Beleid

Bewaartermijnen

GEGEVENS AUTORITEIT

VASTGESTELD document

Inleiding

Bij het uitvoeren van de politietaak en in onze bedrijfsvoering verwerken we gegevens van collega's, verdachten en andere betrokkenen. Deze inbreuk op privacy is onvermijdelijk. Zolang het voor de politietaak of de bedrijfsvoering noodzakelijk is, mogen we deze gegevens verwerken en omgekeerd geldt dus ook; als de noodzaak er niet meer is, stopt de verwerking.

Het zorgvuldig verwijderen en vernietigen van gegevens is dus de uitkomst van een afweging tussen het kunnen uitvoeren van de politietaak en de bedrijfsvoering enerzijds en het borgen van de privacy van collega's, verdachten en andere betrokkenen anderzijds.

Het Uitvoeringskader Privacy & Security by Design (PSbD) beschrijft alle kaders voor de zorgvuldige omgang met gegevens door de politie. Zowel bij het uitvoeren van de politietaak als bij de bedrijfsvoering. Het uitvoeringskader bestaat uit twaalf principes. Principe 8 gaat specifiek over bewaartermijnen:

Gegevens worden niet langer verwerkt dan is toegestaan en worden vernietigd zodra ze niet langer noodzakelijk zijn.

In PSbD wordt toegelicht wat hiermee wordt bedoeld (de rationale);

"De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden. Voor de termijn waarbinnen de gegevens bewaard moeten worden, moet de informatievoorziening waarborgen treffen voor duurzame beschikbaarheid en toegankelijkheid. Deze waarborgen worden uitgewerkt in het Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO). De 'spelregels' voor gegevensbeheer zijn vastgelegd in de Beheerregeling Documentaire Informatie Politie 2017 en de termijnen voor bewaren en vernietigen zijn verzameld in de Generieke Selectielijst voor de Nationale Politie (concept)."[1]

1 Zie p. 61 van het Uitvoeringskader Privacy & Security by Design, versie 2.0

Het principe voor verwijderen en vernietigen van gegevens is dus vrij eenvoudig.

Maar de uitwerking is minder eenvoudig. Zo stelt de Archiefwet 1995 eisen aan de bewaartermijn van overheidsinformatie, maar stellen de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG) eisen aan de termijn van verwijderen en vernietigen van persoonsgegevens. Ook het Wetboek van Strafvordering (Sv) stelt beperkingen bij het verwerken van specifieke politiegegevens.

Om gegevens tijdig te verwijderen en vernietigen moeten we al deze wetten in samenhang overzien. Daarbij zijn veel van de bepalingen 'open' geformuleerd, wat betekent dat we als politie zelf concrete invulling moeten geven aan de bewaartermijn. Dat geeft wat vrijheid maar ook de verantwoordelijkheid het beleid op bewaartermijnen helder op te schrijven en goed te motiveren.

Die verantwoordelijkheid houdt ook in, dat we de politieke realiteit niet uit het oog verliezen bij het daadwerkelijk uitvoeren van dit beleid. Zo heeft de minister van J&V in reactie op de motie van TK lid van Oosten[2] toegezegd cold case informatie vooralsnog niet te vernietigen[3]. Dat houdt voorlopig in dat bepaalde gegevens ook na de bewaartermijn niet worden vernietigd. Voor een analyse van dit besluit en de consequenties verwijzen we naar de Gegevensautoriteit binnen directie IV van politie.

2 kst-35000-VI-37

3 brief van de minister aan de TK in reactie op de moetie van Oosten, kst-29628-859

Doel en doelgroep

In dit beleidskader werken we principe 8 – Bewaren en vernietigen- verder uit. Bijvoorbeeld wordt concreet wanneer termijnen voor verwijderen en vernietigen voor verschillende gegevenssoorten starten en hoe lang ze zijn. We gaan ook in op de begrippen zelf; wat bedoelen we precies met verwerken, wat doen we op systeemniveau als we gegevens verwijderen en wat als we gegevens vernietigen? Door dit uit te werken, stellen we de doelgroep hopelijk in staat de relevante wetsbepalingen, bedrijfsregels, begrippen en bewaartermijnen in samenhang te bezien zodat bij de implementatie daarvan juiste keuzes worden gemaakt. Bijvoorbeeld door grenzen aan gegevensverwerking te stellen in een project of programma. Maar ook indirect, door de bepalingen te vertalen naar requirements voor ontwikkeling van een applicatie of werkproces

Waar dit mogelijk is, verwijzen we naar relevante bestaande kaders, richtlijnen, procedures en werkinstructies.

In het algemene Privacybeleid van de politie zijn wettelijke verplichtingen uitgewerkt in normen. Dit beleidskader moet worden aangemerkt als specifiek beleid ten aanzien van het bewaren van bewaren van persoonsgegevens[1].

Dit document is bedoeld voor:

- Adviseurs op het gebied van (informationele) privacy, waaronder privacyfunctionarissen.
- Programma –en projectmanagers, Senior Business-experts, Product owners en andere betrokkenen bij de ontwikkeling van processen en systemen waarin persoonsgegevens worden verwerkt.
- Functioneel beheerders en andere experts die betrokken zijn bij de inrichting van systemen.
- Lijnmanagers die sturing geven aan de inachtneming van de bewaartermijnen

Beleid

Bewaartermijnen

Inhoud

Hoofdstuk 1: Overzicht van wet- en regelgeving die kaderstellend is voor het bewaren van persoonsgegevens.

Hoofdstuk 2: Begrippen en uit de politiepraktijk waarin we uitleggen wat we met gebruikte termen bedoelen en hoe dit vertaald moet worden naar proces- en systeemontwerp.

Hoofdstuk 3: Concrete bewaartermijnen per categorie van politiegegevens, een afwegingskader voor bewaartermijnen van persoonsgegevens en enkele veelgevraagde beleidsuitspraken over bewaartermijnen.

1. Juridisch kader

In de basis mogen persoonsgegevens niet langer worden verwerkt dan noodzakelijk is voor het doel van de verwerking. De AVG en de Wpg geven echter op een verschillende manier invulling aan dit principe.

