HANDOUT

KVAN

WETEN OF VERGETEN?
hand-out Archiefwet & AVG

Oktober 2024

Inhoudsopgave

Inhoud

Inhoudsopgave 1
WETEN OF VERGETEN? HAND-OUT ARCHIEFWET en AVG 2
Persoonsgegevens? → AVG ! 2
Overheidsdocumenten? → Archiefwet ! 2
Waarden waarop de AVG en de Archiefwet zijn gebaseerd 3
Archiefwet 3
AVG 3
Rechtmatigheid van verwerking persoonsgegevens in overheidsarchieven 3
Meest gestelde vragen over de relatie AVG vs. Archiefwet 4
Ad 1 Wanneer moet je persoonsgegevens archiveren? 4
Ad 2 Hoe verhoudt het principe van doelbinding zich tot archivering? 5
Ad 3 Hoe verhoudt het principe van minimale gegevensverwerking zich tot archivering? 5
Ad 4 Worden bewaartermijnen bepaald op basis van de AVG of de Archiefwet? 5
Ad 5 Hoe worden bewaartermijnen bepaald? 6
Ad 6 Op basis waarvan worden overheidsdocumenten vernietigd? 6
Ad 7 Mogen alle rechtmatig verzamelde persoonsgegevens zonder meer gearchiveerd worden? 7
Ad 8 Hoe voorkom je risico's voor de privacy van betrokkenen bij archivering? 7
Ad 9 Anonimiseren of pseudonimiseren? 8
Ad 10 Hoe weeg je belangen af in de praktijk ? 8

WETEN OF VERGETEN?

HAND-OUT ARCHIEFWET en AVG

Bij het beheer van persoonsgegevens hebben overheidsorganisaties te maken met de Archiefwet én de AVG. In de praktijk leidt dat tot vragen over hoe deze wetten zich tot elkaar verhouden. De handreiking *'Weten of Vergeten'* en deze gecomprimeerde hand-out geven handvatten en aanwijzingen voor de omgang met beide, in onderlinge samenhang.
Deze hand-out en de handreiking richten zich specifiek op het informatiebeheer vóór de uiteindelijke vernietiging of overbrenging van documenten naar een archiefinstelling. [1]

Persoonsgegevens? ⟶ AVG !

Bij het verwerken van persoonsgegevens van (mogelijk) levende personen heb je altijd te maken met de AVG.

BELANGRIJKE AVG-PRINCIPES

- → Rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens
- → Dataminimalisatie
- → Doelbinding

Dit betekent:

- **Baseer iedere verwerking op een grondslag.**
- **Verwerk alleen díe persoonsgegevens, die nodig zijn voor dat doel.**
- **Bewaar de gegevens niet langer dan nodig voor dat doel.**

Overheidsdocumenten? ⟶ Archiefwet !

Anders dan de AVG heeft de Archiefwet alléén betrekking op documenten van de overheid. De wet stelt eisen aan het beheer daarvan.

Belangrijke principes zijn:

→ Overheidsdocumenten in goede, geordende en toegankelijke staat brengen en bewaren
→ Zorgen voor tijdige vernietiging van daarvoor in aanmerking komende documenten.

In deze hand-out verstaan we onder 'archiveren': het uitvoeren van beheeractiviteiten op basis van de Archiefwet.

Daaronder valt onder meer het registreren, bewaren, toegankelijk maken, overbrengen en vernietigen van documenten.

[1]. Zie voor de handreiking https://www.kvan.nl/publicaties/handreiking-avg-en-archiefwet/

Documenten: informatie ongeacht de vorm
Dit kan zijn digitale tekst, een papieren document, geluidsopnamen, beeld, 3D-objecten etc. Definitie volgens de nieuwe Archiefwet 20xx én Wet Open Overheid. [2]

Persoonsgegevens maken vaak onderdeel uit van overheidsdocumenten.
Is dit het geval, dan gelden de AVG en Archiefwet **tegelijkertijd**. Zij zijn niet tegenstrijdig, maar liggen in elkaars verlengde en vullen elkaar op onderdelen aan.

Waarden waarop de AVG en de Archiefwet zijn gebaseerd

Archiefwet

- Efficiënte bedrijfsvoering en geheugen van de overheid, bewijsvoering burger/overheid.
- Authenticiteit en integriteit van overheidsinformatie.
- Transparantie van de overheid, afleggen van verantwoording.
- Reconstructie van het verleden en veiligstellen van cultureel erfgoed.

