BRS
Boa Registratie Systeem

Versie 1.0
Status Definitief
Datum 19 februari 2021

BEWAARTERMIJNENWIJZER
WPG VOOR BOA'S

E-mail info@boaregistratie.nl
Boa Registratie Systeem

INHOUD

INLEIDING

De Wpg bevat diverse bepalingen die beschrijven welke typen gegevens hoe lang verwerkt en vervolgens bewaard mogen worden. Ook de Algemene Verordening Gegevensverwerking (AVG) en de Archiefwet bevatten bepalingen over dit onderwerp. Deze bewaartermijnenwijzer is ervoor bedoeld eenduidigheid te creëren rondom de termijnen en de begrippen die in de diverse wetgeving voorkomen. De begrippen die in deze wijzer gehanteerd worden, worden verderop toegelicht. Raadpleeg deze eerst zodat duidelijk is wat onder begrippen als verwerken en verwijderen wordt verstaan.

Naast genoemde wetgeving en de memorie van toelichting op de betreffende wetten, is bij de totstandkoming van deze wijzer gebruik gemaakt van het document Beleid Bewaartermijnen van de politie, opgesteld door de Gegevensautoriteit en op 13 februari 2020 vastgesteld. Ook is gebruik gemaakt van het *Functioneel Ontwerp BRS – Wpg bewaartermijnen van 2 april 2020.*

VERWERKINGSGRONDSLAGEN: 8, 9 EN 13

De Wpg onderscheidt verschillende doelen waarvoor politiegegevens mogen worden verwerkt: de verwerkingsgrondslagen. Voor de boa zijn dit artikel 8, 9 en 13-verwerkingen.

Artikel 8: Dagelijkse boa-taak

Als de boa persoonsgegevens verzamelt in het kader van de dagelijkse boa-werkzaamheden, vallen die onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Deze gegevens mogen tot vijf jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden benaderd. Bijvoorbeeld via een naam, adres of kenteken. Artikel 8-gegevens kunnen ook voor andere doelen verder worden verwerkt. Bijvoorbeeld een overzicht van proces-verbalen en waarschuwingen voor agressieve honden heeft gehad, kan verder worden verwerkt onder het regime van artikel 13 en daar langer beschikbaar blijven en breed gedeeld worden, bijvoorbeeld om recidive te kunnen bepalen.

Artikel 9: Gerichte verwerkingen

Dit artikel biedt de grondslag om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8-verwerkingen. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict. Ook een gericht onderzoek naar het vergiftigen van vossen of dumping van asbest kan onder artikel 9 vallen, bijvoorbeeld als je verwacht dat het onderzoek langer dan veertig uur duurt. Het doel van een artikel 9-verwerking moet binnen een week worden vastgelegd. Elke artikel 9-verwerking heeft een ‘bevoegd functionaris’; deze kan opdracht geven om deze gegevens voor een ander doel verder te verwerken of om ze te delen met een ketenpartner.

Zodra het oorspronkelijke doel van de verwerking is bereikt, mag je artikel 9-gegevens niet meer gebruiken. Soms is het lastig te bepalen wanneer dit het geval is. In de praktijk is bij artikel 9 de verwerkingstermijn van gegevens vaak langer dan bij artikel 8. Artikel 9-informatie is alleen bestemd voor collega’s (dat kunnen ook opsporingsambtenaren zijn die elders werkzaam zijn) die een rol hebben in de betreffende verwerking. De groep geautoriseerden voor artikel 8-gegevens is veel groter.

Artikel 13: Ter ondersteuning van het werk

Dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9, verder te verwerken. Bijvoorbeeld om een overlast gevend persoon die in een andere gemeente is gaan wonen, te kunnen identificeren. Maar het kan ook gaan om het centraal raadplegen van boetes, gebiedsverboden of bijvoorbeeld gevarenclassificaties. Artikel 13-gegevens worden door de politie vaak landelijk raadpleegbaar gesteld. Hoe lang je deze gegevens mag verwerken en wie er toegang mogen hebben, moet in een bijbehorend reglement worden beschreven. Hiermee mogen sommige gegevens wel vijftien jaar beschikbaar blijven, andere veel korter. Een voorbeeld van een artikel 13-verwerking is dat bij een bestuurlijke strafbeschikking milieu eerst landelijk gecontroleerd moet worden of deze persoon deze afdoening al meer dan drie keer heeft gehad. Dat kan in BRS worden gecontroleerd. Indien dat het geval is, kan hij deze afdoening niet nogmaals krijgen en moet er een tikverbaal opgemaakt worden.

