

Rapport thema-onderzoek Digitaal vernietigen

Archiefinspectie, 21 februari 2023
Corsanummer D230046044

Inhoud

1. Inleiding	3
Archieftoezicht en het uitvoeren van audits	
Onderzoek om inzicht te krijgen in de mate van vernietiging en waarom dit niet gebeurt	
Waarom is vernietiging van digitale informatie nodig	
2. Digitaal vernietigen in Nijmegen	4
Beleid voor digitaal vernietigen is onderdeel van beleid voor informatiebeheer maar ontbreekt	
Procedures voor vernietiging uit het centrale archiefsysteem Corsa en op andere plekken	
Digitaal vernietigen is ingewikkeld en we zijn ons onvoldoende bewust van de noodzaak hiervan	
3. Conclusies uit het onderzoek	6
Wat gaat goed	
Wat moet beter	
Conclusies:	
a. Beleid ontbreekt, digitaal vernietigen gebeurt niet zoals het zou moeten	
b. Digitaal vernietigen is ingewikkeld en daarom moeilijk te organiseren	
c. Kennis in de organisatie over (verantwoord) digitaal vernietigen is onvoldoende	
d. We verplaatsen niet, maar kopiëren onze informatie en bewaren in veelvoud	
e. Digitaal vernietigen is niet altijd technisch of praktisch uit te voeren	
f. Archiefbewustzijn ontbreekt en we voelen geen urgentie om digitaal te vernietigen	
4. Aanbevelingen	8
1. Stel beleid op voor digitaal vernietigen en geef invulling aan de verantwoordelijkheden	
2. Zorg voor grip op het informatiebeheer, vooral op ongestructureerde informatie buiten Corsa	
3. Investeer in digitaal vernietigen	
4. Maak dat vernietiging uit informatiesystemen technisch en praktisch mogelijk is	
5. Organiseer de vernietiging van digitale informatie	
Bijlage a. Verantwoording van de audit	10
Bijlage b. Bevindingen	11
Bijlage c. Artikel Ontspullen en oprommelen	15

1. Inleiding

Archieftoezicht en het uitvoeren van audits

De archiefinspectie brengt rapporten uit als onderdeel van het toezicht op het beheer van de archieven. De inspecteur onderzoekt of de gemeente Nijmegen voldoet aan de Archiefwet. Om de rapporten te kunnen onderbouwen voeren we integrale audits uit naar het informatiebeheer of we onderzoeken een bepaald aspect of thema. De rapporten bieden we aan bij de afdelingsmanagers (opdrachtgevers) met het verzoek actie te ondernemen op de conclusies en aanbevelingen.

Zo ook deze thema-audit naar de mate van digitaal vernietigen binnen onze organisatie. Uit de inspecties weten we dat we in Nijmegen onze digitale informatie veel te lang bewaren. De archiefinspecteurs wilden weten wat de belemmeringen voor vernietigen zijn. Belangrijke conclusie uit de audit is dat digitaal vernietigen alleen kan als ons informatiebeheer op orde is overal binnen de gemeentelijke organisatie en onze systemen op vernietiging zijn ingericht. Niet goed gearchiveerd, betekent ook niet systematisch vernietigd.

Dit rapport van de archiefinspectie geeft inzicht in:

- de wijze waarop in Nijmegen vernietiging van digitale archiefinformatie is geregeld en ingericht;
- de mate waarin daadwerkelijk wordt vernietigd na het verstrijken van de bewaartermijn;
- welke knelpunten we daarbij ervaren en mogelijke verbeterpunten zijn.

In bijlage a. staat een verantwoording van de onderzoeksaanpak. In bijlage b. zijn de bevindingen opgenomen. Bijlage c. bevat een aanvullend achtergrondartikel.

Dit rapport wordt aangeboden aan de concernmanager PIF. De conclusies van dit auditrapport worden verwerkt in het jaarlijkse verslag van de gemeentearchivaris dat bestemd is voor het College.

Waarom digitale informatie vernietigen

In Nijmegen produceren we veel archiefinformatie in digitale vorm en op verschillende plekken. We hanteren de landelijke Gemeentelijke Selectielijst waarin vastligt welke informatie we willen bewaren en hoe lang. Als de bewaartermijn voorbij is, zijn we wettelijk verplicht om de documenten en datasets te vernietigen. We moeten de vernietiging vervolgens kunnen verantwoorden.

Vernietigen maakt de overgebleven informatie beter te beheren en te vinden. Vernietigen vermindert de opslag en bespaart kosten. Vernietigen geeft bovendien minder administratieve last bij Woo-verzoeken en helpt bij privacy en informatiebeveiliging. Wat er niet is hoeft je niet af te schermen.

Als we digitale informatie niet goed of te laat vernietigen lopen we als gemeente risico's, waaronder hogere beheerkosten en het niet voldoen aan wet- en regelgeving. Informatie die niet goed wordt beheerd belemmert de uitvoering van onze taken en kan leiden tot slechte dienstverlening en imagoschade. Gegevens die vernietigd hadden moeten zijn maar ergens bewaard zijn gebleven, blijven vallen onder de openbaarmaking volgens de WOO en het inzagerecht volgens de AVG.

Digitale informatie kent vele vormen, zoals de digitaal geboren of gedigitaliseerde dossiers in Corsa, documenten op netwerkschijven, gegevenssets en documenten in procesapplicaties, e-mails, video's, foto's, chatberichten en websites. Digitaal slaan we onze informatie in meervoud op, want digitale gegevens laten zich gemakkelijk vermenigvuldigen.

Informatie heeft een archiefstatus als deze een rol speelt in een gemeentelijk werkproces of daaruit voortkomt. De status van een digitaal bestand moet duidelijk zijn. Bij archiefstukken hanteren we het begrip archiefexemplaar en digitale kopie. Hybride informatie is een combinatie van digitaal en analoog (= papier). Archiefinformatie is gekoppeld aan metadata die duiding geeft aan de informatie zodat de informatie vindbaar, te beheren en te vernietigen is.

