Beleidskader
PSD by design

Inhoud

1.Inleiding..... 4
1.1. Scope 5
1.2. Doelgroep 5
1.3. Leeswijzer 6
1.4. Definities 6

2.Strategisch kader.....10
2.1. Korpsstrategie 10
2.2. Datavisie en strategie 11
2.3. Enterprise Architectuur 12
2.4. Sturing 12

3.Juridisch kader 14
3.1. Overheidsinformatie 14
3.2. Persoonsgegevens 18
3.3. Specifieke en sectorale wetgeving 19

Dit is deel I:
Beleidskader PSD by design
concept versie 3.0 (2021)

Het beleidskader Privacy en Security en Duurzame toegankelijkheid by design wordt onderhouden en actueel gehouden door de Staf korpsleiding van de politie.

De principes voor de omgang met de gegevens, die horen bij dit beleidskader, zijn beschreven in deel II: 'principes PSD by design'

Deel II:
Principes PSD by design
2021-concept versie 3.0

VASTGESTELD DOCUMENT 223	
Geldigheid	Vanaf 01/11/2021
Locatie	Intranet
Bestandsnaam	PSD by design
Versienummer	3.0
Versiedatum	01/11/2021
Beheerder	Directie IV | Gegevensautoriteit
Vastgesteld door	CIO 01/11/2021

'Met genoegen presenteer ik de derde editie van het Uitvoeringskader Privacy, Security en Duurzame Toegankelijkheid by Design (PSDbd). Wie ook de voorgaande edities kent, ziet dat het binnen de IV organisatie inmiddels vertrouwde begrip "Privacy en Security by Design" is uitgebreid met "duurzame toegankelijkheid', kortweg DUTO.

Met de voortschrijdende digitalisering groeit ook het besef (soms door schade en schande) dat het grootschalig gebruik van nieuwe data-toepassingen op gespannen voet kan staan met de waarden van onze rechtsstaat, zoals de eerbiediging van de persoonlijke levenssfeer of het legaliteitsbeginsel. We hoeven de krant maar open te slaan of we zien hier voorbeelden van. Of het nu gaat om de toeslagenaffaire, een datalek bij een uitvoeringsorganisatie, of het gebruik van sensoren bij de politie: de roep om te kunnen reconstrueren wie wanneer toegang tot welke informatie had en welke besluiten op basis daarvan zijn genomen klinkt steeds vaker en luider. DUTO bewaakt –in een notendop- de beschikbaarheid en betrouwbaarheid van gegevens en overheidsinformatie vanaf het moment van vastlegging tot vernietiging. Door opname in dit uitvoeringskader onderstrepen we het belang hiervan als integraal onderdeel van de zorg voor onze gegevens, naast gegevensbescherming (privacy) en informatiebeveiliging (security).

Dit uitvoeringskader schrijft voor welke principes in acht moeten worden genomen bij de inrichting en ontwikkeling van processen en systemen. Het idee is dat als deze principes goed worden ingebed in het werkingsmechanisme van een proces of applicatie, de juiste verwerking van gegevens daarbinnen ´automatisch´ wordt ondersteund. Dit maakt de omgang met gegevens in de praktijk minder kwetsbaar voor fouten. Het is daarmee een cruciaal instrument binnen het totaalpakket aan technische, procedurele en organisatie-culturele maatregelen voor een toekomstbestendige gegevenshuishouding.

Merk op dat het document niet voor niets een uitvoeringskader heet; er is een belangrijke taak weggelegd voor de collega's die hiermee aan het werk gaan om de principes te vertalen naar praktisch ontwerp. Zonder de inzet en creativiteit van de bouwers en gebruikers gaat PSDbD niet vliegen. Het is dus ook een oproep om met elkaar aan de slag gaan, nu eigenlijk iedereen binnen ons informatie verwerkende bedrijf in een of andere vorm met gegevens te maken heeft.

„...er is een belangrijke taak weggelegd voor de collega's die hiermee aan het werk gaan."

Rest mij de collega's te bedanken die hebben geholpen bij de totstandkoming van deze nieuwe editie. In bijlage NB staat een overzicht van alle betrokken. Veel dank voor jullie bijdrage!

5.1.2.e

1. Inleiding

"Voor je ligt versie 3 van het beleidskader Privacy, Security en Duurzame Toegankelijkheid by design ('PDS by design'). We geven hiermee als Korps continuïteit aan de ingeslagen weg. Namelijk om de omgang met gegevens zo veel mogelijk in ontwerp van processen en systemen te verankeren. Daarmee beschikken we als politie over een langjarige, breed gedragen strategie voor alle gegevens. Die continuïteit geeft houvast. Dat is iets om trots op te zijn; niet op dit document, maar op het feit dat we als organisatie één richting op bewegen.
We hebben nog veel werk te doen. Bestaande applicaties voldoen nog niet aan alle ontwerp-criteria van PSD by design. Ook applicaties die vandaag worden gebouwd, voldoen niet op alle punten. Het mist niet aan visie, maar wel aan een goede doorvertaling van strategie, naar principes, naar maatwerk – advies richting specifieke toepassingen.

We zijn aan de slag met die doorvertaling. PSD by design is in deze nieuwe versie wat nadrukkelijker geknipt in twee zelfstandig leesbare delen. Een meer strategisch stuk dat de context van politie in de omgang met gegevens beschrijft. En een tweede deel waarin principes voor gegevens worden omschreven. Samen met de dienst IV werken we aan een derde deel. Concreet uitvoeringbeleid en bewezen succesvolle ontwerpstrategieën per principe. Bijvoorbeeld generieke voorzieningen, waarmee een toepassing 'plug en play' kan aansluiten op een PSD by design werkwijze. Concreter en gemakkelijker.

De goede omgang met gegevens door politie is een vraagstuk van betrouwbaarheid, van integere omgang met dat vertrouwen en van de moed om de grens op te zoeken. Het is geen beleidsvraagstuk versus de operatie: het is een korpsvraagstuk en we zullen als politie een omgang met gegevens moeten vinden die echt bij ons past.

Ik wil iedereen bedanken die hier op een of andere wijze aan heeft bijgedragen.

5.1.2.e

1.1. Scope

Het beleidskader Privacy en Security en Duurzame Toegankelijkheid by Design (PSD by design) beschrijft principes voor de omgang met gegevens. Die principes zijn overal leidend en geldig waar de politie met gegevens omgaat. Van operatie (politietaak) tot bedrijfsvoering, van basisteam tot korpsleiding en zowel binnen de organisatie als in de samenwerking met ketens en netwerken.

PSD by design stelt ***dat*** er volgens die principes met gegevens moet worden omgegaan, maar schrijft niet uitputtend voor ***hoe*** dat moet. De principes voor omgang met gegevens worden toegelicht met implicaties voor ontwerp, waarmee wordt gedoeld op het ontwerp van de informatievoorziening. Er zijn ook andere ontwerpimplicaties voor operationele processen, kennisproducten, etc., maar die worden hier niet verder uitgewerkt.

PSD by design beschrijft ***design***-principes voor duurzame toegankelijkheid, gegevensbescherming (privacy) en gegevensbeveiliging (security). Dat zijn alle principes die van invloed zijn op de ontwerpkeuzes die we maken bij het ontwikkelen en gebruiken van gegevens en informatievoorziening. Er zijn daarnaast andere principes, die meer ingrijpen op bedrijfscultuur, houding en gedrag of tactische keuzes over bijvoorbeeld de informatiepositie van de politie. Die principes maken geen deel uit van PSD by design, maar er wordt wel naar verwezen.

PSD by design gaat over alle gegevens. Dus ook de gegevens die we 'ruwe data' noemen, de big data, de ongestructureerde gegevens, de 'overheidsinformatie'. Sommige principes gelden alleen voor bepaalde gegevens, bijvoorbeeld alleen voor persoonsgegevens of alleen voor overheidsinformatie.

* Afbeelding: schematisch overzicht van de scope en context PSD by design:[PM afbeelding invoegen]

1.2. Doelgroep

Deel I (hoofdstuk 1, 2 en 3) zijn bedoeld om PSD by design als ***principle-based***-benadering in te leiden en te motiveren: hoe dragen principes bij aan de goede omgang met gegevens, waarom zijn principes hiervoor geschikt en hoe moeten ze worden gelezen? De 'plaats' van PSD by design tussen de andere strategische beleidsdocumenten wordt toegelicht, dus ook de reikwijdte. Deel I wordt afgesloten met een overzicht van het juridisch kader voor de omgang met gegevens door de politie. De doelgroep bestaat uit adviseurs en eenheidsleiding.

Deel II (hoofdstuk 4 en 5) zijn geschreven voor alle collega's die betrokken zijn bij het ontwikkelen of verwerven van technologie waarmee we gegevens verwerken.

PSD by design als geheel is ook geschreven voor organisaties en personen die vanuit een wettelijke taak, een gevoeld maatschappelijk belang of anderszijds behoefte hebben te weten hoe de politie zich tot doel stelt met gegevens om te gaan. De gepubliceerde versie van PSD by design (versie 3.0) is niet geclasssificeerd (openbaar).

1.3. Leeswijzer

Waar in de voetnoot met *zie* .. wordt verwezen naar een bron is die achterin het document bij Bronnen op 53 te vinden, met een link naar de Agora-omgeving van de politie. De externe lezer kan deze brondocumenten, voor zover openbaar, opvragen bij de Gegevensautoriteit van de politie. Ook verwijzingen naar externe bronnen zijn zo veel mogelijk voorzien van een link. Vooral het juridisch kader bevat veel (wets)verwijzingen naar wetten.nl en (voor de AVG) naar eur-lex.europa.eu. In de hoofdstukken erna worden verwijzingen naar de wet voorzien van een link naar hoofdstuk 3, van waaruit het relevante wetsartikel weer is te vinden.

Voor het gericht zoeken naar een onderwerp in de gedrukte versie kan naast de inhoudsopgave gebruik worden gemaakt van de index met trefwoorden op pagina 52.

1.4. Definities

Gegevens

Gegevens zijn een weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat[1]. Voor de omgang met gegevens is onderscheid naar gegevenstype belangrijk, want er worden per gegevenstype andere eisen aan de omgang gesteld.

We onderscheiden referentiegegevens (A) en kernobjectgegevens (B) . Elk operationeel bedrijfsproces maakt gebruik van deze gegevenstypen. Het zijn daarom essentiële onderdelen die met elkaar het fundament vormen voor de gegevenshuishouding van de politie. Voorbeelden van referentiegegevens zijn nationaliteit en strafbaar feit, voorbeelden van kernobjectgegevens zijn personen of voertuigen.