Meer informatie over het onderscheid tussen de verwerkingsgronden? Raadpleeg het Praktijkhandboek Wpg en de “instructie scheidingslijn artikel 8 en 9”.

TERMIJNEN

Termijnen artikel 8: Dagelijkse opsporingstaak

Het uitgangspunt is dat gegevens vijf jaar te verwerken zijn. Wpg art. 8 lid 1 biedt de mogelijkheid deze termijn voor bepaalde gebruikersgroepen te beperken tot één jaar. Vooralsnog zijn noch bij de politie noch in het boa-werkveld groepen aan te wijzen waar een verwerkingsperiode van een jaar passend zou zijn. De belangrijkste reden hiervoor is dat – zowel bij het bepalen van de juiste strafmaat als voor de veiligheid van de opsporingsambtenaar - het noodzakelijk is om te weten wat zich de afgelopen vijf jaar heeft afgespeeld, bijvoorbeeld op een adres, met een persoon of een voertuig. Een periode van een jaar is daarvoor onvoldoende.

Verwijderen

Vijf jaar na de datum van de eerste verwerking (artikel 8, lid 6 Wpg) dienen de gegevens verwijderd te worden. Of zoveel eerder indien blijkt dat gegevens niet meer nodig zijn voor het doel waar ze oorspronkelijk voor verwerkt werden (artikel 8, lid 6 en artikel 4 lid 2 Wpg).

Vernietigen

- Zodra de gegevens niet meer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak (artikel 8, lid 6 Wpg).
- Verwijderde gegevens worden gedurende vijf jaar bewaard en vervolgens vernietigd (artikel 14, lid1 Wpg).
- Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats (artikel 14, lid 4 Wpg).
- Gegevens die zijn verkregen op grond van gemeentelijk cameratoezicht worden na ten hoogste vier weken vernietigd, tenzij er concrete aanleiding bestaat te vermoeden dat die gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit en daartoe verder worden verwerkt.
- Gegevens die zijn verkregen met behulp van ANPR-camera's worden uiterlijk na vier weken vernietigd, tenzij de gegevens overeenkomstig art. 126jj Sv verder mogen worden verwerkt.

Termijnen artikel 9: Gerichte verwerkingen

Verwijderen

- Zodra de gegevens niet meer noodzakelijk zijn voor het doel van het onderzoek.
- Of na verloop van een periode van maximaal een half jaar waarin ze verwerkt worden om te bezien of ze aanleiding geven tot een nieuw onderzoek ('herbruikbare informatie').
- Het doel van het onderzoek is meestal bereikt als alle daders van het strafbare feit zijn opgespoord en vervolgd en de door de rechter opgelegde straf of maatregel geheel ten uitvoer is gelegd. Zodra de boa-werkgever een afloopbericht van het OM ontvangt, bepaalt de bevoegd functionaris of het doel is bereikt en beëindigt hij de verwerking.
- Als de verdachte of veroordeelde is overleden wordt het dossier in overleg met de Officier van Justitie opgelegd en wordt de verwerking beëindigd.
- Artikel 9-verwerkingen waarover geen evident contact met het OM bestaat zoals voorbereidende onderzoeken, veelplegersdossiers of multi-probleemgezinnen, moeten met een handmatig bepaalde datum worden bewaakt door de bevoegd functionaris.

Vernietigen

- Verwijderde gegevens worden gedurende 5 jaar bewaard en vervolgens vernietigd (artikel 14, lid 1 Wpg).
- Voor auditieve en audiovisuele registraties geldt dat de instantie waar de registratie is opgeslagen de Officier van Justitie moet verzoeken om een opdracht tot vernietiging van de registratie. De opdracht tot vernietiging wordt binnen 30 dagen uitgevoerd.
- Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats (artikel 14, lid 4 Wpg).
- Gegevens die na een doorzoeking niet van belang zijn gebleken (artikel 125n Sv), gegevens die mededelingen van geheimhouders bevatten (artikel 126aa Sv) en gegevens die o.a. zijn verkregen door het opnemen van vertrouwelijke communicatie of telecommunicatie (artikel 126cc Sv) moeten eerder worden vernietigd, tenzij de Officier van Justitie anders heeft bepaald

Termijnen artikel 13

Gegevens die verder verwerkt worden onder artikel 13, worden aan het einde van hun verwerkingstermijn niet eerst verwijderd, maar direct vernietigd. Wanneer dit moet gebeuren, dient te blijken uit het bij die verwerking behorende artikel 13-protocol. Deze termijn wordt door de verwerkingsverantwoordelijke bepaald en gemotiveerd en verschilt dus per artikel 13-verwerking. De termijnen voor specifieke artikel13-verwerkingen zijn terug te vinden in de betreffende protocollen en in het verwerkingsregister.

