Wat is digitaal vernietigen?

Handreiking Digitaal vernietigen

<blok>Toelichting</blok>

Het digitaal vernietigen van overheidsinformatie leidt vaak tot discussies over wat het precies wel en niet inhoudt. Vandaar dat we in deze module een toelichting geven bij het onderwerp.

Definitie

Voor de definitie van digitaal vernietigen verwijzen we naar de definitie van het DUTO-proces vernietigen binnen het DUTO-raamwerk. Digitaal vernietigen omvat de activiteiten die nodig zijn om digitale overheidsinformatie op een gecontroleerde manier door of in opdracht van de verantwoordelijke overheidsorganisatie te laten vernietigen. Zodat deze informatie niet meer kenbaar, vindbaar of reconstrueerbaar is in digitale vorm.

Reikwijdte

Digitale overheidsinformatie

Digitale overheidsinformatie is er in vele vormen zoals tekstdocumenten, presentaties, spreadsheets, video's, foto's, (chat) berichten, e-mails, gegevenssets in databases, etc. Deze vormen van overheidsinformatie, die samengesteld zijn uit een verzameling aan elkaar gerelateerde data of gegevens die als eenheid wordt behandeld, noemen we informatieobjecten. Voor meer informatie over de verhouding tussen overheidsinformatie, gegevensobjecten en informatieobjecten zie het Overheidsinformatiemodel.

Informatieobjecten bevinden zich verspreid in verschillende informatiesystemen binnen de organisatie. Ze kunnen zich ook buiten de organisatie bevinden, bijvoorbeeld wanneer deze extern worden gehost (bijv. in een cloud omgeving). Duit komt veel voor bij SaaS-oplossingen. Ook deze informatieobjecten moeten worden vernietigd.

Herkomst van informatie

Een informatieobject is vaak opgebouwd uit verschillende gegevensobjecten. De gegevensobjecten hebben vaak al een hele weg afgelegd voordat ze onderdeel worden van het informatieobject dat je wilt vernietigen. Een voorbeeld: het dossier van een bestuurlijk overleg kan video-opnamen bevatten, zogenaamde videotulen. Deze zijn in uiteindelijke vorm vaak weer geïndexeerd op basis van een agenda. De opnamen worden echter gemaakt met AV-middelen die afkomstig zijn van een andere leverancier en die hebben hun eigen servers. Als hier geen afspraken over bestaan, bestaat er een risico dat deze buiten beheer blijven. Wanneer je een procedure schrijft voor het vernietigen binnen een informatiesysteem is het dus ook belangrijk om overzicht te hebben over het gehele proces waarin de informatieobjecten tot stand zijn gekomen, dat groter kan zijn dan één taakapplicatie.

<kader>

Wanneer spreken we van een kopie?

Wanneer we het hebben over digitaal vernietigen, wordt veelal gezegd dat ook alle kopieën vernietigd dienen te worden. Maar wat is dan precies een kopie? En wanneer is iets een nieuw informatieobject? In het kort spreken we van een kopie als het gaat om een duplicaat van een

informatieobject binnen dezelfde context. Bijvoorbeeld wanneer je een kopie maakt van een vergunningaanvraag door deze naar collega's te mailen voor advies.

Wanneer een informatieobject binnen een nieuwe context wordt gebruikt, spreken we niet van een kopie. Dan spreken we van een nieuw informatieobject. Bijvoorbeeld wanneer er een bezwaar wordt gemaakt op een vergunningaanvraag en de originele aanvraag mee wordt genomen in de beoordeling van het bezwaar. De aanvraag heeft namelijk een andere betekenis binnen de aanvraag van de vergunning en het bezwaar.

