goedkeuren” en “verantwoorden” worden eenmalig door middel van werkafspraken geregeld en vastgelegd. Ze hoeven daarom niet als functionaliteit in een systeem te worden ingericht. De processtap “aanpassen” komt niet voor.

Bijvoorbeeld: IP-adressen van websitebezoekers, interne verzoeken voor het lenen van een dienstfiets, reserveringen vergaderruimte.

# Modeleisen



Onderstaand schema biedt een thematisch overzicht van de modeleisen eisen, waarbij in de kolom “Patronen” is toegelicht op welk patroon of welke patronen ze van toepassing zijn. Op zo hoog mogelijke aggregatie, dus ‘3’ wil zeggen ook alle onderliggende patronen onder het hoofdpatroon 3.

Voor patronen 2 en 3 is de aanname dat wordt aangesloten op reeds bestaande en ingerichte voorzieningen. Wanneer deze voorzieningen er niet zijn, dan kunnen de eisen voor patroon 1 worden gebruikt voor het aanschaffen en/of ontwikkelen van dergelijke voorzieningen.

In de kolom “MoSCoW” is een weging op basis van de MoSCoW-methodiek (Must have, Should have, Could have, Won’t have) toegekend. Deze weging is bedoeld ter referentie.

Daar waar de eisen gebaseerd zijn op eisen uit andere normen, is dat vermeld in de laatste kolom. Een deel van de eisen is (mede) gebaseerd op een functioneel ontwerp van de Vereniging Nederlandse Gemeenten (VNG) voor een generiek vernietigingscomponent. Dat is aangegeven met “FO VNG”.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Eis | Type | MoSCoW | Patronen | Bron(nen) |
| Eisen m.b.t. voorbereiding van vernietiging (functionele eisen en organisatorische randvoorwaarden) | | | | | |
| * + 1. Functionele eisen | | | | | |
| V1 | Van informatieobjecten die voor vernietiging in aanmerking kan een overzicht worden gecreëerd. | Functioneel | M | 1.1 | NEN-ISO 16175-1, 2.1.3  FO VNG |
| V2 | Gebruikershandelingen in het vernietigingsproces zijn traceerbaar | Functioneel | S | 1.1 | NEN-ISO TR 21965, 3.1.10  NEN-ISO 15489-1, 9.9  FO VNG |
| V3 | Het informatiesysteem vraagt om een dubbele bevestiging van de vernietigingsactie | Functioneel | C | 1.1 | FO VNG |
| V4 | Het autoriseren van de vernietigingsfunctie is eenvoudig te configureren | Functioneel | S | 1.1 | FO VNG |
| V5 | Alleen geautoriseerde personen kunnen vernietigen | Functioneel | C | 1.1 | FO VNG |
| V6 | Vernietigingslijsten kunnen worden geëxporteerd naar een acceptabel bestandsformaat conform de Handreiking Voorkeursformaten *[of organisatiespecifieke standaard]* | Functioneel | S | 1.1 | FO VNG |
| V7 | Vernietigingslijsten kunnen worden geconfigureerd op basis van beschikbare metadatavelden. | Functioneel | S | 1.1 | FO VNG |
| V8 | Het is mogelijk om van vernietigingslijsten een geanonimiseerde en een niet-geanonimiseerde versie te maken. | Functioneel | S | 1.1 | FO VNG |
| V9 | Het overzicht van voor vernietiging in aanmerking komende informatieobjecten bevat links waarmee de vermelde informatieobjecten kunnen worden getoond | Functioneel | C | 1.1 | FO VNG |
| V10 | Het is mogelijk om een of meerdere (gemandateerde) collega’s toegang te geven tot (delen van) de vernietigingslijst om deze te kunnen beoordelen | Functioneel | S | 1.1  2.1  3.1 | FO VNG |
| V11 | Het informatiesysteem kan o.b.v. aldaar aanwezige metadata automatisch het moment van vernietiging berekenen | Functioneel | M | 1.1  1.2 | NEN-ISO 16175-1 , R.2.1.1 |
| V12 | Het informatiesysteem kent voldoende metadata toe om het moment van vernietiging te kunnen berekenen. *[Situationeel aanscherpen. Bijvoorbeeld: minimaal een creatiedatum of minimaal een einddatum]* | Functioneel | M, ivt | 1.1  1.2  2.1  2.2  3.1  3.2 | FO VNG |
| V13 | Het is *[op elk aggregatieniveau]* mogelijk om de bewaartermijn aan te passen | Functioneel | M | 1.1 | FO VNG |
| V14 | Het is mogelijk om een toelichting op te nemen over afwijkingen op bewaartermijn | Functioneel | C | 1.1 | FO VNG |
| V15 | Het is mogelijk om bewaartermijnen in bulk aan te passen | Functioneel | S | 1.1 | FO VNG |
| V16 | Het is mogelijk om te herleiden welke informatieobjecten zijn vernietigd. | Functioneel | S | 1.1 2.1 3.1 | NEN-ISO 16175-1 |
