Waarde van digitaal vernietigen

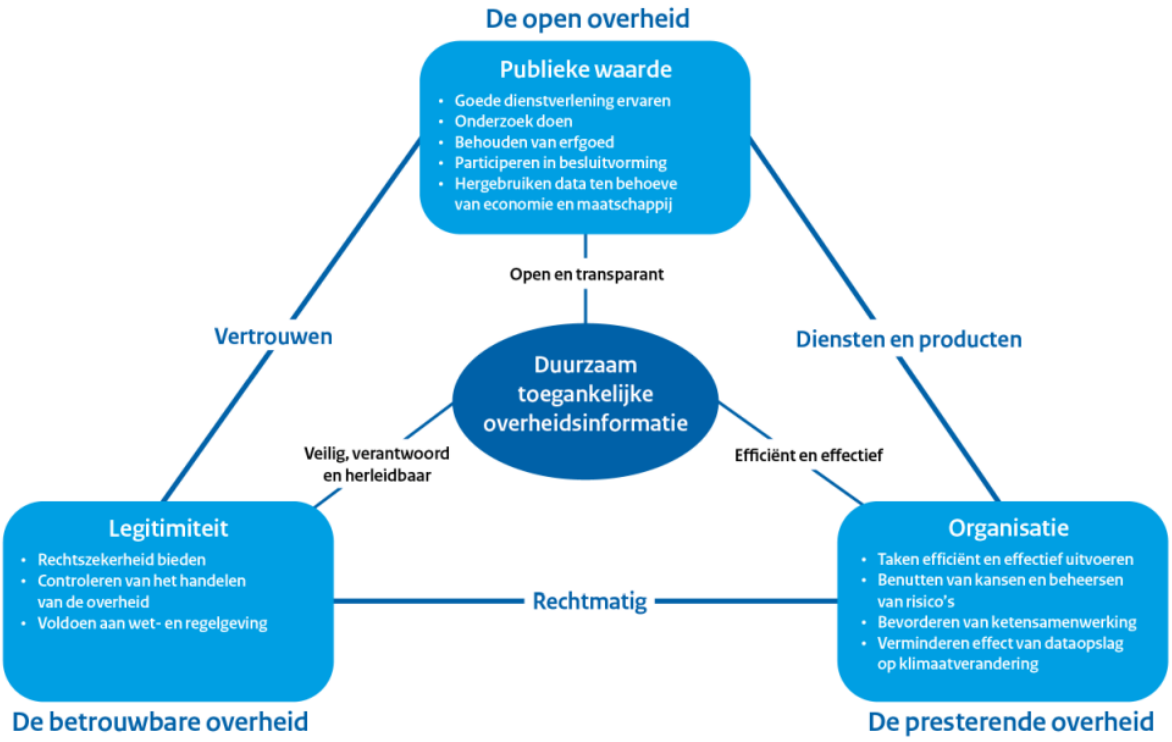
Handreiking Digitaal vernietigen

Waarom is digitaal vernietigen belangrijk?

Om overheidsinformatie duurzaam toegankelijk te maken moet het vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig zijn. Een belangrijk DUTO-proces bij het realiseren hiervan is Vernietigen. Een zeer groot deel van overheidsinformatie behoort tot categorieën informatie met een eindige bewaartermijn. Dat betekent dat het nodig is om procedures en functies in te richten, die er voor zorgen dat overheidsinformatie na vernietiging:

- onvindbaar is,
- niet beschikbaar is,
- onleesbaar is,
- en niet meer te interpreteren is.

Het DUTO-proces vernietigen draagt bij aan het creëren van waarde voor de organisatie. Om dit te illustreren maken we gebruik van de waarde driehoek perspectieven op publieke waarde uit het DUTO-raamwerk



Voor vernietigen komt de nadruk meer te liggen op de perspectieven Legitimiteit en Organisatie, in het bijzonder:

1. *Legitimiteit*.
    a. Vernietigen is nodig om aan wet- en regelgeving te voldoen. Daarbij gaat het niet alleen om de Archiefwet, maar ook zeker om de AVG.
    b. Door gegevens over burgers en bedrijven te vernietigen kan ook rechtszekerheid worden geboden. Zoals bijvoorbeeld het recht om vergeten te worden.
2. *Organisatie*.
    a. Door overheidsinformatie te vernietigen reduceren we de digitale berg informatie. Hierdoor kan overheidsinformatie eenvoudiger worden gevonden en reduceren we complexiteit in onze applicaties.
    b. De overheidsinformatie die is vernietigd, heeft geen impact meer op uitstoot van CO2 door datacentra.
    c. Vernietigde overheidsinformatie vraagt niet om (betaalde) opslagruimte

Voordelen/Kansen en risico's

Om collega's binnen jouw organisatie te overtuigen van het belang van digitaal vernietigen schetsen we nu een aantal risico's en kansen. Deze kun je gebruiken als argumenten om digitaal vernietigen op de kaart te zetten binnen jouw organisatie. De kansen en risico's zijn gestructureerd rond de perspectieven van legitimiteit en organisatie. Kies vooral de argumenten die het beste aanslaan binnen jouw organisatie en gebruik de risico's en kansen die het grootste mogelijke effect hebben binnen jouw organisatie.

Perspectief legitimiteit

Het rechtmatig handelen door de overheid draagt bij aan het vertrouwen dat burgers kunnen stellen in dezelfde overheid. De maatschappij moet er op kunnen vertrouwen dat de overheid zich houdt aan zijn eigen wet- en regelgeving. Daartoe behoort ook het vernietigen van overheidsinformatie wanneer daartoe een wettelijk verplichting geldt. Dat draag niet alleen bij aan compliance met de Archiefwet maar ook met andere wetgeving.