AVG

- Rechtmatigheid, behoorlijkheid en transparantie in de verwerking van persoonsgegevens.
- Doelbinding.
- Dataminimalisatie.
- Juistheid van de persoonsgegevens.
- Opslagbeperking.
- Vertrouwelijkheid en integriteit.

Rechtmatigheid van verwerking persoonsgegevens in overheidsarchieven

De AVG noemt zes rechtmatige grondslagen voor de verwerking van persoonsgegevens. Bij de overheid is die grondslag vaak: wettelijke verplichting, taak van algemeen belang of uitoefening van openbaar gezag. Maar de grondslag kan ook zijn: sluiten van een overeenkomst, toestemming van de betrokkene of gerechtvaardigd belang. Zie artikel 6 van de AVG.

Wanneer persoonsgegevens zijn verwerkt met een rechtmatige oorspronkelijke grondslag, mogen ze verder worden verwerkt op basis van ‘archivering in het algemeen belang', zie artikel 5.1b van de AVG.

LET OP: De Archiefwet en/of ‘archivering in het algemeen belang’ zijn géén zelfstandige grondslagen om persoonsgegevens te verwerken! Daarvoor is allereerst een rechtmatige AVG-grondslag nodig.

---

[2]. De nieuwe Archiefwet treedt naar verwachting in 2016 in werking.

Meest gestelde vragen over de relatie AVG vs. Archiefwet

1. **Wanneer moet je persoonsgegevens archiveren?**
2. **Hoe verhoudt het principe van doelbinding zich tot archivering?**
3. **Hoe verhoudt het principe van minimale gegevensverwerking zich tot archivering?**
4. **Worden bewaartermijnen bepaald op basis van de AVG of de Archiefwet?**
5. **Hoe worden bewaartermijnen bepaald?**
6. **Op basis waarvan worden overheidsdocumenten vernietigd?**
7. **Mogen alle rechtmatig verzamelde persoonsgegevens zonder meer gearchiveerd worden?**
8. **Hoe voorkom je risico's voor de privacy van betrokkenen bij archivering?**
9. **Anonimiseren of pseudonimiseren?**
10. **Hoe weeg je belangen af in de praktijk?**

Ad 1 Wanneer moet je persoonsgegevens archiveren?

Check of de primaire verwerking van persoonsgegevens rechtmatig is volgens de AVG.

- Mag je deze volgens de AVG WEL verwerken?
  → Dan moet je ze als overheid ook archiveren, de Archiefwet geldt.
- Mag je deze volgens de AVG NIET verwerken?
  → Dan mag je ze als overheid NIET archiveren en is de Archiefwet niet aan de orde.

LET OP: Gegevens opslaan is óók een verwerking onder de AVG.

Archiveringsplicht is dus geen reden om persoonsgegevens te bewaren of anderszins te verwerken die je volgens de AVG niet mocht verwerken. Praktijkvoorbeelden van gegevens die niet verwerkt, dus ook niet gearchiveerd mogen worden:

- Gegevens verzameld zonder AVG grondslag.
- Gegevens die alleen dienen ter identificatie van een aanvrager, zoals een kopie paspoort.
- BSN verwerken waar dat niet wettelijk is bepaald en/of niet noodzakelijk is.
- Et cetera.

Bij de archivering van documenten met persoonsgegevens is het nodig om 'passende waarborgen' voor de bescherming van de privacy te geven, zie artikel 89 van de AVG. De AVG noch de regelgeving werken verder uit wat 'passende waarborgen' precies zijn. Wel wordt genoemd dat dit 'technische en organisatorische maatregelen' kunnen zijn. Het is afhankelijk van de situatie. Denk bijvoorbeeld aan informatiebeveiliging, fysieke beveiliging, en het toepassen van bewaartermijnen.

Ad 2 Hoe verhoudt het principe van doelbinding zich tot archivering?

Artikel 5 van de AVG: principe doelbinding
Gegevens niet langer, niet meer en niet anders bewaren dan nodig voor het doel ('voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden')

Dit betekent: Persoonsgegevens verwijderen zodra ze niet meer nodig zijn voor het doel. Dit kan in de praktijk door het toepassen van de vastgestelde bewaartermijnen in de selectielijsten. Selectielijsten zijn gebaseerd op de Archiefwet. Je kunt dit opvatten als een 'passende waarborg' zoals de AVG voorschrijft.

Ad 3 Hoe verhoudt het principe van minimale gegevensverwerking zich tot archivering?

Artikel 5 van de AVG: principe dataminimalisatie
Zo min mogelijk persoonsgegevens verwerken, niet meer dan nodig voor dat doel. ('toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden')
Dit geldt ook voor documenten met persoonsgegevens die op grond van de Archiefwet worden gearchiveerd.

