

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 later⁴¹. 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, SGB0's en preweegdocumenten moeten aan de hand van een expiratedatum 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 blijkt 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 politietaken, 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 blijkt 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 beëindigd⁴³.

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)

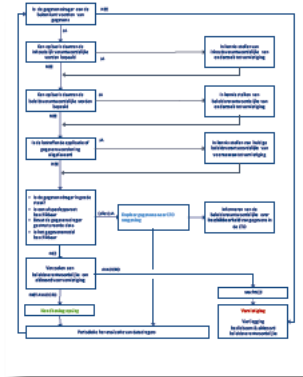
Voor politiegegevens die zijn verwijderd op grond van eerder genoemde artikelen is de termijn voor vernietiging in artikel 14 van de Wpg bepaald. Deze gegevens worden gedurende vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen. 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 statistiek⁴⁴.

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

44 artikel 22 Wpg

Bijlagen

Bijlage 1. Referentieproces vernietigen van gegevensdragers
pag.29



Bijlage 2. Status van onderzoeken in relatie tot archiveren en verwerken
pag.30

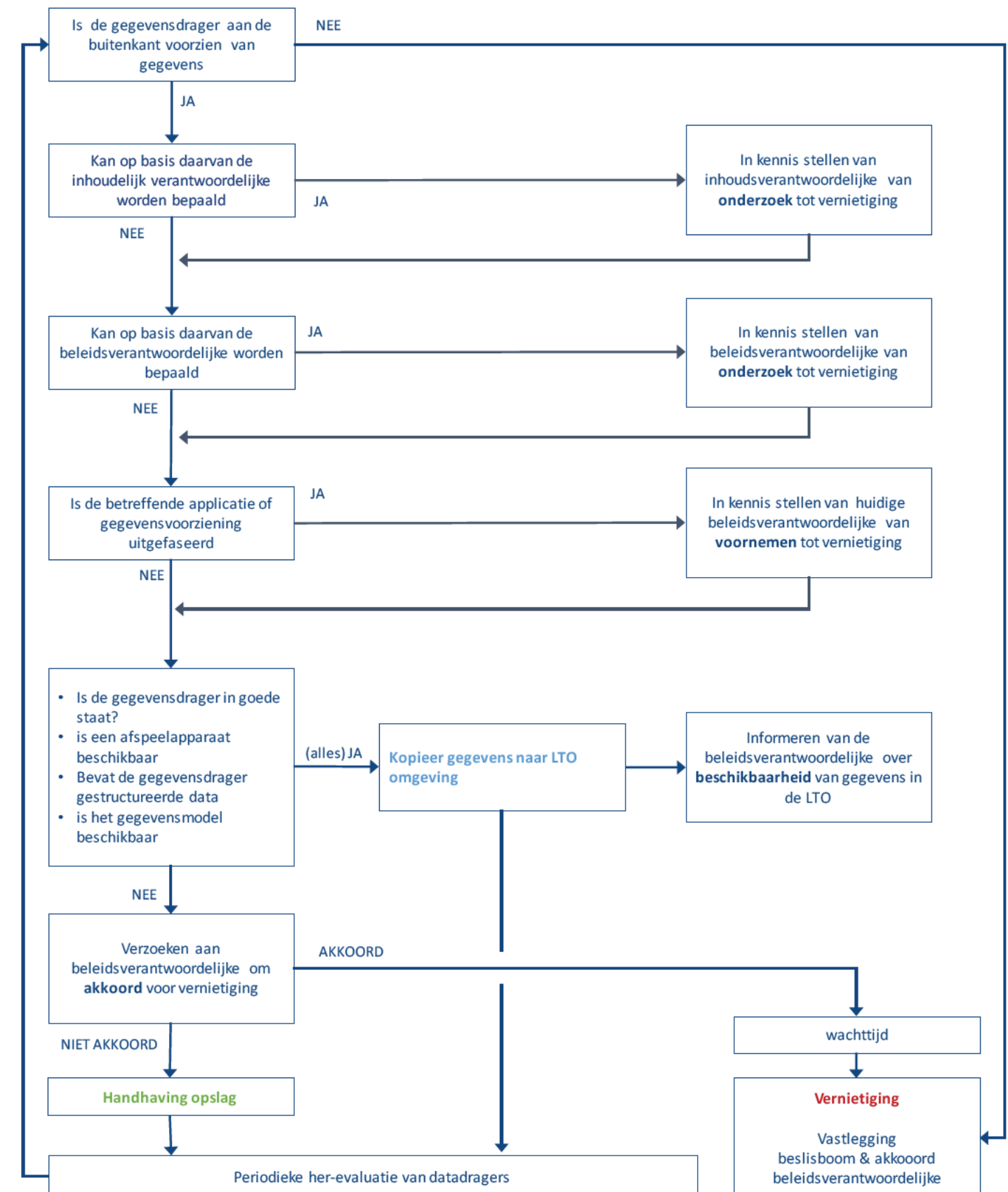


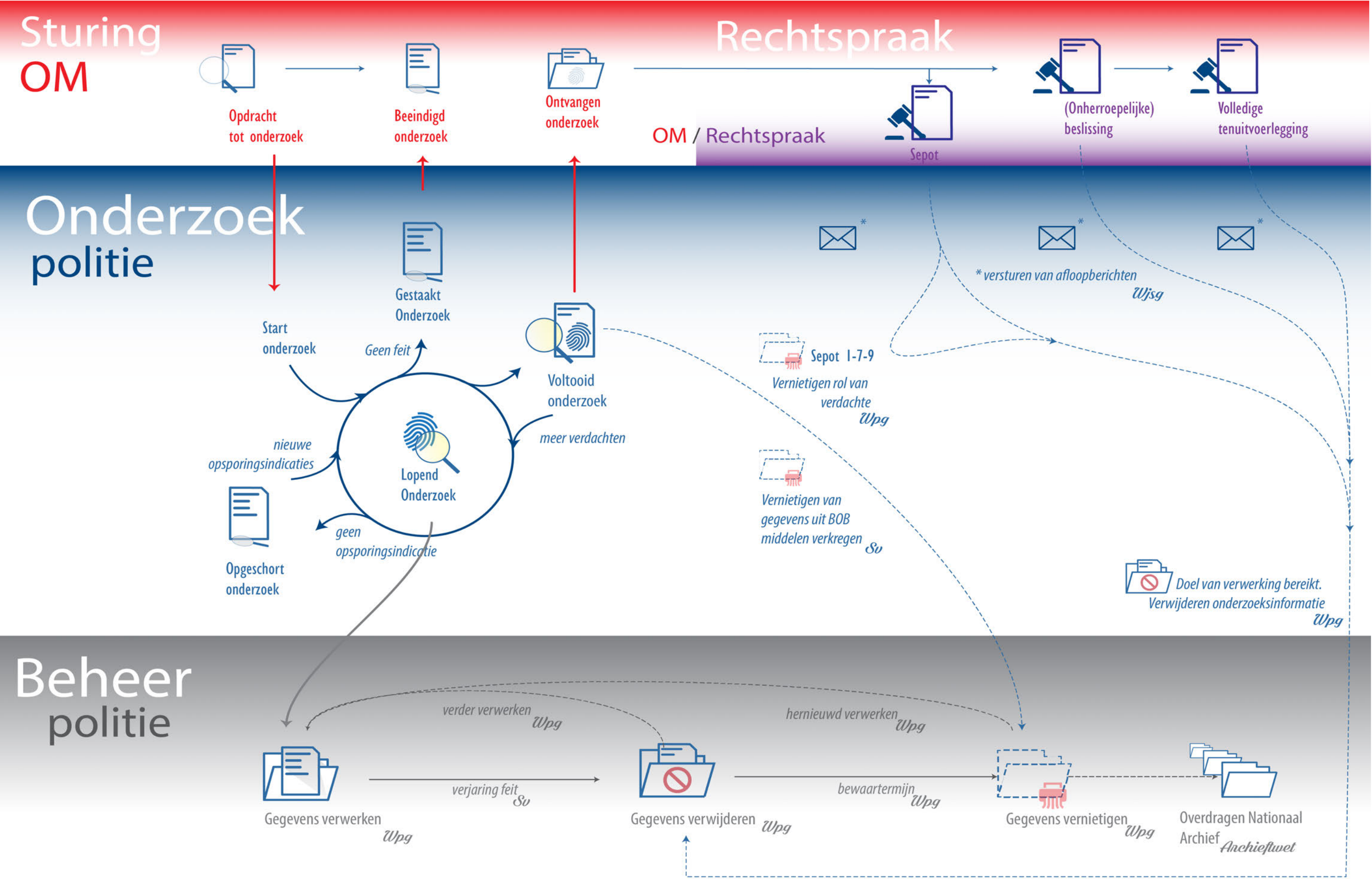
Bijlage 3. Procedure noodvernietiging
pag.32



Procedure noodvernietiging (toelichting normen en standaarden)
pag.34

Bijlage 1. Referentieproces vernietigen van gegevensdragers





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 informatie-dragers 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		Normen voor vernietiging	
In de norm worden zeven veiligheidsklassen geformuleerd die mede zijn gebaseerd op de mogelijkheid tot reproductie van de vastgelegde informatie		Door het classificatieniveau te koppelen aan het gewenste veiligheidsniveau ontslaat de volgende toepassingstabel voor het vernietigen: (zie tabel hieronder)	
- Aanbevolen voor informatiedragers met openbare informatie die onleesbaar gemaakt moet worden: Reproductie met enige inspanning - Aanbevolen voor informatiedragers met organisatie interne informatie die onleesbaar gemaakt moet worden: Reproductie met bijzondere inspanning - Aanbevolen voor informatiedragers met enkele voor de organisatie gevoelige en confidentiële informatie die onleesbaar gemaakt moet worden: Reproductie met aanzienlijke inspanning - Aanbevolen voor informatiedragers met een hoog aantal voor de organisatie een gevoelige en confidentiële informatie dat onleesbaar gemaakt moet worden: Reproductie met buitengewone inspanning - Aanbevolen voor informatiedragers met geheime informatie die onleesbaar gemaakt moet worden: Reproductie met dubieuze (technische) methoden - Aanbevolen voor informatiedragers met geheime informatie waarvoor ongewoon hoge veiligheidsstandaarden gehandhaafd worden: Reproductie technisch niet mogelijk - Aanbevolen voor informatiedragers met geheime informatie waarvoor de strikte veiligheidsstandaarden gehandhaafd worden: Reproductie uitgesloten		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	Materiaalklasse H
Informatie in verkleinde vorm.	Informatie op harddisk met magnetische onderdelen
- F-1 Deeltjes maximaal 160 mm² - F-2 Deeltjes maximaal 30 mm² - F-3 Deeltjes maximaal 10 mm² - F-4 Deeltjes maximaal 2,5 mm² - F-5 Deeltjes maximaal 1,0 mm² - F-6 Deeltjes maximaal 0,5 mm² - F-7 Deeltjes maximaal 0,2 mm²	- 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 O	Materiaalklasse E
Informatie op optische informatiedragers	Informatie op elektronische 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 maximaal 10 mm² - O-6 Deeltjes maximaal 5 mm² - O-7 Deeltjes maximaal 0,2 mm²	- E-1 Medium niet meer functionerend. - E-2 Medium in onderdelen - E-3 Medium in onderdelen en deeltjes maximaal 160 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
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 maximaal 30 mm² - T-6 Deeltjes maximaal 10 mm² - T-7 Deeltjes maximaal 2,5 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	



Kwaliteitshandboek Wpg & AVG

Datakwaliteit begint bij de mens

Door	
Afdeling	Gegevensautoriteit
Versienummer	1.0
Versiedatum	31 juli 2024
Kenmerk	
Status	Definitief – vastgesteld door BOO op 14 februari 2025
Rubricering	Politie INTERN - Bedrijfsvoering