Vernietigen volgens de regels van informatiebeheer houdt in dat (alle versies van) documenten en gegevenssets, afhankelijk van risico's en technologische mogelijkheden, ontoegankelijk worden gemaakt, gewist of verwijderd en dit alles op zo'n manier dat reconstructie onmogelijk is. Anonimiseren is ook een vorm van archiefvernietiging.

2. Digitaal vernietigen in Nijmegen

Beleid voor digitaal vernietigen is onderdeel van het beleid voor informatiebeheer

In Nijmegen hebben we geen actuele uitgangspunten geformuleerd voor ons digitaal informatiebeheer, en evenmin voor het vernietigen van digitale informatie.

We volgen de regels uit de Archiefwet. De verplichting tot vernietigen komt terug in ons Besluit informatiebeheer uit 2013. We hanteren de landelijke selectielijsten voor gemeenten. Onlangs heeft ons college besloten aan te sluiten bij de Selectielijst voor e-mailbewaring welke in de loop van 2023 gaat gelden. We zijn bezig met een visie op document- en bestandsmanagement.

In het Governanceplan Informatiebeheer gemeente Nijmegen (2019) is bepaald dat de afdelingen (en daarbinnen managers en medewerkers) verantwoordelijk zijn voor het informatiebeheer in de onder hen vallende bedrijfsfuncties en werkprocessen. Het gaat daarbij om alle soorten informatie binnen en buiten de gecontroleerde omgevingen. De managers en medewerkers in het primaire proces worden in het beheren van informatie gefaciliteerd en ondersteund door de bureaus in de informatieketen (afdeling PIF).

Vernietiging komt terug in ons beleid voor privacybescherming geformuleerd als 'niet langer bewaren dan noodzakelijk'. Dit is conform de privacywet AVG die bepaalt dat er voor het bewaren van persoonsgegevens een doel, noodzaak en grondslag moet zijn. In de DPIA's benoemt de proceseigenaar hoe lang gegevens worden bewaard en wie verantwoordelijk is voor de vernietiging.

De Wet Politiegegevens dwingt vernietiging van persoonsgegevens en geeft daar termijnen voor.

Ons informatiebeveiligingsbeleid geeft regels voor het beschermen van data tegen onbedoeld verwijderen. Ons beveiligingsbeleid zegt ook dat gegevens moeten worden verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd.

We doen niet aan risicoanalyse of dataclassificatie. Digitaal vernietigen is niet voor elke situatie gelijk. Het type informatie (denk aan vertrouwelijkheid en privacygevoeligheid) bepaalt in grote mate welke risico's de organisatie loopt bij het niet (tijdig en juist) vernietigen van de informatie. Het doel van de risicoanalyse is om te bepalen hoe groot het risico is dat bepaalde informatie te lang wordt bewaard en toegankelijk is en wat conform het veiligheidsniveau een passende vorm van vernietiging is.

Procedures voor vernietiging uit het centrale archiefsysteem Corsa en op andere plekken

Voor het digitaal vernietigen in Corsa kopiëren we de procedures en routines zoals we deze voor analoge dossiers hanteren. Dat houdt in: BDI en RAN vervaardigen lijstwerk van vernietigbare dossiers uit Corsa of laten dat doen door IRvN. We houden rekening met uitzonderingen op de vernietiging. Proceseigenaren worden gevraagd akkoord te gaan met de vernietiging van hun dossiers. Van de verwijdering uit Corsa wordt een Verklaring van vernietiging opgemaakt. Met de verklaring kan

worden aangetoond dat digitale archiefdossiers rechtmatig en volgens de afgesproken procedure daadwerkelijk zijn vernietigd.

BDI heeft procedures opgesteld voor het verwijderen van zaakdossiers en metadata uit Corsa (2021) en voor het (eenmalig) verwijderen van functionele mailboxen (2021). Uit 2018 dateert een Werkwijze controle, vergrendeling en vernietiging van digitale dossiers in Corsa. Voor dossiers over de regelingen Participatiewet, WMO en Jeugd is een procesbeschrijving gemaakt (2021). Dit document regelt de vernietiging van analoge en digitale zaakdossiers in Corsa op basis van IRvN-lijstwerk.

De Handreiking voor het uitfasen van applicaties en migratie (2021) bevat een paragraaf over het bepalen van de informatiewaarde van data in procesapplicaties en geeft strategieën voor het vernietigen dan wel veiligstellen van de data bij uitfasering van een applicatie. Niet migreren bij een uitfasering is een vorm van vernietigen.

Digitaal vernietigen is ingewikkeld en we zijn ons onvoldoende bewust van de noodzaak hiervan

Digitale informatie bevindt zich overal binnen de organisatie en in meerdere verschijningsvormen, deels ongestructureerd en er is veel dubbel. Even zoals bij het veilig omgaan met gegevens zijn er meerdere actoren met een bepaalde verantwoordelijkheid. Bij digitaal vernietigen zijn managers, proceseigenaren, (kwaliteits)medewerkers, informatiebeheerders, archiefinspecteurs, functioneel beheerders en applicatiebeheerders, en soms zelfs leveranciers betrokken.

Digitaal vernietigen is complex. Hoe selecteren we ongestructureerde informatie en voorzien deze van bewaartermijnen? Hoe organiseren we gelijktijdige vernietiging op alle plekken. Wie initieert, controleert en voert uit? Het zit het met vernietiging uit de procesapplicaties, zeker als er koppelingen zijn met andere systemen? Hoe richten we in applicaties ‘vernietiging by design’ in? Gelden vernietigingsrichtlijnen ook voor werkarchieven, mailboxen, chatberichten, websites?