Transactiegegevens maken gebruik van de kernobjectgegevens en de referentiegegevens. Een transactie is een verzameling gegevens over een feit of een gebeurtenis, waarvoor geldt dat deze in meerdere bedrijfsfuncties gebruikt wordt en veelal direct te relateren is aan de wettelijke politietaak: handhaven, opsporen en noodhulp. Transactiegegevens gaan over de uitvoering van het werk. Denk hierbij aan incidenten en aangiftes. Het zijn de gebeurtenissen waardoor de politieorganisatie in beweging komt en activiteiten uitvoert.

De 'overige gegevens' worden door de politie verwerkt in het kader van de politietaak, maar zonder dat zij transacties van de politie weergeven. Ze worden niet verwerkt voor een bedrijfsfunctie, maar zijn daarvan het resultaat of de input. Denk bijvoorbeeld aan sporen of in beslag genomen beeldmateriaal. Dit kunnen dus grote volumes aan gegevens zijn, die niet zijn opgebouwd rondom onze eigen referentiegegevens en kernobjecten, maar een eigen structuur hebben. Als overige gegevens worden geanalyseerd, kan het zijn dat er voertuigen, personen, of verdenkingen van een

1 definitie: www.noraonline.nl/wiki/gegeven

betrokkenheid bij een strafbaar feit in worden herkend. Dan worden die specifieke overige gegevens transactiegegevens (C).

Abeelding: verschillende type gegevens

Big data

Big data is term voor gegevensverzamelingen die te groot, te uiteenlopend in vorm en structuur en vaak ook te veranderlijk zijn om in reguliere databases te kunnen worden opgeslagen. Dit zijn bijvoorbeeld gegevens die afkomstig zijn van grote inbeslagnames, die verzameld worden van internet of social media, die verkregen zijn door middel van interceptie of uit sensoren en die naast tekst ook kunnen bestaan uit multimedia.

Persoonsgegevens

Gegevens gelinkt aan een identificeerbare natuurlijke persoon[2]. Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens (EC).[3]

Gegevens over rechtspersonen zijn geen persoonsgegevens, tenzij ze (ook) gaan over een natuurlijke persoon. Bijvoorbeeld de beheerder of bestuurder van de rechtspersoon. Overleden personen zijn geen personen (in de zin van de wet). Zorgvuldigheidshalve wordt er in de praktijk meestal geen onderscheid gemaakt tussen gegevens over levende en overleden personen.

Politiegegevens

Persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak[4].

Bijzondere categorieën persoonsgegevens

Persoonsgegevens waarvan verwerking grote inbreuk maakt op de persoonlijke levenssfeer. Zoals gegevens over godsdienst of levensovertuiging, ras (dit heeft dus ook betrekking op vrijwel al het beeldmateriaal van personen), seksuele leven, maar ook genetische en biometrische gegevens. Ook vakbondslidmaatschap is een bijzonder persoonsgegeven. Het begrip bestaat zowel in de zin van de AVG als van de Wpg en heeft gelijke betekenis (zie ook Bijzondere categorieën van persoonsgegevens op bladzijde 18).

Privacy

Voor een definitie van privacy wordt hier verwezen naar het privacybeleid[5]en de wetgeving en literatuur hierover. Voor dit document is relevant dat met ***privacy (en security en duurzame toegankelijkheid) by design*** wordt gedoeld op de informationele privacy. Dit is de privacy, voor zover die wordt bepaald door de bescherming van persoonsgegevens. De omgang met gegevens over personen is in grote mate bepalend voor de privacy van personen, maar de bescherming van die gegevens omvat niet de hele context van privacy.

We kunnen met deze principes dus wel de gegevens beschermen, maar niet de privacy, want die is ook afhankelijk van andere factoren. Voor de eenvoud wordt in dit document, dat immers een IV-beleidskader is, de informationele privacy kortweg met 'privacy' aangeduid.

Security

Voor definitie van security wordt hier verwezen naar het securitybeleid5 en de literatuur hierover. Hiermee wordt bedoeld de beveiliging (security) *van informatie,* dus op het smallere begrip informatiebeveiliging en niet de 'security' (toegang panden, persoonsbeveiliging, etc.) als geheel. Het is gebruikelijk te spreken van informatiebeveiliging (IB) en niet van 'gegevensbeveiliging', dus voor de eenvoud doen we dat hier ook.

IB gaat hier wel breder dan dat wat nodig is voor privacy. Voor de bescherming van persoonsgegevens wordt gebruik gemaakt van allerlei vormen van informatiebeveiliging, wegens de 'afschermende' werking die zij heeft. Maar informatiebeveiliging heeft naast privacy

2 definitie: AVG Artikel 4 onder 1 (link)

3 zie ook Europese Unie: Wat zijn persoonsgegevens (ec.europa.eu)

4 definitie: Wet Politiegegevens: artikel 1 onder a (wetten.nl)

5 voor het actuele beleid zie de pagina Bronnen met verwijzingen naar agora bladzijde 65

ook andere doelen, zoals bescherming van de organisatie tegen aanvallen van buiten of catastrofes.

Duurzame toegankelijkheid

Duurzaam toegankelijk betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard.[6] Toegankelijk betekent vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zolang als noodzakelijk. Duurzame toegankelijkheid verlangt een zorgvuldige omgang met gegevens vanaf het moment van vastlegging gedurende hele levenscyclus. Daarom is het onderdeel van PSD by design.

Overheidsinformatie

Overheidsinformatie is alle informatie die de overheid zelf maakt of van een ander ontvangt bij het uitvoeren van haar taken.[7] Hierbij maakt het niet uit welke status zij heeft, in welk systeem zij zit, welke vorm zij heeft, of het digitaal of fysiek bestaat, door wie zij beheerd wordt of uit welk werkproces zij voortkomt. Overheidsinformatie kan bestaan uit persoons- en politiegegevens.

Design

Design of 'ontwerp' is een beschrijving van iets nieuws, of bestaands[8]. In de context van PSD by design wordt er met de toevoeging *by design* uitdrukking gegeven aan het feit dat de goede omgang met gegevens zo veel mogelijk in de werking van technologie zelf wordt geborgd. De gedachte is, dat de goede omgang met gegevens als het ware als een fundamenteel werkingsmechanisme in de technologie wordt opgenomen, 'ingebakken'.

Omdat er bij de eerste ontwikkeling van een technologie de meeste ruimte voor ontwerpkeuzes is, heeft by design een connotatie van 'vanaf de start' gekregen. Dat kan ook een beleidskeuze zijn; om PSD by design primair toe te passen in nieuwe ontwikkelingen, bij wijze van vervangingsstrategie om niet alle bestaande technologie aan te moeten passen. Maar de door het korps gekozen betekenis van by design is wel degelijk dat het evengoed voor bestaande technologie geldt. Sterker nog, de meest betekenisvolle uitwerking van PSD by design zit in de toepassing op de technologie die we vandaag de dag gebruiken.

Een nog iets bredere uitleg van by design is, dat processen en procedures ook worden 'ontworpen'. We komen dan op het terrein van privacybeleid[9]

Het *by-design*-denken heeft de afgelopen jaren een vlucht gekregen. Naast de hiervoor genoemde heeft het er nog een betekenis bij gekregen, namelijk die van *certified* oftewel gegarandeerd. Het is natuurlijk zo, dat een technologie die bepaalde gegevens door ontwerpkeuzes niet opslaat, de goede omgang met gegevens vanzelf een betere dienst bewijst dan technologie die gegevens zonder beperking opslaat en bewaart. Design kan een krachtig en elegant instrument zijn om goede omgang met gegevens te bevorderen. Maar de bijdrage van ontwerp moet ook niet overschat worden. Ook met veilige ontwerpen kan veel misgaan en met de toepassing van PSD by design in technologie alleen zijn de gegevensbescherming, beveiliging en duurzame toegankelijkheid niet gegarandeerd.

Het is daarom goed om bij de principes voor de omgang met gegevens ook de bredere implicaties buiten de informatievoorziening voor ogen te houden. De principes hebben ook implicaties voor sturing, houding en gedrag in de omgang met gegevens (zie ook Sturing op houding en gedrag op pagina 13)

6 definitie: Nationaal Archief (nationaalarchief.nl)

7 definitie: nationaalarchief.nl

8 definitie: wikipedia.nl

9 *zie* privacybeleid

Principes

Principes zijn in onze context richtinggevende afspraken die de kwaliteit van de dienstverlening beschrijven vanuit het perspectief van de maatschappij en overheid[10]. Principes doen 'dat-uitspraken' en gaan niet in op de uitvoering (het 'hoe').

Principes hebben in dit document twee functies;

- vereenvoudiging: veel wetten grijpen gelijktijdig in op de verwerking van gegevens door de politie. de Archiefwet, AVG, Wpg, Sv en Wob bevatten allemaal bepalingen hoe de politie met gegevens (of informatie) moet omgaan. Gegevens zijn gelijktijdig overheidsinformatie, tactische informatie, persoonsgegevens en politiegegevens. Wetgeving kan daardoor best complex worden. Voor de professionals die met gegevens werken kunnen principes helpen overeenkomstige bepalingen uit verschillende wetten onder één noemer te brengen. Principes zijn voor architecten ook herkenbare aangrijpingspunten voor het uitwerken van implicaties in de ontwikkeling en werking van de informatievoorziening.
- richting geven: waar de wet zogenaamde 'open' bepalingen kent, is er voor de politie als verantwoordelijke voor de omgang met gegevens iets te kiezen. We moeten zelf een 'zorgvuldige', 'proportionele' of 'redelijke' omgang met gegevens vinden. Die discretionaire bevoegdheid of regelruimte geeft lucht, maar soms ook onzekerheid over de concrete invulling bij het ontwikkelen van applicaties en voorzieningen. Principes en daarvan afgeleide implicaties voor ontwerp geven houvast en richting voor de organisatie en voorkomen een te grote variëteit in de praktijk.