Documentinformatie

Versiegeschiedenis

Versie	Versiedatum	Samenvatting van de aanpassing
0.1	7 maart 2024	Eerste concept "as is" voor discussiedoeleinden
0.2	20 maart 2024	Opmerkingen ^{5.1.2.e} verwerkt; uitgebreid met AVG en nadere uitwerking
0.3	28 maart 2024	Opmerkingen ^{5.1.2.e} verwerkt n.a.v. zijn review op hoofdlijnen
0.4	16 april 2024	Opmerkingen ^{5.1.2.e} verwerkt n.a.v. zijn review op hoofdlijnen; voorts o.a.: nadere uitwerking AI, belang datagovernance en privacygovernance en basisregistraties, etc.
0.5	13 mei 2024	Verwerken review ^{5.1.2.e}
0.6	21 mei 2024	Verwerken detailreview ^{5.1.2.e}
0.7	4 juli 2024	Verwerken opmerkingen brede review ronde van versie 0.6
0.8	8 juli 2024	Verwerken review ^{5.1.2.e}
0.9	9 juli 2024	Kleine aanvullingen en verbeteringen
0.10	17 juli 2024	Voorlopig definitief maken document
1.0	31 juli 2024	Definitieve versie ten behoeve van besluitvorming
	14 februari 2025	Definitieve versie ongewijzigd vastgesteld door het BOO (Breed operationeel overleg)

Distributie

Versie	Verzenddatum	Naam	Afdeling/functie
0.1	7 maart 2024	^{5.1.2.e}	Gegevensautoriteit-Team Privacy
0.2	20 maart 2024	^{5.1.2.e}	Gegevensautoriteit-Team Datamanagement
0.3	28 maart 2024	^{5.1.2.e}	Gegevensautoriteit-Team Privacy
0.4	16 april 2024	^{5.1.2.e}	^{5.1.2.e}
		^{5.1.2.e}	Gegevensautoriteit-Team Privacy
0.5	13 mei 2024	^{5.1.2.e}	Gegevensautoriteit-Team Datamanagement
0.6	21 mei 2024	^{5.1.2.e}	Team Kwaliteit van Intelligence LE (LX&LO)
		^{5.1.2.e}	Team Kwaliteit van Intelligence (Amsterdam)
		^{5.1.2.e}	Team Kwaliteit van Intelligence (LO)
		^{5.1.2.e}	Team Kwaliteit van Intelligence (NH)
		^{5.1.2.e}	Programma vernieuwend registreren (PVR)
		^{5.1.2.e}	Team bestuursondersteuning (ZB)
		^{5.1.2.e}	^{5.1.2.e}
		^{5.1.2.e}	^{5.1.2.e}
	23 mei 2024	^{5.1.2.e}	^{5.1.2.e}
	5 juni 2024	^{5.1.2.e}	Gegevensautoriteit-Team Datamanagement
		^{5.1.2.e}	^{5.1.2.e}
	11 juni 2024	^{5.1.2.e}	Privacy Platform: leden van het KSG-tje t.b.v. het meelesen van het Kwaliteitshandboek
		^{5.1.2.e}	
		^{5.1.2.e}	
		^{5.1.2.e}	
		^{5.1.2.e}	
		^{5.1.2.e}	
	27 juni 2024	^{5.1.2.e}	Gegevensautoriteit-Team Duto
	2 juli 2024	^{5.1.2.e}	Gegevensautoriteit-Team Privacy

0.7	4 juli 2024	S.12.e	Gegevensautoriteit-Team Privacy
0.8	8 juli 2024	S.12.e	S.12.e
0.9	9 juli 2024	S.12.e	Gegevensautoriteit-Team Duto
0.10	17 juli 2024	S.12.e	Functionaris gegevensbescherming (FG)
		S.12.e	Functionaris gegevensbescherming (FG)
		S.12.e	Medewerker bedrijfsbureau FG
1.0	31 juli 2024		Distributie t.b.v. besluitvorming

Afgenomen interviews/gevoerde gesprekken

Datum	Naam	Afdeling/functie
periodiek	5.12.e	Gegevensautoriteit – Team Privacy
	5.12.e	
14 februari 2024	5.12.e	Team Kwaliteit van Intelligence LE (LX&LO)
14 februari 2024	5.12.e	Team Kwaliteit van Intelligence (Amsterdam)
14 februari 2024	5.12.e	Gegevensautoriteit – Team Datamanagement
15 februari 2024	5.12.e	Gegevensautoriteit – Team Privacy
19 februari 2024	5.12.e	Team Kwaliteit van Intelligence (LO)
19 februari 2024	5.12.e	Team Kwaliteit van Intelligence (NH)
27 februari 2024	5.12.e	CIO Office
5 maart 2024	5.12.e	Gegevensautoriteit – Team Datamanagement
11 maart 2024	5.12.e	Programma vernieuwend registreren (PVR)
18 maart 2024	5.12.e	5.12.e - Politieacademie
19 maart 2024	5.12.e	Gegevensautoriteit – Team Privacy
2 april 2024	5.12.e	Juridisch Adviseur AI en Data Science
16 mei 2024	5.12.e	Gegevensautoriteit – Team Datamanagement
27 juni 2024		
27 juni 2024	5.12.e	Gegevensautoriteit -Team Duto

Inhoudsopgave

Documentinformatie.....	2
Inhoudsopgave	4
1 Inleiding.....	5
1.1 Aanleiding, doelstelling en scope	5
1.2 Doelgroep	5
1.3 Leeswijzer	6
2 Kwaliteitsnormen Wpg & AVG.....	7
2.1 Noodzakelijkheid	7
2.2 Behoorlijk en rechtmatig, toereikend, terzake dienend, niet-bovenmatig	8
2.3 Juistheid en nauwkeurigheid	8
2.4 Onderscheid feiten en persoonlijk oordeel	10
2.5 Onderscheid verschillende categorieën betrokkenen	10
2.6 Verwijderen, bewaren en vernietigen	11
2.6.1 Wpg.....	11
2.6.2 AVG	12
3 Maatregelen en initiatieven ter borging kwaliteit	13
3.1 Datastrategie IV	13
3.1.1 Datastrategie politie 2022-2025	13
3.1.2 Relatie Datastrategie tot kwaliteitsnormen Wpg en AVG	13
3.2 Data-, privacy-, en duto-governance	14
3.3 Privacy en security en duurzame toegankelijkheid by Design (PSDbD).....	14
3.3.1 PSDbD	14
3.3.2 Relatie PSDbD tot kwaliteitsnormen	15
3.4 Metadata in relatie tot datakwaliteit	16
3.5 Gegevensbeschermingseffectbeoordeling (GEB)	17
3.5.1 Uitvoering GEB	17
3.5.2 Relatie GEB tot kwaliteitsnormen	17
3.6 Basisregistraties en generieke gegevensdiensten	18
3.6.1 Tien basisregistraties	18
3.6.2 Relatie basisregistraties tot kwaliteitsnormen	18
3.6.3 Generieke ketenvoorzieningen	19
3.7 Ketenkwaliteit	19
3.7.1 Netwerk Datakwaliteit (NDK).....	19
3.7.2 Relatie NDK tot kwaliteitsnormen Wpg	20
3.7.3 Terugmeldplicht BRP.....	20
3.8 Artificial intelligence (AI).....	20
3.9 Opleiding en herhalingscursussen.....	21
3.10 Motivatie, gedrag en managementaandacht.....	22
3.11 Monitoring en riskmanagement	23
3.11.1 Kwaliteitsmedewerkers.....	23
3.11.2 Riskmanagement	23
3.12 Intern en extern toezicht	24

1 Inleiding

1.1 Aanleiding, doelstelling en scope

Het verzamelen, verwerken, registreren en beheren van data is cruciaal voor de politie. Data zijn onmisbaar om resultaten te bereiken in de operatie, zoals de bestrijding van criminaliteit en het handhaven van de openbare orde.¹ De politie verwerkt niet alleen data bij de uitvoering van haar politietaak. Ook voor de politie als werkgever zijn data belangrijk. Denk aan recruitmentactiviteiten en het personeelsbeheer van de vele duizenden politiemedewerkers.

Datakwaliteit is daarbij een voortdurend punt van aandacht. *Datakwaliteit* of *gegevenskwaliteit* betekent dat gegevens worden verzameld en verwerkt in overeenstemming met de normen die daaraan zijn gesteld. Datakwaliteit is ook maatschappelijk gezien belangrijk. Het draagt bij aan het vertrouwen van de burger in de politie.

Voor politiegegevens gelden wettelijk verankerde kwaliteitsnormen. Deze zijn vastgelegd in de Wet politiegegevens (**Wpg**). Politiegegevens zijn persoonsgegevens die de politie verwerkt in het kader van de *politietaak*.

De Algemene verordening gegevensbescherming (**AVG**) voorziet in kwaliteitsnormen voor persoonsgegevens die de politie verwerkt in het kader van haar *bedrijfsvoering*. Onder bedrijfsvoering vallen bijvoorbeeld recruitment en screening, salaris- en personeelsbeheer, klachtenbehandeling, ICT-servicedesk en facilitair management. Daarnaast geldt de AVG voor de verwerking van persoonsgegevens voor een aantal specifieke taken, zoals de *korpscheftaken*,² de *vreemdelingentaak* en het beheer van de 1-1-2 alarmcentrale.

Het *Kwaliteitshandboek Wpg & AVG* is primair gericht op de belangrijkste kwaliteitsnormen van de Wpg en de AVG en licht deze normen toe.³ Het geeft daarmee geen uitputtend overzicht van andere normen voor datakwaliteit, zoals die bijvoorbeeld in verschillende datamanagement-modellen zijn uitgewerkt. Daarnaast geeft het *Kwaliteitshandboek Wpg & AVG* de initiatieven en maatregelen weer ter borging van dit normenkader. Doel is om *overzicht* te creëren en een *richtinggevend kader* te bieden voor het borgen van kwaliteit van gegevens in overeenstemming met de kwaliteitsnormen uit de Wpg en AVG.⁴

1.2 Doelgroep

Het *Kwaliteitshandboek Wpg & AVG* is gericht tot alle politiemedewerkers die met persoonsgegevens (AVG) en politiegegevens (Wpg) werken en zich afvragen hoe de juridische kwaliteitsnormen geïnterpreteerd moeten worden, zoals bijvoorbeeld medewerkers privacy en data, maar ook leden van de korpsleiding, politiechefs, diensthoofden en directeurs van directies.

¹ Zie ook: Datastrategie politie 2022-2025, 'Data voor veiligheid', p. 7.

² Korpscheftaken zijn taken geregeld in de Wet wapens en munitie, de Omgevingswet (omgevingsvergunning jachtgeweeractiviteit), de Wet particuliere beveiligingsorganisaties en recherchebureaus, de Wet explosieven voor civiel gebruik en het Besluit buitengewoon opsporingsambtenaar.

³ Ter nadere toelichting: de focus ligt op de normen vastgelegd in artikel 3 en 4 Wpg en artikel 5 AVG.

⁴ Naast dit Kwaliteitshandboek Wpg & AVG is er ook een [Praktijkhandboek Wet politiegegevens](#), dat op praktische en laagdrempelige wijze uitleg geeft over onder andere het verwerken van politiegegevens in de praktijk, de bevoegd functionaris, het verstrekken van politiegegevens en de rechten van betrokkenen.

1.3 Leeswijzer

Hoofdstuk 2 behandelt de belangrijkste kwaliteitsnormen die zijn vastgelegd in de Wpg en AVG. Hoofdstuk 3 geeft vervolgens een overzicht van maatregelen en initiatieven binnen de politie die bijdragen aan het borgen van datakwaliteit.

Daar waar in de volgende hoofdstukken van het *Kwaliteitshandboek Wpg & AVG* over **persoonsgegevens** wordt gesproken, gaat het over persoonsgegevens in de zin van de AVG. De term **politiegegevens** wordt gebruikt als het uitsluitend gaat over politiegegevens als bedoeld in de Wpg. Als het over Wpg-politiegegevens én AVG-persoonsgegevens gaat, wordt dit aangeduid met de term **gegevens**. Gaat het over andere data, dan wordt de term **data** gebruikt.

2 Kwaliteitsnormen Wpg & AVG

2.1 Noodzakelijkheid

Eén van fundamentele beginselen van de **Wpg** is het *noodzakelijkheids criterium*, dat in artikel 3 lid 1 van de Wpg is vastgelegd. Dit criterium beschermt de burger tegen te grote inmenging van de politie in de persoonlijke levenssfeer, omdat het beperkingen stelt aan het verwerken van politiegegevens.

Politiegegevens mogen uitsluitend worden verwerkt als dat noodzakelijk is voor één van de wettelijke doeleinden. Deze doeleinden staan in de artikelen 8, 9, 10, 12 en 13 van de Wpg. *Noodzakelijkheid* staat dus niet op zich, maar staat in relatie tot het doeleinde waarvoor de politiegegevens worden verwerkt. Afhankelijk van het doeleinde, kan de uitkomst dus anders zijn. Bij een artikel 9 Wpg opsporingsonderzoek, worden vaak meer politiegegevens verwerkt dan bij het hulp verlenen aan een individuele burger in nood onder artikel 8 Wpg.

