

2. Definities en bedrijfsregels

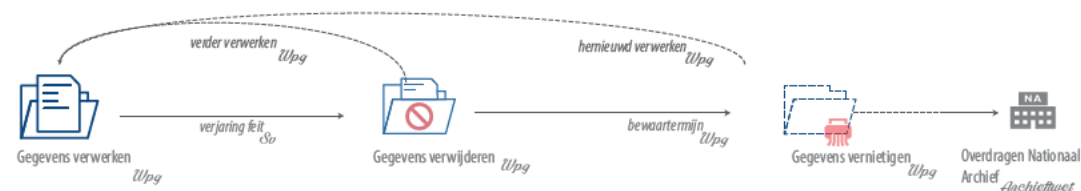
In het juridisch kader hierboven zijn wetten en bepalingen genoemd waarin de verplichting tot bewaren, verwijderen en vernietigen is vastgelegd. Om een praktische vertaling naar werkprocessen en applicaties te maken, gebruiken we bedrijfsregels. Daarvan zijn er al veel beschreven in het document Wpg Begrippen Definities Bedrijfsobjecten¹². De regels in dit document zijn daarop een toevoeging of aanscherping.

- De bedrijfsregels over ‘verwerken’ (3.1 tot 3.3) zijn bedoeld om technische invulling te geven aan de verschillende verwerkingen. Met andere woorden: wat doen we op applicatieniveau en gegevensbeheerniveau als we spreken over archiveren, verwerken, of bijvoorbeeld wissen?
- Bij de bedrijfsregels voor datamanagement (3.4) gaan we in op een aantal beheerprocessen zoals logging en het maken van backups. Om de

bewaartermijn van dit soort gegevens te weten moeten we eerst vaststellen onder welke bepalingen deze verwerkingen vallen;

- De bedrijfsregels over statussen van politieonderzoeken (3.5) ondersteunen die bepalingen in de wet waarin het ‘doel van een verwerking’ een rol speelt. Het doel van de verwerking is in veel gevallen het onderzoek, en afhankelijk van de status van dat onderzoek is het doel bereikt en gaat de termijn voor verwijderen en vernietigen lopen.

¹² Zie de agorasite van de sector GGB: <https://agora.portal.politie.local/sites/ggb/Termen%20en%20definities/Termen%20en%20definities.aspx>



FIGUUR: VERWERKEN VAN GEGEVENS: VERDER VERWERKEN, VERWIJDEREN, HERNIEUWD VERWERKEN, Vernietigen

2.1. Verwerken

De AVG en de Wpg hanteren vrijwel dezelfde definitie van het begrip verwerken. Het verwerken van gegevens omvat 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

2.1.1. Verder Verwerken (Wpg / AVG)

De Wpg en de AVG kennen de term **verder verwerken** voor een verwerking van persoonsgegevens voor een ander doel dan het oorspronkelijke doel.

2.1.2. Hernieuwd Verwerken (Wpg)

Het onder specifieke voorwaarden beschikbaar stellen aan de operatie van reeds verwijderde politiegegevens. Zie ook verwijderen.

2.1.3. Archiveren (Archiefwet)

Archiveren is het zorgdragen voor goed beheer van overheidsinformatie vanaf moment van ontvangst of creatie tot het moment van vernietiging of overbrenging. 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 bijvoorbeeld ook om databasegegevens, ingevulde formulieren, foto's, video's, websites en Tweets.

De activiteit ‘archiveren’ is dus dermate breed dat we liever spreken van (informatie)beheer als parallelle activiteit ter uitvoering van de Archiefwet.

Archiveren eindigt ook, zie hiervoor § 3.3.3 *Overdragen (Archiefwet)* hieronder.

2.2. Beperken van de verwerking

2.2.1. Verwijderen (Wpg)

Onder **verwijderen** verstaan we het buiten de operationele verwerking plaatsen van politiegegevens. Verwijderen is dus een privacybevorderende maatregel, namelijk door het beperken van de toegang. Verwijderde gegevens zijn nog wel beschikbaar, maar alleen voor functioneel beheerders en de zogenoemde poortwachter¹³ voor het doel van een artikel 9-verwerking of een artikel 10-verwerking. In dat geval spreken we van hernieuwd verwerken (§ 2.1.2 2.1.2)

2.2.2. Pseudonimiseren

Onder pseudonimiseren verstaan we 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 personen¹⁴. Bovendien kunnen gepseudonimiseerde bestanden in combinatie met andere bestanden worden verwerkt, zodat de herleidbaarheid weer toeneemt.