Termijnen verwijderde politiegegevens (artikel 14)

Voor gegevens die zijn verwijderd op grond van artikel 8 of 9 is de termijn voor vernietiging in artikel 14 van de Wpg bepaald. Deze gegevens worden gedurende vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen (audits of controle door de Autoriteit Persoonsgegevens). Verder geldt dat deze gegevens in bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10 Wpg ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Dit kan alleen in opdracht van het bevoegd gezag en alleen ten behoeve van een actuele artikel 9- of 10-verwerking. Bijvoorbeeld voor een onderzoek dat nu door de politie wordt uitgevoerd. Gegevens in de bewaartermijn mogen ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.

BEGRIPPEN

Verwerken

De AVG en de Wpg hanteren dezelfde definitie van het begrip verwerken: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen, verwijderen of vernietigen van persoonsgegevens. Kortom alles wat je met gegevens kan doen vanaf het moment van ontstaan tot het moment van vernietiging óf – in uitzonderlijke gevallen- bij overbrenging naar een archiefbewaarplaats.

Verwijderen

In de Wpg wordt met verwijderen bedoeld het buiten de operationele verwerking plaatsen van politiegegevens. Verwijderen is dus een privacybevorderende maatregel, namelijk door het beperken van de toegang. Verwijderde gegevens zijn wel beschikbaar, maar alleen voor functioneel of technisch beheerders, of medewerkers die zich bijvoorbeeld bezig houden met klachtafhandeling of het hernieuwd verwerken.

Bewaren

Politiegegevens (Wpg) die zijn verwijderd worden gedurende vijf jaar bewaard voor het afhandelen van klachten en het verantwoorden van verrichtingen (audits). Verder kunnen deze gegevens in bijzondere gevallen en voor zover dat noodzakelijk is voor een artikel 9-verwerking ter beschikking worden gesteld voor hernieuwde verwerking. Dit kan alleen in opdracht van de Officier van Justitie. Deze gegevens mogen ook verwerkt worden ten behoeve van wetenschappelijk onderzoek en statistiek.

Beëindigen van de verwerking: Vernietigen (Wpg) en Wissen (AVG)
Onder vernietigen (Wpg) verstaan we het onherstelbaar wissen van persoonsgegevens. In de AVG wordt het begrip wissen gehanteerd. Wissen en vernietigen hebben totale werking, ook naar registraties in het verleden. Technische gezien gaat het om ‘zodanig verminken van de informatiedragers (…) dat de vastgelegde content niet meer toegankelijk en beschikbaar is. Uitgangspunt vormen daarbij de normen voor vernietiging van gerubriceerde informatie zoals vastgelegd in de DIN 66399 (2012-10).’

Archiveren

In de Archiefwet wordt archiveren gedefinieerd als het zorgdragen voor goed beheer van overheidsinformatie vanaf het moment van ontvangst of eerste vastlegging tot het moment van vernietiging of overbrenging naar een archiefbewaarplaats. Wat onder overheidsinformatie valt, wordt niet bepaald door de vorm van de informatie, maar door het ontstaan en gebruik ervan. Bij overheidsinformatie gaat het niet alleen om tekstdocumenten, zoals notities en verslagen, maar ook om bijvoorbeeld ingevulde formulieren, foto’s, video’s, websites en Tweets. De activiteit ‘archiveren’ is dus erg breed.

Anonimiseren

Het vernietigen of wissen van identificerende gegevens uit een bestand. De geanonimiseerde data zijn daarmee niet meer herleidbaar tot personen en daarmee is anonimiseren een privacybevorderende maatregel. Geanonimiseerde gegevens vallen niet onder de werking van de AVG of Wpg. De vraag is of de herleidbaarheid in praktijk is uit te sluiten. Een willekeurige geanonimiseerde dataset die tot op detailniveau van personen iets registreert, is op zichzelf anoniem maar bevat per definitie een aanknopingspunt om met andere datasets te combineren. Het in combinatie verwerken van grote op het oog willekeurige gedetailleerde data, is zelfs de kern van big data. Met de publieke beschikbaarheid van grote

hoeveelheden persoonsgegevens, krachtige bigdata-algoritmes en rekenkracht zijn data die verondersteld waren anoniem te zijn, keer op keer toch herleidbaar tot personen gebleken.