Voor *bijzondere politiegegevens* ligt de lat nog hoger. Verwerking mag alleen als dit *onvermijdelijk* is en in aanvulling op verwerking van andere politiegegevens én als de gegevens afdoende zijn beveiligd.⁵

Noodzakelijkheid is ook onder de **AVG** een essentieel criterium. Zo bepaalt artikel 5 lid 1 sub c AVG dat het verwerken van persoonsgegevens zich moet beperken tot wat *noodzakelijk* is voor het doeleinde waarvoor de verwerking plaatsvindt.⁶ Stel dat er een disciplinair onderzoek plaatsvindt door het VIK, dan moet continu de vraag worden gesteld welke persoonsgegevens noodzakelijk zijn voor het verrichten van het onderzoek en welke niet. Hetzelfde geldt voor het opslaan van persoonsgegevens in de -digitale- personeelsdossiers.

Dat *noodzakelijkheid* context gerelateerd is, blijkt ook uit vragen die opkomen rond het gebruik van Artificial Intelligence (AI). De aard en omvang van de gegevens die daarvoor kunnen worden ingezet, zal mede worden bepaald door hetgeen noodzakelijk is om het AI-model goed te trainen en te laten functioneren, waarbij ook aan eisen van proportionaliteit en subsidiariteit moet worden getoetst.

Het noodzakelijkheids criterium krijgt nadere invulling door de vereisten van *proportionaliteit* en *subsidiariteit*. Deze eisen komen erop neer, dat de mate waarin gegevens worden verzameld en verwerkt moet opwegen tegen het doel. Verder moet worden onderzocht of er geen minder ingrijpende alternatieven voor handen zijn. *Handig en je weet maar nooit* zijn soms ook verleidelijke beweegredenen voor het verzamelen en verwerken van gegevens, maar dat is echt iets anders dan noodzakelijkheid als bedoeld in de Wpg en AVG. Het Hof van Justitie van de Europese Unie formuleert het als volgt: *de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen daarvan binnen de grenzen van het strikt noodzakelijke blijven*.⁷ Politied medewerkers moeten dus altijd kritisch zijn bij het verwerken van gegevens bij de uitvoering van hun taken. Wel geldt daarbij dat politied medewerkers tegelijkertijd moeten durven vertrouwen op hun professionaliteit en beslisvermogen en bij de uitvoering van hun werk niet moeten ‘verkrampen’, omdat zij te bang zijn dat iets ‘niet mag van de privacy’.

⁵ Artikel 5 Wpg.

⁶ *Noodzakelijkheid* komt ook terug in de verwerkingsgronden van artikel 6 AVG. Bij de rechtsgrond toestemming is dit niet expliciet vermeld. Uit het Santander-arrest van de Hoge Raad ([ECLI:NL:HR:2011:BQ8097](#)) volgt echter dat bij iedere gegevensverwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit, ook als de verwerking op toestemming is gebaseerd.

⁷ [ECLI: EU:C:2016:970](#), HvJ EU C-362/14, C-203/15 en C-698/15, rechtsoverweging 96.

2.2 Behoorlijk en rechtmatig, toereikend, terzake dienend, niet-bovenmatig

Het vereiste dat de verwerking van gegevens *behoorlijk* en *rechtmatig* moet zijn en *toereikend*, *terzake dienend* en *niet-bovenmatig* gelet op de doeleinden waarvoor ze worden verwerkt, staat **zowel** in de **Wpg** als in de **AVG**.⁸ Het ligt in het verlengde van het noodzakelijkheids criterium.

Behoorlijk, of ook wel gewoon *eerlijk*, betekent dat bij de gegevensverwerking geen sprake mag zijn van misleiding, discriminatie of ongerechtvaardigde schadelijke effecten voor de betrokkenen. Zo moet er voorzichtig worden omgegaan met factoren als afkomst en geboorteland, omdat dit discriminatie in de hand kan werken. Dit kan spelen bij de verwerking van politiegegevens, bijvoorbeeld bij het toepassen van risicotaxatie instrumenten, maar ook bij recruitment waarbij bijvoorbeeld een naam of leeftijd zou kunnen leiden tot discriminatie op afkomst of leeftijd. Een verwerking van gegevens hoort in de lijn der verwachting te liggen van burgers, medewerkers of andere betrokkenen. Zij zouden er niet door moeten worden verrast, zouden zij ervan vernemen.

Of gegevens *toereikend*, *terzake dienend* en *niet-bovenmatig* zijn, kan alleen worden gewogen in relatie tot het doeleinde waarvoor ze zijn verzameld. Het is dus belangrijk het beoogde doeleinde helder voor ogen te hebben. Als politiegegevens worden verwerkt voor het bepalen van een informatiepositie als bedoeld in artikel 10 Wpg kan de uitkomst van deze toets anders zijn dan wanneer politiegegevens worden verwerkt voor een artikel 8 Wpg-verwerking, zoals bijvoorbeeld surveillance op straat. Dit geldt ook voor persoonsgegevens bij AVG-verwerkingen zoals bijvoorbeeld het recruitment- en screeningsproces.⁹ Ook dan moet in gedachten worden gehouden welk doel het verzamelen van de persoonsgegevens dient en wat er in dat verband noodzakelijk is.

De eisen *toereikend*, *terzake dienend* en *niet-bovenmatig* zijn algemeen en ruim geformuleerd. Het betekent aan de ene kant dat er genoeg relevante gegevens moeten zijn. Door onvoldoende gegevens kan een onjuist beeld van een persoon of een situatie ontstaan, terwijl het zorgdragen voor de *juistheid* en *nauwkeurigheid* van gegevens ook een basisnorm is.

Aan de andere kant moet het ook weer niet ‘doorslaan’ door alles maar vast te leggen wat beschikbaar en binnen bereik is. Het is voor de politiemedewerkers een balanceer-act om hier het juiste evenwicht te vinden. Bij het maken van deze afweging kan bijvoorbeeld gekeken worden naar wat maatschappelijk gezien aanvaardbaar wordt geacht.

2.3 Juistheid en nauwkeurigheid

De politie heeft bij het verwerken van politiegegevens een inspanningsverplichting om te voldoen aan het beginsel van *juistheid* en *nauwkeurigheid* uit artikel 4 lid 1 **Wpg**.¹⁰

Het beginsel van *juistheid* en *nauwkeurigheid* moet worden uitgelegd in relatie tot de specifieke kenmerken van het politiewerk. Tijdens een politieonderzoek worden verklaringen afgenomen en vastgelegd die zijn gebaseerd op de subjectieve en niet altijd controleerbare waarneming van een persoon. Dat kan bijvoorbeeld een verklaring zijn van een verdachte of een getuige. Het criterium van juistheid uit het gegevensbeschermingsrecht heeft geen betrekking op de juistheid van een verklaring *zelf*, maar alleen op het feit *dat* een specifieke verklaring is afgelegd.¹¹ De inhoudelijke beoordeling

⁸ Artikel 3 lid 2 Wpg; artikel 5 lid 1 sub a en c AVG.

⁹ Voor de screening van politiemedewerkers gelden niet alleen de AVG-eisen, maar ook de eisen zoals vastgelegd in de artikelen 48q tot en met 48z van de [Politiewet 2012](#) en het bijbehorende [Besluit screening ambtenaren van politie en politie-externen](#).

¹⁰ Zie ook: Tweede Kamer, vergaderjaar 2005-2006, 30 327, nr. 3, p. 32.

¹¹ Zie ook: overweging 30 van [Richtlijn \(EU\) 2016/680](#) van het Europees parlement en de Raad van 27 april

van de juistheid van een verklaring is voorbehouden aan de rechter. Uiteraard moet wel altijd worden gestreefd naar de juistheid van *feitelijke politiegegevens* zoals bijvoorbeeld een naam, adres en woonplaats.

Het correctierecht van een betrokkene houdt direct verband met het beginsel van juistheid.¹² In een zaak over stalking stelde een man dat een melding van stalking en de kwalificatie daarvan *onjuist* was en hij vorderde daarom op grond van de Wpg verwijdering van deze politiegegevens. De hoogste bestuursrechter oordeelde daarop dat het correctierecht niet bedoeld is om *indrukken, meningen en conclusies* waarmee de betrokkene zich niet kan verenigen, te corrigeren of te verwijderen. Als het om correctie van feitelijke politiegegevens gaat, is het aan de betrokkene om aannemelijk te maken dat deze onjuist zijn.¹³ Dat neemt overigens niet weg dat het de verantwoordelijkheid van de politie zelf is actief zorg te dragen voor correcte gegevens. Het is dus niet zo dat de politie slechts reactief, dus naar aanleiding van een rectificatieverzoek van een betrokkene, gegevens hoeft te corrigeren. Uitgangspunt is dat de politie zelf haar registraties op orde houdt.

Het beginsel van juistheid geldt ook in de *keten*. De politie moet als dat *praktisch uitvoerbaar* is de kwaliteit van politiegegevens controleren voordat politiegegevens worden verstrekt. Bij doorzending moet *als dat mogelijk* is noodzakelijke informatie worden toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de juistheid, volledigheid, betrouwbaarheid en actualiteit van de politiegegevens kan beoordelen. Als blijkt dat onjuiste politiegegevens zijn verstrekt, stelt de politie de ontvanger daarvan op de hoogte.¹⁴ De ontvanger moet deze dan rectificeren of vernietigen of de verwerking ervan beperken.¹⁵

Ook voor persoonsgegevens die de politie verwerkt op grond van de **AVG** geldt het beginsel van *juistheid*. Dit staat in artikel 5 lid 1 sub d AVG. Ook hier geldt dat *juistheid* niet los van de context kan worden gezien. Stel dat een politiemedewerker het niet eens is met een beoordeling door zijn leidinggevende. Dan kan deze medewerker niet met een beroep op de AVG zijn beoordeling 'rectificeren' omdat deze onjuist zou zijn. Het doel van de beoordeling is te evalueren wat er goed gaat en wat beter kan. Dergelijke bevindingen zijn geen 'onjuistheden' in de zin van de AVG die achteraf kunnen worden 'gerectificeerd'.¹⁶ Ook hier geldt verder dat de politie altijd moet streven naar de juistheid van feitelijke persoonsgegevens, zoals bijvoorbeeld de naam en leeftijd van een medewerker. Leeftijd kan bijvoorbeeld bepalend zijn voor bepaalde arbeidsvoorwaarden, zoals het aantal vrije dagen.

Als een betrokkene op grond van de AVG de rectificatie van zijn persoonsgegevens heeft verzocht en de politie honoreert dit verzoek, dan moet de politie ook eventuele ontvangers daarvan op de hoogte stellen. Ook hier geldt dus een verantwoordelijkheid voor juistheid van persoonsgegevens in de *keten*.

2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

¹² Artikel 28 lid 1 Wpg.

¹³ Afdeling bestuursrechtspraak van de Raad van State 18 maart 2020, [ECLI:NL:RVS:2020:807](#) rechtsoverweging 4.1.

¹⁴ Artikel 4 lid 4 Wpg.

¹⁵ De Wpg regelt beperking van de verwerking in artikel 28 lid 2. Als de ontvangende partij aan de AVG is onderworpen, zal rectificatie, vernietiging of beperking van de verwerking moeten plaatsvinden overeenkomstig hetgeen de AVG daarover bepaalt.

¹⁶ Zie hiervoor: Hof van Justitie van de EU, 20 december 2017, Nowak, [ECLI:EU:C:2017:994](#), rechtsoverweging 46 tot en met 53.