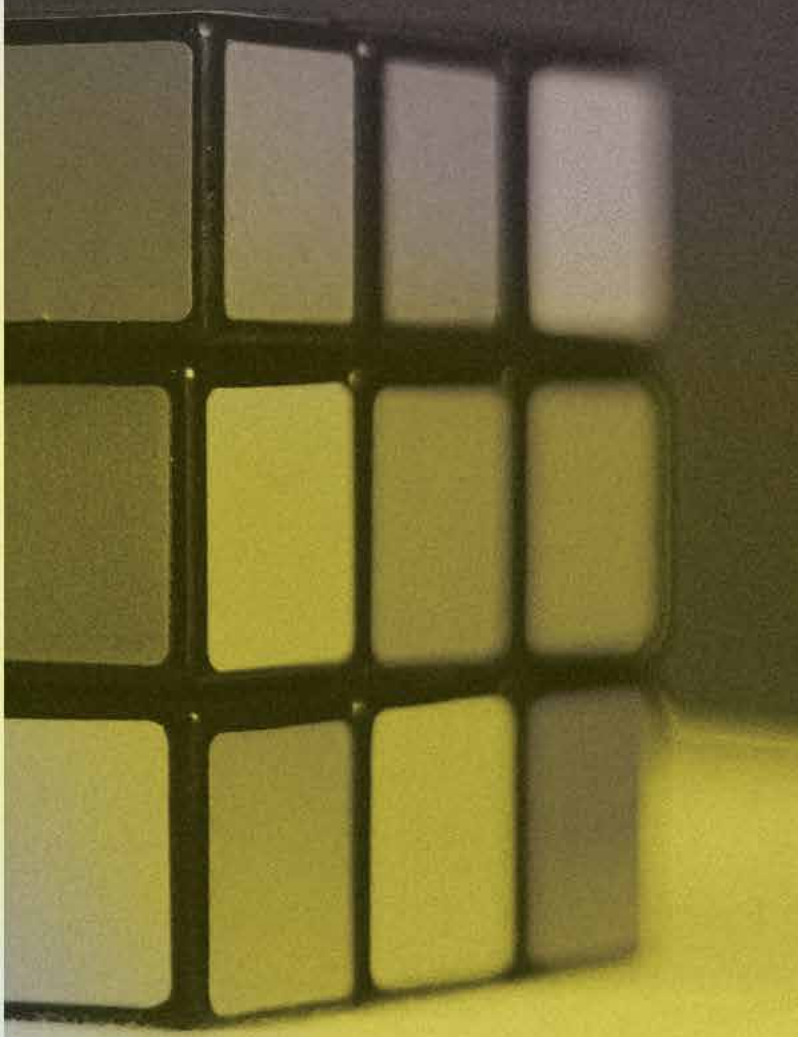
10 definitie: noraonline.nl (november 2020)

2. Strategisch kader

2.1. Korpsstrategie

PSD by design is een architectuurkader voor de omgang met gegevens. De implicaties zullen veranderen met de ontwikkeling van het applicatielandschap, de informatievoorziening en operationele prioriteiten, maar de omgang met gegevens zal naar verwachting aan dezelfde principes moeten blijven voldoen. De principes zijn dus duurzaam en stabiel.

Goede omgang met gegevens is essentieel, maar niet het eerste en enige belang van het korps. Veiligheid van collega's, van de maatschappij en uitvoering van de politietaak staan onveranderd bovenaan de prioriteitenlijst. Daarvoor kunnen gegevens, mits goed gebruikt, in combinatie met informatietechnologie van doorslaggevend belang zijn. Dat belang wordt ook onderschreven in de korpsstrategie[11], waarin IV een sleutelrol krijgt toebedeeld.



11 *zie* korpsstrategie

2.2. Datavisie en strategie

Er is er op bijna elk aspect van het politiewerk een visie geschreven waarin data een belangrijke of zelfs kritieke factor is. Data is een succesfactor in bijna ieder aspect van politiewerk, in bijna ieders portefeuille. En toch benut de politie gegevens, 'data', nog niet in alle gevallen optimaal voor de politietaak. Het belang van gegevens wordt door iedereen in het korps onderschreven, maar vaak wel vanuit een verschillend perspectief. Binnen de politie zijn die perspectieven de volgende[12]

- Operationeel perspectief: data in de functie van politiewapen. Data voegt vanuit dit perspectief altijd waarde toe en het is dus zaak zo veel mogelijk data te vergaren en te waarderen. De visie vanuit dit perspectief is: hoe meer, hoe beter en de vraag aan IV is om middelen te verschaffen om met de groeiende mogelijkheden om te kunnen blijven gaan.
- IV-perspectief: data als cruciaal, verbindend element in de IV. De visie vanuit dit perspectief is gericht op het leveren van een veilige, betrouwbare en wendbare IV voor het politiewerk[13], waarbij data een van de pijlers van deze IV is. Data wordt als cruciaal gezien omdat zij een robuust, 'duurzaam' element van de IV vormt. Door te investeren in relevante en hoogwaardige data en algoritmes kan functionaliteit flexibel worden ontwikkeld naar de behoeftes van het politiewerk.
- Legitimiteitsperspectief: Data als een verantwoordelijkheid, met morele, ethische lading. De politie heeft toegang tot heel veel persoonlijke informatie doordat zij uitvoering geeft/mag geven aan de politietaak. De legitimiteit van de politie leunt op gezag en traditie, maar vooral op vertrouwen van de samenleving dat we met deze data omgaan conform wettelijke en morele kaders. De visie vanuit dit perspectief is gericht op rechtmatige en moreel aanvaardbare inzet van data, zoals je dat van de politie mag verwachten. Op een goede gegevenshuishouding, compliance aan de wet (privacy, informatiebeveiliging, duurzame toegankelijkheid) en een foutloze, transparante verwerking van gegevens over personen, feiten, delicten en het verband daartussen (de zaak).

Om de visie van de politie op data te begrijpen moet er oog zijn voor elk van deze perspectieven. Geen van deze drie is het 'juiste' en daarmee de andere 'onjuist', maar afhankelijk van de plek in de organisatie zal het ene perspectief luider klinken dan het andere.

*Afbeelding: Korpsstrategie met data als crusiaal element (centraal)

12 *zie*: concept opdracht Datavisie en strategie

13 *zie*: vernieuwde IV strategie

2.3. Enterprise Architectuur

De Enterprise Architectuur (EA) beschrijft de functie die de structuur van de organisatie heeft voor de politie.

De structuur van de organisatie wordt in de EA beschreven vanuit diverse perspectieven, zoals de schikking van organisatorische eenheden, van processen en van de systemen.

De EA beschrijft deze in samenhang en maakt helder waarom dit de passende structuur voor de politie is. De EA is opgebouwd uit deelarchitecturen, zoals de ketenarchitectuur, de architectuur voor informatiebeveiliging en de gegevensarchitectuur.

PSD by design is onderdeel van de EA.Het beschrijft immers de functie die gegevenshuishouding heeft voor de politie. Zowel de structuur als het gebruik van de gegevenshuishouding zijn specifiek, 'op maat' voor de politie ingericht volgens de principes uit PSD by design. Bepaalde principes zijn sterk gericht op de structuur, zoals principes over het volgen van standaarden en principes over generieke voorzieningen. Andere principes zijn meer gericht op het gebruik, vooral de principes voor de omgang met persoonsgegevens.

De korpsleiding kan besluiten (tijdelijk) af te wijken van een principe, tegen de achtergrond van andere belangen. Dit zal dan geëxpliciteerd moeten worden in een besluit.

2.4. Sturing

2.4.1. Planning en control

Strategische privacydoelen komen via de kaderbrief terecht in jaarplannen en op de uitvoering daarvan wordt gereflecteerd in de managementrapportage en managementgesprekken. Goede omgang met gegevens is immers een operationele ('business-')verantwoordelijkheid en moet ook op deze manier worden georganiseerd. Aan de goede omgang met gegevens zijn meetbare doelstellingen verbonden, met rapportages, risicoanalyses en audits. PSD by design is een belangrijk onderdeel in de planning-en-control-cyclusv als het gaat om het meten (en verbeteren) van de omgang met gegevens, waaronder de compliance aan wet-en regelgeving[14].

Een belangrijk control-instrument voor de compliance aan de principes van PSD by design vormt de nulmeting (of de opvolgers daarvan). Door op het niveau van applicaties en voorzieningen vast te stellen in welke mate de werking van applicaties leidt tot goede omgang met gegevens, ontstaat overzicht en inzicht. Bij het ontwerp en de bouw van applicaties en voorzieningen moeten waarborgen worden ingebouwd om te voldoen aan de eisen van PSD by design. Bouw en ontwerp moeten worden getoetst en er moeten audits en onderzoeken op worden uitgevoerd[15]. Daadwerkelijke controles op broncode en registratie van de bevindingen

14 Zie het beleidskader Privacy in control (Bronnen pagina 53)

15 Dergelijke *definitions of done* worden bijvoorbeeld door het compliance office privacy opgesteld.

zijn nodig om vast te stellen of aan de regels is voldaan. Dat vormt weer input voor de gezamenlijke prioritering.

> De uitgevoerde nulmeting op PSD by design is een goed voorbeeld van het meten van de doelstellingen van PSD by design. Ook voor het informatie-beveligingsbeleid zijn in 2020 de portefeuillehouders uitgenodigd om hier met de CISO hun risicobereidheid te definiëren en met het Kwartier IB vorm te geven in de jaarplannen die bij elkaar komen in het hoofdbesluitvormingsmoment.

Een ander controle-instrument is de risicoanalyse, waarmee een verantwoordelijke voor gegevens inschat welke risico's er op de aspecten van privacy, security en duurzame toegankelijkheid bestaan. Hoewel niet ieder risico hoeft op voorhand hoeft te worden afgedekt – er wordt een kostenafweging tussen maatregelen en het risico zelf gemaakt– neemt de politie altijd een 'baseline' van beveiliging in acht waarmee gegevens over personen conform wettelijke verplichting worden beschermd. Dit is beschreven in de informatiebeveiligingsarchitectuur[16].

2.4.2. Sturing op houding en gedrag

De principes voor omgang met gegevens hebben ook implicaties voor houding en gedrag.[17] Het formuleren van principes is zonder betekenis als er geen professionals zijn die om die principes vragen en hieraan betekenis willen geven in de applicaties en voorzieningen die zij (helpen te) ontwikkelen.

De selectie en ontwikkeling van medewerkers op competenties voor de omgang met gegevens is dus voorwaardelijk. De leiding moet hier bij de instroom en doorstroom van medewerkers aandacht voor hebben. De werkgever heeft verschillende middelen die (al of niet verplicht) aan de medewerker kunnen worden aangeboden, zoals opleidingsmateriaal op één of meer aspecten in dit document. Er zijn handboeken en instructies gewijd aan de Wpg en (bijvoorbeeld) het verstrekken van politiegegevens, en profchecks en dilemma-games die medewerkers uitdagen na te denken over vraagstukken rondom privacy en security. Als die producten en middelen niet (geheel) voldoen is het de verantwoordelijkheid van de lijn om dat aan te geven (behoeftestelling).

Een bijzonder aandachtspunt is wel dat, waar de omgang met gegevens als kerncompetentie wordt gehanteerd voor collega's die de politietaak uitvoeren, het besef van wettelijke kaders en andere normen bij de ondersteuningsorganisatie niet vanzelfsprekend is.