Afdelingen (managers en medewerkers) zijn verantwoordelijk voor hun informatie en het tijdig vernietigen daarvan. Er is weinig bewustzijn in de organisatie over de noodzaak van dit vernietigen op alle plekken waar digitale informatie wordt bewaard. In Corsa is daar aandacht voor, vernietiging in de bronsystemen of van (ongestructureerde) informatie op andere plekken, zoals netwerkschijven, gebeurt nauwelijks en zeker niet systematisch.

In de huidige taakopvatting en met de huidige capaciteit zorgen de informatiebeheerders voor monitoring, dat medewerkers met Corsa om kunnen gaan en dat de archivering in Corsa mogelijk is. Voor advisering over vernietiging van informatie op andere plekken dan Corsa is te weinig tijd en BDI heeft hierin weinig overzicht en doorzettingsmacht.

3. Conclusies uit het onderzoek

Wat gaat goed

- Corsa is voor een deel opgeschoond: metadata van eerder vernietigde documenten en dossiers zijn verwijderd; digitale zaakdossiers uit het sociaal domein zijn vernietigd; van enkele processen zijn de digitale kopieën vernietigd tegelijk met de analoge dossiers;
- Incidenteel zijn gegevens uit procesapplicaties vernietigd: o.a. JVS (leerplicht en RMC)
- Vervanging van een procesapplicatie is een natuurlijk moment waarop we nadenken over de waarde van de data en de keuze tot meenemen naar de opvolger of vernietigen; uitfasen leidt vaak tot digitaal vernietigen van een deel van de gegevens of alle data uit de oude applicatie;
- Het komt vaker voor dat leveranciers procesapplicaties of nieuwe releases aanbieden met een functionaliteit voor selectie en vernietiging.

Wat moet beter

Ons informatiebeheer is niet op orde, daar begint het mee: niet gearcheeerd is ook niet goed beheerd en systematisch vernietigd. Vernietigbare dossiers blijven te lang staan in Corsa en procesinformatie blijft achter in onze procesapplicaties. We weten niet hoe digitaal vernietigen buiten Corsa moet. We verwijderen informatie zonder ons over de vernietiging te verantwoorden. We denken daar niet over na of laten ons afschrikken door de complexiteit en wat we daarvoor moeten regelen. We houden weinig rekening met de bijzondere aspecten van digitale informatie: in veelvoud aanwezig, technisch complex, veel ongestructureerd, en verwijderd is niet altijd weg.

Conclusies uit het onderzoek naar de mate van digitaal vernietigen binnen onze gemeente:

- a. Beleid ontbreekt, digitaal vernietigen gebeurt niet zoals het zou moeten
- b. Digitaal vernietigen is ingewikkeld en daarom moeilijk te organiseren
- c. Kennis in de organisatie over (verantwoord) digitaal vernietigen is onvoldoende
- d. We verplaatsen niet, maar kopiëren onze informatie en bewaren in veelvoud
- e. Digitaal vernietigen is niet altijd technisch of praktisch uit te voeren
- f. Archiefbewustzijn ontbreekt en we voelen geen urgentie om digitaal te vernietigen

a. Beleid ontbreekt, digitaal vernietigen gebeurt niet zoals het zou moeten

- Voor digitaal vernietigen gebruiken we de procedures die gelden voor Corsa en analoge dossiers; we hebben geen beleid en geen procedures voor vernietigen van álle soorten digitale informatie;
- Rollen en handelingen voor digitaal vernietigen zijn niet uitgewerkt. Het is onduidelijk wat precies de verantwoordelijkheid (taak en het mandaat) is van BDI als het gaat om digitaal vernietigen van informatie buiten Corsa. We weten niet wie vernietiging buiten Corsa of gelijktijdige vernietiging moet initiëren en hoe de procedure loopt;
- Bij decentrale archivering verschuiven de archiveringshandelingen, ook hoe we vernietiging uitvoeren. Procedures, kwaliteitszorg en ondersteuning sluiten niet altijd meer aan;
- We doen niet aan risicoanalyse en houden weinig rekening met de bijzondere aspecten van digitale informatie (in veelvoud aanwezig, technisch complex, veel ongestructureerd).

b. Digitaal vernietigen is ingewikkeld en daarom moeilijk te organiseren

- Digitale informatie bevindt zich overal binnen de organisatie en is voor een deel ongestructureerd en onbeheerd of bevindt zich in procesapplicaties;
- Dezelfde digitale gegevens worden in veelvoud bewaard; we weten niet wat de waarde en status van een gegevensbestand is en in welke mate de informatie overlapt;

- Digitale gegevens kunnen zich in meerdere aan elkaar gekoppelde systemen bevinden en in verschillende processen worden toegepast. Gegevens worden meervoudig gebruikt, vernietiging op de ene plek heeft gevolgen voor het gebruik elders;
- Verwijderd betekent niet altijd weg (back-ups, gegevens worden gekopieerd of uitgewisseld en blijven elders bestaan).

c. Kennis in de organisatie over (verantwoord) digitaal vernietigen is onvoldoende

- Te weinig kennis over de soorten werkprocessen en bewaartermijnen;
- Onvoldoende kennis van de applicaties om op bepaalde momenten selecties klaar te zetten voor vernietiging;
- Signalering, advisering en ondersteuning bij het digitaal vernietigen door BDI gaat over Corsa en niet over de bronsystemen of (ongestructureerde) informatie op andere plekken;
- Digitale documenten worden door medewerkers verwijderd zonder rekening te houden met bewaartermijnen, gelijktijdige vernietiging op andere plekken, uitzonderingen of het verantwoorden van de vernietiging.

d. We verplaatsen niet, maar kopiëren onze informatie en bewaren in veelvoud

- Bij de koppeling naar het archiefsysteem Corsa of het handmatig archiveren in Corsa kiezen we voor ‘kopiëren’ waarbij dezelfde bestanden achterblijven in het bronsysteem, mailbox of schijf. Lang niet altijd is duidelijk wat de (archief)originelen zijn en in het beste geval is gelijktijdige vernietiging niet geregeld;
- We houden gegevens bewust achter in de procesapplicatie, op de schijf of in onze mailbox, omdat we er dan snel bij kunnen of omdat dit nodig is voor de bedrijfsvoering.