Er zijn ook vormen van pseudonimisering, zoals cryptografische hashing, waarbij de herleidbaarheid naar persoonsgegevens nihil mag worden verondersteld. Deze hashing dient te voldoen aan specifieke voorwaarden. De Rijksoverheid heeft een meer praktische handreiking pseudonimisering beschikbaar gesteld met instructies voor pseudonimisering

van persoonsgegevens.¹⁵

2.2.3. Verwerkingsbeperking (AVG en Wpg)

De AVG en de Wpg bieden beide de mogelijkheid van verwerkingsbeperking¹⁶, 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 dit geverifieerd moet worden.

In de Wpg wordt dit ook wel 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. De kaders voor het instellen van autorisaties voor het in beslotenheid verwerken van gegevens zijn uitgewerkt in het autorisatiebeleid¹⁷.

2.2.4. Rectificeren (AVG en Wpg)

Onder rectificeren verstaan we 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;
- Bij het opvragen van gegevens uit de periode vóór de rectificatie worden de oorspronkelijke gegevens getoond. Gegevens uit het verleden gaan dus niet verloren.

2.3. Beëindigen van de verwerking

2.3.1. Vernietigen (Wpg) en Wissen (AVG)

Onder vernietigen verstaan we het onherstelbaar wissen van persoonsgegevens. In de AVG wordt het begrip wissen gehanteerd, in de Wpg wordt het begrip vernietigen aangehouden. Wissen en vernietigen hebben totale werking, ook naar registraties in het verleden. (Vergelijk rectificatie hierboven).

Voor de technische invulling van vernietigen c.q. wissen wordt aangesloten bij de procedure Noodvernietiging fysieke en digitaal. Daarin wordt het begrip praktisch ingevuld als het 'zodanig verminken van de informatiedragers (...) dat de vastgelegde content niet meer de toegankelijk en beschikbaar is. Uitgangspunt vormen daarbij de normen voor vernietiging van gerubriceerde informatie zoals vastgelegd in de DIN 66399 (2012-10).'

13 De functionaris die namens de operatie beoordeelt of aan specifieke voorwaarden is voldaan om de gegevens opnieuw beschikbaar te stellen

14 Zie ook "2.2.3. Verwerkingsbeperking (AVG en Wpg)" op page 12

15 <https://www.rijksoverheid.nl/documenten/richtlijnen/2018/02/15/stroomschema-pseudonimisering-avg>

16 Artikel 18 van de AVG en artikel 28 van de Wpg

17 Agora, autorisatiebeleid politie 2016 – 2020 ([link](#))



2.3.2. Anonimiseren

Onder anonimiseren verstaan we 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 big data algoritmes en rekenkracht zijn data die verondersteld waren anoniem te zijn, keer op keer toch herleidbaar tot personen gebleken.

2.3.3. Overdragen (Archiefwet)

Overheidsinformatie die blijvend bewaard moet worden als onderdeel van cultureel erfgoed moet na twintig jaar¹⁸ 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 wijzigt;

- Ligt het zorgdragerschap (eigendom) voor die archieven niet meer bij Politie maar bij de minister voor Cultuur. (OCW)
- Het regime voor openbaarheid van de Wet openbaarheid bestuur (de Wob) in de Archiefwet. Overgedragen overheidsinformatie is dus niet meer op te vragen met een beroep op de Wob.

De zorgdrager kan voor een bepaalde termijn beperkingen aan de openbaarheid stellen, om redenen van privacy of veiligheid van de staat, zijn bondgenoten, of ter voorkoming van onevenredige benadeling of bevoordeling van betrokkenen of derden. Redenen die bij politiekegevens vaak aan de orde zullen zijn.

Na het overdragen moeten de duplicaten of werkkopieën van de overgebrachte archiefbescheiden worden vernietigd¹⁹.