In dit hoofdstuk wordt eerst weergegeven met welke aspecten van de AVG rekening moet worden gehouden. Daarna wordt uitgebreider ingegaan op het juridisch kader met betrekking tot het verwijderen en vernietigen van politiegegevens. Dit kader wordt gevormd door verschillende wettelijke bepalingen en uitvoeringsregelingen. Deze hebben enerzijds tot doel de politie te laten beschikken over de persoonsgegevens die nodig zijn voor een goede bedrijfsvoering en uitvoering van de politietaak en anderzijds de persoonlijke levenssfeer van de burger in verband met het vastleggen en verstrekken van persoonsgegevens te beschermen.

Daar waar duiding wordt gegeven aan onderdelen van de AVG, of aan aspe cten die voor zowel de AVG als de Wpg relevant zijn, gebruiken we het begrip ‘persoonsgegeven(s)’. Als specifiek wordt ingegaan op elementen uit de Wpg dan hebben we het over ‘politiegegeven(s)’.

1.1. Algemene Verordening Gegevensbescherming

In de AVG is bepaald hoe de politie moet omgaan met persoonsgegevens. Algemene uitgangspunten daarbij zijn:

- Persoonsgegevens moeten worden bewaard zodanig dat de betrokkene niet langer is te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt
- Persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wo rden verwerkt
- De verwerkingsverantwoordelijke informeert de betrokkene over de periode gedurende welke de gegevens worden opgeslagen of (tenminste) over de criteria ter bepaling van die bewaarter mijn. Organisaties bepalen dus zelf hoe lang zij persoonsgegevens verwerken, rekening houdend met het doel van de verwerking. Daarbij kunnen bewaartermijnen uit meer specifieke wet- en regelgeving overigens leidend zijn, zoals bijvoorbeeld de belastingwetgeving
- Ook hebben betrokkenen het recht op gegevenswissing, bijvoorbeeld wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of de betrokkene zijn of haar toestemming intrekt.

Voor zover persoonsgegevens binnen de politieorganisatie worden verwerkt op grond van de AVG, vooral in de bedrijfsvoering en als het gaat om vreemdelingenzaken en de korpscheftaken, moet dus voorafgaand aan de verwerking bepaald worden binnen welke beoogde termijn de gegevens worden gewist. De verantwoordelijke bepaalt en motiveert de bewaartermijn en dit moet vervolgens zijn beslag krijgen in applicaties en werkprocessen. Daarnaast speelt het onderwerp bewaartermijnen, in het kader van transparantie en verantwoording, een belangrijk rol in het privacystatement (actieve informatieplicht), bij het verwerkingsregister en desgevraagd bij verzoeken om inzage of wissing.

1.2. Wet en Besluit politiegegevens

In de Wpg en het Besluit politiegegevens (Bpg) is bepaald hoe de politie moet omgaan met politiegegevens. Algemene uitgangspunten daarbij zijn:

- Politiegegevens worden slechts verwerkt voor zover ze noodzakelijk zijn voor in de Wpg beschreven doeleinden.
- Politiegegevens worden uitsluitend voor een ander doel verwerkt voor zover de Wpg daar uitdrukkelijk in voorziet, de verwerking niet onverenigbaar is met het doel waarvoor ze zijn verkregen en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.
- De nodige maatregelen worden getroffen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.

Ter invulling van het eerste uitgangspunt zijn in de Wpg de volgende doelen voor de verwerking van politiegegevens bepaald:

- Politiegegevens voor uitvoering van de dagelijkse politietaak (artikel 8);
- Politiegegevens voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9);
- Politiegegevens voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10);
- Politiegegevens voor controle en beheer van informanten (artikel 12), en
- Politiegegevens voor ondersteunende taken (artikel 13).

Het doel is dus bepalend voor de wijze waarop politiegegevens mogen worden gebruikt en onder welke voorwaarden en op welk moment de gegevens verwijderd of direct vernietigd moeten worden. Deze termijnen worden bepaald in de hierboven genoemde wetsartikelen en staan ook in hoofdstuk 4 (Bewaartermijnen) van dit document genoemd.

In het algemeen geldt dat gedurende de gehele verwerkingsperiode beoordeeld moet worden of de gegevens voor een andere doel verder verwerkt kunnen worden.

1.3. Wetboek van Strafrecht (Sr)

De Wpg stelt dus belangrijke voorwaarden aan het verwerken van politiegegevens, maar staat die verwerking toe zolang er een verwerkingsgrond bestaat. Om te kunnen bepalen of dit nog het geval is, moet ook naar het Wetboek van Strafrecht (Sr) gekeken worden. Politiegegevens kunnen immers nog noodzakelijk zijn totdat de onderliggende zaak onherroepelijk is geworden. Als de zaak niet is opgelost en ook niet is ingezonden naar het OM, dan wordt het onderzoek weliswaar voortgezet, maar vaak op een minder intensief niveau. De gegevens moeten beschikbaar blijven voor het geval er nieuwe aanknopingspunten zijn. Verwerking van de politiegegevens blijft dan noodzakelijk tot uiterlijk het moment dat de feiten waarop het onderzoek zich richt verjaard zijn. De verjaringstermijnen zijn beschreven in artikel 70 Sr.

1.4. Wetboek van Strafvordering (Sv)

Zoals vermeld moeten politiegegevens worden verwijderd of vernietigd zodra dit door enige wettelijke bepaling wordt vereist[2]. Dergelijke bepalingen zijn onder andere te vinden in Sv in het kader van bijzondere opsporingsbevoegdheden.

Zo worden termijnen gesteld in verband met de bewaring en vernietiging van processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door bijvoorbeeld het opnemen van vertrouwelijke communicatie (tappen) of de vordering van telecommunicatiegegevens, voor zover die niet bij de processtukken zijn gevoegd[3]. Maar ook ten aanzien van processen-verbaal of andere voorwerpen die mededelingen van geheimhouders bevatten[4] en ten aanzien van gegevens die zijn vastgelegd tijdens een doorzoeking en die van geen betekenis zijn voor het onderzoek[5].