→ Het is aan te raden doelbinding en minimale gegevensverwerking in de praktijk uit te voeren door 'privacy by default and design' + 'archiving by design'.
Dat wil zeggen: richt processen en systemen al vanaf de vorming van processen, documenten en dossiers zó in, dat:

- niet teveel persoonsgegevens worden verwerkt;
- deze niet te lang worden bewaard.

Ad 4 Worden bewaartermijnen bepaald op basis van de AVG of de Archiefwet?

Op basis van AVG én Archiefwet wordt bepaald hoe lang je persoonsgegevens mag bewaren.

- In de praktijk worden bewaartermijnen voor categorieën overheidsinformatie vastgelegd in zogenaamde selectielijsten.
- Deze selectielijsten zijn verplicht en worden vastgesteld op basis van de Archiefwet.
- Bij het vaststellen van bewaartermijnen wordt rekening gehouden met zowel de AVG - principes waaronder dataminimalisatie en doelbinding, als met de Archiefwet principes waaronder bewijsvoering, verantwoordings- en reconstructiefunctie.
- Vanuit de AVG kan het, naast vaststellen van bewaartermijnen voor categorieën informatie, zinvol zijn om in de selectielijst specifieke bewaartermijnen voor bepaalde persoonsgegevens op te nemen.

Het vaststellen en toepassen van bewaartermijnen is onderdeel van een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Ook is het een onderdeel van de verplicht te treffen organisatorische en technische 'passende maatregelen'.

Mocht blijken dat een bewaartermijn uit de selectielijst niet voldoet aan de uitgangspunten van de AVG, dan is het nodig om de lijst - in overleg met de archivaris - aan te passen.

Ad 5 Hoe worden bewaartermijnen bepaald?

Bewaartermijnen worden vastgesteld in selectielijsten, die verplicht zijn op basis van de Archiefwet. Een bewaartermijn wordt per categorie informatie vastgesteld (niet voor afzonderlijke documenten).

- Denk aan categorieën als beleid, uitvoering, begrotingscyclus of communicatie.
- Documenten zijn onderdeel van zaak-/projectdossiers en dergelijke die tot een categorie horen.
- Persoonsgegevens maken doorgaans onderdeel uit van documenten.

Bewaartermijnen op grond van de Archiefwet gelden dus óók voor persoonsgegevens in documenten binnen categorieën informatie. Bij het vaststellen van de termijnen wordt rekening gehouden met AVG-principes.

Bewaartermijnen die in andere (sectorale) wetgeving zijn vastgelegd worden overgenomen in de selectielijsten. Voorbeeld: de bewaarplicht van 7 jaar voor financiële gegevens uit de Algemene Wet inzake Rijksbelastingen wordt overgenomen in selectielijsten.

Wanneer er geen bewaartermijn in enige wet is vastgelegd, dan wordt deze door de archiefvormende verwerkingsverantwoordelijke (bestuurlijk verantwoordelijke) vastgesteld met behulp van een daarvoor ontwikkelde methodiek.

Ook in het verwerkingenregister op grond van de AVG worden bewaartermijnen opgenomen.

Voor een goede naleving van zowel AVG als Archiefwet is het uiteraard vereist, dat beide termijnen overeenstemmen.

→ Stem bewaartermijnen altijd af in overleg tussen experts AVG én experts Archiefwet.
→ Zo komt een samenhangende en juiste lijst van bewaartermijnen en de toepassing ervan tot stand. Dit bevordert een goede afstemming en toepassing van de termijnen.

Ad 6 Op basis waarvan worden overheidsdocumenten vernietigd?

Vernietiging van overheidsdocumenten is op grond van de Archiefwet verplicht na afloop van de vastgestelde bewaartermijn.

- De meeste overheidsinformatie wordt op termijn vernietigd.
- Van vernietiging wordt op grond van het Archiefbesluit een verklaring opgesteld.
- Een klein deel van de informatie is van zoveel maatschappelijke en historische waarde dat ze niet wordt vernietigd, maar permanent bewaard. Ook dit is in de selectielijsten vastgelegd.

Ad 7 Mogen alle rechtmatig verzamelde persoonsgegevens zonder meer gearchiveerd worden?

- Ja, dat is zelfs verplicht, totdat de bewaartermijn uit de selectielijst is verstreken.
- Op basis van de AVG dient bij alle verwerkingen steeds aandacht besteed te worden aan principes als doelbinding, dataminimalisatie en passende waarborgen voor de privacy.
- Tijdens de creatie- of ontvangstfase van documenten - de primaire verwerking - worden daarom de principes 'archiving by design' en 'privacy by default and design' toegepast.