18 Er is een aanpassing van de Archief wet voorzien waarin deze termijn van 20 jaar wordt teruggebracht naar 10 jaar

19 Bron: <https://www.nationaalarchief.nl/archiveren/kennisbank/overbrenging>



2.4. Bedrijfsregels datamanagement

2.3.4. Vervreemding (Archiefwet)

Vervreemding is de overdracht van eigendom door de zorgdrager van het archief aan een andere zorgdrager of een natuurlijk of rechtspersoon van archiefbescheiden. Hiervoor is toestemming nodig van de Minister van Cultuur (OCW).²⁰

Onder overdracht verstaan we de faseverandering van dynamisch archief (waarbij de lijn verantwoordelijk is voor het beheer) naar semi-statisch archief (waarin DIV het beheer overneemt).

In bepaalde gevallen is overbrenging naar het rijksarchief aan de orde, in plaats van vernietigen (Wpg) of wissen (AVG). Dat is bij informatie die van waarde is als bestanddeel van cultureel erfgoed of voor historische onderzoek.

2.4.1. Productiedata voor testen en opleiden

Bij het verwerken van productiedata voor testen en opleiden worden gegevens uit een geautomatiseerd systeem gedupliceerd met als doel deze in een testomgeving²¹ te gebruiken voor het testen van een geautomatiseerd systeem of gebruik in een opleidingsomgeving.

De testdata en opleidingsdata zijn een 'afslag' (duplicaat) van productiedata en worden eventueel nabewerkt om geschikt te zijn voor specifieke toepassing. De gegevens worden van het moment van de afslag niet meer actueel gehouden; verwerkingen op het productiesysteem worden niet uitgevoerd op deze gedupliceerde gegevens. De verwerking van productiedata voor testen en opleiden valt onder de AVG, voor zover het persoonsgegevens betreffen.

Verwerken van productiedata voor testen en opleiden onder de AVG is wegens de gevoeligheid alleen mogelijk met instemming (onthefing) van de dienst IM²². Het is ook mogelijk data voor testen en opleiden uit willekeurige gegevens op te bouwen, of op basis van geanonimiseerde productiedata (zie 2.3.2 2.3.2). In dat geval valt de verwerking niet onder de AVG of Wpg. De bewaartermijn dient door de verwerkingsverantwoordelijke te worden vastgesteld.

21 OTAP, omgeving voor ontwikkelen, testen, acceptatie en in productie brengen

22 Hoofd GGB namens deze, zoals besproken in afstemmingsoverleg DirIV, IM en ICT 16 oktober 2019



2.4.2. Trainingsdata voor slimme algoritmen (Wpg)

Bij het verwerken van politiegegevens voor het trainen van slimme algoritmen worden politiegegevens uit een geautomatiseerd systeem gedupliceerd met als doel de routines van een geautomatiseerd systeem (door te) ontwikkelen. Ook hier worden de gegevens vanaf het moment van dupliceren niet meer actueel gehouden. Net als bij productiedata voor testen en opleiden is het trainen van slimme algoritmes met trainingsdata een verwerking onder de AVG. De bewaartermijn dient door de verwerkingsverantwoordelijke te worden vastgesteld.

2.4.3. Gegevensbackup

Het maken van een (gegevens-) backup is het regelmatig²³ dupliceren van (persoons)gegevens, met als doel de beschikbaarheid ervan te borgen en te bevorderen. Die beschikbaarheid kan worden bedreigd door bijvoorbeeld een calamiteit (brand, water, diefstal) maar ook door onzorgvuldige of moedwillig onjuiste bewerking. De back-up is door tussenkomst van een applicatiebeheerder beschikbaar voor de eindgebruiker.

Het maken van een backup dient dus hetzelfde doel als de oorspronkelijke verwerking onder de AVG of de Wpg. De bewaartermijn van de oorspronkelijke verwerking loopt in feite door in de backup.

23 De frequentie van het maken van een back-up is doorgaans een aantal maal per dag tot elke maand, maar andere frequenties zijn niet ongewoon

2.4.4. Redundante gegevensopslag

Een redundante gegevensopslag is een duplicaat van (persoons)gegevens dat voortdurend²⁴ gelijk (synchroon) wordt gehouden met de oorspronkelijke gegevens. Elke verwerking van het gegeven wordt zonder tussenkomst van de gebruiker ook uitgevoerd op de duplicaten, waarmee de gebruiker ervaart dat het gegeven maar één keer in het geautomatiseerde systeem voorkomt. Bij bijvoorbeeld beperkte bandbreedte of beperkte toegang tot gegevensdragers neemt daarmee de gemiddelde beschikbaar of de betrouwbaarheid van het systeem toe.