</kader>

Vernietigen van kopieën op back-ups

In de papieren informatiehuishouding wordt vernietiging begrepen als het fysiek tenietdoen van stukken. In de digitale informatiehuishouding gaat het niet primair om vernietiging van fysieke dragers, de hardware, maar om het wissen, verwijderen of ontoegankelijk maken van informatieobjecten. Dat betekent dat de gegevens waaruit het informatieobject bestaat niet meer zijn te reconstrueren, waardoor het als geheel niet meer toegankelijk te maken is. Dit geldt in beginsel ook voor aanwezige **back-ups** van de documenten en bijbehorende metadata, hoewel het wenselijk of zelfs noodzakelijk kan zijn om bepaalde metagegevens te behouden om te bewijzen dat de vernietigde informatieobjecten hebben bestaan en dat zij op de juiste wijze zijn vernietigd.

Houdt rekening met de risico's van het niet vernietigen van kopieën op back-ups. Bepaal daarom in hoeverre en op welke manier informatie op back-ups wordt meegenomen in het proces van digitaal vernietigen. Afhankelijk van de aard van de informatie kunnen hierbij verschillende back-upstrategieën worden toegepast, bijvoorbeeld wanneer het gaat om privacygevoelige of bedrijfskritische gegevens. Het is de verantwoordelijkheid van overheidsorganisaties om deze risico's in kaart te brengen en passende maatregelen te treffen. Daarbij is het van belang om tijdig afstemming te zoeken binnen de organisatie met betrokken partijen, zoals IT-afdelingen, informatiebeveiliging specialisten en functioneel beheerders, zodat afspraken worden vastgesteld en het proces van digitaal vernietigen zorgvuldig en effectief kan worden uitgevoerd.

Wettelijke grondslag voor vernietiging

De wettelijke grondslag voor vernietigen ligt in artikel 5.3, lid 1 van de Archiefwet en daarbij nog specifieker; het selectiebesluit.

"Het verantwoordelijke overheidsorgaan treft *passende maatregelen* om ervoor te zorgen dat de documenten waarvan de bewaartermijn, bedoeld in artikel 5.1, tweede lid, onderdeel b, is verstreken en die niet op grond van artikel 5.1, vijfde lid, onderdeel c, van vernietiging zijn uitgezonderd, worden *vernietigd*."

Informatieobjecten waarvan de bewaartermijn uit het selectiebesluit zijn verlopen, en niet zijn uitgezonderd van vernietiging, moeten dus worden vernietigd. Daarbij worden ook enige eisen gesteld om tot rechtmatige vernietiging over te kunnen gaan:

- Er zijn beheerregels opgesteld ten aanzien van vernietiging (Archiefwet 4.2.2 b.)
- Er is een procesbeschrijving voor vernietiging (Archiefbesluit 4.1.1)
- Er is een verklaring opgesteld van de vernietiging (Archiefbesluit 4.1.2

<blok>Methoden van vernietiging</blok>

De wijze/methode van vernietiging die gehanteerd wordt is afhankelijk van plek waar de informatieobjecten zich bevinden. Informatieobjecten kunnen zijn opgeslagen in:

- Een **informatiesysteem** waarin de informatieobject zijn gemaakt en/of beheerd en/of opgeslagen worden. Een informatiesysteem kan intern worden beheerd maar ook extern (in de cloud) worden gehost waarvoor 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.
- **Fysieke gegevensdragers** (elektromagnetische dragers, optische en solid-state dragers, harde schijven, beveiligde servers)

Naast de plek waar de informatieobjecten plaatsvinden speelt de vertrouwelijkheid/risicogevoeligheid van de gegevens ook een belangrijke rol wat voornamelijk bepaald of gegevens enkelvoudig of meervoudig overschreven dienen te worden.

Vernietiging en fysieke dragers

Eenmalig of meervoudig overschrijven

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. De informatie wordt een keer volledig vervangen door andere gegevens (bijvoorbeeld nullen, willekeurige tekens) op de opslagdrager (harddisk, SSD, USB, etc.).

Voorbeeld: Je wist een oud document uit een database of op een harde schijf en overschrijft de opslaglocatie één keer. Iemand met standaardtools kan de data niet meer eenvoudig terughalen

Meervoudig overschrijven
De informatie wordt **meerdere keren overschreven** met verschillende patronen, zodat het vrijwel onmogelijk is om de oorspronkelijke gegevens te herstellen.