Praktisch betekent dit:

→ Verwerk alleen de persoonsgegevens die nodig zijn voor het doel.
→ Zorg ervoor dat de persoonsgegevens juist zijn en zonodig worden gecorrigeerd.
→ Regel aspecten als toegang, autorisatie, beveiliging etc.
→ Volg hierbij zoveel mogelijk het beleid van je organisatie.
→ Bewaar de persoonsgegevens gedurende de bewaartermijn van het document.
→ Vernietig het document met de persoonsgegevens zodra de bewaartermijn is verstreken.

Ad 8 Hoe voorkom je risico's voor de privacy van betrokkenen bij archivering?

De AVG geeft in artikel 89 aan dat verwerking van persoonsgegevens in het kader van 'archivering in het algemeen belang' moet gebeuren met 'passende waarborgen' voor de privacy.

- Wat passende waarborgen zijn is afhankelijk van de situatie.
- Besteed hier bij de ontwerp- en inrichtingsfase van processen en systemen al expliciet aandacht aan.
- Dit is het 'by design'-principe: privacy by default and design én archiving by design.

→ Sla documenten/gegevens op in een daarvoor toegerust systeem.
→ Zorg ervoor dat privacygevoelige informatie alleen raadpleegbaar is voor medewerkers die daar uit hoofde van hun functie bij moeten kunnen.
→ Mail geen privacygevoelige informatie rond en sla deze niet op in open, niet-beveiligde netwerkmappen. Dat bemoeilijkt het toepassen van bewaartermijnen en toegangsbeheer.

De AVG-principes gelden ook voor de manier waarop een organisatie persoonsgegevens opvraagt of ontvangt. Zo is het niet altijd nodig om ter identificatie van personen kopie-paspoorten op te vragen. Volg een andere werkwijze met minder impact op de privacy, gebruik bijvoorbeeld DigID.

Leg, indien nodig, verantwoording af in een risicoanalyse - DPIA in vaktermen - over welke persoonsgegevens worden verwerkt, wat daarvan het risico is en welke beschermende maatregelen worden genomen. Of dit nodig is, is afhankelijk van hoe risicovol de verwerking is en van intern beleid. Zie artikel 35 van de AVG.

Het is bij het aanmaken en verwerken belangrijk om de interne voorschriften te volgen als het gaat om het vermelden van namen en gegevens van medewerkers, ontvangers en/of opstellers van documenten.

Bij het archiveren is het raadzaam om eenmaal rechtmatig verkregen persoonsgegevens discreet te verwerken.

- Een vergunningsdossier bijvoorbeeld krijgt bij voorkeur een volgnummer.
- Gebruik liever geen verwijzingen met persoonsgegevens zoals "De heer F. Ictief, geboren te 01-01-1980".
- Leg indien nodig verantwoording af in een risicoanalyse (DPIA) met daarin over welke persoonsgegevens het gaat en hoe ermee wordt omgegaan.

Ad 9 Anonimiseren of pseudonimiseren?

Anonimiseren en pseudonimiseren zijn technische maatregelen die je als onderdeel van de passende waarborgen volgens artikel 89 van de AVG kunt treffen.

→ *Anonimiseren*: persoonsgegevens onherroepelijk verwijderen uit de bron, de AVG is dan niet meer van toepassing.

→ *Pseudonimiseren:* gegevens niet onherroepelijk wissen uit de bron, maar alleen uit een (raadpleeg)kopie.
Dit kan bijvoorbeeld door een sleutel herstelbaar en toegankelijk te houden. De AVG blijft dan van toepassing. Hiervoor zijn verschillende technieken beschikbaar. Pseudonimisering vindt bijvoorbeeld plaats bij het maken van gebruikskopieën in het kader van de Woo.

Op grond van de Archiefwet moeten documenten authentiek en integer blijven tijdens de hele bewaartermijn. Zo kunnen zaken gereconstrueerd worden en kunnen de documenten dienen als bewijs. Dat staat haaks op het permanent vernietigen van persoonsgegevens uit documenten. Daarom zal pseudonimiseren van overheidsdocumenten meestal de voorkeur hebben. Bij anonimiseren worden immers achteraf gegevens onherroepelijk verwijderd uit een document of dossier, waardoor het document niet meer integer en authentiek is en niet meer als bewijs kan dienen.
Toch kunnen zich situaties voordoen waarbij het herleiden naar personen niet meer van belang is. Organisaties moeten hierbij een zeer zorgvuldige afweging maken, waarbij de verschillende vakgebieden privacy én archiefrecht worden betrokken.
Anonimiseren kan onrechtmatige vernietiging van overheidsinformatie betekenen.