Het doel van de redundante opslag is dus beschikbaarheid of betrouwbaarheid van de dienstverlening. De verwerking van persoonsgegevens in een configuratie met redundante opslag heeft directe werking op alle duplicaten in de opslag en is dus een verwerking voor het oorspronkelijke doel. De bewaartermijn is daarmee die van de oorspronkelijke verwerking.

24 De frequentie van synchronisatie van gegevens en redundante opslag varieert van milliseconden tot een dag, maar andere frequenties zijn niet ongewoon.

2.4.5. Logging

Logging is het registreren van verwerkingen van gegevens in een geautomatiseerd systeem. De Wpg stelt logging verplicht voor bepaalde verwerkingen op persoonsgegevens, als één van de maatregelen;

- om de rechtmatigheid van de verwerking van persoonsgegevens te waarborgen
- voor het uitvoeren van interne controles
- ter waarborging van de integriteit en de beveiliging van de politiegegevens
- voor strafrechtelijke procedures.

De AVG stelt logging niet verplicht. De verwerking van logginggegevens heeft tot doel om de redenen voor handelingen als raadplegen, wijzigen etc. (op basis van de Wpg of AVG) te kunnen vaststellen. De loggingsgegevens zelf zijn daarmee persoonsgegevens in de zin van de AVG, indien de gegevens tot personen herleidbaar zijn. De verplichting tot logging, evenals de bewaartermijn van loggingsgegevens, is voor de politie uitgewerkt in het beleidskader logging²⁵.

2.4.6. Documentatie

Documentatie is het schriftelijk vastleggen van bepaalde gegevensverwerkingen met als doel daar verantwoording over af te kunnen leggen. De Wpg kent een documentatieplicht²⁶ tot vastleggen van de volgende gegevens;

- de doelen van onderzoeken bedoeld in artikel 9, lid 2 Wpg
- de verstrekking of doorgifte van politiegegevens;
- de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing op een verzoek in het kader van rechten van betrokkene;
- een inbreuk op de beveiliging van persoonsgegevens, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.

De privacyfunctionaris kan aan de hand van deze gegevens toezicht houden. Deze gegevens zijn gegevens in de zin van de Wpg en moeten bewaard blijven tot ten minste de datum waarop de laatste controle/audit heeft plaatsgevonden.²⁷

25 Agora; Beleidskader logging ([link](#))

26 Artikel 32 lid 1 Wpg

27 Artikel 32, lid 4 Wpg



2.5. Bedrijfsregels politieonderzoeken (artikel 9 Wpg)

Termijnen voor het verwerken van gegevens hebben een startmoment in het operationele proces. Deze momenten zijn te vinden in de bedrijfsregels rondom de start en eventuele verjaring van een delict en van het openen en sluiten van onderzoeken. In dit beleid op bewaartermijnen worden volledigheidshalve de relevante bedrijfsregels toegelicht²⁸.

2.5.1. Pleegdatum / datum feit

Datum waarop het vermeende feit volgens het PV is gepleegd. De termijn voor verjaring van het feit start in beginsel een dag na de pleegdatum.²⁹ De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval eindigt bij verjaring³⁰.

2.5.2. Voltooid onderzoek

Een onderzoek is voltooid als het operationele politie onderzoek is afgesloten, het onderzoeksdoel is behaald en de dossiers van alle verdachten, inclusief dat van de intellectuele dader, zijn overgedragen aan het OM. Het voortduren van de grond voor de verwerking is nader uitgewerkt in par 4.4 (Politiegegevens voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9)) op pagina 23.

28 Voor de statussen van artikel 9 onderzoeken wordt verwezen naar het document Beëindigen artikel9 onderzoeken (versie 26.06.2018) van de werkgroep Summit.
29 Let op: in artikel 71 Sr worden enkele uitzonderingen genoemd waarbij de termijn op een ander moment start.
30 Zie voor de verjaringstermijnen paragraaf 3.4.1 Verwijderen op pagina 22 e.v.