Er zal dus juist bij niet-executieve collega's en medewerkers in de ondersteuning scherper gelet moeten worden op het verkrijgen en onderhouden van de vereiste competenties voor de juiste omgang met gegevens, zeker nu het onderscheid tussen de verschillende organisatieonderdelen in de loop der jaren steeds kleiner wordt gemaakt: 'We zijn immers allemaal de politie.'[18]

16 zie Informatiebeveiligingsarchitectuur versie 1.0, september 2016 (Bronnen op pagina 53)

17 zie (principes) op pagina 13

18 *zie* Beleidskader vakmanschap en security

3. Juridisch kader

3.1. Overheidsinformatie

3.1.1. Archiefwet

De wijze waarop overheidsorganisaties dienen om te gaan met de archieven die zij vormen, is nauwkeurig beschreven in verschillende wetten en richtlijnen. De belangrijkste zijn hierbij de Archiefwet 1995, het Archiefbesluit 1995 en de Archiefregeling 2009[19]. De Archiefwet is van toepassing op a*lle* informatie die de politie creëert of ontvangt bij het uitvoeren van haar taken. Wat onder het begrip archiefinformatie valt, wordt bovendien niet bepaald door de vorm van de informatie, maar door het ontstaan en gebruik ervan. Het gaat hierbij dus niet alleen om tekstdocumenten (papier of digitaal), maar ook om databasegegevens, transactieberichten, foto's, video's, websites en uitingen op sociale media.

Een belangrijke voorwaarde die de wetgever stelt aan archieven is dat zij in 'goede, geordende en toegankelijke staat' worden beheerd. De lijst van kwaliteitseisen die invulling geeft aan deze begrippen is vastgelegd in het rijksbrede normenkader Duurzame Toegankelijkheid van Overheidsinformatie[20] (DUTO). Dit normenkader is inmiddels onderdeel van de informatiearchitectuur van de politie.

Op basis van deze algemene regels is een specifieke Beheerregeling Documentaire Informatie Politie 2017[21] opgesteld. De Beheerregeling geeft een nadere uitwerking van de taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeheer voor de politie en werkt een aantal nadere aspecten van het (documentair) informatiebeheer verder uit. De Beheerregeling is opgesteld door de directeur FM, in samenspraak met de directeur IV en in afstemming met de directeur PDC. De Beheerregeling beschrijft de verantwoordelijkheden voor de verwerking van informatie vanuit het perspectief van digitale duurzaamheid. Daarbij hoort ook het uiteindelijk bewaren of vernietigen van informatie.

19 Wetten.nl: Archiefwet 1995, het Archiefbesluit 1995 en de Archiefregeling (2009)

20 zie Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO)

21 zie Beheerregeling Documentaire Informatie Politie

De Archiefwet vereist dat overheidsorganen een selectielijst opstellen waarin ze beschrijven welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven. Bij de bepaling van de vernietigingstermijn in de selectielijst is rekening

gehouden met de AVG, de Wpg, het Wetboek van Strafrecht en het Wetboek van Strafvordering. Ook het Besluit justitiële en strafvorderlijke gegevens bevat regels over verwijdertermijnen.

De Wpg geeft invulling aan wat de Archiefwet vereist: de Wpg beschrijft welke gegevens hoe lang bewaard worden. Voor artikel 8-gegevens (dagelijkse politietaak) geldt in de Wpg vijf jaar verwerken, dan vijf jaar bewaren en daarna vernietigen. Voor artikel 9 (reguliere opsporing) eist de Wpg dat gegevens zo lang verwerkt worden als voor het doel noodzakelijk is. Dit is in de selectielijst verder uitgewerkt op basis van de verjaringstermijnen uit het Wetboek van Strafrecht. [22]

*Figuur 1: Diverse wetten levren input op selectielijst en daarin gestelde bewaartermijnen

22 zie Archiefwet en Wpg (notitie) voor een uitegebreidere toelichting hoe de selectielijst, de Archiefwet en de Wpg zich tot elkaar verhouden

3.1.2. Wet hergebruik van overheidsinformatie en Wet openbaarheid van Bestuur

De Wet hergebruik van overheidsinformatie[23] (Who) biedt burgers, bedrijven en onderzoeksinstellingen de mogelijkheid om bij een bestuursorgaan een verzoek in te dienen om overheidsinformatie beschikbaar te maken. Deze informatie wordt dan (zoveel mogelijk) in een machinaal leesbare vorm beschikbaar gesteld, zodat de informatie geschikt is voor hergebruik. De Nederlandse regelgeving over hergebruik van overheidsinformatie is gebaseerd op de Europese Hergebruikrichtlijn I uit 2003 en de Hergebruikrichtlijn II uit 2013. De richtlijn uit 2003 werd geïmplementeerd in de Wet openbaarheid van bestuur[24] (Wob) met de gedachte dat hergebruik uitgaat van reeds openbare informatie. Deze artikelen in de Wob zijn vervallen met de inwerkingtreding van de nieuwe Who.

De Wob biedt de burger de mogelijkheid te verzoeken om overheidsgegevens te openbaren. De Who gaat verder en staat hergebruik toe voor andere doeleinden dan waar de informatie in eerste instantie voor bedoeld was. Het gaat om alle informatie die overheidsinstanties produceren en verzamelen, zoals statistieken en geografische informatie.

De Who kent geen verplichting tot digitaliseren specifiek voor hergebruik, wel een inspanningsverplichting. Het is dus de bedoeling dat gevraagde informatie zo veel mogelijk machineleesbaar, via elektronische weg en in open bestandsformaat wordt verstrekt. De wet omvat geen verplichting tot het bijwerken van de kwaliteit van gegevens voordat ze verstrekt kunnen worden.

Openbaarheid en transparantie

De Wob regelt welke overheidsinformatie openbaar is (of op verzoek openbaar dient te worden gemaakt) vanaf het moment van ontstaan tot het moment dat (gearchiveerde) informatie wordt overgebracht naar een archiefbewaarplaats. Daarna is de openbaarheid geregeld in de Archiefwet.

De Wob en Archiefwet kennen beide uitzonderingsgronden op de openbaarheid[25]. Vaak houden deze verband met het werkproces waarin de informatie ontstaat of wordt gebruikt en/of met specifieke inhoud van de informatie. Bij een Wob-verzoek uit dit zich in het niet openbaar maken van documenten of het weglakken van informatie. Op het moment van overbrenging naar een archiefbewaarplaats dient te worden meegegeven welke beperkingen van toepassing zijn. Dit is de verantwoordelijkheid van de politie. Uitzonderingen moeten per geval worden gewogen. Het enkele feit dat informatie wordt opgevraagd die is verkregen bij uitvoering van de politietaak, is niet voldoende. Het belang van de opsporing en vervolging moet in het specifieke geval opwegen tegen het belang van openbaarmaking[26].

Hergebruik

Voor hergebruik is er de Who. Naast deze bestaande wetgeving is de Wet open overheid (Woo) in voorbereiding[27]. De Woo is bedoeld om overheden transparanter te maken en moet ervoor zorgen dat overheidsinformatie beter vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren is. De Woo vervangt de Wob.

De Woo ziet toe op twee zaken, namelijk op de actieve openbaarmaking van de politie-

23 Wetten.nl: Wet hergebruik van overheidsinformatie

24 Wetten.nl: Wet openbaarheid van bestuur

25 WOB artikel 10 lid 1 onder d) "Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit (d) Persoonsgegevens betreft als bedoeld in de artikelen 9, 10 en 87 van de Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt

26 Wet openbaarheid van bestuur, Artikel 10 lid 2 onder c: Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen [het belang van] c. de opsporing en vervolging van strafbare feiten.

27 Het wetsvoorstel is op 26 januari 2021 aangenomen door de TK en de wet treedt naar verwachting in 2023 in werking.

informatie en op de verplichting om in een periode van acht jaar na in werking treden, de informatiehuishouding op orde te brengen.

Met dit laatste punt is ook expliciet gemaakt dat duurzaam informatiebeheer een verplichting is om aan de verantwoordingseisen uit de Woo te voldoen.

3.1.3. Stelsel van basisregistraties

Het stelsel van basisregistraties is een samenhangende set van overheidsinformatie rondom bepaalde kernobjecten, zoals gebouwen, adressen, personen, etc. Het stelsel van basisregistraties bestaat uit, momenteel tien, afzonderlijke basisregistraties waarin de kernobjecten worden beheerd, ook in onderlinge samenhang met andere kernobjecten. Om die relaties te onderhouden (welke persoon woont op welk adres, bestuurt welk voertuig, etc.) nemen basisregistraties ook gegevens van elkaar over.

Het doel van dit stelsel is een doelmatig en efficiënt beheer van een beperkt aantal gegevens, die nodig zijn voor de uitvoering van de taken van de overheid. De basisregistraties, inclusief hun onderlinge samenhang en de gemeenschappelijke voorzieningen die nodig zijn voor verzameling, verspreiding en gebruik[28] hebben elk een eigen wettelijk kader. De wettelijke kaders liggen dus op het niveau van de betreffende basisregistratie, niet op stelselniveau.

De politie maakt als bestuursorgaan met een publieke taak deel uit van dit stelsel. Als afnemer (de politie heeft geen rol als bronhouder) zijn we bijvoorbeeld wettelijk verplicht terug te melden wanneer wij 'gerede twijfel' hebben bij de juistheid van een gegeven dat afkomstig is van een externe bron.

Stelselafspraken en het opsporingsbelang

Voor de politie kunnen de stelselafspraken basisregistraties op gespannen voet komen te staan met het belang van de opsporing, als uit het bevragen of terugmelden valt af te leiden dat er bij de politie belangstelling is ontstaan naar een persoon, locatie, bedrijf, voertuig, etc.

De neiging kan dan zijn niet terug te melden, of een eigen registratie bij te houden die min of meer synchroon wordt gehouden met de bron en die de politie onbespied kan raadplegen. Er zijn echter elegantere oplossingen denkbaar, die wel passen binnen de stelselafspraken en die de politie niet voor allerlei beheersproblemen stelt[29].

*Figuur: stelselplaat basisregistraties, versie 1.2 (oktober 2020).
Bron: https://www.digitaleoverheid.nl/

28 bron: Visie op het stelsel van basisregistraties (2010)

29 zie Visie op terugmelden

3.2. Persoonsgegevens

3.2.1. Algemene verordening Gegevensbescherming

Op de verwerking van persoonsgegevens is in beginsel de Algemene verordening gegevensbescherming[30] (AVG) van toepassing. De AVG geldt voor alle personen, ondernemingen, organisaties en overheidsinstellingen die persoonsgegevens verwerken, dus ook voor de politie. Echter, de AVG wordt buiten toepassing gesteld voor verwerking van persoonsgegevens met het oog op de uitvoering van (kortweg) de politietaak.