e. Digitaal vernietigen is niet altijd technisch of praktisch uit te voeren

- Applicaties beschikken niet over een vernietigingsfunctionaliteit of het is ingewikkeld en duur;
- De informatie is niet gestructureerd en gemetadateerd, noch voorzien van de juiste definities en kwaliteitsniveau, waardoor bewaartermijnen niet kunnen worden bepaald en selecties niet goed te maken zijn.

f. Archiefbewustzijn ontbreekt en we voelen geen urgentie om digitaal te vernietigen

- We beschrijven onze werkprocessen en handelingen, en vergeten dat informatiebeheer en vernietiging onderdeel zijn van het proces en geregeld moeten zijn;
- Corsa is het archiefsysteem, informatie buiten Corsa is niet in beeld als ‘archief’ of ‘persoonsgegevens’ waar je wat mee moet;
- Vernietiging van de ongestructureerde informatie staat of valt met iemand die hiervan weet en zich verantwoordelijk voelt; dat geldt ook voor functioneel beheerders van procesapplicaties;
- Medewerkers weten niet hoe om te gaan met berichten in mailboxen of documenten op netwerkschijven en andere plekken. De instructie op INsite voldoet niet en of leeft niet.

4. Aanbevelingen

Onderstaande aanbevelingen kunnen opgenomen worden in een plan van aanpak met prioritering. Digitaal vernietigen is onderdeel van ons totale informatiebeheer. Voor een aantal acties geldt dat ze niet eigenstandig zijn, maar opgepakt kunnen worden als onderdeel van de inrichting van het informatiebeheer of andere verbeteracties.

1. **Stel beleid op voor digitaal vernietigen en geef invulling aan de verantwoordelijkheden**
2. **Zorg voor grip op het informatiebeheer, vooral op de ongestructureerde informatie buiten Corsa**
3. **Investeer in digitaal vernietigen**
4. **Maak dat vernietiging uit informatiesystemen technisch en praktisch mogelijk is**
5. **Organiseer de vernietiging van digitale informatie**

Stel beleid op voor digitaal vernietigen en geef invulling aan de verantwoordelijkheden	<p>Beleid voor digitaal vernietigen is onderdeel van het totale informatiebeheerbeleid, met toezicht in de vorm van rapportering.</p> <p>Stel vast hoe we in onze organisatie digitaal vernietigen willen organiseren.</p> <p>Leg beleid en procedures voor digitaal vernietigen vast in een kwaliteitssysteem. Zorg dat elke rol weet wat wordt verwacht, wat de handelingen zijn en dat er mandaat is.</p> <p>Voer risicoanalyse in. Houdt rekening met de bijzondere aspecten van digitale informatie.</p> <p>Toets periodiek beleid, procedures en verantwoordelijkheden om onszelf te kunnen verbeteren.</p>
Zorg voor grip op het informatiebeheer, vooral op de ongestructureerde informatie buiten Corsa	<p>Breng per bureau en werkproces in beeld waar informatie wordt opgeslagen en wat de status daarvan is. Beschrijf wie voor welke beheeromgevingen verantwoordelijk is, wie vernietiging moet initiëren en uitvoeren en wat de digitale tegenhangers zijn die tegelijk moeten worden vernietigd.</p> <p>Stel procedures op voor digitaal vernietigen en beschrijf de handelingen, de beslismomenten, de controles en de wijze van verantwoording.</p> <p>Geef medewerkers handzame richtlijnen voor de omgang met informatie in werkarchieven, mailboxen, social media en netwerkschijven.</p>
Investeer in digitaal vernietigen	<p>Aan digitaal vernietigen zijn kosten verbonden. De kosten zijn afhankelijk van hoe digitaal vernietigen op de verschillende plekken en in de verschillende applicaties wordt gerealiseerd. Naast de kosten voor inzet van mensen of inschakeling van derden, moet rekening worden gehouden met bijvoorbeeld aanschafkosten of ontwikkelkosten voor de vervanging of aanpassing van informatiesystemen.</p> <p>Onderzoek hoe digitaal vernietigen op de verschillende plekken en in de verschillende applicaties kan worden gerealiseerd.</p> <p>Investeer in kennis over digitale vernietiging.</p>

<p>Maak dat vernietiging uit informatiesystemen technisch en praktisch mogelijk is</p>	<p>Breng de applicaties, werkprocessen en informatiestromen in beeld. Bepaal vervolgens waar en hoe digitaal vernietigd moet worden.</p> <p>Pas bestaande applicaties aan, zo nodig met een aanvullende vernietigingsfunctionaliteit.</p> <p>Let bij aanschaf en inrichting van nieuwe applicaties op de wijze waarop vernietiging mogelijk is en kan worden uitgevoerd. Vraag door op de GIBIT-eisen (hoe dan...).</p> <p>Richt nieuwe systemen in volgens het principe ‘vernietiging by design’.</p> <p>Vergroot de mogelijkheden tot geautomatiseerd vernietigen. Zorg dat zaakdossiers via metadata worden voorzien van bewaartermijnen. Maak het mogelijk om uitzonderingen op vernietigen aan te geven.</p>
<p>Organiseer de vernietiging van digitale informatie</p>	<p>Zorg voor kennis over digitaal vernietigen en richt een project op om de aanwezigheid van informatie in beeld te brengen en de achterstand in digitaal vernietigen op te lossen.</p> <p>Voer risicoanalyses uit en maak vernietigingsrisico’s onderdeel van de dataclassificatie.</p> <p>Voorkom dubbeling van archiefinformatie en zorg dat bij het overzetten van documenten en data de gegevens in de bronomgeving worden verwijderd.</p> <p>Waar dat niet mogelijk is, maak transparant wat de archiefexemplaren zijn en wat kopie is.</p> <p>Organiseer gelijktijdige vernietiging op alle plekken. Maak sterfhuisconstructies van grote verzamelingen ongestructureerde informatie.</p> <p>Zorg dat nadien kan worden aangetoond dat informatie rechtmatig en volgens de procedures is vernietigd.</p> <p>Organiseer jaarlijks een ‘voorjaarsschoonmaak’, een dag of week waarin alle medewerkers hun digitale omgevingen opruimen aan de hand van instructies, wegwijzers en met hulp van informatiebeheerders.</p>