2.5.3. Gestaakt onderzoek

Beëindigd onderzoek omdat zich geen strafbaar feit heeft voorgedaan. De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval eindigt.

2.5.4. Opgeschort onderzoek

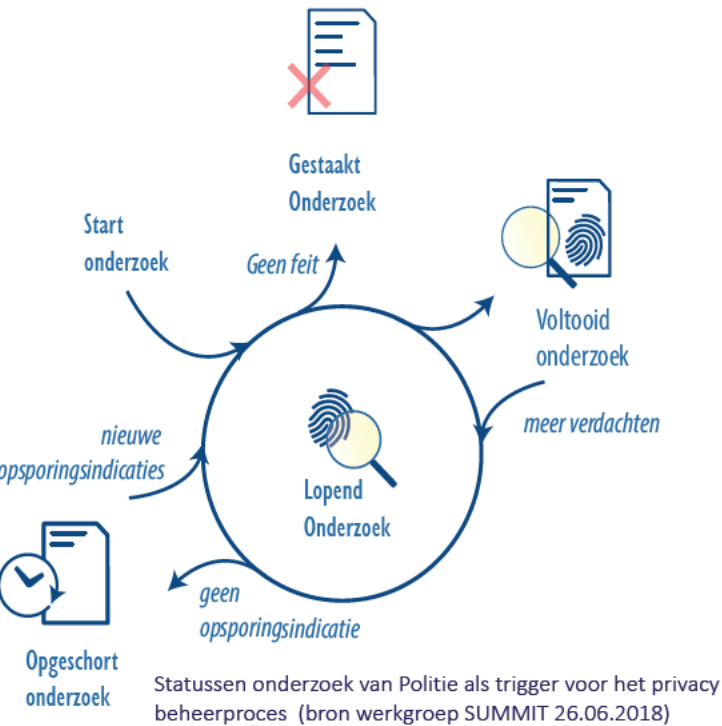
Onderzoek waarbij het onderzoeksdoel niet (volledig) is behaald. Niet alles is ingezonden en het betreft geen cold case. De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval blijft bestaan.

2.5.5. Cold case

Een opgeschort (of lopend) onderzoek dat door het bevoegd gezag de status cold case heeft gekregen. De grond voor verwerking voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval blijft bestaan.

2.5.6. Overzicht

Schematisch zien de statussen onderzoek en de relatie met het beheerproces er als volgt uit;



3. Bewaartermijnen

3.1. Overheidsinformatie (Archiefwet)

De Archiefwet verplicht de politie om overheidsinformatie in goede, geordende en toegankelijk staat te brengen en te bewaren. Dat geldt voor alle informatie, ook voor persoons- en politiegegevens. Van vernietiging³¹ wordt daarom afgezien als de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden na 20 jaar overgebracht naar een archiefbewaarplaats. Daarbij worden beperkingen aan de openbaarheid gesteld en zijn de gegevens niet meer (zonder vordering) voor operationele doeleinden beschikbaar.

De politie heeft een selectielijst³² opgesteld aan de hand waarvan wordt bepaald welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven. De vernietigingstermijnen van politiegegevens komen in de selectielijst overeen met bewaartermijnen uit de Wpg en Sv. Daarmee is geborgd dat we met de uitvoering van het selectiebeleid zowel de Archiefwet uitvoeren, als de Wpg.

De bewaartermijnen voor overige gegevens vinden hun grondslag in van toepassing zijnde wetgeving, bijvoorbeeld fiscaal recht, of op basis van belangenafweging (belang van de bescherming van de persoonlijke levenssfeer versus belang taakuitvoering, belang voor verantwoording, belang cultureel erfgoed etc.).

De plicht tot het bewaren van persoonsgegevens op basis van de Archiefwet 1995 is een andere dan het bewaren van persoonsgegevens voor eigen verwerkingsdoeleinden. De verwerkingsverantwoordelijke komt pas aan de plichten van de Archiefwet 1995 toe, wanneer de gegevens reeds in overeenstemming met de AVG worden verwerkt (zie onder IV. en de uitspraak van de Raad van State 23 augustus 2017 onder V).