Hier wordt dus een belangrijke beperking gesteld aan het verwerken van politiegegevens gedurende het onderzoek. Gegevens die niet (meer) nodig zijn voor dat onderzoek moeten eerder worden vernietigd.

Ook in het kader van de identiteitsvaststelling van verdachten, veroordeelden en getuigen, het bewaren van kentekengegevens en het bewaren van auditieve en audiovisuele registraties worden specifieke bewaartermijnen gesteld.

2 artikel 4, lid 2 Wpg
3 artikel 126cc en artikel 126dd Sv
4 artikel 126aa Sv
5 artikel 126nn Sv

1.4.1. Besluit bewaren en vernietigen niet-gevoegde stukken

In dit besluit worden nadere voorschriften gegeven omtrent de wijze waarop de processen-verbaal en andere voorwerpen[6] worden bewaard en vernietigd. Zo dient de officier van justitie een bevel tot vernietiging af te geven en wordt uiteengezet wat onder ‘vernietiging’ wordt verstaan.

1.4.2. Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen

Om er zeker van te zijn dat een verdachte is wie hij zegt te zijn, moet de opsporingsambtenaar de identiteit van de verdachte vaststellen[7]. De foto’s en vingerafdrukken worden weliswaar afgenomen in het kader van de uitvoering van de politietaak en vallen daarmee onder de werking van de Wpg, maar voor wat betreft de verdere verwerking van die gegevens, zoals de bewaartermijnen, is Sv[8] en het Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen leidend.

1.4.3. Besluit tot vaststelling van nadere regels voor het vastleggen en bewaren van kentekengegevens op grond van artikel 126jj van het Wetboek van Strafvordering door de politie

In dit besluit worden nadere voorschriften gegeven omtrent de wijze waarop ANPR-gegevens (hits) aangewend mogen worden voor een onderzoek. Voor het overige moeten de gegevens vier weken na vastlegging worden vernietigd.[9]

1.4.4. Aanwijzing auditief en audiovisueel registreren van verhoren van aangevers, getuigen en verdachten

In het belang van de waarheidsvinding is het wenselijk dat in bepaalde gevallen aangiften en/of verhoren auditief of audiovisueel worden opgenomen. In genoemde aanwijzing en het bijbehorende protocol wordt niet alleen voorgeschreven in welke gevallen dit nodig is, maar ook hoe lang de registraties bewaard mogen worden en op welke wijze ze vernietigd moeten worden.

6 zoals bedoeld in artikel 126cc Sv

7 artikel 27a en 55c Sv

8 artikelen 27b en 55c Sv

9 artikel 126jj, lid 2 Sv en artikel 9, lid 5 van het AN-PR-besluit

1.5. Wet en besluit justitiële en strafvorderlijke gegevens

Deze wet regelt de verwerking van justitiële gegevens, strafvorderlijke gegevens en persoonsdossiers bij onder andere de Justitiële Informatiedienst en de arrondissementsparketten. De Wet en het Besluit justitiële en strafvorderlijke gegevens (Wjsg en Bjsg) spelen in eerste instantie dan ook geen rol bij het vraagstuk van verwijderen en vernietigen van politiegegevens. Indirect zijn een paar bepalingen uit het Bjsg echter wel relevant omdat zij de grondslag vormen voor de verstrekking van zogenaamde afloopberichten.

Politiegegevens die in het kader van een (omvangrijk) strafrechtelijk onderzoek worden verwerkt[10], moeten worden verwijderd indien zij niet langer noodzakelijk zijn voor het doel van het onderzoek. Dat zal vaak het geval zijn nadat de zaak onherroepelijk is geworden. In het Bjsg is geregeld [11]dat justitiële gegevens kunnen worden verstrekt aan de politie om te kunnen voldoen aan de naleving van de verplichting uit de Wpg om politiegegevens te verwijderen/vernietigen indien deze niet meer noodzakelijk zijn voor de uitvoering van de politietaak. Deze gegevens worden verstrekt in de vorm van afloopberichten

10 artikel 9 Wpg

11 artikel 11b

1.6. Archiefwet 1995

De gegevens die politie verwerkt vallen vanaf het moment van vastlegging zowel onder de werking van de AVG of Wpg als onder die van de Archiefwet 1995 (Archiefwet). De Archiefwet verplicht overheidsorganen om overheidsinformatie in goede, geordende en toegankelijk staat te brengen en te bewaren. Met de term overheidsinformatie worden alle informatieobjecten bedoeld, dus documenten, beeld- en/of geluidsmateriaal, informatie van websites of apps, e-mails etc., die door de politie wordt opgemaakt of ontvangen.

De Archiefwet vereist dat overheidsorganen een selectielijst opstellen aan de hand waarvan wordt bepaald welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven.
De politie heeft de vernietigingstermijnen in de selectielijst in overeenstemming gebracht met de eerdergenoemde bewaartermijnen uit de Wpg en Sr.

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 Bedrijfsobjecten[12]. 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 verwijdere 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 poortwachter[13] 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 personen[14]. 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 pseudonomisering 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 autorisatiebeleid[17].

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)” on 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)

2.2.4. 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).’

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 jaar[18] 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 politiegegevens vaak aan de orde zullen zijn.

Na het overdragen moeten de duplicaten of werkkopieën van de overgebrachte archiefbescheiden worden vernietigd[19].

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.

20 Archiefwet 1995, artikel 8

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 testomgeving[21] 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 gevoelgheid alleen mogelijk met instemming (ontheffing) van de dienst IM[22]. 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 regelmatig[23] 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 voortdurend[24] 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 logging[25].

25 Agora; Beleidskader logging (link)

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 documentatieplicht [26] 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]

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 toegelicht[28].

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 verjaring[30].