Bijlage a. Verantwoording van de audit

Uitvoering en interviews

Het onderzoek naar digitaal vernietigen is uitgevoerd door 5.1.2e in de periode september-december 2022. Opdrachtgever is 5.1.2e, manager PIF. De archiefinspecteur levert een rapport met conclusies en aanbevelingen. Over de audit en de resultaten is overleg geweest met de FG en CISO. De conclusies worden verwerkt in het jaarlijkse verslag van de gemeentearchivaris.

Het onderzoek volgt de algemene uitgangspunten en principes van auditing. Als lokale kaders gelden de Archiefverordening, het Besluit Informatiebeheer en de nadere uitwerking in beleid, besluiten en procedures van gemeente Nijmegen.

In het kader van het onderzoek zijn gesprekken gevoerd waarvan verslagen zijn gemaakt. De gesprekspartners kregen de mogelijkheid om de gespreksverslagen aan te vullen. Ze kunnen de bevindingen in de verslagen gebruiken voor het doorvoeren van verbeteringen in de eigen archivering en vernietiging. De bevindingen en conclusies in dit rapport zijn algemeen gehouden.

Gesprekken zijn gevoerd met:

5.1.2e	Staffunctionaris Bureau Leerplicht en RMC	<i>o.a. JVS, Insite, netwerkschijf</i>
5.1.2e	functioneel beheerder afdeling Financiën	<i>o.a. Coda, Corsa, Lias, Crescendo, Sagitta, AAC</i>
5.1.2e	Stafmedewerker afdeling Zorg en Inkomen	<i>o.a. GWS-suite, Corsa, Allegro en Florus</i>
5.1.2e	Coördinator Rechtsbescherming Juridische Zaken	<i>o.a. XS4JZ->JZ4all, Corsa, Access-database, netwerkschijf</i>
5.1.2e en	Manager bureau Schulphulpverlening en kwaliteitsmedewerker SHV en GKB.	<i>o.a. Allegro, Corsa, Insite, VIS2-> Gidso</i>
5.1.2e	Adviseur Verzekeringen	<i>o.a. AAG en Corsa, netwerkschijf</i>
5.1.2e	Informatieadviseur bureau Ontwikkeling	<i>o.a. SharePoint en Trello</i>
5.1.2e	Contractmanager/assetmanager VSA	<i>o.a. Planon, Corsa, Facilitator, netwerkschijf</i>
5.1.2e	Manager bureau Belastingen	<i>o.a. Gouw, Corsa, netwerkschijf</i>
5.1.2e	Projectassistent Stadsrealisatie	<i>o.a. Corsa, IBIS, SharePoint, netwerkschijf</i>
5.1.2e	Stafmedewerker P&O en functioneel beheerder YouForce	<i>o.a. Beaufort, YouForce, netwerkschijf</i>
5.1.2e en 5.1.2e	Adviseur Inkoop en Aanbesteden en functioneel beheerder van Negometrix; en projectondersteuner inkoop	<i>o.a. Negometrix, Tended, Corsa, netwerkschijf</i>
5.1.2e	Privacyofficer en adviseur Juridische Zaken	<i>o.a. Cybermanager, Corsa, netwerkschijf</i>
5.1.2e en	Informatiecoördinator Vergunningen; allround medewerker Vergunningen.	<i>o.a. VIP, WRS, Corsa, netwerkschijf</i>
5.1.2e	Informatiebeheerder BDI	<i>Corsa</i>

Bijlage b. Bevindingen

- 1. Versnipperde informatie: digitale gegevens worden linksom vernietigd en rechtsom bewaard**
- 2. We weten niet de gevolgen zijn van niet/ te laat vernietigen van gegevens; geen risicoanalyses**
- 3. Vernietiging uit het archiefsysteem Corsa gebeurt nog maar weinig**
- 4. Documenten en gegevens worden overgezet in Corsa én blijven achter in de procesapplicaties**
- 5. Systematische vernietiging uit procesapplicaties gebeurt nauwelijks**
- 6. Uitfasering van procesapplicaties als natuurlijk moment om digitaal te vernietigen**
- 7. Documenten op netwerkschijven zijn van iedereen en niemand**
- 8. Informatie in een berichtenapp als sms, WhatsApp en Signal zijn ook archief**
- 9. Medewerkers in Nijmegen beheren hun werkmappen en mailboxen naar eigen inzicht**

Versnipperde informatie: digitale gegevens worden linksom vernietigd en rechtsom bewaard