Voor nadere uitleg van juistheid en nauwkeurigheid, kan inspiratie worden ontleend aan het veel gebruikte Data Management Body of Knowledge model (DAMA DMBOK) dat onder meer gaat over gegevenskwaliteit en gegevensbeveiliging. Aan dit model kan een aantal kenmerken worden ontleend, dat inhoud geeft aan het totaalbegrip juistheid. Het gaat hierbij om correctheid, referentiële integriteit, volledigheid, nauwkeurigheid, aannemelijkheid en validiteit. Een korte uitleg van deze begrippen is opgenomen in het Raamwerk en stappenplan gegevenskwaliteit Strafrechtsketen.¹⁷

2.4 Onderscheid feiten en persoonlijk oordeel

Op basis van artikel 4 lid 3 **Wpg** moeten politiegegevens die op *feiten* zijn gebaseerd voor zover *mogelijk* worden onderscheiden van politiegegevens die op een *persoonlijk oordeel* zijn gebaseerd. Dit voorschrift heeft daarmee het karakter van een inspanningsverplichting.¹⁸ De Wpg en ook het Besluit politiegegevens (Bpg) geven niet aan *hoe* dit moet worden vormgegeven. Dat is ter beoordeling en beslissing van de politie zelf.

Met de woorden *voor zover mogelijk* wordt duidelijk dat het hier *niet* om een absolute verplichting gaat. Dat heeft er mee te maken dat het karakter van politiegegevens gedurende een onderzoek kan wijzigen door nieuwe informatie en inzichten. Politiegegevens waarvan eerst was aangenomen dat deze op een persoonlijk oordeel berusten, kunnen later in een onderzoek van feitelijke aard blijken te zijn en andersom.

Ook moet niet uit het oog worden verloren dat veel politiegegevens niet los van hun context kunnen worden gezien. In een proces verbaal bijvoorbeeld, kunnen op feiten gebaseerde politiegegevens en politiegegevens gebaseerd op een persoonlijk oordeel nauw met elkaar samenhangen. Het onderscheid tussen feiten en persoonlijk oordeel moet dan zoveel mogelijk blijken uit de manier waarop een gebeurtenis is weergegeven, maar je kunt het niet ‘zomaar uit elkaar trekken’.

Het relatieve karakter van dit voorschrift en het feit dat hier dus genuanceerd mee moet worden omgegaan, wordt versterkt door richtlijn 2016/680¹⁹ die aan dit onderscheid geen rechtsgevolgen verbindt.²⁰

2.5 Onderscheid verschillende categorieën betrokkenen

De **Wpg** bepaalt in artikel 6b dat de politie *in voorkomend geval* en *voor zover mogelijk* een duidelijk onderscheid moet maken tussen politiegegevens betreffende verschillende categorieën betrokkenen. Het gaat hier kort gezegd over (i) verdachten, (ii) slachtoffers, (iii) getuigen of andere derden en (iv) veroordeelden. De formulering geeft blijk van een zekere marge van de politie bij de invulling van deze verplichting.²¹ Het voorschrift heeft het karakter van een inspanningsverplichting. Net zoals bij het onderscheid tussen politiegegevens op basis van feiten en persoonlijk oordeel, is het

¹⁷ Het [Raamwerk en stappenplan gegevenskwaliteit Strafrechtsketen](#) van 11 november 2015 heeft mede op basis van dit DMBOK-model de hier genoemde kenmerken benoemd. Zie pagina 9 en pagina 11 van dit Raamwerk.

¹⁸ In het concept voor de Consensusrijkswet voor de Carib in relatie tot -kort gezegd- persoonsgegevens en politiegegevens (en voor commentaar gedeeld met de politie), die aanhaakt op de AVG, Wpg en Wjsg, wordt ook aangegeven dat deze verplichting als een inspanningsverplichting moet worden gezien.

¹⁹ [Richtlijn \(EU\) 2016/680](#) van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

²⁰ Zie ook: [Tweede kamer, vergaderjaar 2017-2018, 34 889, nr.3](#), p. 63; zie voorts: Tekst en Commentaar Privacy- en gegevensbeschermingsrecht onder redactie van G.J. Zwenne en H.R. Kranenborg, 7^e druk, p. 413.

²¹ Zie: [Tweede kamer, vergaderjaar 2017-2018, 34 889, nr.3](#), p. 66.

onderscheid tussen de verschillende categorieën van betrokkenen relatief. Zo kan de status van personen in de loop van een onderzoek veranderen. Iemand die zich eerst als getuige heeft aangediend, kan later transformeren tot verdachte en andersom.

Ook is het mogelijk dat één persoon, meerdere hoedanigheden heeft. Stel dat bij een voorval meneer A mevrouw B slaat en mevrouw B slaat meneer A en vervolgens zijn vriendin mevrouw C, die op haar beurt meneer A weer een klap verkoopt: in een dergelijke casus kan één persoon meerdere rollen hebben, zoals verdachte, slachtoffer en getuige.

Het maken van onderscheid tussen de verschillende categorieën betrokkenen mag overigens geen afbreuk doen aan de onschuldpresumptie zoals gewaarborgd in het Europees handvest en het EVRM.²²

2.6 Verwijderen, bewaren en vernietigen

2.6.1 Wpg

Onjuiste politiegegevens moeten onverwijld worden vernietigd (of gerectificeerd).²³ Dat sluit aan bij het beginsel dat politiegegevens juist en nauwkeurig moeten zijn. Verder moeten politiegegevens worden verwijderd of vernietigd als zij niet langer noodzakelijk zijn voor het doel waarvoor ze worden verwerkt of als dit door een wettelijke bepaling wordt vereist.²⁴ Politiegegevens moeten in ieder geval worden vernietigd na afloop van de bewaartermijn genoemd in artikel 14 Wpg.²⁵ Het is echter ook mogelijk dat politiegegevens niet worden vernietigd maar worden overgebracht naar een archiefbewaarplaats, bijvoorbeeld als ze onderdeel zijn van cultureel erfgoed of ten behoeve van historisch onderzoek.

De principes voor verwijderen en vernietigen van politiegegevens lijken redelijk overzichtelijk. Maar de uitwerking is minder eenvoudig. Niet alleen de Wpg en het Bpg zijn van belang, verschillende wettelijke bepalingen en uitvoeringsregelingen vormen gezamenlijk het kader voor het verwijderen en vernietigen van politiegegevens. Ook het Wetboek van Strafvordering, het Wetboek van Strafrecht, de Wet justitiële en strafvorderlijke gegevens en de Archiefwet 1995 zijn relevant. Om politiegegevens tijdig te verwijderen en te vernietigen moeten al deze wetten in onderlinge samenhang worden gezien.

De politie geeft in het *Beleid Bewaartermijnen* het juridisch kader voor deze wettelijke regelingen en hoe zij zich tot elkaar verhouden.²⁶ Ook gaat het *Beleid Bewaartermijnen* in op de vertaling van deze regels naar de uitvoeringspraktijk. Verder is van belang dat de geldende bewaartermijnen zoals die voortkomen uit de verschillende wettelijke regelingen samenkomen in de *Generieke selectielijst voor de informatie van de politie*.²⁷

Hierbij moet er overigens ook oog voor zijn dat maatschappelijk en politiek gemotiveerde omstandigheden impact kunnen hebben op bewaarbeleid. Zo heeft de korpschef in verband met de opsporing van *cold cases* besloten niet standaard alle politiegegevens te vernietigen na het verstrijken van de huidige bewaartermijn op grond van de Wpg. De Minister van J&V schrijft in zijn brief aan de Tweede Kamer van 4 februari 2019 achter deze keuze van de korpschef te staan.²⁸ Er zijn

²² Artikel 48 [Europees Handvest](#), artikel 6 lid 2 [EVRM](#); zie ook overweging 31 van [Richtlijn \(EU\) 2016/680](#).

²³ Artikel 4 lid 1 Wpg.

²⁴ Artikel 4 lid 2 Wpg.

²⁵ Artikel 14 ziet op politiegegevens die op grond van artikel 8, 9 en 10 Wpg zijn verwijderd, vervolgens nog vijf jaar worden bewaard en dan worden vernietigd. Bepalingen over bewaartermijnen van artikel 12 en 13 Wpg gegevens worden gegeven in die artikelen zelf.

²⁶ *Beleid bewaartermijnen*, 13 februari 2020, versie 1.0, vastgesteld door BBVO (Lid Korpsleiding).

²⁷ Staatscourant 2020, nr. 26744.

²⁸ [Kst-29628-859](#), brief van de Minister van Justitie en Veiligheid aan de Tweede Kamer, d.d. 4 februari 2019.

vanuit de politie inmiddels wel gesprekken gaande met het ministerie van J&V over nieuwe wetgeving met langere bewaartermijnen om recht te doen aan de belangen van *cold case* zaken.

2.6.2 AVG

De AVG geeft in tegenstelling tot de Wpg geen specifieke bewaartermijnen. Artikel 5 van de AVG bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld.

De politie moet daarom aan de hand van het criterium *niet langer bewaren dan noodzakelijk voor de doeleinden* zelf concrete bewaartermijnen bepalen voor de diverse categorieën persoonsgegevens. Bij het bepalen van deze *maximum bewaartermijnen* voor persoonsgegevens, moeten wél de eventuele toepasselijke wettelijke *minimum bewaartermijnen* in acht worden genomen. Er staan *minimum bewaartermijnen* in andere wetten dan de AVG, zoals fiscale wetten en wetten op het gebied van arbeidsomstandigheden. Denk bijvoorbeeld aan de minimale fiscale bewaartermijn van 7 jaar voor salarisgegevens.

De politie geeft in het *Beleid Bewaartermijnen* ook het juridisch kader voor het bepalen van de AVG-bewaartermijnen en de vertaling daarvan naar de praktijk. De bewaartermijnen die de politie heeft bepaald voor de verschillende categorieën van persoonsgegevens zijn te vinden in de *Generieke selectielijst voor de informatie van de politie*.²⁹ Een voorbeeld is de termijn voor persoonsgegevens voor werving en selectie voor afgewezen kandidaten: hiervoor geldt dat de politie één maand na einde van de procedure de persoonsgegevens vernietigt, wat kan worden verlengd tot één jaar, maar alleen als de afgewezen kandidaat daarvoor toestemming heeft gegeven.

²⁹ Staatscourant 2020, nr. 26744.

3 Maatregelen en initiatieven ter borging kwaliteit

3.1 Datastrategie IV

3.1.1 Datastrategie politie 2022-2025

De *Datastrategie politie 2022-2025*, 'Data voor veiligheid' beschrijft dat politiewerk meer en meer datagedreven wordt: politiewerk is mensenwerk met data.³⁰ De Datastrategie beweegt zich binnen de contouren van relevante wet- en regelgeving zoals de AVG, Wpg en de Wet open overheid (Woo) en heeft oog voor de ethische aspecten van gegevensgebruik.

Eén van de speerpunten van de Datastrategie is een *professionele organisatie*. Politiewerk is mensenwerk met data als essentieel bedrijfsmiddel. Goede verwerking, goed beheer en vindbaarheid van gegevens zijn vaak het verschil tussen succes en falen van de individuele collega en de organisatie als geheel.³¹

Een ander belangrijk speerpunt is het creëren van een *optimale gegevenshuishouding*. Dit speerpunt sluit aan bij één van de vier ambities die de politie uitspreekt in de *IV-strategie voor 2022-2025*.³² Onderdeel van de ambitie *data gedreven politiewerk* is het waar mogelijk loskoppelen van data en systemen, het eenmalig vastleggen van data en veilige ontsluiting daarvan aan de gebruiker.

Het [Programma Datagedreven Samen Werken](#) sluit aan op de Datastrategie. Het Programma is de katalysator voor de ambitie van de politie om -met haar partners- in 2028 haar taak op handhaving van de rechtsorde en hulpverlening slagvaardiger en efficiënter met behulp van data te realiseren. Onderdeel van de doelstellingen van het Programma is een optimale gegevenshuishouding en het toetsbaar voldoen van datagedreven werken aan wettelijke eisen en interne regelgeving.³³

3.1.2 Relatie Datastrategie tot kwaliteitsnormen Wpg en AVG

De Datastrategie legt met een beschrijving van de *optimale gegevenshuishouding* een *fundament voor datakwaliteit* binnen de politie. Een optimale gegevenshuishouding vormt de basis voor het kunnen voldoen aan de kwaliteitsnormen als weergegeven in hoofdstuk 2 van dit document.

Onderdelen van een *optimale gegevenshuishouding* zijn volgens de Datastrategie onder meer:

- datacentrisme;
- het inrichten van processen via het CSAE-model (collect, store, analyse, engage);³⁴

³⁰ [Datastrategie politie 2022-2025](#), 'Data voor veiligheid', oktober 2022, definitief-v1.0. Hierin wordt datagedreven werken omschreven als: "Datagedreven werken is werken op basis van feiten, die verzameld worden in de vorm van data, geanalyseerd worden naar informatie, samen met domeinkennis op de juiste manier geïnterpreteerd worden naar bruikbare inzichten, en om op basis van deze inzichten een zo geïnformeerd mogelijk besluit te nemen."