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

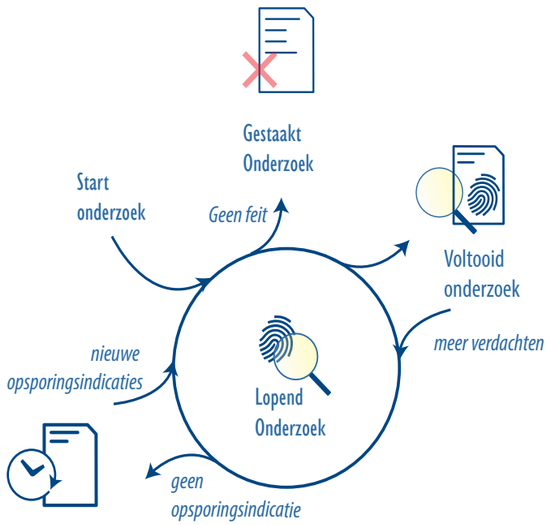
Onderzoek waarbij het onderzoeksdoel niet (volledig) is behaald. Niet alles is ingezonden en het betreft geen cold case. De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval blijft bestaan.

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;



Statussen onderzoek van Politie als trigger voor het privacy beheerproces (bron werkgroep SUMMIT 26.06.2018)

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 vernietiging[31] 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 selectielijst [32]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 vastgesteld[34] en voor medische gegevens in principe 15 jaar[35].

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

Wat zijn de doeleinden van de gegevensverwerking?	Aan de hand van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden bepaalt de verwerkingsverantwoordelijke hoe lang het noodzakelijk is de persoonsgegevens te bewaren[1].
Wanneer is dit doel bereikt?	Bepaal wanneer het niet meer nodig is de gegevens langer te bewaren. Bijvoorbeeld bij de beëindiging van een dienstverband of de afhandeling van een klacht.
Wat is de aard van de gegevens?	Bij het bepalen van de bewaartermijn houdt de verwerkingsverantwoordelijke rekening met de aard van de gegevens; hoe gevoeliger de gegevens, hoe minder snel een lange bewaartermijn te rechtvaardigen is. Houd er rekening mee dat voor het bewaren van bijzondere persoonsgegevens en strafrechtelijke gegevens er hogere eisen gelden voor de beveiliging, bijvoorbeeld door middel van versleuteling of beperking van de toegang[2].
Welke gegevens zijn noodzakelijk om te verwerken[3]?	Alleen gegevens die strikt noodzakelijk zijn voor het doel mogen worden verwerkt. Na verloop van tijd moet gekeken worden of (alle) vastgelegde gegevens nog wel nodig zijn voor de doeleinden van de gegevensverwerking.
Wat is een redelijke (gepaste) bewaartermijn?	Ga na, gelet op het doel van de verwerking en de aard van de gegevens, wat een redelijke termijn is en let er daarbij op dat de gegevens door tijdsverloop hun relevantie of geldigheid kunnen verliezen.

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 rondzwerft. 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 cameratoezicht[37] 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 rechtsor de 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 Grootschalig Bijzonder Optreden (SGBO), 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 afluisteren 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 zodat beoordeeld kan worden of gegevens op grond van artikel 9, lid 4 Wpg verwijderd moeten worden[39]. In dat kader worden de volgende gegevens verstrekt:

- het parketnummer;

en indien het feit is geseponeerd:

- 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 gelegd[42];

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 strafbepalingen[40];

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.

38 Aanwijzing voor de opsporing

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.

Verjaringstermijnen conform artikel 70 Sr zijn gedefinieerd op basis van de voorziene straf.

De termijn van verjaring begint op de dag nadat het strafbare feit is gepleegd, of in sommige gevallen later[41]. Zo begint de termijn bij een zedendelict met een minderjarig slachtoffer bij het meerderjarig worden van het slachtoffer. (tabel)

Artikel 9-verwerkingen waarover geen evident contact met het OM bestaat zoals voorbereidende onderzoeken, veelplegerdossiers, SGBO's en preweegdocumenten moeten aan de hand van een expiratiedatum worden bewaakt door de bevoegd functionaris.

41 Artikel 71 Sr

Straf	Verjaringstermijn Art 70
Overtreding	3 jaar
Misdrijf met geldboete, hechtenis of gevangenisstraf van drie jaar of minder	6 jaar
Misdrijf met gevangenisstraf van meer dan drie jaar	12 jaar
Misdrijf met gevangenisstraf van acht jaar of meer	20 jaar
Misdrijf met gevangenisstraf van twaalf jaar of meer	Geen verjaring

3.4.2. Beoordelen

Zolang het doel van het onderzoek nog niet is bereikt, beoordeelt de bevoegd functionaris voortdurend of gegevens aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking als bedoeld in artikel 10 Wpg.

Nadat de bevoegd functionaris heeft geconstateerd dat het doel van het onderzoek is bereikt, heeft hij maximaal een half jaar de tijd om dit een laatste keer te beoordelen. Pas daarna moet tot verwijdering worden overgegaan.

3.4.3. 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 OvJ moet verzoeken om een opdracht tot vernietiging van de registratie. De opdracht tot vernietiging wordt binnen 30 dagen uitgevoerd.[42]
- 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.

42 Zie voor de volledige procedure de Aanwijzing auditief en audiovisueel registreren van verhoren van aangevers, getuigen en verdachten (2018A008)

3.5. Politiegegevens voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10)

Voor politiegegevens die worden verwerkt voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde zijn termijnen voor verwijdering en vernietiging in artikel 10 van de Wpg bepaald. Het gaat hier om gegevensverwerking om inzicht te verwerven in de betrokkenheid van bepaalde personen bij bepaalde ernstige strafbare feiten of bij handelingen die kunnen wijzen op het beramen of plegen van bepaalde categorieën van misdrijven die ernstige bedreigingen voor de rechtsorde opleveren of bij handelingen die een ernstige schending van de openbare orde vormen. Dit artikel ziet op de meer permanente vormen van gegevensverwerking. Deze meer permanente verwerking van gegevens is nodig in verband met de aard van de misdrijven of handelingen die in het geding zijn, zoals hierna bij de toelichting op het eerste lid aan de orde komt.

3.5.1. Verwijderen

Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van de verwerking worden ze verwijderd. Daartoe worden de gegevens periodiek gecontroleerd.

Uiterlijk 5 jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de politiegegevens van betrokkene op grond van het doel, worden de gegevens verwijderd (artikel 10, lid 6 Wpg).

3.5.2. Vernietigen

- Verwijderde gegevens worden gedurende 5 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).