Pseudonimiseren
Pseudonimiseren is het vervangen van de identificerende gegevens uit een bestand met een zogenaamd pseudoniem. De gepseudonimiseerde data worden los van de identificerende gegevens en bijbehorend pseudoniem beheerd. Pseudonimiseren is dus een privacybevorderende maatregel, namelijk door het beperken van de herleidbaarheid. Deze beperking van de herleidbaarheid is per definitie niet volledig, doordat de datasets in combinatie weer herleidbaar zijn naar personen. Daar komt bij dat gepseudonimiseerde bestanden in combinatie met andere bestanden kunnen worden verwerkt, waardoor de herleidbaarheid toeneemt.

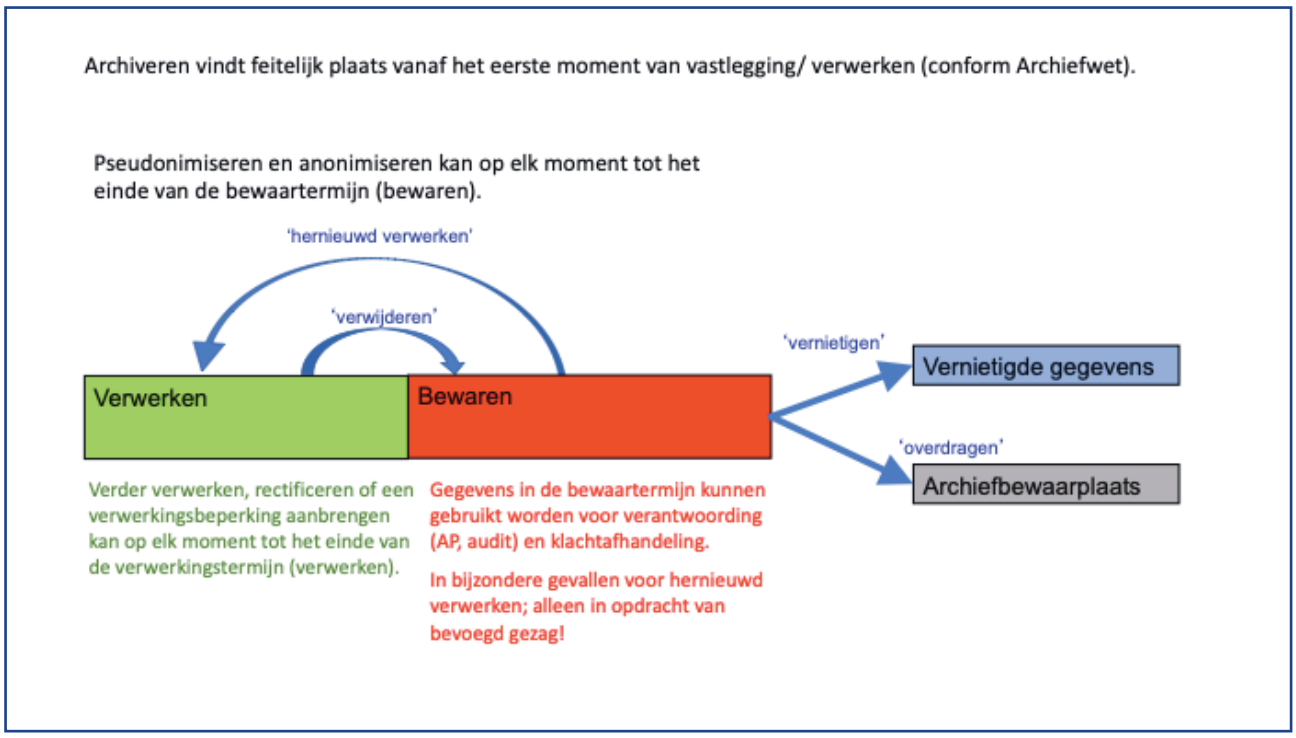
Verder Verwerken
De Wpg en de AVG kennen de term verder verwerken voor een verwerking van persoonsgegevens voor een ander doel dan het oorspronkelijke doel. Dit is bijvoorbeeld het geval als gegevens eerst een art. 8-label hebben en later een art.13-label krijgen.

Hernieuwd Verwerken
In de Wpg bestaat de mogelijkheid om onder specifieke voorwaarden reeds verwijderde politiegegevens beschikbaar te stellen voor operationele doeleinden.

