

Proces bewaren en vernietigen

Voorbeelddocument

Versie: Januari 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen procesbeschrijving voor het bewaren en vernietigen van gegevens. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het proces definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Geef hier aan wie het document goedkeurt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties> |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc189074589)

[2 Procesbeschrijving 5](#_Toc189074590)

# Inleiding

Het bewaar- en vernietigingsproces is enerzijds bedoeld om te voorkomen dat <naam schoolbestuur> gegevens langer bewaart dan nodig en anderzijds om ervoor te zorgen dat we voldoen aan wettelijke verplichtingen om gegevens te bewaren. Daarnaast zorgen we er met deze procesbeschrijving voor dat gegevens op een juiste manier worden verwijderd. Deze procesbeschrijving geeft weer hoe het bewaar- en vernietigingsproces wordt uitgevoerd binnen <naam schoolbestuur>. De procesbeschrijving sluit aan bij het bewaartermijnenbeleid van **<**naam schoolbestuur>.

Op grond van de Algemene verordening gegevensbescherming (AVG) geldt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Sommige persoonsgegevens moeten een wettelijk vastgestelde periode worden bewaard, terwijl voor andere gegevens <naam schoolbestuur> zelf richtlijnen heeft opgesteld op basis van noodzaak en behoefte. Zijn persoonsgegevens niet meer nodig voor het doel waarvoor ze zijn verzameld? Of is de wettelijk vereiste bewaartermijn verstreken? Dan moeten deze gegevens worden vernietigd. Daarnaast gelden voor andere gegevens van <naam schoolbestuur> ook andere wettelijke vereisten die voortvloeien uit onderwijswetgeving en de Archiefwet.

Het onnodig bewaren van (persoons)gegevens brengt onnodige kosten met zich mee, maar vergroot ook de risico’s op ongeautoriseerde toegang, onrechtmatige verwerking en datalekken. Daarom is het van groot belang dat <naam schoolbestuur> zorgvuldig omgaat met het bewaren en vernietigen van gegevens.

# Procesbeschrijving

In deze procesbeschrijving wordt in stappen uiteengezet op welke manier (persoons)gegevens binnen <naam schoolbestuur> worden bewaard en vernietigd. Het gaat om zowel gegevens als persoonsgegevens in de breedste zin van het woord: gegevens van leerlingen, leraren, medewerkers, zowel in papieren (analoge) als digitale vorm en handmatig of geautomatiseerd verwerkt.

Het bewaar- en vernietigingsproces bestaat uit de onderstaande 5 stappen die er samen voor zorgen dat het bewaren en tijdig vernietigen van (persoons)gegevens binnen <naam schoolbestuur> goed kan worden uitgevoerd. Aan de hand van dit proces maken we als organisatie inzichtelijk en beheersbaar op welke manier gegevens worden opgeslagen en verwijderd. Dit stappenplan kan worden gebruikt om bewaartermijnen te bepalen en te helpen met het vernietigen van de gegevens na afloop van deze termijn(en). Bij elke stap wordt aangegeven wie hiervoor in de praktijk verantwoordelijk is.

* **Stap 1:** Bepalen bewaartermijn
* **Stap 2:** Bepalen ontwerp vernietigingsmethoden
* **Stap 3:** Bepalen impact van de vernietiging
* **Stap 4:** Opstellen mitigatieplan
* **Stap 5:** Uitvoeren vernietiging van gegevens

Hieronder lichten we elke stap toe.

## Bepalen bewaartermijn

Zodra duidelijk is welke categorieën (persoons)gegevens worden verwerkt, moet de systeem- en/of proceseigenaar de toepasselijke bewaartermijnen vaststellen. Uitgangspunt hierbij is dat het doel is gekoppeld aan het gebruik in een systeem, applicatie of proces. <Naam schoolbestuur> maakt voor het bepalen van bewaartermijnen van (persoons)gegevens gebruik van het Bewaartermijnenoverzicht. In dit overzicht kan worden opgezocht hoelang een school (categorieën van) gegevens of documenten mag bewaren. Dit overzicht bevat wettelijke bewaartermijnen en richtlijnen die gelden voor situaties waarvoor geen specifieke wettelijke bewaartermijnen bestaan.

De bewaartermijn van gegevens wordt allereerst bepaald door wet- en regelgeving. De wettelijke bewaartermijnen van de meest voorkomende (persoons)gegevens staan in het Bewaartermijnenoverzicht. Ontbreekt een wettelijke bewaartermijn? Dan biedt het Bewaartermijnenoverzicht een richtlijn voor het bewaren van de meest voorkomende (persoons)gegevens. Je kunt hier alleen van afwijken in overleg met de privacy officer en/of IBP’er. Voor gegevens waarvoor geen wettelijke bewaartermijn of richtlijn bestaat, geldt het uitgangspunt dat gegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor de gegevens worden gebruikt. In dit geval bepaalt het schoolbestuur zelf de bewaartermijn en wordt de motivering hiervan vastgelegd door de systeem- en/of proceseigenaar. Dit gebeurt in overleg met de privacy officer en/of IBP’er.

De beveiligingsmaatregelen voor het bewaren van de gegevens worden bepaald door middel van de security baseline van <naam schoolbestuur>.