3.6. Politiegegevens voor controle en beheer van informanten (artikel 12)

Voor politiegegevens die worden verwerkt voor controle en beheer van informanten zijn termijnen voor verwijdering en vernietiging in artikel 12 van de Wpg bepaald. Het gaat hier om gegevens omtrent informanten en om integrale verslagen van de met de informanten gevoerde gesprekken. De gegevens moeten worden afgeschermd en dienen niet voor operationeel gebruik. De informatie die wordt verwerkt op grond van artikel 12, kan slechts tot maximaal vier maanden na de start van de verwerking ter beschikking worden gesteld voor verdere verwerking met het oog op de uitvoering van de dagelijkse politietaak, een onderzoek als bedoeld in artikel 9 of een analyse van artikel 10.

3.6.1. Verwijderen

Gegevens moeten direct worden vernietigd en worden niet voorafgaand verwijderd.

3.6.2. Vernietigen

- Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens elk half jaar gecontroleerd.
- Uiterlijk 10 jaar na de datum van laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van politiegegevens van betrokkene voor dit doel (artikel 12, lid 6 Wpg).

3.7. Politiegegevens voor ondersteunende taken (artikel 13)

Voor politiegegevens die verder worden verwerkt ter ondersteuning van de geldt dat de termijn door de verwerkingsverantwoordelijke zelf moet worden bepaald. In een protocol moet onder andere worden vastgelegd voor welk doel de gegevens verder worden verwerkt, om welke categorieën van personen en gegevens het gaat en wanneer de verwerking wordt beëindigd[43].

Bij doelen kan worden gedacht aan

- het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten (afgerond procesdossier);
- het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte (bijvoorbeeld VVC-zaken);
- identificatie van personen of zaken (HAVANK, FCM);
- het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen (OPS, NSIS, BVH);
- het verkrijgen van landelijk inzicht in specialistische onderwerpen (overvallen, kinderporno, voetbalvandalisme etc.) .

3.7.1. Verwijderen

Gegevens moeten direct worden vernietigd en worden niet voorafgaand verwijderd.

3.7.2. Vernietigen

Uit een artikel 13-protocol moet blijken binnen welke termijn of in welke gevallen het verder verwerken van de betreffende gegevens wordt beëindigd. Deze termijn moet door de verwerkingsverantwoordelijke bepaald en gemotiveerd worden en verschilt dus per artikel 13-verwerking. De termijnen voor specifieke artikel13-verwerkingen zijn dan ook terug te vinden in de betreffende protocollen en in het verwerkingsregister.

In afwijking van het voorgaande volgt de termijn voor het bewaren van vingerafdrukken die worden verwerkt in HAVANK uit artikel 9 van het Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen. In dit geval is het dus niet aan de verwerkingsverantwoordelijke om deze termijn te bepalen.

3.8. Verwijderde politiegegevens (artikel 14)

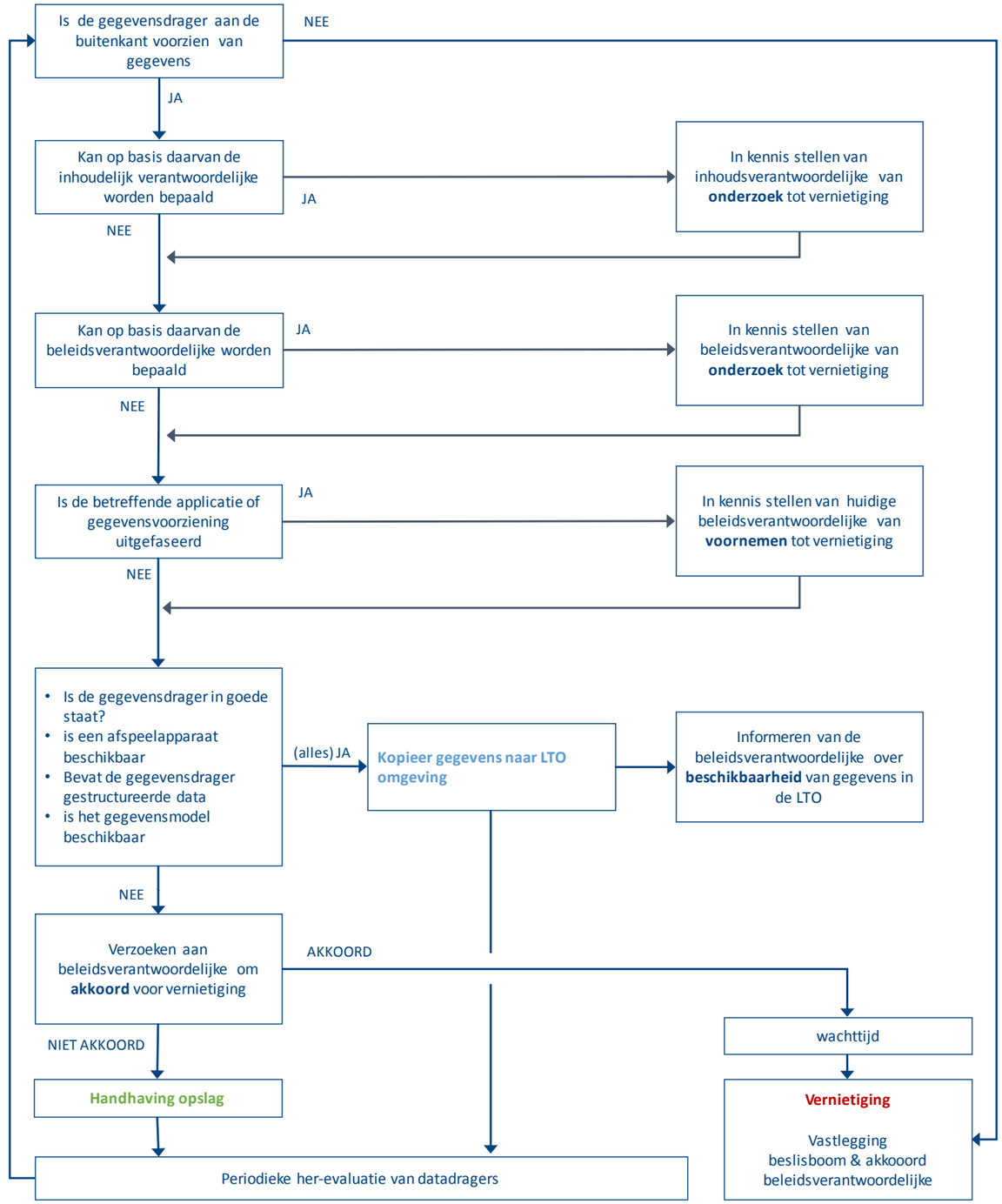
Voor politiegegevens die zijn verwijderd op grond van eerder genoemde artikelen is de termijn voor vernietiging in artikel 14 van de Wpg bepaald. Deze gegevens worden gedurende vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen. Voor het overige geldt dat deze gegevens in bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10 ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Dit kan alleen in opdracht van het bevoegd gezag. Deze gegevens komen ook in aanmerking voor verwerking ten behoeve van wetenschappelijk onderzoek en statistiek[44].