³¹ [Datastrategie politie 2022-2025](#), 'Data voor veiligheid', oktober 2022, definitief-v1.0. p. 10, hier wordt het speerpunt *Professionele organisatie* nader toegelicht.

³² IV-Strategie Politie 2022-2025, werken aan de IV voor het politiewerk van morgen, 'Sneller, Simpel en Samen', april 2022, versie 1.0.

³³ Programma Datagedreven Samen Werken, Doelenboom – januari 2024.

³⁴ Uit de bijdrage van dr. mr. Erik H.A. van de Sandt aan de deskundigenbijeenkomst WG AI van de Eerste Kamer: *De noodzaak van omvattende raamwerken voor begrip van, én grip op, datagedreven werken: (...) In de Collect-fase wordt ruwe data verzameld, in Store wordt de verzamelde data genormaliseerd en opgeslagen als informatie, in Analyze worden relevante informatiepunten bij elkaar gebracht tot clusters en kennis hierover*

- het onderscheiden van data naar bron en soort;
- het creëren van een *chain of evidence* door metagegevens te koppelen aan informatieobjecten zodat zicht bestaat op *de zeven gouden w's van data*;³⁵
- het ontwikkelen van gerichte toepassingen die zorgen dat data vindbaar, toegankelijk, uitwisselbaar en herbruikbaar is.

Voor een gedetailleerde beschrijving van de elementen van een optimale gegevenshuishouding wordt verwezen naar hoofdstuk 4 van de Datastrategie.³⁶ Eén van de in dit verband lopende initiatieven is het project *Open op Orde*, met als opdracht de informatiehuishouding versneld op orde te brengen.³⁷

3.2 Data-, privacy-, en duto-governance

Bij het voldoen aan taken en verplichtingen binnen een organisatie, moet helderheid bestaan over *wie*, *waarvoor* verantwoordelijk is en hoe hiërarchische structuren en overlegstructuren vorm krijgen. Dat geldt ook in relatie tot het naleven van kwaliteitsnormen voor gegevens binnen de politie.

In 2024 geeft de politie daarom vol gas op het nader inrichten en implementeren van zowel een *privacygovernance* als een *datagovernance*.³⁸ In dit Kwaliteitshandboek kan op die ontwikkeling nog niet vooruit worden gelopen. Op het gebied van duurzame toegankelijkheid (duto) is de governance geregeld en vastgelegd in de Beheerregeling DI Politie 2017.³⁹

3.3 Privacy en security en duurzame toegankelijkheid by Design (PSDbD)

3.3.1 PSDbD

De politie hanteert voor geautomatiseerde systemen de principes van privacy en security by design en default.⁴⁰ Ook duurzame toegankelijkheid van informatie is hierbij van belang.⁴¹ Volgens deze principes wordt de goede omgang met persoonsgegevens en politiegegevens en de duurzame toegankelijkheid daarvan zo veel mogelijk in de werking van de technologie zelf geborgd. Het *Beleidskader & principes PSD by design* van de politie geeft hiervoor de basis door de wettelijke eisen verder uit te werken.⁴²

Het *Beleidskader & principes PSD by design* formuleert acht principes voor het beheer en de bescherming van persoonsgegevens en politiegegevens. Het gaat om (i) enkelvoudige vastlegging, (ii) structuur en kenmerken, (iii) duurzame toegankelijkheid, (iv) kwaliteit, (v) informatiebeveiliging,

verwerkt tot intelligence, en in **Engage** wordt deze intelligence uitgelopen totdat er interventies kunnen worden uitgevoerd die gebaseerd zijn op feiten.(...).

³⁵ De zeven W's van data: (i) Wie is verantwoordelijk en wie heeft gewijzigd, gecreëerd, etc.; (ii) Wat is het beveiligingsniveau; (iii) Waar bevindt het zich en waar komt het vandaan; (iv) Waarmee controleren we de integriteit; (v) Op welke wijze zijn de gegevens getransformeerd; (vi) Wanneer zijn de gegevens gecreëerd en wanneer worden ze verwijderd, vernietigd of gearhiveerd; (vii) Waarom hebben we deze gegevens(grondslag).

³⁶ Zie voor een verdere toelichting van het speerpunt 'optimale gegevenshuishouding', pagina 10 t/m 12 van de Datastrategie politie 2022-2025, 'Data voor veiligheid', oktober 2022, definitief-v1.0.

³⁷ Open op Orde politie, veranderopgave 2021-2026, directie FM, afdeling services, team DIV kwartiermaker programma Open op Orde, definitief, versie 1.0, versie datum 22 juni 2021.

³⁸ De privacygovernance, voorstel tot verbetering, versie 1.0, 29 januari 2024, kenmerk 2024-0006312.

³⁹ Regeling van de korpschef van de politie van 20 september 2017, nummer 001, houdende beheersregels voor de documentaire informatie ([Beheerregeling DI Politie 2017](#)), stcrt. 2017 nr. 56416, 9 oktober 2017.

⁴⁰ Artikel 4a Wpg en artikel 25 AVG.

⁴¹ Duurzame toegankelijkheid van informatie wordt vaak afgekort tot DUTO. Onder DUTO wordt verstaan dat informatie vindbaar, beschikbaar, leesbaar, interpreteerbaar, toekomstbestendig en betrouwbaar moet zijn.

⁴² Beleidskader en principes PSD by design, versie 3.0, versiedatum 1 november 2021, p. 22- 63.

(vi) doelbinding, (vii) privacy by default en (viii) verantwoording. Het *Beleidskader & principes PSD by design* geeft een uitgebreide toelichting op deze principes. De *Toolkits PSD by design* vertalen deze algemene principes in een aanpak voor de uitvoeringspraktijk, zoals concrete instructies voor architecten, product owners en ontwikkelteams die zijn betrokken bij het ontwikkelen van nieuwe systemen voor de politie.⁴³

PSD by design heeft de krachtigste uitwerking als er vanaf het begin rekening mee wordt gehouden. Bij de aanschaf en ontwikkeling van nieuwe systemen of de aanpassing van bestaande systemen liggen de ontwerpkeuzes nog niet vast en zijn aanpassingen op de beoogde systemen en de bijbehorende werkprocessen vaak nog mogelijk. Het achteraf aanpassen van systemen en werkprocessen blijkt in de praktijk veelal zeer complex en kostbaar. Dat geldt bijvoorbeeld voor bepaalde onderdelen van *legacy systemen* van de politie die al lange tijd in gebruik zijn, zoals BVH en SumMIT. Daarom is het belangrijk bij de start van een initiatief voor de ontwikkeling of aanschaf van een geautomatiseerd systeem hieraan aandacht te besteden. Op dat moment kan het verschil nog worden gemaakt. Het Programma Vernieuwend Registreren (PVR) dat met de ontwikkeling van RAPP⁴⁴ uiteindelijk moet leiden tot vervanging van BVH en SumMIT heeft de PSDbD principes verankerd in zijn aanpak.

3.3.2 Relatie PSDbD tot kwaliteitsnormen

Door toepassing van PSDbD principes, neemt een systeem de politiemedewerker zoveel mogelijk aan de hand om een registratie *juist* en *nauwkeurig* te verrichten. Bijvoorbeeld door onvolledigheden of onvolkomenheden in een registratie te ‘flaggen’. Andere voorbeelden zijn het beperken van vrije invulvelden, het gebruik van *drop-down* velden en het uitsluitend kunnen afsluiten van een registratie indien bepaalde noodzakelijke velden juist en volledig zijn ingevuld.

In politiesystemen kunnen PSDbD principes eraan bijdragen dat een goede aansluiting op de *basisregistraties* plaatsvindt.⁴⁵

De mogelijkheden om door toepassing van PSDbD principes het onderscheid tussen *feiten* en *persoonlijk oordeel* te faciliteren, zijn redelijk beperkt. Dat blijft uiteindelijk mensenwerk.

Bedacht moet worden dat rekening houdend met de bron en het soort politiegegevens, bepaalde politiegegevens *naar hun aard al feitelijk van karakter zijn*. Politiegegevens uit *sensoren*, zoals allerlei vormen van camerabeelden, zijn gezien hun wezen feitelijk van aard.⁴⁶ Dat geldt ook voor politiegegevens onttrokken aan één van de tien *basisregistraties*.

Bij politiegegevens ingegeven in de registratieve politiesystemen zoals BVH en SumMIT kan zowel sprake zijn van politiegegevens op basis van *feiten* als politiegegevens op basis van een *persoonlijk oordeel* en zullen deze van elkaar moeten zijn te onderscheiden, voor zover dat mogelijk is. Daarbij moet wel rekening worden gehouden met de complexiteit en de nuances van de praktijk van alle dag, waarin het onderscheid tussen feit en persoonlijk oordeel soms verschuift. Van een waarneming die eerst persoonlijk van aard leek, kan in een later stadium vast komen te staan dat het om een feit gaat en andersom. Een systeem moet dan de flexibiliteit hebben om met deze verandering van kleur om te gaan.

Ook komt het veel voor dat *feiten* en *persoonlijke waarneming* onlosmakelijk met elkaar zijn verbonden. Denk bijvoorbeeld aan de weergave van een geweldsincident in een proces-verbaal.

⁴³ De Toolkits PSD by design zijn al grotendeels ontwikkeld; afronding van de Toolkits wordt verwacht in 2024.

⁴⁴ RAPP staat voor: Registratieve Registratie Politie Processen.

⁴⁵ Zie voor uitleg over basisregistraties paragraaf 3.6.1.

⁴⁶ Het *duiden* van deze gegevens kan uiteraard wel gekleurd worden door een persoonlijk oordeel.

Veelal zal de oplossing daarom moeten worden gezocht in de context van de betreffende politiegegevens en de wijze waarop deze zijn geformuleerd. Bijvoorbeeld door in een proces-verbaal expliciet weer te geven als sprake is van een persoonlijk oordeel.⁴⁷ Wel is het zo dat RAPP politiemedewerkers hierbij in de toekomst tot op zekere hoogte zal ondersteunen, bijvoorbeeld door het laten zien van pop-ups die aandacht vragen voor het maken van dit onderscheid.

Op het onderscheiden van de verschillende categorieën betrokkenen, te weten *verdachte*, *slachtoffer*, *getuige* of *veroordeelde* zoals voorgeschreven in artikel 6b Wpg, kan een registratief systeem ook worden ingericht.⁴⁸ Dit gebeurt -hoewel nog niet altijd vlekkeloos- in de huidige registratieve politiesystemen en wordt in RAPP verder vervolmaakt doordat aan personen een rol moet worden 'gehangen'. Het biedt daarmee een helpende hand aan een politiemedewerker die mutaties verricht in de politiesystemen. Daarbij wordt er rekening mee gehouden dat niet altijd sprake is van een absoluut onderscheid omdat bijvoorbeeld een verdachte gedurende een opsporingsonderzoek tot getuige kan transformeren en andersom.⁴⁹

Het Expertisecentrum Privacy (ECP) draagt in belangrijke mate bij aan het implementeren van privacy by design in het IV-voortbrengingsproces door deel te nemen aan het Readiness-traject van het IV Control Framework. Voorafgaand aan de initiatie van een IV-project beoordeelt het ECP of voldoende rekening wordt gehouden met de privacyrisico's die kunnen ontstaan bij de inrichting en ingebruikname van projectproducten waarmee persoons- en politiegegevens kunnen worden verwerkt.

3.4 Metadata in relatie tot datakwaliteit

Metadata zijn nodig om van data betekenisvolle informatie te maken. Het gaat in feite om '*data over data*'. Daarmee wordt bedoeld dat metadata de eigenschappen en kenmerken van andere data weergeven. Metadata zijn onmisbaar voor de ontsluiting en het beheer van andere data. Een voorbeeld is de datum en het tijdstip (*timestamp*) waarop een mutatie werd gemaakt.