## Bepalen ontwerp vernietingsmethoden

Het vernietigen van (persoons)gegevens kan op verschillende manieren gebeuren. De systeem- en/of proceseigenaar stelt in overleg met de privacy officer en/of IBP’er vast welke vernietigingsmethode in welke situatie moet worden toegepast:

* **Fysieke vernietiging**.Papieren documenten moeten fysiek worden vernietigd. Dit houdt in dat deze worden versnipperd en afgevoerd via een gespecialiseerd vernietigingsbedrijf. Dit moet grondig en veilig gebeuren. Reconstructie van gegevens en documenten mag niet langer mogelijk zijn. Ook gegevensdragers (bijvoorbeeld schijven uit datacenters) moeten fysiek worden vernietigd. De vernietiging moet gecontroleerd en aantoonbaar plaatsvinden, inclusief een formele vastlegging dat de gegevens daadwerkelijk zijn vernietigd. Bij hergebruik van gegevensdragers en mobiele devices, moeten gegevens van de vorige gebruiker worden verwijderd.
* **Geautomatiseerde of handmatige verwijdering**. Het geniet de voorkeur om digitaal bewaarde gegevens geautomatiseerd te verwijderen. Dit biedt meer zekerheid en veiligheid dan handmatige acties.Is geautomatiseerde verwijdering niet mogelijk? Dan kunnen de gegevens handmatig worden verwijderd. Dit verloopt via een procesmatige aanpak, waarbij periodiek gegevens worden geschoond. De vernietiging moet gecontroleerd en aantoonbaar plaatsvinden, zodat achteraf een vastlegging aanwezig is van de verwijdering.
* **Ontoegankelijk maken**.In sommige gevallen moeten gegevens nog wel bewaard blijven voor een bepaald doel, maar mogen deze niet meer worden gebruikt voor andere doeleinden. In deze gevallen kan een scheiding worden gemaakt tussen applicaties om toegang tot de gegevens onmogelijk te maken voor specifieke toepassingen en/of personen.
* **Anonimisering**.Het is niet noodzakelijk gegevens te vernietigen wanneer deze niet meer kunnen worden aangemerkt als persoonsgegevens. Anonieme gegevens kunnen bijvoorbeeld nog worden gebruikt voor statistische analyse. Het is van belang om ervoor te zorgen dat het op geen enkele wijze meer mogelijk is de gegevens direct dan wel indirect tot een persoon te herleiden. Hierbij moet rekening worden gehouden met de mogelijke koppeling van gegevens binnen andere systemen. Voor het anonimiseren van persoonsgegevens gelden strenge regels. Dit gebeurt alleen in overleg met de privacy officer en/of IBP’er.

## Bepalen impact van de vernietiging

Na het vaststellen van de vernietigingsmethode, en voor het overgaan tot daadwerkelijke vernietiging, moet een inschatting worden gemaakt van de (mogelijke) impact op de processen binnen <naam schoolbestuur>. Hierbij wordt rekening gehouden met alle manieren waarop de gegevens worden gebruikt. De systeem- en/of proceseigenaar moet in kaart brengen wat de mogelijke consequenties kunnen zijn als de gegevens worden vernietigd. Denk bijvoorbeeld aan afhankelijkheden van andere processen, systemen, applicaties en procedures.

## Opstellen mitigatieplan

Op basis van de vastgestelde vernietigingsmethode en de (mogelijke) impact van de vernietiging, stelt de systeem- en/of proceseigenaar een mitigatieplan op. Dit mitigatieplan beschrijft op welke manier de mogelijke impact van de vernietiging kan worden gemitigeerd. Voorafgaand dient overleg plaats te vinden met de privacy officer en/of IBP’er.

## Uitvoeren vernietiging van gegevens

Is de vernietigingsmethode bepaald en eventuele impact gemitigeerd? Dan moet worden overgegaan tot de daadwerkelijke vernietiging van gegevens. In veel situaties is het raadzaam om vernietiging in verschillende fases uit te voeren. In de praktijk betekent dit bijvoorbeeld dat een set van gegevens eerst in quarantaine wordt geplaatst om te bezien of onverhoopt problemen optreden in andere systemen of processen. Is dit het geval? Dan kan de set van gegevens uit quarantaine worden gehaald om de problemen eerst op te lossen voordat de definitieve verwijdering plaatsvindt.

De vernietiging van de gegevens is de verantwoordelijkheid van de systeem- en/of proceseigenaar. Deze eigenaar moet aan het schoolbestuur kunnen aantonen dat de vernietiging heeft plaatsgevonden. In het geval van fysieke vernietiging is het belangrijk dat dit door een gecertificeerde dienstverlener gebeurt.

Gegevens in back-up
Wanneer gegevens volgens het bewaartermijnenbeleid uit systemen worden verwijderd, staan ze soms nog steeds in een back-up. Ze zijn dus nog niet definitief verwijderd. Terwijl het uitgangspunt is dat persoonsgegevens ook uit back-ups moeten worden verwijderd.

Soms is het technisch niet mogelijk om specifieke gegevens uit een back-up te verwijderen, maar alleen de hele back-up te vernietigen. Dat is niet wenselijk. In dat geval worden back-ups niet verwijderd, tenzij de gegevens bij het terugzetten alsnog worden verwijderd uit de back-up. Overleg voorafgaand met de privacy officer en/of IBP’er.

Digitaliseren en vernietigen van papieren gegevens

(Persoons)gegevens die op papier zijn ontvangen, mag je gedigitaliseerd bewaren. Daarna mag je het papieren document vernietigen. Het is wel belangrijk dat de digitale kopie exact overeenkomt met het papieren document en dezelfde informatie bevat.