43 artikel 13, lid 4 Wpg j artikel 6:2, lid 1 Bpg

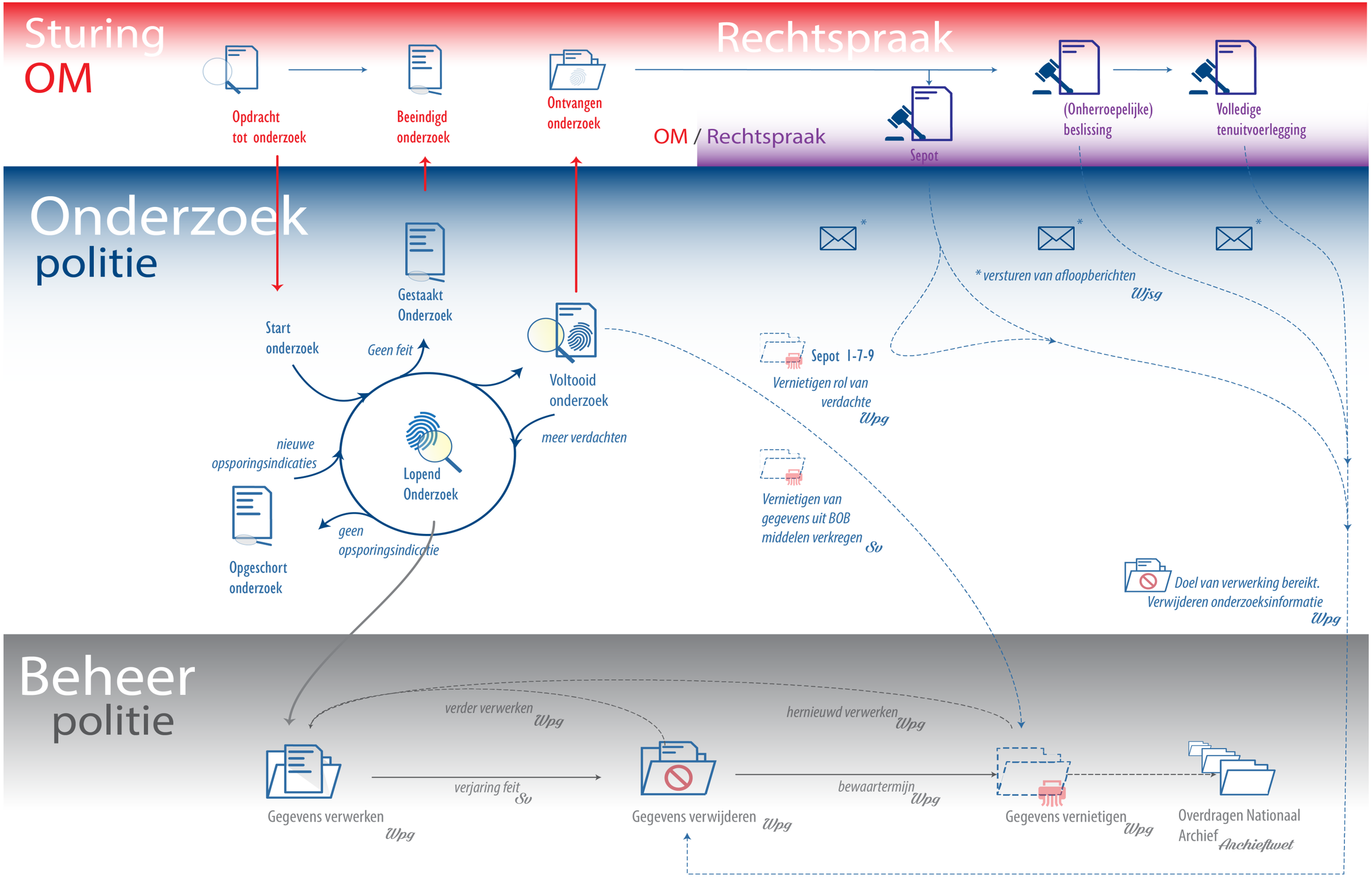
44 artikel 22 Wpg

Bijlagen

Bijlage 1. Referentieproces vernietigen van gegevensdragers



Bijlage 2. Status van onderzoeken in relatie tot archiveren en verwerken



Bijlage 3. Procedure noodvernietiging

(Oorspronkelijk
Kaderrichtlijn Noodvernietiging Politieinformatie)
Directie FM / Strategisch Beleid Services
Directie IV / Gegevensautoriteit
2018

Context

Vernietiging van politieinformatie geschiedt op basis van de Wet politiegegevens (Wpg), de Algemene Verordening Gegevensbescherming (AVG) en de vastgestelde selectielijst voor de politie (Archiefwet). De procedures die daarbij worden gehanteerd zijn vastgelegd in protocollen en het handboek DIV Politie.

Er kunnen zich echter situaties voordoen waarbij van de gestandaardiseerde werkwijzen en de bewaartermijnen Wpg, AVG en selectielijst wordt afgeweken.