In het *Ontwerpkader toepassingsprofiel metagegevens politie (TMP)*, zijn onder meer beleidsregels opgenomen voor het toepassen van metadata.⁵⁰ Hierin is te lezen dat metadata meerdere doelen kunnen dienen. Eén van deze doelen is om de politie in staat te stellen aan de eisen van de Wpg en AVG te voldoen. Zo kunnen metagegevens bijvoorbeeld duiden voor welk doeleinde een politiegegeven wordt verwerkt (bijv. artikel 8 Wpg of artikel 9 Wpg) en de registratiedatum vastleggen, zodat deze informatie kan worden gebruikt voor het beheren van de verwerkings-, verwijderings- en vernietigingstermijnen van politiegegevens. Dit geldt ook voor AVG-gegevens, waarbij aan een persoonsgegeven metadata kunnen worden gehangen zoals bijvoorbeeld een timestamp of een AVG-verwerkingsgrondslag.⁵¹

Metadata zijn dus essentieel voor de kwaliteit van gegevens. Dat geldt ook specifiek in relatie tot de *juistheid* en *nauwkeurigheid* van gegevens. Metagegevens zijn onmisbaar om de authenticiteit van gegevens vast te stellen, omdat zij vertellen waar informatie vandaan komt en wie het gemaakt, aangepast of gebruikt heeft. Ook geven ze op die manier hulp bij het beoordelen van de betrouwbaarheid van gegevens.

⁴⁷ Zie ook: Naleving Wet politiegegevens, Audit naar bestaan en werking, vierde cyclus, periode 2019 t/m 2022, p. 60.

⁴⁸ NB: de politiesystemen onderscheiden nog meer rollen dan de vier die de Wpg noemt.

⁴⁹ Zie hiervoor ook de nadere uitleg in paragraaf 2.5.

⁵⁰ Zie: Ontwerpkader toepassingsprofiel metagegevens politie, 29 september 2016, vs. 1.1. Het ontwerpkader zal t.z.t. vervangen worden door het MDTO (Metagegevens Duurzaam Toegankelijke Overheidsinformatie).

⁵¹ De verwerkingsgrondslagen uit de AVG staan in artikel 6 sub a tot en met f.

3.5 Gegevensbeschermingseffectbeoordeling (GEB)

3.5.1 Uitvoering GEB

Voordat een nieuw geautomatiseerd systeem of een belangrijke wijziging op een bestaand geautomatiseerd systeem in gebruik wordt genomen, bekijkt de politie of een *GEB* moet worden uitgevoerd.⁵² Dit is aan de orde als sprake is van een *hoog risico* voor de rechten en vrijheden van betrokkenen. Dat zijn degenen van wie politiegegevens of persoonsgegevens worden verwerkt, zoals burgers of politiemedewerkers. Het *Beleidskader registerplicht en GEB* geeft richtlijnen voor het uitvoeren van een GEB.

De politie hanteert standaardmodellen voor het opstellen van een GEB. Een GEB bestaat in principe uit vijf hoofdonderdelen: (i) een managementsamenvatting, (ii) een samenvatting van het advies van de functionaris gegevensbescherming (FG), (iii) een beschrijving van de gegevensverwerking, (iv) een beoordeling van de rechtmatigheid van de gegevensverwerking en (v) de risico's en de maatregelen om de risico's weg te nemen of te beperken.

Over de in een GEB voorgestelde risico mitigerende maatregelen dient besluitvorming plaats te vinden. Maatregelen die niet geïmplementeerd worden, moeten als restrisico worden geaccepteerd. Als risico's echter onvoldoende kunnen worden weggenomen of beperkt en daarmee een *hoog risico* blijft bestaan, dan moet de politie de Autoriteit Persoonsgegevens (AP) raadplegen vóór de start van de voorgenomen gegevensverwerking. Dit is zowel een Wpg- als AVG-verplichting.⁵³ Als een *voorafgaande raadpleging* moet plaatsvinden, wordt de Gegevensautoriteit hierover tijdig geïnformeerd en kan de Gegevensautoriteit hierbij desgewenst adviseren.

De implementatie van de maatregelen en de besluitvorming over restrisico's moet goed worden gedocumenteerd, bij voorkeur in een risicomanagementsysteem.

3.5.2 Relatie GEB tot kwaliteitsnormen

Een belangrijk onderdeel van een GEB bij het onderzoeken van de privacyrisico's is het toetsen of de beoogde gegevensverwerking *noodzakelijk* is.

Zoals beschreven in paragraaf 2.1 van dit document krijgt het noodzakelijkheidscriterium nadere invulling door de vereisten van *proportionaliteit* en *subsidiariteit*. Een GEB hoort antwoord te geven op de vraag of de beoogde gegevensverwerking zoals in de GEB is beschreven proportioneel is in relatie tot het doel en of er geen minder ingrijpende middelen zijn te bedenken om het doel te bereiken.

Stel bijvoorbeeld dat de politie een nieuw camerasysteem gaat ontwikkelen, dan kan in de GEB worden onderzocht of de daarmee gemaakte beelden noodzakelijk zijn voor het doel waarvoor het wordt aangeschaft. Privacyrisico's kunnen dan bijvoorbeeld worden beperkt door beelden die niet noodzakelijk zijn direct te verwijderen of deze onherkenbaar te maken door ze te 'blurren'.

Een GEB wordt in principe uitgevoerd vóórdat met een bepaalde gegevensverwerking wordt gestart. Als juist op dat moment al een toets op noodzakelijkheid, proportionaliteit en subsidiariteit plaatsvindt, dan kan dat in belangrijke mate bijdragen aan het borgen van de Wpg en AVG kwaliteitsnormen. Belangrijk is wie verantwoordelijk is voor de opvolging van GEB-bevindingen, de besluitvorming daarover, de implementatie van de maatregelen en de acceptatie van eventuele restrisico's. Dit en andere facetten zullen nog verder ingekleurd moeten worden.⁵⁴

⁵² Artikel 35 AVG en artikel 4c Wpg. Een GEB wordt vaak Data Protection Impact Assessment (DPIA) genoemd.

⁵³ Artikel 33b Wpg en artikel 36 AVG.

⁵⁴ Voor 2024 staat op de agenda dat het Beleidskader registerplicht en GEB (versie 2.0, versiedatum 8 november 2019) wordt vernieuwd. Daarin moet dit worden meegenomen.

3.6 Basisregistraties en generieke gegevensdiensten

3.6.1 Tien basisregistraties

De politie maakt bij de uitvoering van haar politietaak gebruik van basisregistraties. Een basisregistratie is een door de overheid officieel aangewezen registratie met daarin data van hoogwaardige kwaliteit, die door alle overheidsinstellingen worden gebruikt bij de uitvoering van hun taken. Er zijn 10 basisregistraties:

- [BRP](#) – Basisregistratie personen (bestaat uit ingezetenen en niet-ingezetenen)
- [HR](#) – Handelsregister
- [BAG](#) – Basisregistratie Adressen en Gebouwen
- [BRT](#) – Basisregistratie Topografie
- [BRK](#) – Basisregistratie Kadaster
- [BRV](#) – Basisregistratie Voertuigen (kentekenregister)
- [BRI](#) – Basisregistratie Inkomen
- [WOZ](#) – Basisregistratie Waarde Onroerende Zaken
- [BGT](#) – Basisregistratie Grootschalige Topografie (voorheen GBKN)
- [BRO](#) – Basisregistratie Ondergrond

Deze 10 basisregistraties zijn onderdeel van het [Stelsel van Basisregistraties](#). Stelselvoorzieningen vergemakkelijken de data-uitwisseling tussen de basisregistraties onderling en waarborgen de *juistheid* van data. Door digitale koppelingen met de basisregistraties kan de politie data uit de basisregistraties afnemen.

Een basisregistratie moet aan [twaalf eisen](#) voldoen. Deze eisen zijn in 2003 geformuleerd in het kader van het Actieprogramma Elektronische Overheid. Een aantal belangrijke vereisten is: de registratie is bij wet geregeld, de basisregistratie wordt door de hele overheid gebruikt en er is een *streng regime voor kwaliteitsborging*.

3.6.2 Relatie basisregistraties tot kwaliteitsnormen

De politie gebruikt data uit de basisregistraties bij de uitvoering van de politietaak. Dit borgt zoveel mogelijk de *juistheid* en de *nauwkeurigheid* van de politiegegevens zoals bedoeld in artikel 4 lid 1 **Wpg**, omdat unieke bronnen met authentieke data van hoge kwaliteit worden gebruikt als input voor registraties door de politie.

Verder geldt dat politiegegevens ontleend aan de basisregistraties als vanzelf als een *feit* kwalificeren en niet als een persoonlijk oordeel. Artikel 4 lid 3 Wpg stelt het verplicht dit onderscheid te maken. Velden in politiesystemen die op basis van de basisregistraties zijn gevuld, zijn dus als *feit* aan te merken.

Voor de Basisregistratie personen (BRP) is van groot belang voor de operatie. Hieraan worden data ontleend zoals BSN, voornamen, achternaam, voorvoegsel achternaam, geboortedatum, geboorteplaats, geboorteland, geslachtsaanduiding, nationaliteit, huwelijkse staat en geregistreerd partnerschap, woonplaats, straatnaam, huisnummer en postcode.

De politie heeft autorisaties voor de geautomatiseerde systematische verstrekking van data uit de BRP in verband met de uitvoering van de politietaak. Systematische verstrekking vindt plaats op basis van

een besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.⁵⁵ In een besluit staat welke data over welke categorieën van personen en in welke gevallen aan de politie worden verstrekt. Grofweg kan hierbij onderscheid worden gemaakt tussen *spontane verstrekking* aan de politie op basis van een *afnemersindicatie* en verstrekking van data *op verzoek* van de politie. Spontane verstrekking op basis van een afnemersindicatie houdt in dat als er nieuwe informatie is, de politie ongevraagd en automatisch een update uit de BRP ontvangt ten aanzien van personen die al in de politiesystemen staan. Verstrekking op verzoek vindt bijvoorbeeld plaats via een applicatie op Mobiel Effectief Op Straat (MEOS) waarmee een politiemedewerker de BRP in een concreet geval rechtstreeks kan raadplegen.

In 2020 is een *Beleid op afnemersindicaties* ontwikkeld, dat als uitgangspunt hanteert dat een afnemersindicatie niet voor alle personen vermeld in de politiesystemen wordt geplaatst, maar uitsluitend ten aanzien van categorieën personen voor wie het actueel houden van hun politiegegevens extra belangrijk is, zoals verdachten of personen met een risicoclassificatie. Dit om ook recht te doen aan het beginsel van *noodzakelijkheid*, dat is uitgelegd in hoofdstuk 2 van dit document. Het *Beleid op afnemersindicaties* is toentertijd niet formeel vastgesteld, maar in 2024 worden stappen gezet dit beleid aan te passen aan de laatste ontwikkelingen en inzichten en alsnog te formaliseren en daarna te implementeren.

De politie kan de BRP ook raadplegen in verband met het uitvoeren van het vreemdelingentoezicht. De verwerking van deze data valt onder het **AVG**-regime. Ook voor *politiebetrouwbaarheidsonderzoeken*, het screenen dus van politiemedewerkers en externen die bij de politie (gaan) werken, kan de BRP worden geraadpleegd.⁵⁶ Ook dit valt onder de **AVG**.

3.6.3 Generieke ketenvoorzieningen

Net als bij het gebruik van basisregistraties, vermindert het gebruik van zogenoemde *generieke ketenvoorzieningen* de kans op onjuistheden in de gebruikte data, omdat data ontleend wordt aan één generieke databron die door meerdere partijen wordt gebruikt. Voorbeelden van generieke ketenvoorzieningen zijn de strafrechtketendatabank (SKDB) en het Justitieel Documentatie Systeem (JD-Online).⁵⁷

3.7 Ketenkwaliteit

3.7.1 Netwerk Datakwaliteit (NDK)

De politie is deelnemer van het Netwerk Datakwaliteit (NDK). Het NDK is een samenwerkingsverband van ketenpartners in de strafrechtsketen. Het richt zich op het oplossen van datakwaliteit-issues in het berichtenverkeer tussen ketenpartners. De samenwerking vindt plaats op basis van een jaarplan met geprioriteerde *user stories*. Andere ketendeelnemers zijn het Openbaar Ministerie (OM), de rechtspraak, het Centraal Justitieel Incasso Bureau (CJIB), Dienst Justitiële Inrichtingen (DJI), Justid, Raad voor de Kinderbescherming (RvdK) en 3 reclasseringsorganisaties (3RO). Verder is de politie in het NDK tevens de liaison voor de bijzondere opsporingsdiensten. Het NDK valt onder het Duurzaam Digitaal Stelsel (DDS) dat per 1 januari 2023 van start is gegaan.⁵⁸

⁵⁵ Besluit van de Rijksdienst voor Identiteitsgegevens inzake de autorisatie voor systematische verstrekking i.v.m. de uitvoering van politietaken d.d. 23 januari 2020, kenmerk 2020-0000007356; Besluit van de Rijksdienst voor Identiteitsgegevens inzake de autorisatie voor systematische verstrekking i.v.m. de uitvoering van politietaken d.d. 25 november 2020, kenmerk 2020-0000630287; Besluit van de Rijksdienst voor Identiteitsgegevens inzake de autorisatie voor systematische verstrekking i.v.m. de uitvoering van politietaken d.d. 25 november 2020, kenmerk 2020-0000630531.