Voor de politie komt dit erop neer dat de AVG exclusief van toepassing is op alle verwerkingen van persoonsgegevens voor de bedrijfsvoering, alsmede enkele taken die de politie uitvoert op verzoek van het ministerie van Justitie en Veiligheid. De AVG biedt zogenaamde open normen en biedt de mogelijkheid gegevens te verwerken voor een zelf te definiëren gerechtvaardigd doel, voor zover dit op een behoorlijke en zorgvuldige wijze gebeurt. De AVG stelt een (limitatief) aantal gerechtvaardigde algemene verwerkingsdoelen.

Behalve dat de AVG bepalingen kent met betrekking tot de doelen, termijnen en vereiste zorgvuldigheid van de verwerking, worden ook de rechten van personen over wie de gegevens worden verwerkt (de 'betrokkenen') geregeld (zie ook Rechten van betrokkenen op bladzijde 63 e.v.). Verder stelt de AVG als eis dat er passende technische en organisatorische maatregelen worden getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Bijzondere categorieën van persoonsgegevens (AVG)

Verwerking van bijzondere categorieën van persoonsgegevens onder de AVG is in beginsel verboden. Deze mogen alleen worden verwerkt onder uitdrukkelijke (vrijwillige) toestemming, of duidelijke openbaarmaking, of een zwaarwegend algemeen belang of wanneer deze gegevens noodzakelijk zijn tijdens een gerechtelijke procedure.

AVG staat verwerking van persoonsgegevens betreffende strafrechtelijke veroordeling en strafbare feiten onder zeer strikte voorwaarden toe, doorgaans alleen onder toezicht van de overheid[31]. In de praktijk zullen dit soort gegevens vaak met het oog op de politietaak worden verwerkt, dus niet onder de AVG maar onder de Wet politiegegevens. Verwerking van gegevens over personen werkzaam voor de politie in het kader van bedrijfsvoering valt onder de AVG.

3.2.2. Medezeggenschap

Verwerking van gegevens over personen werkzaam voor de politie in het kader van bedrijfsvoering valt onder de AVG.. De Ondernemingsraad heeft op basis van de Wet op de ondernemingsraden[32] instemmingsrecht op een deel van deze verwerkingen[33].

3.2.3. Wet politiegegevens

De verwerking van persoonsgegevens[34] voor de uitvoering van de politietaak valt onder de werking van de Wet politiegegevens (Wpg). Precies daar waar de AVG buiten toepassing is gesteld is dus de Wpg van toepassing. De gedachte daarbij is dat de AVG in opzet onvoldoende begrenzend is. De politie zou vanuit haar taak bijna onbeperkt noodzakelijkheid kunnen aanvoeren als grond voor verwerking. De wetgever heeft er voor gekozen evenwicht te creëren tussen het belang van effectieve taakuitvoering enerzijds en bescherming van de persoonlijke levenssfeer van burgers anderzijds. Verwerking van politiegegevens is onder voorwaarden alleen toegestaan voor een aantal

30 eur-lex.europa.eu: Algemene verordening gegevensbescherming

31 AVG artikel 10

32 Wetten.nl : Wet op de ondernemingsraden

33 WOR artikel 27 lid 1 onder k en l

34 Naast de politie zijn dat andere organisaties die (deels) de politietaak uitvoeren: Rijksrecherche, Koninklijke Marechaussee en bijzondere opsporingsdiensten: FIOD-ECD, ISZW (voorheen SIOD), NVWA-IOD en ILT/IOD

expliciet omschreven doelen. De voorwaarden voor doelmatigheid zijn bij de Wpg al van te voren vastgelegd.

Verstrekking vanuit de Wpg is beperkt tot expliciet in de wet omschreven organisaties, een zogenaamd gesloten wetsregime.

Bijzondere categorieën van persoonsgegevens (Wpg)

Verwerking van bijzondere categorieën van persoonsgegeven mag onder de Wpg plaatsvinden, maar alleen wanneer dit voor het gerechtvaardigde doel onvermijdelijk is en de gegevens in aanvulling op andere persoonsgegevens worden verwerkt. Ook hier geldt zorgvuldige verwerking, waaronder beveiliging, als voorwaarde.

3.3. Specifieke en sectorale wetgeving

Naast de wetgeving die specifiek de verwerking van gegevens regelt, zijn er ook in andere wetten bepalingen die van invloed zijn op de omgang met gegevens door de politie. Zo regelt de Wet justitiële en strafvorderlijke gegevens (Wjsg) de verstrekking van berichten van de Justitiële Informatiedienst en de arrondissementsparketten over de afloop van zaken. De Telecommunicatiewet bevat regels op het gebied van e-mail, spam en cookies bij het gebruik van internet. Ook is er sectorale wetgeving die aan de politie taken en bevoegdheden toebedeelt voor de verwerking van gegevens, bijvoorbeeld de Wegenverkeerswet, belastingwetten en vreemdelingenwetgeving.

Een opsomming van de wetten en bepalingen die werking hebben op de omgang door de politie met gegevens, wordt hier niet gegeven. Daarvoor zijn de verdragen, wetten en besluiten te raadplegen, alsmede jurisprudentie die in de loop der jaren is ontstaan[35]. Het 'juridisch kader' is wat dat betreft voortdurend in beweging en een architectuurkader is niet het document om dat in een foto te vangen.

Waar dit relevant is komen deze bepalingen terug in specifiek beleid voor de omgang met gegevens, bijvoorbeeld het verstrekkingenbeleid of het beleid bewaartermijnen.

35 Zie uitspraken.rechtspraak.nl voor een overzicht

Principes

PSD by design

Inhoud

4.Principes voor beheer van gegevens.....22
4.1. Enkelvoudige vastlegging 22
4.2. Structuur en kenmerken 26
4.3. Duurzame toegankelijkheid 32
4.4. Kwaliteit 35
4.5. Informatiebeveiliging 40

5.Principes voor bescherming van persoons gegevens 42
5.1. Doelbinding 42
5.2. Privacy by default 48
5.3. Verantwoording 59

Dit is deel II:

Principes PSD by design
concept versie 3.0 (2021)

De principes voor de omgang met gegevens die hier zijn beschreven horen bij het beleidskader PSD by design versie 3.0

Deel I:
Beleidskader
PSD by design versie 3.0

4.1. Enkelvoudige vastlegging

Gegevens worden enkelvoudig vastgelegd

Gegevens over één object worden beheerd als één logische entiteit.

Ratio: ekelvoudige vastlegging is een principe dat bijdraagt aan efficiëntie en kwaliteit van verwerking van gegevens. Van kernobjecten zijn of worden **basisregistraties** aangelegd waarin de gegevens centraal worden beheerd. **Referentiegegevens** worden als een **standaard** beheerd, zodat voorzieningen die kenmerken aan objecten willen kunnen toekennen (bijvoorbeeld maatschappelijke klasse aan een delict), een centrale bron ter beschikking hebben. Door deze gegevensverzamelingen als **gegevensdienst** aan te bieden kunnen generieke voorzieningen worden getroffen om de gegevenskwaliteit te waarborgen en het gegevensbeheer te organiseren.

Enkelvoudige vastlegging is niet hetzelfde als eenmalige opslag, of opslag op één plaats. Gegevens worden vaak op meerdere plaatsen opgeslagen, bijvoorbeeld om redenen van continuïteit, performance of bescherming tegen gegevensverlies. Het gaat er daarbij om de consistentie te waarborgen; alle verwijzingen naar gegevens over één object worden als één entiteit beheerd.

4. Principes voor beheer van gegevens

4.1.1. Basisregistraties

Van kernobjecten zijn of worden basisregistraties aangelegd

De gegevens van een kernobject worden enkelvoudig vastgelegd in een (kern)register, ongeacht hoe vaak hetzelfde object in verschillende processen geregistreerd is. De gegevens van die objecten blijven bij elk politieproces gelijk en deze zijn dus uitermate geschikt om enkelvoudig vastgelegd te worden.

Voor kernobjectgegevens die door meerdere overheidsinstanties gebruikt worden, zijn basisregistraties ingericht. Door al bekende gegevens binnen de overheid met elkaar te delen, kan de overheid efficiënter en eenduidiger opereren en de dienstverlening verbeteren. Zo hoeft een burger of bedrijf bepaalde gegevens niet steeds opnieuw aan te leveren, maar volstaat één melding.

Voor het gebruik van de basisregistraties gelden spelregels voor gegevensbeheer en -gebruik waar de politie als afnemer dus ook aan gebonden is. Allereerst is dat het verplichte gebruik: vraag de burger niet om gegevens die de overheid al heeft. Een andere verplichting die bijdraagt aan de gegevenskwaliteit is het verplicht terugmelden van geconstateerde onjuistheden. De informatievoorziening van de politie heeft toepassingsdiensten ontwikkeld om op een zorgvuldige en rechtmatige manier gegevens uit basisregistraties te kunnen betrekken. Ook is er een visie op terugmelden geformuleerd[36] waarin aandacht is voor het opsporingsbelang in relatie tot het belang van de stelselafspraken en het principe van terugmelden[37].

Metagegevens

Voor metagegevens geldt net als voor referentiegegevens: eenmaal vastgelegde kenmerken dienen te worden gebruikt en niet opnieuw te worden ingevoerd of afgeleid. Daarnaast is ook het toepassingsprofiel metadata, een template, zelf een vorm van enkelvoudige vastlegging en meervoudig gebruik.

Transactiegegevens

Een transactiegegeven wordt in de regel in één applicatie vastgelegd. Het komt voor dat gegevens over transacties door functionaliteit van meerdere applicaties worden verwerkt. Is dat het geval, dan kan voor enkelvoudige vastlegging van deze transactiegegevens een transactieregister met dataservices worden toegepast. Een zaak kan bijvoorbeeld worden gestart in meerdere voorzieningen. Door deze enkelvoudig vast te leggen en als een entiteit te beheren kan de consistentie over meerdere toepassingen worden bewaakt.

Referentiegegevens

Referentiegegevens zijn een veelgebruikte toepassing van het principe van enkelvoudige vastlegging. Het is een generiek voorkomen van een kenmerk dat enkelvoudig wordt vastgelegd (meervoudig wordt gebruikt) en niet door het operationele proces of het bedrijfsvoeringproces wordt gewijzigd. Door te onderkennen dat de kernobjecten overeenkomstige kenmerken hebben en deze als referentiegegeven te beheren, ontstaat kwaliteit en consistentie van vastlegging. Door de kleuren van voertuigen in een tabel vast te leggen, voorkomen we dat we voor een voertuig telkens de kleur zelf moeten omschrijven (zalmroze/oker/lichtbruin) en kunnen we trefzeker zoeken op kenmerken.