- In alle interviews is doorgevraagd over de vindplaatsen van (archief)informatie. Documenten worden opgeslagen in Corsa, in procesapplicaties, op netwerkschijven, in NextCloud, in functionele postbussen, in mailboxen, op telefoons en in samenwerkingsomgevingen als Insite, SharePoint en MS365.
- Versnippering en overlap. Het ontbreekt in onze organisatie aan overzicht van waar zich digitale informatie bevindt en wat de status daarvan is. Lang niet altijd is duidelijk wat de (archief)originelen zijn en gelijktijdige vernietiging is niet geregeld.
- Bij vernietiging van analoge of digitale dossiers vraagt BDI aan de proceseigenaar of er digitale tegenhangers op andere plekken zijn. BDI laat gelijktijdige verwijdering van decentraal bewaarde digitale gegevens over aan de proceseigenaren en heeft daar weinig zicht op en zeggenschap over. Voor adviseren breder dan Corsa is te weinig tijd en het overzicht ontbreekt. Niet duidelijk is waar de verantwoordelijkheid van de proceseigenaren hierin overgaat in een actie die BDI moet doen.
- Een deel van de digitale documenten in Corsa betreft scans van papieren documenten uit de periode 2010-2019. De papieren originelen worden in afwachting van vervanging in dagdozen bewaard. Bij vernietiging van hybride dossiers blijft de originele archiefinformatie bestaan.
- Op dit moment blijft vernietiging digitaal beperkt tot Corsa (sociaal domein, waarbij gelijktijdige vernietiging van data uit de applicaties weer eigen belemmeringen kent), in JVS (leerplicht en RMC) en bij de uitfasering van procesapplicaties. Bij vertrek van een bestuurder of medewerker worden accounts opgeheven en persoonlijke schijven en mailboxen verwijderd. Het systematisch gelijktijdig vernietigen van gelijksoortige informatie (digitaal en analoog) op alle plekken komt verder niet voor.

We weten niet de gevolgen zijn van niet/ te laat vernietigen van gegevens; geen risicoanalyses

- In Nijmegen hebben we geen totaaloverzicht van informatie en de waarde daarvan. Informatie wordt op verschillende plekken en dubbel bewaard. Risicoanalyses maken we niet. We nemen de risico's van te vroeg, te laat of onrechtmatig vernietigen niet mee in de dataclassificatie.
- Digitale informatie kan zich in meerdere systemen bevinden en in meer processen of in een ketenproces worden gebruikt. We hebben niet altijd in beeld in welke processen of procesapplicaties we bepaalde data gebruiken, en kunnen daarom niet goed selecteren en verwijderen. Verwijdering van verkeerde data kan dit leiden tot het niet kunnen vinden van informatie die elders nog nodig is.
- Gehoord: gegevens in de procesapplicatie of op de netwerkschijf blijven daar opgeslagen, omdat 'de dossiers in Corsa worden vernietigd en we hebben ze nog nodig.' Soms is behoefte aan historische informatie, die langer reikt dan de bewaartermijnen van de dossiers in Corsa.

Andere reden: 'de archiefdossiers zijn analoog en op onze netwerkschijf hebben we de informatie digitaal beschikbaar'.

Vernietiging uit het archiefsysteem Corsa gebeurt nog maar weinig

De vernietiging van digitale dossiers in Corsa wordt geïnitieerd door BDI die daar de proceseigenaren bij betrekken als onderdeel van de te volgen verantwoordingsprocedure.

Uitgezonderd het sociaal domein is afgelopen jaren weinig digitaal vernietigd in Corsa, met als oorzaken:

- Het betreft digitale dossiers die nog jong zijn en de bewaartermijn is nog niet verstreken;
- Dossiers zijn niet afgesloten, omdat de procesinformatie niet meegekomen is naar Corsa en het zaakresultaat niet bekend is of de kwaliteit nog gecontroleerd moet worden. Van dossiers die niet zijn afgesloten kan de bewaartermijn niet worden vastgesteld (o.m. wabo-dossiers);
- Vernietigen in Corsa kan afhankelijk zijn van het kunnen vernietigen in de procesapplicatie (scheiding documenten-procesmetadata, benadering document vanuit de applicatie in Corsa via een link).
- In Corsa staan documenten waarvan BDI niet het beheer heeft (o.m. facturen via CODA op te vragen). Geen vernietiging omdat proceseigenaren hier geen actie op nemen (niet bewust, niet op gewezen).

Documenten en gegevens worden overgezet in Corsa én blijven achter in de procesapplicaties

- In de procesapplicaties worden gegevens geregistreerd, notitievelen gevuld en documenten opgeslagen. In een groot aantal processen wordt gewerkt in de applicatie en gearchiveerd in Corsa waarbij de documenten met de metadata handmatig of via een koppeling (bij voorkeur geautomatiseerd) in Corsa komen. Bij het overzetten naar Corsa vanuit de bron is sprake van kopiëren en blijft de informatie óók staan in de applicatie.

Systematische vernietiging uit procesapplicaties gebeurt nauwelijks

Mogelijke oorzaken:

- Proceseigenaren en functioneel beheerders zijn zich niet bewust van het moeten vernietigen en worden daar niet op gewezen;
- Oudere applicaties zijn aangeschaft en ingericht in een tijd waarin vernietiging minder belangrijk leek en het analoge dossier/Corsa-dossier alle informatie bevatte. Functionaliteiten om te archiveren en te vernietigen ontbreken soms geheel. Het is technisch niet altijd mogelijk of kan alleen handmatig via scripts of met hulp van de leverancier;
- Bij de aanschaf van nieuwe procesapplicaties hanteren we de GIBIT-voorwaarden en proberen we in te spelen op eisen voor archivering en archiefvernietiging. Verwijdering van gegevens is volgens de leverancier bijna altijd mogelijk. We eisen de mogelijkheid om te vernietigen, maar we vragen niet goed door op welke wijze dat mogelijk is en kan worden ingericht (handmatig, via een dashboard, door de functioneel beheerder, alleen door de leverancier).
- Inrichting van vernietiging-by-design wordt doorgeschoven naar het tweede plan. Om gegevens systematisch te kunnen vernietigen moeten we bij de inrichting keuzes maken over structuur, metadata, automatisch toe te voegen bewaartermijnen, uitzonderingen, en het daadwerkelijk kunnen vernietigen op het juiste veiligheidsniveau (vernietiging-by-design). Als zaakdossiers niet zijn afgesloten of niet voorzien zijn van statusaanduidingen kunnen geen selecties worden gemaakt op bewaartermijn en inhoud.
- In bestaande applicaties is bij de inrichting van de processen weinig rekening gehouden met de inhoudelijke metadata die nodig zijn om op een gebruiksvriendelijke wijze slimme selecties te kunnen maken en vernietiging te kunnen doorvoeren en verantwoorden.
- Het tussentijds vernietigen van gegevens uit procesapplicaties is vaak technisch complex. Data worden hergebruikt in meerdere werkprocessen en procesapplicaties zijn soms gekoppeld. Vernietiging in de ene applicatie kan het gebruik van data (gegevens, metadata) elders blokkeren;
- Het kan gaan om jonge applicaties en pas digitaal ingerichte werkprocessen en de bewaartermijn nog niet verstreken.