Wet open overheid

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

Mogelijke risico's

Nb.: dit is geen uitputtende lijst

Bron risico	**Gebeurtenis**	**gevolg**
Indien overheidsinformatie niet wordt vernietigd,…	…wordt het door de toenemende omvang van informatie moeilijker verzoeken op tijd te beantwoorden,…	…het vertrouwen van de burger geschaad wordt

	…wordt het waarschijnlijker dat informatie die vernietigd had moeten zijn openbaar gemaakt moet worden en dat daarmee zichtbaar is dat informatie onrechtmatig bewaard wordt,…	…waardoor reputatie van een organisatie(onderdeel) schade oploopt, …toezichthouders sancties opleggen

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. De Archiefwet biedt daarbij de grondslag voor de bewaartermijnen. 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.

Mogelijke risico's

Nb.: dit is geen uitputtende lijst.

Bron risico	**Gebeurtenis**	**gevolg**
Indien overheidsinformatie niet wordt vernietigd,…	…is de kans groter dat gevoelige persoonsgegevens zonder doelbinding onrechtmatig bewaard blijven,…	…met als gevolg dat de toezichthouder sancties oplegt.
	…burgers, bedrijven en werknemers ten onrechte in aanraking met de overheid komen omdat het recht om vergeten te worden, is geschonden,…	…waardoor het aantal geschillen en juridische procedures toeneemt.

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.

Mogelijke risico's

Nb.: dit is geen uitputtende lijst.

Bron risico	Gebeurtenis	gevolg
Indien overheidsinformatie niet wordt vernietigd,…	…is de kans groter dat bij een beveiligingsincident grote hoeveelheden vertrouwelijke gegevens uitlekken die onrechtmatig bewaard gebleven zijn,…	…met als gevolg dat reputatie van een organisatie schade oploopt en bestuurders ter verantwoording worden geroepen.
		…met als gevolg dat toezichthouders sancties opleggen.

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 (digitale) overheidsinformatie, in de vorm van informatieobjecten, waarvan de bewaartermijn is verstreken en die niet van vernietiging is uitgezonderd, te vernietigen.

Let op:

- *Het is van belang om bij het vernietigen van digitale overheidsinformatie ook de kopieën te vernietigen.*
- *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.*

Bron risico	Gebeurtenis	gevolg
er geen procedure is voor het vernietigen van overheidsinformatie,	er niet regulier en gecontroleerd vernietigd wordt zodat achterstanden ontstaan	er kosten voor beheer toenemen.
er geen procedure is voor het vernietigen van overheidsinformatie,	het vernietigingsproces niet uitgevoerd wordt omdat niet duidelijk is wie verantwoordelijk is	wet- en regelgeving niet nageleefd wordt.
er geen procedure is voor het vernietigen van overheidsinformatie,	vernietiging ongecontroleerd wordt uitgevoerd	informatie wordt vernietigd op basis van onjuiste gronden.

er geen procedure is voor het vernietigen van overheidsinformatie,	vernietiging niet op passende wijze wordt uitgevoerd	informatie die als vernietigd beschouwd werd toch nog teruggevonden kan worden.
er geen functionaliteit is om overheidsinformatie te vernietigen,	applicaties 'vervuild' raken met onbetrouwbare overheidsinformatie	fouten worden gemaakt in de besluitvorming en dienstverlening aan burgers.

1. Perspectief Organisatie

Overheidsorganisaties creëren, ontvangen en beheren grote hoeveelheden informatie. Door de digitalisering is de omvang van overheidsinformatie enorm toegenomen. Dit maakt van het DUTO-proces vernietigen een belangrijk instrument om de aanwas van informatie beheersbaar te maken.

Een groot gedeelte van alle overheidsinformatie komt voor vernietiging in aanmerking. (Zie ook: (Alles bewaren? Beter van niet.) Nadat de bewaartermijn volgens de selectielijst is verstreken vormt deze informatie ballast voor de informatiehuishouding. Niets vernietigen betekent het laten voortbestaan en groei van onnodige lasten.

Kansen

Nb.: dit is geen uitputtende lijst.

Bron kans	**Gebeurtenis**	**gevolg**
Omdat overheidsinformatie wordt vernietigd conform de vigerende selectielijst,…	…neemt de kans toe dat bij een zoekvraag de juiste informatie naar voren komt,…	…met besparing op het gebied van administratieve lasten tot gevolg (bijvoorbeeld bij Woo-verzoeken).
	…is het volume data minder groot en draaien back-ups sneller en efficiënter,…	…met besparing op het gebied van technisch beheer tot gevolg.
	…worden toekomstige conversie- en migratietrajecten minder omvangrijk en complex,…	…met besparing op de inzet van mens en middelen tot gevolg
	…wordt geen informatie bewaard die je niet meer nodig hebt en wordt minder bijgedragen aan de groeiende vraag naar opslagcapaciteit,…	…met minder milieubelasting en tot gevolg.

	wordt in informatiesystemen geen informatie bewaard die je niet meer nodig hebt,…	…met een kostenbesparing tot gevolg voor het hosten, beheren, licenties en onderhoud.

Risico's

Bron risico	**Gebeurtenis**	**gevolg**
Indien overheidsinformatie niet wordt vernietigd,…	…is de kans groter dat geaggregeerde gegevens onbetrouwbaar zijn omdat ze vervuild zijn met niet actuele gegevens,…	…waardoor een organisatie verkeerde conclusies trekt