Referentiegegevens zijn stabiel, maar niet onveranderlijk. Standaarden worden beheerd en nieuwe referentiestandaarden worden ontwikkeld, als gevolg van ontwikkeling in het werk van de politie of externe ontwikkelingen. Bijvoorbeeld met de opkomst van *cryptocurrency* is de behoefte aan een standaard voor cryptovaluta ontstaan. Verandering van criminaliteit-en veranderende behoefte aan managementinformatie- leidt tot andere

36 zie Visie op terugmelden

37 zie Visie op terugmelden, over het onthullingsrisico bij gebruik van publieke en commerciële gegevensdiensten.

maatschappelijke klasses. Als nieuwe landen ontstaan (c.q. worden erkend), wordt de landentabel onderhouden, etc.

Naarmate de gegevenshuishouding complexer wordt moeten referentiegegevens als een standaard worden beheerd en als een dienst wordt aangeboden. De dienstverlening zal verschillen al naar gelang het een externe (bijvoorbeeld postcodes) of een interne referentiestandaard (zoals maatschappelijke klasses of gevarenklasses) is. Ze bestaat in elk geval uit het beschikbaar stellen van de gegevens, inclusief definities en een indicatie van de kwaliteit. Ook een wijzigingsproces en (in het geval van een externe bron) ook gegevens over de betreffende dienstenniveau-overeenkomst met die leverancier of bronhouder moet zijn gedefinieerd.

Inrichting binnen de politie

Binnen de politieorganisatie is de afdeling GGB de interne leverancier van referentiegegevens. Deze afdeling verzamelt bij in- en externe aanbieders referentiegegevens en ontwikkelt in samenwerking met gegevensverantwoordelijken referentiestandaarden.

GGB maakt hiervoor afspraken omtrent de betekenis, mogelijke inhoud, de wijze van levering, de updatefrequentie en verzorgt de distributie van de ontwikkelde standaard.

Daar waar mogelijk en nodig maakt de politie gebruik van externe referentiegegevens. BijvoorbeelSpir-it[38]. Deze organisatie levert referentiegegevens voor de hele strafrechtsketen aan vanuit de rechtspraak.

Overige gegevens

Voor overige gegevens geldt hetzelfde; een digitaal spoor, een conversatie op social media of registratie van een verhoor wordt enkelvoudig vastgelegd en kan door een applicatie (niet-destructief) worden bewerkt, zodat een deel ervan, of een geanonimiseerde versie ervan, in de toepassing wordt getoond. Bijvoorbeeld naar een *bodycam*-opname van twee uur kan in een applicatie worden verwezen met een tijdframe, waarbinnen het relevante stukje video kan worden getoond

38 Zie bijvoorbeeld rechtspraak.nl/Organisatie-en-contact/Organisatie/Landelijke-diensten/Spir-it

4.1.2. Voorzieningen voor continuïteit en performance (backup en redundantie)

Gegevens en back-ups worden als één logisch object beheerd

Een redundante opslagvoorziening heeft gegevens over een object op meerdere locaties staan. Als het bestand wordt gewijzigd, gewist, vernietigd, etc. gebeurt dit op alle redundante locaties ook. Het gegeven wordt beheerd als één logisch object.

Dit geldt ook voor een gegevensback-up. Als gegevens over een object (dat kan ook een persoon zijn) worden verwerkt, moet die verwerking ook op de back-up plaatsvinden. Dat kan op hetzelfde moment, maar ook later, bij het herstel vanuit de back-uplocatie (rollback). Dan kunnen ook de bewerkingen die vanaf het gekozen moment van herstel zijn verricht, opnieuw worden verricht en is weer voldaan aan enkelvoudige vastlegging.

4.1.3. Generieke gegevensdiensten

Generieke gegevensdiensten worden waar mogelijk toegepast

Om de informatievoorziening wendbaar en toekomstvast in te richten, worden toepassingsdiensten zo veel mogelijk generiek gemaakt. Dat betekent dat diensten die op meerdere plekken in de informatievoorziening voorkomen worden ingevuld met een generieke voorziening. Gegevensdiensten kunnen binnen de politie worden gebruikt, maar er zijn ook gegevensdiensten die door de hele keten worden gebruikt. Hierdoor ontstaan generieke bouwstenen waarmee gemakkelijk nieuwe toepassingsdiensten gerealiseerd kunnen worden en waarmee vernieuwingen met een eenmalige implementatie gemakkelijk in de hele informatievoorziening (in de keten) kunnen worden doorgevoerd.

Voorbeeld

Voorbeelden van generieke ketenvoorzieningen zijn de strafrechtketendatabank (SKDB), het Justitieel Documentatie Systeem (JD-Online) en het Centraal Digitaal Depot (CDD+). Het register vingerafdrukken HAVANK is een politieregister dat diensten levert aan de keten. de politie levert zelf ook toepassingsdiensten die door ketenpartners gebruikt worden zoals de basisvoorziening vreemdelingen (BVV). Voor het gebruik van deze diensten gelden spelregels die zijn vastgelegd in gebruiksovereenkomsten en convenanten.
In de informatievoorziening wordt de bevraging en de informatie-uitwisseling met deze systemen door middel van berichtenverkeer met politiesystemen uitgevoerd (in plaats van drecte systeemkoppelingen).. Op die manier kunnen ook de normen voor zorgvuldig en rechtmatig gebruik het beste worden gehandhaafd.

Een generieke gegevensvoorziening voor bijvoorbeeld geografische informatie (landkaarten en luchtfoto's) kan door meerdere toepassingen worden gebruikt. Kaartmateriaal hoeft daardoor

maar één keer te worden ingekocht en nieuwe kaarten kunnen eenvoudig in alle toepassingen worden doorgevoerd. Andere voorbeelden van generieke toepassingsdiensten zijn: autorisatie en authenticatie, logging en monitoring, maar ook matching- en vertaaldiensten. Veel van de normen en richtlijnen voor zorgvuldige en rechtmatige gegevensverwerking die in dit beleidskader beschreven worden, kunnen het beste met voorzieningen in de vorm van generieke diensten worden ingericht.

Gegevensdiensten kunnen ook worden gerealiseerd in de vorm van generieke gegevensvoorzieningen waarlangs gegevens kunnen worden beheerd en bevraagd, die in meerdere onderliggende systemen zijn opgeslagen. Gegevensdiensten zorgen er vooral voor dat het gegevensbeheer en de toepassingsdiensten onafhankelijk van elkaar worden georganiseerd.

Informatiebeveiligingsdiensten

Bij het samenstellen van informatiebeveiligingsdiensten wordt gebruik gemaakt van de ontwerprichtlijnen en beveiligingsconcepten die worden voorgeschreven door de informatiebeveiligingsarchitectuur. Een aantal van die beveiligingsconcepten is als principe in dit uitvoeringskader opgenomen:

- Kader logging
- autorisatie
- metagegevens
- kwaliteitszorg

4.2. Structuur en kenmerken

Gegevens hebben een structuur en kenmerken

Ratio: door de ordeningseigenschappen van gegevens te onderkennen en herkennen ontstaat de mogelijkheid om ze optimaal in te zetten voor het politiewerk. Door deze kenmerken kunnen gegevens worden beschermd en beveiligd en toegankelijk worden gehouden. De plaats in een datastructuur kan ook als metadata aan gegevens worden meegegeven. Zo ontstaat een datastructuur die als data-laag op zichzelf staat en robuust is tegen veranderingen in het IV-landschap.

Kenmerken kunnen direct bij registratie van gegevens worden toegekend. Aanvullend kunnen kenmerken ook worden afgeleid uit gegevens, op grond van generieke kennis over dit specifieke soort gegevens. Deze manieren van ontsluiting van gegevens (vooraf en achteraf) kunnen elkaar aanvullen.

4.2.1. Procesgericht en zaakgericht

Overheidsinformatie wordt gestructureerd naar zaken

Zaakgericht werken[39]

Informatiebeheer van overheidsinformatie is gericht op openbaarheid en transparantie van de overheid. De vraag wat de overheid heeft gedaan en op basis van welke informatie ze heeft gehandeld, staat centraal en vormt ook het ordeningsprincipe voor alle documenten die de neerslag zijn van dat handelen. [40] Overheidsinformatie wordt dus niet geordend op documenten, maar op activiteiten.

Nu voert een organisatie als de politie wel honderden verschillende activiteiten uit en de overheid als geheel vele duizenden. Om overzicht te creëren worden overeenkomstige

39 *Zie* Principes Zaakgericht werken, concept versie

40 *Zie* Beheerregeling van de politie

activiteiten aangeduid als een 'zaak'. Dit is niet de 'politiezaak' zoals we die binnen de politie kennen, maar een zaak als type activiteit van de overheid met een overeenkomstig doel en resultaat. Dat mag enigszins losjes worden gezien. Vanuit het perspectief van 'zaakgericht werken' is de afhandeling van winkeldiefstal (in alle varianten)één zaak, ondanks alle verschillende manieren waarop dat proces wordt uitgevoerd. Veel verschillende activiteiten binnen het PDC vallen ook onder één zaak, omdat ze min of meer allemaal als een dienstverlenend proces (met een aanvraag, levering en afhandeling) kunnen worden gezien.

De Nederlandse Overheid Referentie Architectuur[41] (NORA) omschrijft dit ook wel als 'zaakgericht werken'. Waarbij een zaak een samenhangende hoeveelheid werk, met een duidelijke aanleiding en een duidelijk resultaat is. Deze vereenvoudiging van de activiteiten van de overheid heeft grote voordelen voor het ordenen van overheidsinformatie.

Statusovergangen

Het concept van zaakgericht werken legt een frame van statusovergangen over de werkprocessen heen. In het politiewerk kan de rol van een betrokkene veranderen van getuige naar verdachte, of de status van de zaak van lopend naar ingestuurd of gesloten.

Het aantal stappen in een werkproces is een veelvoud van het aantal statussen. Verantwoording bestaat uit reconstructie van de statusovergangen, niet van alle processtappen. Statussen doorloop je altijd chronologisch en bij elke statusovergang kunnen de doorlopen processtappen worden geregistreerd om zo te borgen dat bepaalde (essentiële) processtappen zijn uitgevoerd.

Voor informatiebeheer is dus een zaaksysteem van belang dat gebruik maakt van goed beschreven politieprocessen. Een zaaksysteem draagt bij aan de doelen van openbaarheid en transparantie, maar kan ook belangrijk bijdragen aan de sturing en coördinatie van de dienstverlenende processen van de politie.