Verwerkingsbeperking
De AVG en de Wpg bieden beide de mogelijkheid van verwerkingsbeperking. Dit gebeurt door opgeslagen gegevens te markeren met als doel de verwerking ervan in de toekomst te beperken, bijvoorbeeld omdat de juistheid daarvan door de betrokkene wordt betwist en deze geverifieerd moet worden. In de Wpg wordt dit ook aangeduid met het begrip afschermen. Naast de eerder genoemde betwiste (on)juistheid moet gedacht worden aan situaties waarbij vernietiging niet aan de orde kan zijn omdat de gegevens moeten worden bewaard als bewijsmateriaal. Het beperken van de verwerking geldt voor alle gebruikers. Als de toegang tot specifieke verwerkingen van bepaalde gegevens (inzien, wijzigen, etc.) voor bepaalde personen of groepen van personen wordt beperkt, wordt autorisatie toegepast. Hier kunnen overwegingen van bijvoorbeeld tactische aard of van veiligheid van betrokkenen aan ten grondslag liggen. Dit zijn dan echter geen beperkingen van de verwerking in de zin van de AVG of Wpg.

Rectificeren
De AVG en Wpg verstaan onder rectificeren het aanvullen van onjuiste of onvolledige gegevens met gegevens die wel juist of volledig zijn. Het resultaat daarvan zijn de gerectificeerde gegevens. Het effect van rectificeren is dus tweeledig: bij het opvragen van de actuele gegevens worden de gerectificeerde gegevens getoond en bij het opvragen van gegevens uit de periode vóór de rectificatie worden de oorspronkelijke gegevens getoond. Gegevens uit het verleden gaan dus niet verloren.

Overdragen
De Archiefwet schrijft voor dat overheidsinformatie die blijvend bewaard moet worden als onderdeel van cultureel erfgoed na twintig jaar moet worden overgedragen naar een archiefbewaarplaats. Het overdragen kan met goedkeuring van de minister van Cultuur worden opgeschort. Na het overdragen van de originele archiefbescheiden/informatie-objecten ligt het zorgdragerschap (eigendom) voor die archieven niet meer bij Natuurnetwerk maar bij de minister voor Cultuur. Overgedragen overheidsinformatie is niet meer op te vragen met een beroep op de Wob (Wet openbaarheid bestuur).



Figuur 1 Schematische weergave van begrippen rondom verwerkings- en bewaartermijnen

VOORBEELDEN VAN TOEPASSING IN BRS

Artikel 8: Deze gegevens mogen vijf jaar verwerkt worden:
Situatie: Een mutatie met 1 incident wordt op 1-1-2020 aangemaakt. Op 1-2-2020 wordt aan deze mutatie een incident toegevoegd. De mutatie (gemaakt op 1-1 en gewijzigd op 1-2) wordt 5 jaar na datum vastleggen eerste incident in deze mutatie verwijderd. Dat betekent dat beide incidenten daarmee verwijderd worden, inclusief de algemene tekst van de mutatie. Bij meerjarig onderzoek zijn deze gegeven op verzoek wel beschikbaar, want ze zijn nog niet vernietigd.

De veronderstelling hierbij is dat een mutatie met meerdere incidenten waarbij die incidenten langer dan een half jaar uit elkaar liggen, een typische art. 9-verwerking is, zoals een onderzoek naar een blaffende hond waar dan meerdere keren wordt gepost en opgetreden. In dat geval zal bij juist gebruik van het systeem en juiste labeling, deze mutatie als art. 9 worden gelabeld waardoor een andere verwijderingsmechanisme van toepassing wordt.

Artikel 9: Deze gegevens mogen tot een half jaar na een onherroepelijk vonnis, of zodra het doel van het onderzoek bereikt is, worden verwerkt

Situatie: Op 1-1-2020 wordt door de Boa aangegeven dat de mutatie is afgehandeld maar op 1-2-2020 worden een of meerdere data-elementen toch gewijzigd. De einddatum van de mutatie is 1-1-2020. Daarna is er nog 6 maanden tijd om gegevens over te hevelen/ te hergebruiken voor een ander onderzoek of verwerking. Daarna gaan ze de bewaartermijn in. 1-2-2020 is dus de eerste maand van deze 6-maandsperiode.

Artikel 13: De termijnen per data-element worden door de regiegroep vastgesteld. Wat gebeurt er met de termijnen nadat een of meerdere data-elementen worden gewijzigd of toegevoegd? In theorie kan een data-element zowel een art. 8 als 9 als 13-label hebben, maar in de praktijk is een mutatie 8 of 9 (als een boa en een BF dat aangeven). Is het 8, dan kan na 5 jaar een 13-label van toepassing blijken te zijn. Dan wordt een subset van data-elementen uit deze mutatie langer beschikbaar dan de verwerkingstermijn van 5 jaar uit art. 8.

Boa Registratie
systeem

info@boaregistratie.nl