Uitfasering van procesapplicaties als natuurlijk moment om digitaal te vernietigen

- Bij de uitfasering van procesapplicaties zijn verschillende strategieën mogelijk voor de data die in de applicatie staat, zoals migratie naar de nieuwe applicatie of verwijdering. De uitfasering van een applicatie is een natuurlijk moment om data op te schonen. Niet migreren is een vorm van vernietigen. Binnen IRvN bewaakt changemanagement het naleven van de toets op de aanwezigheid van archiefinformatie in een uit te faseren applicatie. Voor SaaS-applicaties blijft een dergelijke toets vaak achterwege.

Documenten op netwerkschijven zijn van iedereen en niemand

- Proceseigenaren en medewerkers zijn zich niet bewust van het moeten vernietigen en worden daar niet op gewezen; wat niet in Corsa staat is niet in beeld als archief waar je wat mee moet;
- De informatie op netwerkschijven en in samenwerkingsomgevingen is grotendeels ongestructureerd. De schijven bevatten een mix van documentatie, werkinstructies, rapportages, verslagen en uitvoeringsdocumenten. Documenten die als archiefexemplaar in Corsa staan, blijven voor raadpleging op de netwerkschijven eveneens bewaard. Sommige bureaus hanteren een indeling met submappen op naam medewerker. Variatie in soort informatie, benaming van documenten en omdat de schijf van iedereen is, maken het moeilijk een goede afweging te maken over wat nog actueel of belangrijk is. Bewaartermijnen zijn moeilijk toe te passen op ongestructureerde informatie. Opschoning gebeurt alleen als iemand zich daar verantwoordelijk voor voelt. Na vertrek van medewerkers, beëindiging van projecten of verandering van de organisatiestructuur blijven mappen onbeheerd voortbestaan;
- Omdat de archiefinformatie in Corsa (op analoog, digitale zaakdossiers) als dé archiefexemplaren gelden, gebeurt vernietiging op netwerkschijven (door de medewerkers) ad hoc en buiten de procedures voor archiefvernietiging om. Digitale documenten worden verwijderd zonder rekening te houden met bewaartermijnen, gelijktijdige vernietiging op andere plekken, uitzonderingen of het verantwoorden van de vernietiging.

Informatie in een berichtenapp als sms, WhatsApp en Signal zijn ook archief

- Het gebruik van berichtenapps neemt toe door de laagdrempeligheid en gebruiksvriendelijkheid van het medium om snel informatie uit te wisselen in chatberichten. WhatsApp en Sms-berichten op zowel zakelijke als privételefoons van bestuurders en ambtenaren vallen onder de reikwijdte van de WOO als de berichten in het kader van het werk zijn verstuurd. Werkgerelateerde chatberichten vallen óók onder de Archiefwet.
De gemeente Nijmegen heeft geen beleid voor het veiligstellen en beheren van chatberichten en groepsapps. Bestuurders en andere sleutelfiguren delen hun chatberichten niet graag, ook al zijn ze werkgerelateerd. Vernietiging gebeurt naar eigen inzicht van de gebruiker en met het opheffen van het account na het uitdienstreden of aftreden.

Medewerkers in Nijmegen beheren hun werkmappen en mailboxen naar eigen inzicht

- We bewaren werkelijk álles in onze persoonlijke omgeving: concepten en definitieve versies, operationele berichten, documentatie. We kopiëren liever onze documenten dan dat we afgaan op het gedeelde archiefstuk in ons archiefsysteem en samenwerkingsomgeving.

- Bekend is dat mailboxen van medewerkers duizenden mails van vele jaren terug bevatten. Mailboxen en persoonlijke netwerkmappen worden nu standaard 6 maanden na vertrek van een medewerker zonder meer verwijderd.
- Nijmegen conformeert zich aan de Selectielijst voor e-mailbewaring welke in de loop van 2023 gaat gelden. Deze selectielijst bepaalt de vernietiging van complete mailboxen van bestuurders en medewerkers na 7 jaar. Mailboxen van een aantal sleutelfiguren worden afgevangen voor permanente bewaring. De toepassing van de Selectielijst voor e-mailbewaring wordt voorbereid. Het integraal bewaren voor 7 jaar en daarna jaarlijks systematisch vernietigen van mailboxen van medewerkers is nog niet gepland.
- In 2021 is een richtlijn opgesteld voor het dichtzetten en opruimen van 50 functionele mailboxen, inclusief inhoud. Proceseigenaren bepalen op basis van een risicoanalyse de bewaartermijn (1 of 7 jaar) en geeft opdracht aan IRvN tot dichtzetten resp. verwijderen. Het betrof een eenmalige actie.

Bijlage c. Artikel Ontspullen en oprommelen

5.1.2e 23-02-2023

Na de Bronstijd en nog enkele tijden stapt de mensheid in het Digiliticum, zoals we het Digitale Tijdperk kunnen noemen. Er was een crisis voor nodig om ons massaal te laten Teamen en Zoomen. 24/7 kunnen we online zijn, is ons doen en laten vastgelegd en zijn we te traceren.