Zaaktypen

Herbruikbaarheid is dus van belang. De procesgang tussen twee statussen mag bij verschillende organisatieonderdelen iets verschillen zonder dat dit van invloed is op de configuratie van het zaaktype. Onderdeel van het zaakgericht werken is het principe dat overeenkomstige werkstromen en werkprocessen eenzelfde afhandeling (op hoofdlijnen!) hebben. Hiertoe onderscheiden we patronen die we zaaktypen noemen. Een zaaktype heeft bepaalde inrichtingsparameters en bedrijfsregels. Het wordt allemaal vastgelegd in een Zaaktypen Catalogus.

Resultaattypen

De uitkomst (het resultaat) van de werkstroom of het werkproces wordt geclassificeerd naar soort; het resultaattype. Bij de combinatie zaaktype -resultaattype hoort een bewaartermijn[42].

Zo is duidelijk hoe lang het bijbehorende gearchiveerde zaakdossier moet worden bewaard (blijvend bewaren of vernietigen).

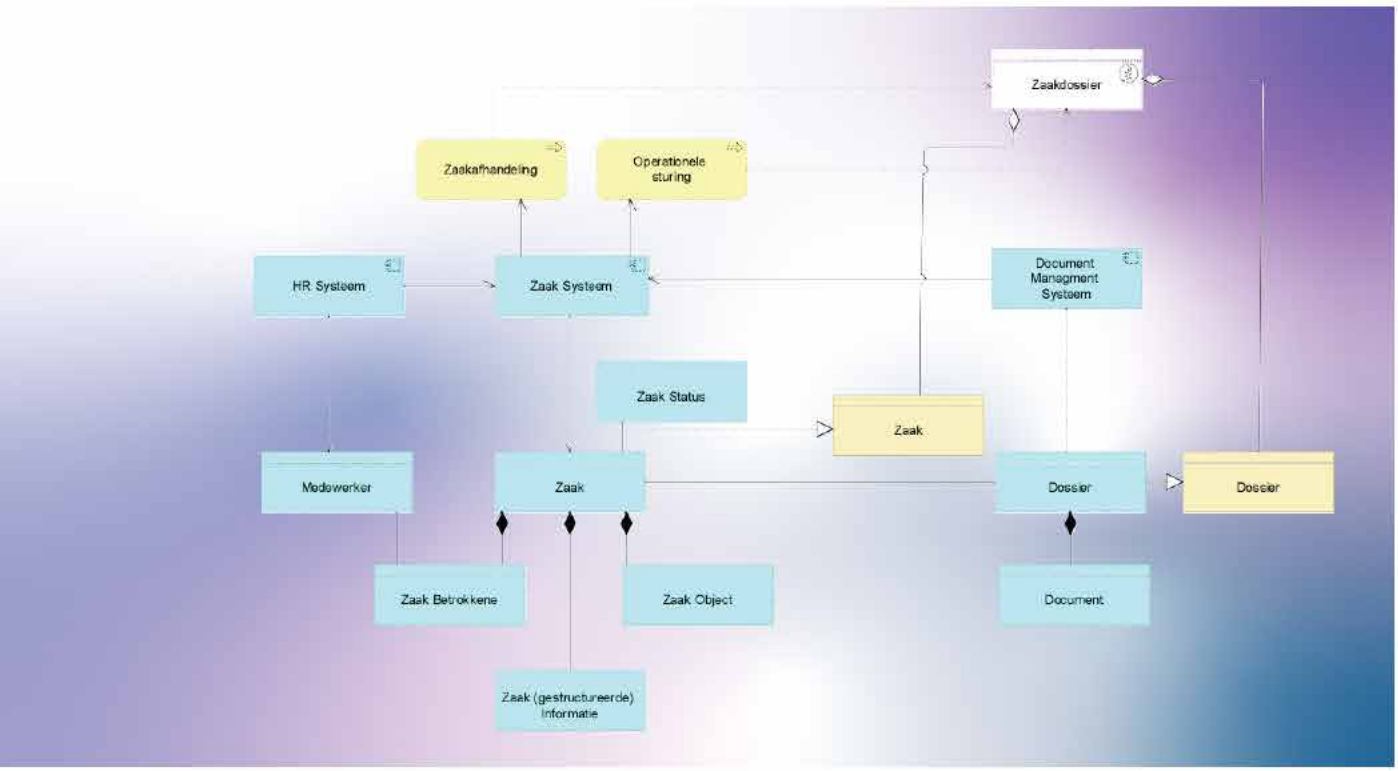
Zaakgericht archiveren

Het behandelen van zaken volgens gestandaardiseerde zaaktypen en resultaattypen is een goede manier om de kwaliteit van de werkstroom of het werkproces te definiëren en vast te leggen en daarmee te borgen.

Het digitale 'zaakdossier' bundelt, tijdens de behandeling, alle informatie over de inhoud en het proces van een zaak. Met zaakgericht archiveren kun je vanuit het perspectief van het onderliggende zaakdossier alle relevante informatie rondom de zaak verzamelen, toegankelijk, vindbaar, herbruikbaar en duurzaam beheren.

41 lees meer over de Nederlandse Overheids Referentie Architectuur op Noraonline.nl/wiki/NORA:

42 bron: noraonline.nl/wiki/NORA



Afbeelding: Proces en zaakgericht werken: schematisch overzicht met belangrijkste entiteiten

De volgende basisregels gelden voor het vullen en archiveren van een zaakdossier:

1. alle informatie die bij een zaak hoort en voor die zaak relevant en van belang is, wordt beschouwd als zaakinformatie;
2. alle zaakinformatie wordt, zodra deze beschikbaar is, digitaal opgeslagen en gebundeld in een bij de zaak horend zaakdossier;
3. zaakinformatie wordt gearchiveerd, oftewel opgeslagen als 'digitaal bewijs' van het handelen van de organisatie, zodra uit de combinatie van de inhoud en context van de informatie op enig moment volgt dat zij voor archivering in aanmerking komt;
4. informatie in het zaakdossier die niet langer relevant en van belang is voor een zaak, zoals achterhaalde en niet voor archivering in aanmerking komende conceptteksten, wordt verwijderd uit het zaakdossier zodra die informatie gemist kan worden;
5. bij het afsluiten van een zaak wordt alle (nog niet gearchiveerde) zaakinformatie in het zaakdossier óf alsnog gearchiveerd óf verwijderd uit het dossier en indien van toepassing ook vernietigd;
6. zodra bij het sluiten van een zaak[1] het zaakdossier nog slechts gearchiveerde zaakinformatie bevat, wordt dit dossier als geheel ook gearchiveerd.

1 zie Beleid Bewaartermijnen voor de criteria van een gesloten zaak

4.2.2. Toepassingsprofiel metadata

Het toepassingsprofiel metadata bevat een minimaal noodzakelijke set van gegevenskenmerken

De basisset is binnen de politie het Standaard Toepassingsprofiel Metagegevens Politie en is een standaard waarin alleen de ***noodzakelijke*** metagegevens per object zijn opgenomen. Door de standaard te gebruiken wordt geborgd dat van gegevens altijd voldoende relevante kenmerken worden vastgelegd[43] om te voldoen aan wet- en regelgeving. Om de belasting voor de operatie of bedrijfsvoering beperkt te houden, moet de hoeveelheid kenmerken die niet geautomatiseerd kan worden toegevoegd, bij registratie beperkt blijven. Hier is een verband met **kwaliteit van informatie**; de gegevens zijn van voldoende metagegevens voorzien als voldaan is aan alle wettelijke plichten (= toepassingsprofiel metagegevens) en als hieraan voldoende gegevens zijn toegevoegd om de gegevens vindbaar te maken voor het onderzoek of –algemener– het doel waarvoor ze nodig zijn. Het verder verrijken van gegevens voordat duidelijk is dat deze daadwerkelijk nodig zijn is een hoge investering met een onzekere opbrengst.

Wel kan er vanuit wetenschappelijk oogpunt of de behoefte aan beleids- en sturingsinformatie aanleiding zijn gegevens verder te analyseren om onderlinge verbanden of kenmerken te ontdekken en vast te leggen. Dat kan zeer de moeite waard zijn, maar moet van geval tot geval worden beoordeeld.

Politiegegevens worden beschermd met extra kenmerken: uit de verwerking moet, voor zover mogelijk, blijken of een persoon verdachte, slachtoffer of getuige is of dat het om een derde gaat die contact heeft met een verdachte of veroordeelde[44]. Ook moeten, voor over mogelijk, politiegegevens die op feiten zijn gebaseerd worden onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd[45], bijvoorbeeld bij de vastlegging van politiegegevens in mutaties en processen-verbaal.

Worden er persoonsgegevens geautomatiseerd van kenmerken voorzien, dan moeten ook feiten (harde metadata) en meningen (afgeleide kenmerken met een bepaalde betrouwbaarheid) worden onderscheiden.

In het toepassingsprofiel metagegevens zijn daarom de volgende kenmerken opgenomen

- Grondslag voor verwerking;
- Voor gegevens die worden verwerkt onder artikel 9 en 10 Wpg
  - De herkomst van de gegevens
  - De wijze van verkrijging;
- Logginggegevens van elke verwerking (o.a. timestamp, user).

43 Voor zover de gebruiker hiertoe door de applicatie in staat wordt gesteld

44 Wpg artikel 6b

45 Wpg artike 4 derde lid

4.2.3. Classificatie informatiebeveiliging

De beveiliging wordt ingericht op basis van proceskenmerken

De politie hanteert voor de toepassing van informatiebeveiliging een scherp normenkader. Dat kader is in de informatiebeveiligingsarchitectuur verder uitgewerkt. Naast de scherpere inhoudelijke normen is het normenstelsel van de politie ook flexibel, in die zin dat per beveiligingsprincipe (beschikbaarheid, integriteit en exclusiviteit) gekozen kan worden voor de niveaus hoog, midden en laag. De getalsmatige richtlijnen kunnen op basis van de risico's, het belang van het proces en de informatie, naar beneden of boven worden bijgesteld.

Binnen de politie verschilt de mogelijke impact van een verstoring in een politieproces per beveiligingsprincipe. Om deze reden is het belangrijk om te nuanceren per politieproces door een goede afweging te maken per beveiligingsprincipe. Door een afweging per beveiligingsprincipe te maken ontstaan er 27 verschillende combinaties van beveiligingsniveaus. Uit de praktijk zal blijken of een aantal niveaus vaker of zelden voorkomt in verband met het creëren van standaardservicepakketten vanuit de Dienst ICT.

Voorbeeld:

Voor de noodhulp:

- beveiligingsprincipe beschivkbaar; beveiligingsniveau hoog;
- beveiligingsprincipe integriteit: beveiligingsniveau hoog;
- beveiligingsprincipe exclusiviteit: beveiligingsniveau midden.