⁵⁶ Autorisatiebesluit voor de korpschef van de politie, Rijksdienst voor Identiteitsgegevens, 24 april 2023, Staatscourant 2023 nr. 27579 – 17 oktober 2023.

⁵⁷ Zie ook: Beleidskader PSD by Design, versie 3.0 (2021), p. 25.

⁵⁸ Zie ook: [Ministerie van Justitie en Veiligheid, Departementaal Informatieplan 2024-2027](#), p. 9.

3.7.2 Relatie NDK tot kwaliteitsnormen Wpg

Het Wpg-beginsel van *juistheid* geldt ook voor de *keten*, zoals toegelicht in paragraaf 2.3 van dit document. Het NDK is in het leven geroepen, omdat binnen de strafrechtketen datakwaliteit continu aandacht verdient. De politie is uiteraard een belangrijk onderdeel van de strafrechtketen. Als data in systemen van ketenorganisaties onvolledig, inconsistent of onjuist zijn of niet tijdig worden aangeleverd, dan zouden professionals in de strafrechtketen verkeerde beslissingen kunnen nemen met mogelijk verstrekking gevolgen voor de samenleving en burgers.

Via het NDK werken specialisten, waaronder specialisten van de politie, nauw samen om data-gerelateerde issues in en tussen de informatiesystemen in de strafrechtketen op te lossen. Deze issues komen in beeld bij door NDK uitgevoerde bestandsvergelijkingen en door meldingen van gebruikers. Met de doorgevoerde verbeteringen, wordt de datakwaliteit in de keten verhoogd en worden fouten opgelost en in de toekomst voorkomen.

3.7.3 Terugmeldplicht BRP

De zogenaamde *terugmeldplicht* voor de basisregistratie personen is geregeld in de Wet basisregistratie personen (Wet BRP), het Besluit basisregistratie personen (Besluit BRP) en in het Bpg.⁵⁹ Voor de politie betekent dit dat zij melding doet aan het college van burgemeester en wethouders als zij afwijkingen signaleert tussen data die zij uit de BRP ontvangt en data die haar uit eigen of andere bronnen bekend zijn. Dat geldt ook bij *twijfel* over de juistheid van de uit de BRP ontvangen data.

Op deze manier draagt de politie bij aan de verhoging van de datakwaliteit van data in de basisregistratie personen. Van deze '*kwaliteitsimpuls*' profiteert de politie zelf ook weer bij volgende raadplegingen, omdat het bijdraagt aan de *juistheid* en *nauwkeurigheid*.

De terugmeldplicht is wettelijk geregeld in artikel 2:34 Wet BRP en artikel 27 van het Besluit BRP. De daaruit voortvloeiende verstrekking is geregeld in artikel 4:2 lid 4 Bpg.⁶⁰ Daarin staat dat politiegegevens in verband met de terugmeldplicht *kunnen* worden verstrekt. Dit lijkt ruimte te geven voor enige afweging, zoals het achterwege laten van een terugmelding als opsporingsbelangen zich daartegen verzetten. De hoofdregel is echter dat terugmelding dient plaats te vinden. In de praktijk gebeurt dit nog beperkt, hetgeen heeft geleid tot de pilot *Makkelijk Melden* in 2023. De resultaten van de pilot waren positief. Er dient gekeken te worden hoe hieraan verdere opvolging wordt gegeven.

3.8 Artificial intelligence (AI)

Artificial Intelligence (AI) maakt een stormachtige ontwikkeling door. De politie volgt deze ontwikkeling op de voet en brengt in kaart op welke wijze AI kan ondersteunen bij het uitvoeren van de politietaken. De politie heeft de *HUB voor Advanced Analytics en AI* in stelling gebracht om initiatieven op dit vlak te ondersteunen en te coördineren.

Voor de ontwikkeling van AI-modellen zijn data nodig. Vaak wordt gezegd dat data de *brandstof* voor AI zijn. Er zijn nog veel vragen te beantwoorden over het gebruik van politiegegevens (Wpg) en persoonsgegevens (AVG) voor het voeden van datasets voor AI-modellen. Los van de uitkomst van deze discussies staat in ieder geval vast dat een goede datakwaliteit, waarvoor een duidelijke *data governance* en een goede *data hygiëne* randvoorwaardelijk zijn, noodzakelijk is om te zorgen dat de

⁵⁹ Zie ook: [Twaalf eisen basisregistraties](#).

⁶⁰ Artikel 4:2 lid 4 Bpg: Politiegegevens die worden verwerkt overeenkomstig de artikelen 8 en 13, eerste lid, van de wet, kunnen worden verstrekt aan het college van burgemeester en wethouders en de Minister van Binnenlandse Zaken en Koninkrijksrelaties, met het oog op signalering van veranderingen in de gegevens die in de basisregistratie personen zijn opgenomen.

ontwikkeling en output van AI-modellen rechtmatig en zo betrouwbaar mogelijk is. Dit betekent ook dat de kwaliteitsnormen als beschreven in hoofdstuk 2 van dit document, onverminderd gelden voor politiegegevens (Wpg) en persoonsgegevens (AVG) die in datasets worden gebruikt ten behoeve van AI-modellen.

De politie staat nu nog redelijk aan het begin van een enorme stap voorwaarts met betrekking tot AI. Een goed begin is het halve werk dus de politie dient zorg te dragen voor kwalitatief hoogwaardige datasets die de AI-modellen trainen binnen de mogelijkheden van de wettelijke kaders. Dit staat overigens niet op zichzelf. Ook andere initiatieven zoals de ontwikkeling van synthetische datasets voor het trainen van AI-modellen en inzet op het voorkomen of minimaliseren van *bias* hebben grote betekenis.

3.9 Opleiding en herhalingscursussen

Politiegegevens worden verzameld en verwerkt in vele verschillende systemen en applicaties. De belangrijkste *registratieve* politiesystemen zijn BVH en SummIT. Om politiegegevens juist vast te leggen en daarmee een goede datakwaliteit te borgen, moeten politiemedewerkers goed bekend zijn met de werking en mogelijkheden van deze systemen en applicaties. Opleiding is daarvoor cruciaal en dit moet al beginnen op de Politieacademie. Na de initiële kennismaking met de belangrijkste systemen en applicaties, zal de kennis up to date moeten worden gehouden door het volgen van verplichte herhalingscursussen.⁶¹

In 2023 is het document *Landelijke werk-en invoerafspraken SummIT* tot stand gebracht dat de werk- en invoerafspraken voor SummIT weergeeft.⁶² De werkafspraken beschrijven hoe het systeem gebruikt wordt in de opsporingsuitvoering. De invoerconventies beschrijven de wijze waarop politiegegevens eenduidig worden vastgelegd in SummIT. Verdieping en uitleg is terug te vinden in de gebruikershandleiding en werkinstructies op de intranetpagina van SummIT. Deze documentatie geeft politiemedewerkers en hun leidinggevenden richting en houvast bij het gebruik van SummIT en naleving hiervan bevordert de kwaliteit van politiegegevens. Voor BVH bestaat een BVH-ABC waar gebruikers in duidelijke processtappen kunnen zien wat er minimaal vereist is voor een goede mutatie. Landelijke invoerafspraken voor BVH zijn er echter niet en moeten nog tot stand worden gebracht.

Niet alleen de werking van de politiesystemen en -applicaties is essentieel voor het verzekeren van een goede datakwaliteit, ook een stevige basiskennis van de **Wpg** is daarvoor onmisbaar.⁶³ De Wpg zal dus onderdeel moeten zijn van het curriculum van de Politieacademie en de kennis hierover zal van tijd tot tijd opgefrist moeten worden tijdens de dienst. Daarvoor moet dan ook de tijd en ruimte worden geboden.

Voor het verwerken van persoonsgegevens onder de **AVG** is opleiding evenzo onontbeerlijk. Ook hier is kennis van het gebruik van de systemen én van de AVG van belang voor de datakwaliteit. VIK klachtenbehandelaars registreren hun bevindingen bijvoorbeeld in het documentmanagementsysteem *Documentum*. Zij moeten dus op de hoogte zijn van de AVG-eisen in relatie tot hun werkzaamheden en ook goed de eisen en mogelijkheden kennen van het systeem waarmee zij werken. Dit geldt ook voor andere onderdelen waar AVG-verwerkingen plaatsvinden,

⁶¹De verplichting tot zorg voor het op peil houden van voldoende kennis en vaardigheden op het gebied van het informatieproces binnen de politie, gegevensbeschermingsrecht en methoden en technieken van informatieanalyse is voor bepaalde categorieën politiemedewerkers zelfs expliciet wettelijk geregeld in artikel 6 lid 6 Wpg en artikel 2:9 Bpg.

⁶² <https://intranet.politie.local/downloads/1206/landelijke-werk--en-invoerafspraken-summ-it.html>

⁶³ Zie ook het Jaarplan 2024 van de Functionaris Gegevensbescherming: De FG's hebben kennisborging van de Wpg als thema genoemd voor hun activiteiten voor 2024, waarmee dit onderwerp extra gewicht krijgt.

zoals op HRM-gebied en ook voor de AVG-verwerkingen voor specifieke taken, zoals de korpscheftaken, de vreemdelingentaak en het beheer van de 1-1-2 alarmcentrale.

Een laatste punt van aandacht in relatie tot opleiding, ongeacht of het om het Wpg- of AVG-domein gaat, is de zogenaamde *datageletterdheid*. Kort gezegd is dat het vermogen om zinvolle informatie af te leiden uit data, dus het vermogen om data te lezen, te analyseren en te begrijpen en daaruit correcte conclusies te trekken.⁶⁴ Ook wordt hiertoe gerekend het herkennen wanneer data op onrechtmatige of onethische wijze wordt verwerkt. Zowel in de bedrijfsvoering als bij het politiewerk is de professionele en bewuste omgang met data niet meer weg te denken en dit zal zich alleen nog maar verder ontwikkelen. Datageletterdheid is daarom een factor van belang in het streven naar een goede datakwaliteit en zal onderdeel moeten zijn van de competenties van politiemedewerkers. Opleiding levert daaraan een belangrijke bijdrage.

3.10 Motivatie, gedrag en managementaandacht

Vooraf voor de registratieve *politiesystemen* zoals BVH en SummIT is de menselijke factor van groot belang voor de datakwaliteit. Juist bij het maken van mutaties in de basispolitiesystemen moeten politiemedewerkers de afweging maken welke data *noodzakelijk* zijn om vast te leggen, welke data relevant zijn en welke niet.⁶⁵

Ook is het belangrijk dat politiemedewerkers aandacht besteden aan *nauwkeurigheid* en het registreren van *correcte* gegevens. Veel voorkomende voorbeelden uit de praktijk zijn het vergeten van huisnummers en het achterwege laten van het invullen van de toelichting (modus operandi-MO). Tijdens een lopend onderzoek kunnen collega's daar later hinder van ondervinden bij de uitvoering van hun taken, doordat dan bijvoorbeeld alsnog gezocht moet worden naar de juiste en volledige politiegegevens. Ook voor inzageverzoeken van betrokkenen zijn correcte gegevens belangrijk. Buiten kijf staat dat politiesystemen alleen nuttige en bruikbare informatie opleveren als zij op nauwkeurige wijze zijn gevoed met de juiste data.

Politiemedewerkers moeten dus gestimuleerd worden mutaties op de juiste wijze te verrichten. Ook moet er tijd genoeg zijn om dit essentiële onderdeel van het werk te kunnen uitvoeren. Nu is 'administratie' niet altijd ieders favoriete bezigheid, maar door bijvoorbeeld actief zichtbaar te maken op welke manier dit kan bijdragen aan het oplossen van zaken kan hiervoor de motivatie worden verhoogd. Ook de inzet en focus van de politie op datagedreven werken zoals uitgesproken in de Datastrategie IV 2022-2025 kan hierbij helpen.