Ad 10 Hoe weeg je belangen af in de praktijk ?

De uitvoeringspraktijk van informatiebeheer kan weerbarstig zijn. Bijvoorbeeld wanneer na de primaire verwerking een ander inzicht ontstaat over de noodzaak of grondslag om bepaalde persoonsgegevens te verwerken.

→ Dan is belangrijk: houd rekening met verschillende perspectieven en weeg belangen af vóórdat een besluit wordt genomen om documenten te bewaren of vernietigen.
→ Betrek bij een besluit tot vernietiging van persoonsgegevens zowel privacy-expertise als expertise over de Archiefwet.

Voorbeeld: aanvraag van een gehandicaptenparkeerplaats via een dienstverleningssysteem.

→ Facilitaire aanvragen krijgen meestal een bewaartermijn van 2 jaar.
Bij een aanvraag gehandicaptenparkeerplaats kunnen echter bijzondere (medische) persoonsgegevens zijn verwerkt. Een organisatie kan dan besluiten om dit soort aanvragen te pseudonimiseren (of te anonimiseren) vanwege de gevoelige aard. Idealiter heeft die maatregel dan een legitieme basis in de selectielijst.

Een andere praktijk is om onderscheid te maken tussen *persoonsgegevens die nodig zijn voor de behandeling van de zaak en voor bewijs*, en *gegevens die tijdelijk nodig zijn*.
De belangrijke gegevens kunnen bewaard worden in de applicatie of in een document. De overige gegevens – zoals in het voorbeeld de medische gegevens - kunnen dan na bijvoorbeeld 6 weken of na het verstrijken van een bezwaartermijn verwijderd of teruggezonden worden.
Het systeem of de procesapplicatie is bij voorkeur daarop ingericht (privacy by design en archiving by design). Ook zo'n onderscheid in bewaartermijnen moet besproken worden bij vaststelling van een selectielijst.

Maatregelen kunnen zo nodig worden gecombineerd.
Wanneer bijvoorbeeld in het kader van de Woo een document beschikbaar moet worden gesteld, is het vaak nodig om de informatie te ontdoen van persoonsgegevens. In de ontwerpfase kan het systeem of de applicatie daar al op ingericht worden. Bijvoorbeeld door in het datamodel vast te leggen welke gegevenselementen wel of niet voor publicatie in aanmerking komen.

AVG en Archiefwet in combinatie met Woo en wissingsverzoek
Een openbaar te maken document - bijvoorbeeld onder de Wet Open Overheid - kan gepseudonimiseerd (gelakt) beschikbaar worden gesteld.

- Bij publicatie van een kopie zonder persoonsgegevens dient het originele document omwille van de authenticiteit wel bewaard te blijven, met alle persoonsgegevens daarin.
- Dit origineel dient beperkt toegankelijk te zijn bijvoorbeeld door middel van autorisaties en/of andere beveiligingsmaatregelen.
- Daarnaast kan bepaalde informatie uit het geopenbaarde document op een website worden gepubliceerd in gepseudonimiseerde vorm.
- Ook hier is het van belang om kennis van zowel AVG, Archiefwet als ook van de Woo te betrekken en af te wegen.

Voorbeeld wissingsverzoek:
Bij verzoeken om vergetelheid (of vernietigingsverzoeken) op grond van artikel 17 van de AVG:

- Zorg dat de organisatie een procedure heeft vastgesteld en deze ook volgt.
- Via deze procedure bepaalt de organisatie in hoeverre het recht op vernietiging van persoonsgegevens van toepassing is. Let daarbij op de uitzonderingen in artikel 17.
- Betrek ook de bewaartermijn uit de selectielijst, zodat deze gerespecteerd blijft.
- Schakel de juiste deskundigheid in: privacyfunctionaris + Archiefwet-deskundige.
- Laat de beslissing niet over aan willekeurige medewerker die het verzoek het eerst binnenkrijgt.

Voorbeeld: een burger vraagt om het wissen van zijn vergunningaanvraag nadat hij deze heeft ingetrokken.

Een medewerker zou kunnen denken: de vergunning gaat niet door

→ Dus de aanvraag kan wel gewist worden.

Maar: in de selectielijst is een bewaartermijn vastgesteld voor ingetrokken aanvragen.

→ Dat betekent dat die documenten pas na afloop van die bewaartermijn kunnen worden vernietigd.