31 Artikel 14, lid 1 Wpg.
32 De selectielijst staat op agora [\(link\)](#)

3.2. Bedrijfsvoeringsgegevens (AVG)

De AVG verplicht de verwerkingsverantwoordelijken na te gaan of ze gehouden zijn aan wettelijke vastgestelde termijnen. Wanneer er geen wettelijk vastgestelde termijn is, dient de verwerkingsverantwoordelijke de termijn zelf vast te stellen. Daarbij bieden de vragen die gesteld worden bij een GEB goede aanknopingspunten voor een zorgvuldige motivering van de bewaartermijnen. Daarnaast is door het ministerie van J&V een stappenplan voor het beschrijven van bewaartermijnen opgesteld.³³

3.2.1. Bewaartermijn bij wet voorgeschreven

Bekijk welke wetgeving op de gegevensverwerking van toepassing is, en of er bij of krachtens die betreffende wet een bewaartermijn is vastgesteld.

Voor fiscale gegevens is de bewaarplicht bijvoorbeeld op 7 jaar vastgesteld³⁴ en voor medische gegevens in principe 15 jaar³⁵.

3.2.2. Verwerkingsverantwoordelijke bepaalt bewaartermijn

Indien er geen wettelijke bewaartermijn voor de gegevensverwerking is vastgesteld, dan moet de verwerkingsverantwoordelijke de bewaartermijn bepalen. Dit kan aan de hand van de vragen in het schema op de volgende pagina.

33 2 november 2018 | Bewaartermijn persoonsgegevens in de AVG, F. Makhloufi V.D.W. van Dijk, Justid (voorbeelden aangepast)
34 artikel 52, lid 4, Awr
35 artikel 7:454 BW

- 1 artikel 5 lid 1 onderdeel b AVG
- 2 Zie verder artikel 32 AVG
- 3 artikel 5 lid 1 sub c AVG: minimale gegevensverwerking

BRON: JUSTID- BEWAARTERMIJN PERSOONSgegevens IN DE AVG [35]

3.3. Politiegegevens voor uitvoering van de dagelijkse politietaak (artikel 8)

Voor politiegegevens die worden verwerkt bij de uitvoering van de dagelijkse politietaak zijn termijnen voor verwijdering en vernietiging in artikel 8 van de Wpg bepaald. Het gaat om gegevens die worden verwerkt in het kader van de basispolitiezorg. De werkzaamheden bestaan uit surveillance, afhandeling van verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels. Onder eenvoudige recherchewerkzaamheden wordt verstaan het onderzoeken van diefstallen en inbraken, het veilig stellen van sporen en het opnemen van een aangifte van een inbraak (VVC-zaken). Eerste hulp wordt bijvoorbeeld verleend als een persoon met een psychose op straat rondzwervt. In het kader van het handhaven van wetten en regels wordt bijvoorbeeld de algemene plaatselijke verordening gehandhaafd en de Wet op de economische delicten, waarin overtreding van bepalingen uit onder meer milieuwetten strafbaar zijn gesteld.

In geval van VVC-zaken bepaalt de politie (al dan niet in afstemming met OM) of een zaak wordt opgepakt en beslist (al dan niet in afstemming met OM) over vroegtijdig beëindigen van een zaak zonder geïdentificeerde verdachte. Het OM geeft een kader voor het oppakken en beëindigen en beslist over vervolging en sepot (bij zaak met geïdentificeerde verdachte).³⁶

Uitgangspunt is dat gegevens voor elke geautoriseerde vijf jaar beschikbaar zijn. De toegang beperken tot gegevens ouder dan één jaar wordt alleen rol-gebaseerd gedaan voor landelijk vastgestelde gebruikersgroepen. Vooralsnog zijn er geen groepen geselecteerd. Verwijderen

In ieder geval vijf jaar na de datum van de eerste verwerking (artikel 8, lid 6 Wpg).

3.3.1. Vernietigen

- Zodra ze 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, lid 1 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 cameratoezicht³⁷ 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.

36 Aanwijzing voor de opsporing

37 Artikel 151c, lid 9 Gemeentewet

3.4. Politiegegevens voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9)

Voor politiegegevens die worden verwerkt voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval zijn termijnen voor verwijdering en vernietiging in artikel 9 van de Wpg bepaald.