Leidinggevend en spelen een grote rol bij het borgen van datakwaliteit door hiervoor bij hun medewerkers aandacht te vragen, dit onderwerp te maken van werkoverleg en hen aan te spreken als het beter kan. Dit geldt overigens niet alleen in relatie tot de registratieve systemen, maar ook ten aanzien van andere door de politie gebruikte systemen, applicaties en tools. Dit vraagt ook om een cultuur van elkaar durven aanspreken op dit onderwerp -uiteraard op een opbouwende manier- en het besef dat kritisch naar elkaar kijken niet in de weg staat aan loyaliteit: *Not everything that is faced can be changed, but nothing can be changed until it is faced*.⁶⁶ Wat hierboven voor politiegegevens is gezegd, geldt naar analogie voor persoonsgegevens die de politie verwerkt onder de **AVG**.

⁶⁴ Zie ook: <https://nl.wikipedia.org/wiki/Datageletterdheid>

⁶⁵ Zie ook artikel 8.1 van de Beheerregeling DI Politie 2017: *Politiemedewerkers zijn verantwoordelijk voor het in goede, geordende en toegankelijke staat opslaan en beheren van inkomende en uitgaande documenten, alsmede van intern gerichte documenten, die worden ontvangen, opgemaakt of gebruikt bij de uitvoering van de dagelijkse taken.*

⁶⁶ Citaat van James Baldwin, Amerikaans schrijver en sociaal criticus, aangehaald door Janny Knol, korpschef, n.a.v. haar eerste oriënterende maanden als korpschef.

3.11 Monitoring en riskmanagement

3.11.1 Kwaliteitsmedewerkers

De primaire verantwoordelijkheid voor datakwaliteit in de registratieve systemen ligt bij de politiemedewerkers en hun leidinggevendenden. Toch is een belangrijke schakel in het borgen van datakwaliteit dat deze primair verantwoordelijken *ondersteuning* krijgen van *kwaliteitsmedewerkers*. Op dit moment is echter niet landelijk op structurele wijze voorzien in deze wijze van monitoring. Kwaliteitsmedewerkers monitoren verrichte registraties in de belangrijkste registratieve politiesystemen en signaleren mogelijke registratiefouten. Op die manier kan worden voorzien in het corrigeren of laten corrigeren van fouten en omissies. Ook geeft dit de mogelijkheid datakwaliteitsrapportages uit te brengen zodat leidinggevendenden sturing kunnen geven en verbeteringen kunnen bewerkstelligen. Naar aanleiding van bevindingen kunnen kwaliteitsmedewerkers een stimulerende rol spelen door politiemedewerkers en hun leidinggevendenden te helpen en te adviseren over kwaliteitsverbeteringen en hen te laten zien hoe verhoging van datakwaliteit kan leiden tot betere resultaten.

3.11.2 Riskmanagement

De politie zet in op de verdere professionalisering van het riskmanagement. Voor gegevenskwaliteit is van belang dat inzichtelijk is welke verbeterpunten er zijn, maar vooral ook om inzicht te hebben in de voortgang van de implementatie van verbeterpunten.

Initiatieven zijn in ontwikkeling om in GEB's geconstateerde risico's en de daarbij behorende mitigerende maatregelen zoveel mogelijk centraal inzichtelijk te maken. Ook tekortkomingen en risico's geconstateerd in audits en de daarbij behorende verbetermaatregelen kunnen hierin worden meegenomen. Voor GEB's uitgevoerd binnen het *Programma intensivering privacy* is gestart met een overzicht van risico's en maatregelen in een zorgvuldig tot stand gebracht excel format (Centraal risicoregister), dat als input dient voor de online werkomgeving *Vena*. *Vena* geeft de mogelijkheid tot samenwerking en distributie van werkpakketten onder degenen die verantwoordelijk zijn de maatregelen te implementeren. Met behulp hiervan kan de voortgang worden gemonitord en kunnen rapportages worden ontwikkeld.

Vanzelfsprekend is het daarbij wel van belang dat duidelijkheid bestaat *wie verantwoordelijk is* voor de opvolging en implementatie van de in dergelijke overzichten weergegeven maatregelen. Daarvoor is een heldere privacygovernance en datagovernance noodzakelijk (zie paragraaf 3.2), opdat opvolging wordt geborgd.

Binnen een nader te bepalen termijn moet de politie op zoek naar meer geavanceerde Governance, Risk en Compliance (GRC) tooling die past bij het privacyvolwassenheidsniveau waaraan de politie zich heeft gecommitteerd.⁶⁷

⁶⁷ Zie: Privacybeleid, 10 januari 2020, versie 1.0, p. 11: de politie committeert zich aan privacyvolwassenheid niveau 3: *Op niveau 3 verwerkt de politie gegevens, waarbij keuzes zijn en worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau. Het beleid is formeel vastgesteld op organisatieniveau en daarmee bekrachtigd als beleid voor de gehele politieorganisatie. De vereisten vanuit de organisatie zijn ook vertaald naar de inrichting van de context, de systemen en de beheerprocessen. De politieorganisatie leert bedrijfsbreed, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op alle niveaus. Er is structurele evaluatie van en rapportage over de gegevensverwerking (en beveiliging van gegevens) naar het hogere management, wat tot aanpassing van het organisatiebrede beleid kan leiden. **Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. De leiding is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces op alle niveaus.***

3.12 Intern en extern toezicht⁶⁸

Zowel de **AVG** als de **Wpg** verplicht de politie tot het aanstellen van een *Functionaris gegevensbescherming* (FG).⁶⁹ De FG houdt toezicht op het verwerken van gegevens in overeenstemming met de Wpg, AVG en andere daaronder vallende regelingen. Ook de *privacyfunctionaris* heeft een in de **Wpg** verankerde rol om te adviseren en erop toe te zien dat politiegegevens in overeenstemming met de Wpg worden verwerkt. De **AVG** kent de positie van *privacyfunctionaris* niet. Eens per jaar moet de politie op grond van de **Wpg** een *interne Wpg-audit* verrichten, mede in voorbereiding op een externe Wpg-audit.⁷⁰ Deze interne audits worden uitgevoerd door de interne auditdienst van de politie. Onderdeel van de Wpg-audit is *kwaliteitsmanagement*, waarbij ook *datakwaliteit* onder de loep wordt genomen. *Interne AVG-audits* zijn niet expliciet wettelijk gereguleerd.

Eens in de vier jaar wordt een *externe Wpg-audit* uitgevoerd, zo schrijft de **Wpg** voor.⁷¹ Bij de externe Wpg-audit wordt expliciet stilgestaan of is voldaan aan de Wpg kwaliteitsnormen zoals die nader zijn toegelicht in hoofdstuk 2 van dit document. De **AVG** kent geen parallelle bepaling die verplicht tot een externe audit.

De *Autoriteit Persoonsgegevens* (AP) heeft een toezichthoudende taak, die zowel in de **Wpg** als **AVG** is belegd.⁷² De AP kan in het kader van haar toezichthoudende taken onder meer adviseren, waarschuwen, een last onder dwangsom opleggen en bestuurlijke boetes opleggen.

* * * * *

⁶⁸ Op deze plaats wordt slechts summier ingegaan op toezicht. Toezicht zal nader vorm worden gegeven in een nog op te stellen *Beleidskader toezicht*.

⁶⁹ Artikel 36 lid 3 sub a Wpg, artikel 37 t/m 39 AVG.

⁷⁰ Artikel 33 lid 5 Wpg, artikel 6:5 lid 5 Bpg en artikel 3 van de Regeling periodieke audit politiegegevens.

⁷¹ Artikel 33, lid 1 Wpg, artikel 6:5, lid 1 Bpg, Regeling periodieke audit politiegegevens.

⁷² Artikel 35-35c Wpg; artikel 55, 57-58 en 83 AVG.

Kies een item. **van een art. 36 SIS-signalering**

Dit betreft een verplicht formulier voor het aanvragen/verlengen van signaleringen van personen met oog op onopvallende/ gerichte controle ex art. 36.3 Verordening (EU) 2018/1862.

Dit formulier is opgesteld in ondergeschiktheid aan de officier van justitie volgens, in overeenstemming met art. 36.3 Verordening (EU) 2018/1862 en het Kaderbesluit 2002/584/JBZ, met het oog op het signaleren van personen voor onopvallende controle of gerichte controle ter opsporing, onderzoek of de vervolging van strafbare feiten, met het oog op de tenuitvoerlegging van een strafrechtelijk vonnis en ter voorkoming van gevaar voor de openbare veiligheid.

Ik verzoek op basis van dit formulier om de desbetreffende persoon te signaleren in het Schengen Informatiesysteem.

Elk veld dient ingevuld te worden.

a) Persoonsgegevens:

Achternaam:

Voorvoegsel:

Voornamen:

Geboortedatum:

Geboorteplaats:

Geboorteland:

Nationaliteit:

Geslacht:

Maak een keuze

*Verblijfplaats en/ of
bekend adres:*

Persoonsnummer(s):

Documentnummer(s):

SUMM-IT bak:

Mutatienummer:

b) Reden van signalering (maak een keuze):

- ☒ *Er bestaan duidelijke aanwijzingen dat een persoon een van de in artikel 2, leden 1 en 2, van Kaderbesluit 2002/584/JBZ genoemde strafbare feiten beraamt of pleegt;*
- ☐ *De in artikel 37, lid 1, bedoelde informatie noodzakelijk is voor de tenuitvoerlegging van een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel ten aanzien van een persoon die is veroordeeld voor één van de in artikel 2, leden 1 en 2, van Kaderbesluit 2002/584/JBZ genoemde strafbare feiten;*
- ☐ *Op grond van een algemene beoordeling van een persoon, met name op grond van de door hem gepleegde strafbare feiten, doet vermoeden dat hij in de toekomst in artikel 2, leden 1 en 2, van Kaderbesluit 2002/584/JBZ genoemde strafbare feiten zou kunnen plegen.*

c) Het in artikel 2, leden 1 en 2, van Kaderbesluit 2002/584/JBZ genoemde strafbare feit:

Kies een item.

d) Toetsing (alle opties zijn verplicht en dienen aangevinkt te worden):

- ☐ Het gestelde doel van deze verstrekking staat in verhouding tot de (mogelijke) privacy inbreuk van betrokkene(n) waarbij de grondrechten en fundamentele vrijheden van de betrokkene niet prevaleren boven het algemeen belang van de doorgifte (**proportionaliteitstoets**) (verplicht)
Klik of tik om tekst in te voeren.
- ☐ Voor deze verstrekking zijn geen minder ingrijpende middelen beschikbaar om het gestelde doel te bereiken (**subsidiariteitstoets**) (verplicht)
Klik of tik om tekst in te voeren.
- ☐ Er is voldoende rekening gehouden met negatieve neveneffecten (verplicht)

e) Andere voor de zaak relevante omstandigheden:

(Noot: Vermeld hier alle omstandigheden die relevant zijn ten behoeve van de signalering. Denk hierbij aan eventuele opsporingsindicaties en correspondentie met het buitenland.)

f) Soort signalering (maak een keuze):

☒ *Onopvallende controle: actie onopvallend gegevens verzamelen*

☐ *Gerichte controle: actie gerichte controle/ gegevens verzamelen*

g) Duur van de signalering (max. 1 jaar):

Gelieve hieraan te geven tot welke datum de signalering van kracht dient te zijn en de signalering heroverwogen dient te worden:

h) Aanspreekpunt voor de signalerende autoriteit:

Organisatie/ afdeling:

Naam contactpersoon:

Adres:

Tel:

Email:

i) Akkoord van de signalerende autoriteit: *

Naam:

Functie (titel/ rang): Officier van Justitie

Adres:

Datum:

LET OP: ik ga akkoord met de aanmaak van de signalering in het Schengen Informatie Systeem door dit formulier per mail toe te sturen aan het regionaal invoer centrum** en vast te leggen in SUMM-IT.

De officier die de signalering aanmeldt dient deze ook in te trekken.

* Indien de naam van de officier van justitie niet gedeeld kan worden i.v.m. veiligheid dan graag een verwijzing naar het aanspreekpunt.

**** Contactgegevens regionaal invoer centrum:**

5.1.2.i