| V17 | De bewaartermijn kan op verschillende aggregatieniveaus worden aangegeven (werkproces, zaakdossier, document). De waardering kan daarbij overerven van een hoog, naar een laag aggregatieniveau. | Functioneel | S | 1.1  1.2  2.1  2.2 | NEN-ISO 16175-1, R2.1.1 |
| V18 | Als de bewaartermijn in de selectielijst wordt gewijzigd, moet de betreffende metadata kunnen worden aangepast. Als peildatum voor de mutatie wordt de datum genomen dat de nieuwe selectielijst van kracht is. Bewaartermijnen van voor deze peildatum blijven onveranderd. | Functioneel | S | 1.1  2.1 | NEN-ISO 16175-1, R2.1.1 |
| V19 | Er kan in bulk worden vernietigd (zonder limiet aan het aantal informatieobjecten) | Functioneel | M | 1.1 | FO VNG |
| V20 | Het vernietigingsproces kan volledig geautomatiseerd worden uitgevoerd (waar mogelijk en juridisch toegestaan) | Functioneel | M | 1.2 | FO VNG |
| * + 1. Organisatorische eisen | | | | | |
| V21 | Er is een beschrijving van de type informatieobjecten die volledig geautomatiseerd worden vernietigd | Organisatorisch | M | 1.2  2.2  3.2 |  |
| V22 | In geval van SAAS: Opdrachtnemer vernietigt uitsluitend in opdracht van opdrachtgever en levert na afronding een verklaring van vernietiging | Dienstverlening | M | 1.1 |  |
| V23 | Er is een proces ingericht om voor vernietiging in aanmerking komende informatieobjecten voorafgaand aan de vernietiging te controleren. | Organisatorisch / Functioneel | M | 1.1 1.2 2.1 2.2 3.1 3.2 | ISO 15801, 6.11 |
| V24 | Er is een beschrijving van hoe het vernietigingsproces wordt uitgevoerd en welke actoren daarin een rol hebben. | Organisatorisch | S | 1.1 2.1 | NEN-ISO 16175-1, 2.1.2 |
| * + 1. Specifieke eisen m.b.t. koppelingen | | | | | |
| K1 | De oplossing kan koppelen met de vernietigingscomponent op basis van *[de van toepassing zijnde koppelingsstandaard(en)]* | Functioneel | M | 2.1 |  |
| K2 | De oplossing kan koppelen met *[de archiefapplicatie (zoals DMS of e-depot) op basis van de van toepassing zijnde koppelingsstandaard(en)]* | Functioneel | M | 3.1 |  |
| 1. Eisen m.b.t. feitelijke vernietiging zelf | | | | | |
| V25 | Het is gedurende *[vastgestelde periode]* mogelijk om een uitgevoerde vernietigingsactie terug te draaien. | Functioneel | C | 1.1 | NEN-ISO 16175-1 |
| V26 | Informatieobjecten kunnen na het verstrijken van de bewaartermijn worden vernietigd. Het vernietigen van  informatieobjecten leidt tot het volledig wissen of ontoegankelijk maken van deze informatieobjecten. Hierbij wordt ook de vermelding in de index vernietigd, zodat er geen vermeldingen meer zijn in zoekresultaten (niet zijnde de vernietigingslijst). | Functioneel | M | 1.1 1.2 2.1 2.2 3.1 3.2 | NEN-ISO 16175-1, 2.1.6  NEN-ISO 15489 2016, 9.9  BIO 8.3.2.3  FO VNG |
| Eisen aan component | | | | | |
| V27 | Informatieobjecten in één keer in alle aangesloten bronnen kunnen vernietigen | Functioneel | M | Nvt (t.b.v. 2.1 en 2.2.) | FO VNG |
| 3. Eisen m.b.t. situatie na vernietiging | | | | | |
| * + 1. Functionele eisen | | | | | |
| V28 | Het is mogelijk om een rapport te genereren waaruit blijkt dat informatieobjecten zijn vernietigd. | Functioneel | S | 1.1 2.1 3.1 | NEN-ISO 16175-1, R2.1.5 |
| * + 1. Organisatorische Eisen | | | | | |
| V29 | Back-ups worden niet langer dan *[periode]* bewaard, om te voorkomen dat al vernietigde informatieobjecten weer hersteld kunnen worden. | Organisatorisch (igv on premise)  Dienstverlening (igv SAAS) | S | 1.1  1.2  2.1  2.2 | Moreq, 514 |
| V30 | Bij een back-up-recovery, wordt een vernietigingsactie die is uitgevoerd na het moment waarop de back-up is gemaakt, opnieuw uitgevoerd zodat reeds vernietigde gegevens niet opnieuw in de productieomgeving beschikbaar zijn | Organisatorisch (igv on premise)  Dienstverlening (igv SAAS) | M | 1.1  1.2  2.1  2.2  3.2 |  |

# DUTO-Relaties

**Koppelt aan DUTO-waarde:**

* 2. Legitimiteit – Voldoen aan wet- en regelgeving
* 3. Organisatie – Efficiënte en effectieve taakuitvoering, in control zijn op informatiebeheer, bijdragen aan klimaatdoelstellingen

**Koppelt aan DUTO-kenmerk:**

* Betrouwbaar