Dat is het geval wanneer extra inspanningen worden geleverd om gericht omvangrijke hoeveelheden gegevens te vergaren ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval. De term 'gericht' heeft betrekking op de verwerking van grote hoeveelheden gegevens met betrekking tot bepaalde personen. Behalve in geval van opsporingsonderzoeken zal dit ook het geval zijn bij gegevens die worden verwerkt in het kader van een veelplegerdossier of een Staf Grootchalig Bijzonder Optreden (SGBBO), zoals grote demonstraties, ontruimingen, Koningsdag, de Sinterklaasintocht en andere grootschalige evenementen. Er is in elk geval sprake van gerichte verwerking in de zin van artikel 9 zodra een rechercheonderzoek is aangemeld, een verkennend onderzoek wordt gestart en zodra bijzondere opsporingsmethoden worden ingezet, zoals stelselmatige observatie en het af luisteren van telecommunicatie. In zulke gevallen gaat het immers om een omvangrijke gegevensverwerking over personen, ten aanzien van wie de precieze betrokkenheid bij de te onderzoeken strafbare feiten nog niet vast staat.



3.4.1. Verwijderen

- Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van het onderzoek;
- Of na verloop van een periode van maximaal een half jaar waarin ze verwerkt worden teneinde te bezien of ze aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 (artikel 9, lid 4 Wpg).

In geval van HIC/ondermijnende criminaliteit gaat de politie over tot een opsporingsonderzoek. Het OM heeft het gezag over de opsporing. Het OM beslist over duur en wijze van de opsporing en (mogelijke) beëindiging van de opsporing, in samenspraak met de politie. Tevens beslist het OM over al dan niet vervolging van de geïdentificeerde verdachte.³⁸

De Justitiële Informatiedienst (JustID) verstrekt aan de politie gegevens over door het OM genomen vervolgingsbeslissingen, uitspraken door de strafrechter en gegevens over de tenuitvoerlegging van straffen en maatregelen (ook wel afloopberichten). Deze gegevens worden verstrekt

38 Aanwijzing voor de opsporing

zodat beoordeeld kan worden of gegevens op grond van artikel 9, lid 4 Wpg verwijderd moeten worden³⁹. In dat kader worden de volgende gegevens verstrekt:

- het parketnummer;

en indien het feit is geseponneerd:

- de datum van de beslissing;
- de sepotcode en de bijkomende sepotgrond of sepotgronden;
- de bij de beslissing tot voorwaardelijk seponeren gestelde voorwaarden;
- de datum waarop aan alle gestelde voorwaarden is voldaan;

indien over het feit bij strafbeschikking is beslist;

- de datum waarop de strafbeschikking volledig ten uitvoer is gelegd⁴²;

indien een voorlopige maatregel op grond van de Wet op de economische delicten is opgelegd:

- de aanduiding van de voorlopige maatregel;
- de beëindiging, verlenging, wijziging, intrekking of opheffing;
- indien over het feit bij rechterlijke uitspraak is beslist; de inhoud van de uitspraak, waaronder de kwalificatie van het feit en de daarbij betrokken strafbepalingen⁴⁰;

indien de rechterlijke beslissing ten uitvoer is gelegd;

- de datum en de wijze waarop de tenuitvoerlegging is beëindigd;
- de datum en de wijze waarop de taakstraf of vrijheidsstraf is aangevangen en beëindigd;

indien de volledige tenuitvoerlegging niet is gerealiseerd, de datum van tenuitvoerlegging van de vervangende straf.

Doorgaans is het doel van het onderzoek gerealiseerd wanneer alle daders van het strafbare feit zijn opgespoord en vervolgd en de door de rechter opgelegde straf of maatregel daadwerkelijk geheel ten uitvoer is gelegd. Zodra voor alle ingezonden verdachten één van de afloopberichten is ontvangen, bepaalt de bevoegd functionaris of het doel is bereikt. Daarnaast zijn er ook andere omstandigheden die leiden tot verwijdering:

- verdachte-veroordeelde is overleden;
- het dossier wordt in overleg met OvJ/hopper opgelegd en de verjaringstermijn is verstreken.

39 Artikel 11b Besluit justitiële en strafvorderlijke gegevens

40 Aanvullend aan de gegevensleveringen die in het besluit zijn bepaald, zijn er afspraken met Justid en OM over het ontvangen van afloopberichten met de datum waarop de uitspraak onherroepelijk is geworden.