De manier waarop we met gegevens omgaan leidt tot grote hoeveelheden rommel. Zoveel rommel dat er naast de WorldCleanup Day ook een Digitale Cleanup Day wordt georganiseerd. Onze dataconsumptie vraagt inmiddels al drie keer meer energie dan wordt geproduceerd door alle zonnepanelen ter wereld samen. De cijfers spreken elkaar tegen: de datacenters stellen dat hun aandeel in het energieverbruik al jaren stabiel blijft en de meest efficiënte manier van data-opslag is. Dit zijn dan niet de Total Costs of Ownership, zoals de kosten van de bouw van de datacenters, de duizenden servers die worden gebruikt en regelmatig vervangen, het drinkwater dat wordt gebruikt om de datacenters te koelen. Dataopslag en dataverkeer eisen veel van het milieu.

Het verwerken van e-mails kost ons gemiddeld meer dan 3 uur per dag. We leven vanuit onze mailbox. Elk jaar zorgt het internet met de ondersteunende systemen voor 900 miljoen ton CO₂-uitstoot en de voorspellingen geven aan dat binnen 10 jaar 20% van onze totale energieproductie opgaat aan digitale informatie. Eén terabyte aan gegevens zou qua CO₂-uitstoot gecompenseerd moeten worden door 100 jonge bomen, al kun je hiervoor beter olifantsgras planten. Digitalisering is een wolf in schaapskleren. Hoe dit alles is ontstaan zou vele regels vullen, en die ruimte is mij niet gegeven. Hoe lossen we het op?

Het antwoord klinkt simpel: door op te ruimen. Meer dan ooit is er behoefte aan. Niet alleen op kantoor maar ook thuis hebben professional organizers de agenda vol aan klanten die het overzicht over hun materiële eigendommen kwijt raken. Ontspullen is de nieuwe manier om gelukkig te worden.

Hoe pak je dat aan? We moeten alle gegevens verwijderen die we niet (meer) nodig hebben voor onze bewaarmotieven. Dit hoort een permanente zorg te zijn van de informatieprofessional! Eerst zul je grip moeten krijgen op je totale informatiehuishouding, dus alle gegevens die in je organisatie worden bijgehouden, want meten is weten. Marie Kondo doet dit door alle items in huis te verzamelen op een centrale plaats en dan te bepalen wat een "spark of joy" geeft; wij inventariseren wat we hebben, waarom we het hebben, hoe lang we het nodig denken te hebben (conform de voorschriften die eisen stellen over de bewaartermijn) en na te gaan wat het verdere nut is van het beheer. Uitgangspunt daarbij is gegevens zo snel als mogelijk vernietigen. Om dat te organiseren ga je met de gebruikers in gesprek welke informatie relevant is, hoe lang nog en welke niet (meer). Je legt in een informatieplattegrond vast welke informatie aanwezig is in welke systemen en welke verzamelingen. Hierbij is het uitgangspunt om informatie eenmalig op te slaan en meervoudig te gebruiken. Heb je een bewaarlijst/selectielijst, dan neem je deze regels mee in je beoordeling. Wat direct weg kan, gaat meteen weg (dubbelen bijvoorbeeld), wat nog enige tijd bewaard moet worden krijgt een bewaartermijn (conform de afspraken) en wordt daarna verwijderd. Neem hierin de hele afdeling mee: vertel hen over het bewaarbeleid van mailboxen, over appgebruik, bespreek de ergernissen rondom systemen en hoe die vermeden kunnen worden en hoe je -samen!- hun informatiehuishouding beter gaat opzetten. Maak samen met de gebruikers een SPOT, Single Point of Truth: een plaats binnen de informatiehuishouding waar een groep gebruikers afsprekt de informatie te concentreren. Dat kan bijvoorbeeld een bepaald systeem zijn (een vergunningensysteem), een teamsite of een dossier dat gezamenlijk wordt onderhouden. Spreek af dat iedereen in deze SPOT de informatie opslaat en hou contact met je gebruikers om de afspraken op te volgen. Elimineer overbodige informatie: alles wat niet meer nodig is, moet weg, want kost energie en zorgt voor CO₂-uitstoot. Duurzaamheid betekent: weg met je digitale rommel! Schaft je organisatie een

nieuw systeem aan: regel dan het archiefbeheer -samen met de gebruikers- meteen in dat systeem. Archiving by design leert je hoe je dit aanpakt.

We sluiten daarbij aan op de manier van werken van de medewerker en degene met wie hij of zij samenwerkt. Werken zij naar tevredenheid met een specifieke procesapplicatie? Neem die dan als uitgangspunt voor het archiveren. Hebben zij een werkstroom ingericht in een systeem, die hen veel werk uit handen neemt? Dan is dat de manier van werken die wij, informatiespecialisten, gaan ondersteunen. Hebben zij gegronde bezwaren tegen een systeem en werken ze samen in Sharepoint? Leg de werkwijzen vast in een documentair structuurplan: een inrichtingsplan voor de informatiehuishouding.

Dan is er nog één punt te regelen: wat doen we met het dossier nadat het afgehandeld is. Wordt dit door een centrale afdeling geschoond op dubbelingen, concepten e.d.? Kan het -bij een kortere bewaartermijn- in de applicatie blijven met daarbij het jaar van vernietiging, of moet het uit de applicatie (de schijven ook als applicatie beschouwen) en opgeslagen worden ergens, waar het wel gelezen kan worden, maar niet meer veranderd, en gemakkelijk teruggevonden.

Die omgeving, dat is het e-depot. Hebt u al nagedacht hoe de toekomstige gebruikers hun informatie gaan zoeken? Begin daar eens mee voordat u een systeem inricht waarin niemand iets terug kan vinden.....

(Dit artikel verscheen eerder in het blad Od van januari 2023).

bron: <https://kia.pleio.nl/groups/view/ed34c36f-c1d8-4c75-ada1-8a2eef311946/kennisplatform-green-it-digitaal-erfgoed/blog/view/33c5ab7b-54d8-4d4a-bcfd-ab162f95a886/ontspullen-en-oprommelen>

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	10, 15