Dit betreft de noodvernietiging ex artikel 9, lid 2 van de Archiefwet 1995. In bijzondere omstandigheden kan deze noodvernietiging in werking treden. De maatregel wordt genomen wanneer er sprake is van bijzondere omstandigheden waarbij informatie (papier of digitaal) met gerubriceerde of vertrouwelijke informatie gecompromitteerd dreigt te raken.

Bijzondere informatie

Onder bijzondere informatie wordt de informatie verstaan waarvan de kennisneming door niet geautoriseerde personen nadelige gevolgen kan hebben voor de belangen van de staat en/of zijn bondgenoten en/of één of meer ministeries en daaronder ressorterende diensten, bedrijven en instellingen. Dit is binnen de politie die informatie die valt onder de rubriceringen' politie zeer geheim' en 'politie geheim'.

Onder compromittering wordt verstaan de kennisname dan wel de mogelijkheid tot kennisname van bijzondere informatie door niet-geautoriseerde personen.

Bijzondere omstandigheden

De bijzondere omstandigheden waaronder tot noodvernietiging van documenten kan worden overgegaan zijn:

- Bij zware (natuur)rampen;
- In geval van (dreigende) oorlogsomstandigheden;
- Bij terroristische aanslagen en oproeren.

Scope

Deze kaderrichtlijn richt zich op zowel de papieren – als de digitale informatiedragers binnen de politie en betreft

zowel de gerubriceerde informatie die is vastgelegd in het dynamische proces (die dagelijks wordt gebruikt binnen het operationele- en bedrijfsvoeringproces) als de gerubriceerde informatie die langdurig is vastgelegd in archiefruimten en archiefsystemen met het oog op het belang van verantwoording, bedrijfsvoering of het cultuur-historisch belang.

Opdracht

Een noodvernietiging van gerubriceerde politie-informatie, en dus de informatiedragers waarop de documenten zijn vastgelegd, vindt plaats op aanwijzing van de minister-president, de minister van Veiligheid en Justitie of de korpschef van politie.

Vernietiging

Vernietiging houdt in dat de informatiedragers een dusdanige bewerking ondergaan, dat de informatie die daarop is vastgelegd niet meer te lezen en niet meer herleidbaar is. De noodvernietiging gebeurt door het zodanig verminken van de informatiedragers (zoals papier, Cd's/Dvd's, harde schijven, geluidsbanden, usb-sticks, microfilms, data-tapes, en dergelijke) 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).

Aangezien het hier gerubriceerde informatie betreft zal de vernietiging van de informatiedragers vallen binnen de veiligheidsklassen 4 tot en met 7. Zie bijlage DIN 66399 (2012-10).

Bestanden

In ieder van de regionale eenheden en de landelijke eenheid maakt de teamleider DIV, in samenwerking met de proceseigenaren van de informatie en Functioneel Beheer, een overzicht in welke informatiebestanden en taakapplicaties gerubriceerde informatie is opgenomen, waar die documentbestanden zijn geplaatst en door wie deze worden beheerd.

De landelijke teamchef DIV draagt, in overleg met het hoofd IM, zorg voor een landelijk uitvoeringsprotocol, zorgt dat in iedere eenheid de middelen aanwezig zijn om tot noodvernietiging over te kunnen gaan en dat deze middelen in werkzame staat verkeren.

Verklaring

Indien de omstandigheden dit toelaten, wordt van de noodvernietiging een verklaring opgesteld die een globaal overzicht bevat van de vernietigde bestanden en de wijze waarop de vernietiging heeft plaatsgevonden.

Procedure noodvernietiging (toelichting normen en standaarden)

(Oorspronkelijk
Bijlage bij Kaderrichtlijn Noodvernietiging
Politieinformatie)

Inleiding

Er zijn verschillende normen te onderscheiden die zich richten op het vernietigen van informatiedragers met vertrouwelijke informatie. Te noemen zijn de NEN 15713 of de DIN 66399. Voor de vernietiging van confidentiële van de politie hebben we er voor gekozen om als uitgangspunt de DIN 66399 te hanteren. Reden hiervoor is dat, in tegenstelling tot in de NEN 15713, in de DIN 66399 ook de classificatieniveau 's worden benoemd met een daar aan gekoppelde norm voor vernietiging per soort informatiedrager.

DIN 66399

De DIN 66399 is een norm die is uitgegeven door het Deutschen Institut für Normung. Het betreft hier een (industrie)norm voor het vernietigen van informatiedragers en de daarop vastgelegde informatie conform vastgestelde richtlijnen Binnen de norm wordt een risicoanalyse gemaakt op grond van de op de drager vastgelegde informatie (classificatieniveau 's). Daarnaast benoemd de norm verschillende groepen van informatiedragers en daarmee de manier waarop de vastgelegde informatie wordt gepresenteerd (materiaalklassen). Het classificatieniveau en, de materiaalklasse en de veiligheidsklasse bepalen in deze norm de wijze waarop vernietiging van de vastgelegde informatie plaats heeft (veiligheidsklassen).

Classificatieniveaus

De volgende classificatieniveau 's worden onderscheiden:

Classificatieniveau 1

Standaard gevoeligheid van de informatie.
Het betreft hier informatie bedoeld voor grote groepen mensen. Kennisname van de informatie door onbedoelde openbaarheid heeft minimale schade voor de organisatie of personen tot gevolg.

Classificatieniveau 2

Hoge gevoeligheid. De vastgelegde informatie is van confidentiële aard. De informatie is bedoeld voor een kleine groep personen. Kennisname door niet geautoriseerde personen kan ernstige schade voor de organisatie of personen tot gevolg hebben.

Classificatieniveau 3

Zeer hoge gevoeligheid. De vastgelegde informatie is van zeer confidentiële of geheime aard. De informatie is bedoeld voor een zeer kleine groep geautoriseerde personen. Ongeautoriseerde kennisname kan zeer ernstige voor de organisatie of personen tot gevolg hebben.

Materiaalklassen

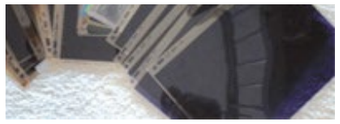
Op grond van de huidige stand van de techniek worden de volgende materiaalklassen onderscheiden:

Materiaalklasse P

Informatie in zijn 'originele' fysieke vorm. Denk hierbij aan papier, films, negatieven, foto's. Deze worden ook wel aan gegeven als veiligheidsklasse.