Voorbeeld: Een oud dossier met persoonsgegevens wordt drie keer overschreven, telkens met andere patronen. Hierdoor is het extreem moeilijk voor iemand om de originele informatie te reconstrueren, zelfs met geavanceerde technieken.

Waarom zou je in de huidige tijd eenmalig of meervoudig willen overschrijven terwijl tegenwoordig verwijdering/vernietiging geautomatiseerd kan plaatsvinden binnen een informatiesysteem (en gerelateerde databases)?

Een (automatische) vernietiging in een informatiesysteem verwijdert de records logisch, bijvoorbeeld een DELETE in de database of een markering “verwijderd” in de front-end van de gebruiker die de record niet meer zichtbaar maakt. Dit is niet hetzelfde als fysiek overschrijven van de data op de drager. De bits kunnen nog bestaan totdat ze door nieuwe data worden overschreven. Ander voorbeeld: vanuit een informatiesysteem verwijder je bij een profiel van een klant een document “vergunningsaanvraag xxx”. Op de achtergrond wordt in de database de verwijzing naar het bestand verwijdert middels een DELETE. Hiermee is enkel de verwijzing naar het bestand (vanuit de database en dus het informatiesysteem) ongedaan gemaakt terwijl het bestand fysiek nog steeds op de harde schrijf staat.

Vernietigen met behoud van metadata (tombstone)

Hoewel metagegevens onlosmakelijk aan informatieobjecten verbonden zijn, kan het nodig zijn om bepaalde metagegevens te behouden. Terwijl het informatieobject zelf vernietigd wordt. Bijvoorbeeld om de vernietiging vast te leggen, of voor het maken van een zogeheten ‘tombstone’. Dat is een ‘grafschrift’ waarin de vernietiging vermeld staat. En wordt weergegeven wanneer iemand een link naar het betreffende informatieobject gebruikt.

Tombstones zijn ook nuttig wanneer andere records of informatiesystemen nog naar het object verwijzen, omdat ze voorkomen dat links of relaties breken. Ze laten zien dat het object heeft bestaan en vernietigd is, zonder dat de inhoud zelf beschikbaar is. In grote systemen of bij automatische vernietiging dragen tombstones bij aan transparantie. Daarnaast kunnen ze worden toegepast voor juridische of organisatorische bewijslast, bijvoorbeeld bij overheidsinformatie onder de Archiefwet of privacygevoelige data onder de AVG, waarbij moet worden aangetoond dat informatie correct is verwijderd.

Vernietigen van verwijzingen

Overheidsinformatie kan zich grofweg op twee manieren verplaatsen:

1. Het vermenigvuldigen van het informatieobject voor gebruik in andere contexten
2. Het ter beschikking stellen van het informatieobject voor gebruik in andere contexten

Voor de eerste situatie is een andere manier van vernietigen nodig dan voor de tweede situatie. Bij de eerste situatie worden de informatieobjecten binnen hun eigen context met hun eigen bewaartermijn vernietigd. Bij de tweede situatie worden de verbintenissen tussen het informatieobject en de verschillende contexten vernietigd. In essentie hebben wordt het informatieobject ontoegankelijk gemaakt binnen een bepaalde context. In die zin is het informatieobject ook niet meer toegankelijk, vindbaar en kenbaar binnen de gebruikscontext.

Anonimiseren en pseudonimiseren

[in hoeverre spreken we van vernietiging van gegevens bij anonimiseren en pseudonimiseren?]

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. Pseudonomisering is **géén vernietiging** van gegevens omdat de gegevens blijven bestaan; de gegevens zijn enkel technisch afgeschermd.

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. In de praktijk betekent dit dat de persoonsgegevens “vernietigd” zijn voor privacydoeleinden. Technisch bestaat de informatie nog wel (bijvoorbeeld statistische data), maar het identificeerbare aspect is vernietigd en niet meer herleidbaar naar een persoon.