Materiaalklasse F

Informatie in verkleinde vorm. Denk hierbij aan microfilms of folies



Materiaalklasse O

Informatie op optische informatiedragers. Denk hierbij aan Cd's DVD, Blu-ray

Materiaalklasse T

Informatie op magnetische informatiedragers. Denk hierbij aan diskettes, magneetbandcassettes en ID-kaarten.

Materiaalklasse H

Informatie op harddisk met magnetische onderdelen.

Materiaalklasse E

Informatie op elektronische informatiedragers. Denk hierbij aan USB-flashdrives, SSD harddisks, chipkaarten.

Veiligheidsklassen

In de norm worden zeven veiligheidsklassen geformuleerd die mede zijn gebaseerd op de mogelijkheid tot reproductie van de vastgelegde informatie

1. Aanbevolen voor informatiedragers met openbare informatie die onleesbaar gemaakt moet worden: Reproductie met enige inspanning
2. Aanbevolen voor informatiedragers met organisatie interne informatie die onleesbaar gemaakt moet worden: Reproductie met bijzondere inspanning
3. Aanbevolen voor informatiedragers met enkele voor de organisatie gevoelige en confidentiële informatie die onleesbaar gemaakt moet worden:Reproductie met aanzienlijke inspanning
4. Aanbevolen voor informatiedragers met een hoog aantal voor de organisatie een gevoelige en confidentiële informatie dat onleesbaar gemaakt moet worden: Reproductie met buitengewone inspanning
5. Aanbevolen voor informatiedragers met geheime informatie die onleesbaar gemaakt moet worden: Reproductie met dubieuze (technische) methoden
6. Aanbevolen voor informatiedragers met geheime informatie waarvoor ongewoon hoge veiligheidstandaarden gehandhaafd worden: Reproductie technisch niet mogelijk
7. Aanbevolen voor informatiedragers met geheime informatie waarvoor de strikte veiligheidstandaarden gehandhaafd worden: Reproductie uitgesloten

Normen voor vernietiging

Door het classificatieniveau te koppelen aan het gewenste veiligheidsniveau ontslaat de volgende toepassingstabel voor het vernietigen: (zie tabel hieronder)

Per materiaalklasse vloeien daaruit de volgende normen voor vernietiging voort:

Materiaalklasse P

Informatie in zijn ‘originele’ fysieke vorm.

- P-1 Deeltjes maximaal 2000 mm² of stroken van maximaal 12 mm. Lengte van de stroken onbeperkt
- P-2 Deeltjes maximaal 800 mm² of stroken van maximaal 6 mm. Lengte van de stroken onbeperkt
- P-3 Deeltjes maximaal 320 mm² of stroken van maximaal 2 mm. Lengte van de stroken onbeperkt
- P-4 Deeltjes maximaal 160 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 6 mm
- P-5 Deeltjes maximaal 30 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 2 mm
- P-6 Deeltjes maximaal 10 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 1 mm
- P-7 Deeltjes maximaal 5 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 1 mm

	Veiligheids-klasse 1	Veiligheids-klasse 2	Veiligheids-klasse 3	Veiligheids-klasse 4	Veiligheids-klasse 5	Veiligheids-klasse 6	Veiligheids-klasse 7
Classificatie niveau 1	•[1]	•[1]	•				
Classificatie niveau 2			•	•	•		
Classificatie niveau 3				•	•	•	•

[1] Deze combinatie kan niet gebruikt worden voor persoonlijke informatie.

Materiaalklasse F

Informatie in verkleinde vorm.

- F-1 Deeltjes maximaal 160 mm^2
- F-2 Deeltjes maximaal 30 mm²
- F-3 Deeltjes maximaal 10 mm²
- F-4 Deeltjes maximaal 2,5 mm²
- F-5 Deeltjes maximaal1,0 mm²
- F-6 Deeltjes maximaal 0,5 mm²
- F-7 Deeltjes maximaal 0,2 mm²

Materiaalklasse O

Informatie op optische informatiedragers

- O-1 Deeltjes maximaal 2000 mm²
- O-2 Deeltjes maximaal 800 mm²
- O-3 Deeltjes maximaal 160 mm²
- O-4 Deeltjes maximaal 30 mm²
- O-5 Deeltjes maximaal10 mm²
- O-6 Deeltjes maximaal 5 mm²
- O-7 Deeltjes maximaal 0,2 mm²

Materiaalklasse T

Informatie op magnetische informatiedragers

- T-1 Medium niet meer functionerend
- T-2 Medium in meerdere onderdelen en deeltjes maximaal 2000 mm²
- T-3 Deeltjes maximaal 320 mm²
- T-4 Deeltjes maximaal 160 mm²
- T-5 Deeltjes maximaal30 mm²
- T-6 Deeltjes maximaal 10 mm²
- T-7 Deeltjes maximaal 2,5 mm²

Materiaalklasse H

Informatie op harddisk met magnetische onderdelen

- H-1 Schijf niet meer functionerend
- H-2 Gegevensdrager beschadigd
- H-3 Gegevensdrager vervormd
- H-4 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 2000 mm²
- H-5 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 320 mm²
- H-6 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 10 mm²
- H-7 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 5 mm²

Materiaalklasse E

Informatie op elektronische informatiedragers

- E-1 Medium niet meer functionerend.
- E-2 Medium in onderdelen
- E-3 Medium in onderdelen en deeltjes maximaal160 mm²
- E-4 Gegevensdrager in onderdelen en deeltjes maximaal 30 mm²
- E-5 Gegevensdrager in onderdelen en deeltjes maximaal 10 mm²
- E-6 Gegevensdrager in meerdere onderdelen en deeltjes maximaal 1 mm²
- E-7 Gegevensdrager in meerdere onderdelen en deeltjes maximaal 0,5 mm²

Vastgesteld Document	
Versie	1.0
Datum	13/02/2020
Vastgesteld door	BBVO (Lid Korpsleiding)
Is dit de laatste versie? Controleer dat hier of scan de QR code	

v