In de tabel wordt voor de overzichtelijkheid uitgegaan van laag, midden en hoog. Deze termen zijn in de architectuur nader uitgewerkt per beveiligingskenmerk, in totaal negen kenmerken. Deze kenmerken fungeren als een brug in taalgebruik tussen business en uitvoering. Ze zijn in verschillende documenten vastgelegd.[46]

v

		Laag	Midden	Hoog
Beschikbaarheid	Proces	Functioneert in principe ongestoord tijdens de afgesproken dienstverleningsuren, .. .		
	verstoringen	Maximaal 20 per jaar;	Maximaal 12 per jaar;	Maximaal 6 per jaar;
		maximaal 16 uur, gemiddeld 8 uur.	Maximaal 8 uur, gemiddeld 4 uur.	Maximaal 1 uur, gemiddeld ½ uur
	Totale storingsduur per jaar	160 uur.	48 uur.	3 uur.
Exclusiviteit	Toegang	Toegang tot het proces is voorbehouden aan bevoegd personeel, onbevoegden worden geweerd.		
	Informatie braak-bestendigheid (duur)	8 uur.	24 uur.	1 week.
	Bestendigheid tegen misbruik van procesonderdelen (voorbereidingstijd in uren)	Minimaal 8 uur	Minimaal 24 uur	Minimaal 1 week.
	Detectie en respons	Misbruik van een of meerdere bouwstenen van het proces wordt direct gesignaleerd		
		In het geval van misbruik worden direct na signalering tegenmaatregelen genomen.		
	Herstel naar normaal	binnen 16 uur		Binnen 8 uur
Integriteit		Het proces is reproduceerbaar, controleerbaar en wordt één keer per maand gecontroleerd.		
	Herstel is mogelijk naar eerder moment	Binnen 24 uur.	Binnen 16 uur.	Binnen 8 uur.

.

4.3. Duurzame toegankelijkheid

Overheidsinformatie is duurzaam toegankelijk

Ratio: Duurzame toegankelijkheid (DUTO) gaat over toegankelijkheid van overheidsinformatie die toekomstbestendig is. Er ligt een relatie tussen eisen aan de kwaliteit van gegevens en eisen aan duurzame toegankelijkheid. Waar kwaliteit ingaat op de aspecten die gegevens waardevol maken, gaat DUTO over de toegankelijkheid van de gegevens, ook op de langere termijn. 'Beschikbaarheid' is ook een kwaliteitsaspect, want wat niet beschikbaar is kan geen waarde toevoegen. Maar DUTO geeft een concreter toetsings kader om te beoordelen of informatie bestand is tegen de veranderingen in de manier waarop, of omstandigheden waaronder, gegevens worden opgeslagen en ontsloten.

Informatie moet duurzaam toegankelijk zijn om **verantwoording** af te kunnen leggen over ons handelen als (overheids)organisatie en om te bewaren wat cultuurhistorisch van belang is. Op gegevensniveau ligt er een relatie met het herkennen van een structuur van **processen en zaken** in informatie (zie Procesgericht en zaakgericht op bladzijde 26). Op het niveau van de informatievoorziening is dit vertaald in eisen aan **conversie** en **migratie**.

4.3.1. Duurzame toegankelijkheid

De waarde van informatie is bestand tegen veranderingen, ook op de lange termijn

Digitalisering van overheidsinformatie brengt met zich mee dat informatie vluchtig is en kwetsbaar. De focus verschuift van archivering na afloop van het werkproces naar informatiebeheer vanaf het eerste moment dat informatie in een werkproces beschikbaar komt. Met andere woorden: Informatiebeheer (gericht op toegankelijk maken) en informatiegebruik (gericht op gebruik voor het werkproces) komen samen te vallen op hetzelfde moment

Informatie wordt beschouwd als toegankelijk wanneer ze voor de juiste personen en op het juiste moment vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar is.[47] Informatie is vervolgens ook *duurzaam* toegankelijk als ze, vanaf het moment van ontstaan en voor zo lang als ze nodig is, vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar blijft. Dit betekent dat de inhoudelijke waarde van de informatie bestand moet zijn tegen veranderingen, ook op lange termijn.

47 Bron: Normenkader duurzame toegankelijkheid overheidsinformatie (DUTO).

Vindbaar
1. doorzoekbaar
2. metagegevens

Leesbaar
3. bestandsformaat
4. weergave
5. export

Beschikbaar
6. recht op inzage
7. openbaar deelbaar
8. bewaartermijn
9. vernietiging
10. overdracht

Interpreteerdbaar
11. informatiemodel
12. rubricering

Betrouwbaar
13. beveiligd

Vindbaar

1. De informatie van de politie is op efficiënte, effectieve wijze doorzoekbaar en vindbaar voor daartoe geautoriseerde medewerkers, binnen acceptabele tijd en inspanning. Het doorzoeken en vinden van informatie kan op alle momenten en locaties waarop die personen dat noodzakelijk achten.
2. De informatie van de politie is voorzien van volledige en actuele metagegevens conform het Toepassingsprofiel Metagegevens Politie

Leesbaar

3. De informatie van de politie wordt opgeslagen in het oorspronkelijke bestandsformaat én in een duurzaam toegankelijk bestandsformaat. Het gekozen duurzaam toegankelijke formaat is conform de voorkeursformaten van het Forum Standaardisatie, het Nationaal Archief en/of de standaard zoals afgesproken in ketenververband.
4. Van elke informatieobject van de politie is een weergave beschikbaar, binnen redelijke tijd en inspanning, voor daartoe geautoriseerde medewerkers. Dit kan op alle momenten en locaties waarop die personen dat noodzakelijk achten.
5. Van elk informatieobject van de politie is een export beschikbaar, binnen redelijke tijd en inspanning, voor daartoe geautoriseerde medewerkers. Dit kan op alle momenten en locaties waarop die personen dat noodzakelijk achten.

Beschikbaar

6. De informatie van de politie is zonder technische of procedurele belemmeringen in te zien en te gebruiken door alle personen die daartoe geautoriseerd zijn op basis van wet- en regelgeving en intern politiebeleid. Dit recht op inzage geldt zowel voor de politiemedewerkers zelf als voor gebruikers van buiten de organisatie.
7. Als een informatieobject van de politie slechts gedeeltelijk is in te zien en te gebruiken, dan zijn er een weergave en export beschikbaar waarin alleen de openbare delen zijn opgenomen.
8. de politie past een vastgestelde selectielijst toe op al haar informatie door aan elk informatieobject een bewaartermijn toe te kennen. Dit geldt voor de informatieobjecten die zijn gecreëerd of ontvangen vanaf de vorming van de Nationale Politie, per 1 januari 2013, alsmede voor alle historische informatie die de politie beheert vanuit eerdere organisatievormen.
9. De informatie van de politie wordt niet eerder en niet later vernietigd dan is aangegeven in de selectielijst [PM] die van toepassing is. Na het vernietigen is er een verklaring van vernietiging beschikbaar, opgesteld conform intern politiebeleid.
10. De informatie van de politie die, conform de selectielijst, in aanmerking komt voor blijvende bewaring wordt binnen twintig jaar overgebracht naar een archiefbewaarplaats. Na het overbrengen is er een verklaring van overbrenging beschikbaar, opgesteld conform intern politiebeleid.

Interpreteerbaar

11. Er is een informatiemodel met een beschrijving van alle informatieobjecten die de politie ontvangt en creëert bij de uitvoering van haar taken, inclusief de onderlinge samenhang, structuur en betekenis.
12. Door rubricering van informatie wordt bepaald aan welk toegankelijkheidsniveau de informatieobjecten moeten voldoen.

Betrouwbaar

13. De informatieobjecten van de politie zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen, conform de geldende wet- en regelgeving en het interne politiebeleid.

4.3.2. Conversie en migratie

Gegevens blijven toegankelijk in nieuwe toepassingen door conversie en migratie

Conversie en migratie van gegevens zijn middelen om de context, inhoud, vorm en structuur van de digitale gegevens te behouden, waarmee op de lange termijn de authenticiteit, integriteit, betrouwbaarheid, leesbaarheid en raadpleegbaarheid van de gegevens wordt veiliggesteld.

Onder conversie wordt verstaan: het omzetten van een informatieobject van het ene medium naar het andere, of van het ene formaat naar het andere.[48] Conversie pas je toe als een informatieobject onvoldoende toegankelijk is of dreigt te worden. Het resultaat van de conversie is een reproductie (gelijkluidende weergave) die het origineel vervangt in een andere gedaante (format) of op een andere drager. Bijvoorbeeld het overzetten van een informatieobject op een CD-rom naar een fileshare, of het omzetten van een TIFF naar JPEG.

Onder migratie wordt verstaan: een handeling waarbij informatieobjecten worden overgezet van het ene systeem naar het andere, met behoud van authenticiteit, integriteit, betrouwbaarheid, leesbaarheid en raadpleegbaarheid.[49]

Bij migratie komen de gegevens in een volledig nieuwe omgeving terecht van hard- en of software (dus van besturings- en/of toepassingsprogrammatuur). Bijvoorbeeld: bij het uitfaseren van systemen zoals HKS of onderdelen van BVH moeten de gegevens die daarin zijn opgeslagen worden veiliggesteld in een omgeving waar ze beheerd kunnen worden. Dit kan het nieuwe vervangende systeem zijn of een tijdelijke voorziening die het in ieder geval mogelijk maakt om gegevens te raadplegen, te corrigeren en op termijn te verwijderen.

4.3.3. Generieke voorziening en dienst

Er is een generieke voorziening voor duurzaam informatiebeheer

Een generieke voorziening voor Duurzaam Informatiebeheer is noodzakelijk voor adequaat dossier- en documentbeheer. Er is een nauwe relatie tussen documentmanagement, dossiermanagement en case management.

Deze generieke dienstverlening voor duurzaam informatiebeheer wordt op een uniforme wijze ingericht voor de organisatie. Al bij procesontwerp is het relevant rekening te houden met de beschreven generieke informatiebeheer activiteiten en de daarvoor ontwikkelde informatie-services. Een afwijking van de architectuur dient altijd goed onderbouwd te worden. Bestaande werkprocessen, organisatieonderdelen en informatievoorziening moeten mogelijk (her)ontworpen worden om aan te sluiten bij deze dienstverlening.

Informatie is vanaf het ontstaan al digitaal deelbaar. Nieuwe informatie wordt direct in een procesondersteunende applicatie opgeslagen die voldoet aan dit beleidskader. Het Documentmanagement systeem (DMS) voldoet daaraan en kan voor andere procesondersteunende applicaties de informatie duurzaam toegankelijk bewaren.

48 Begrippenkader DUTO (ontleent aan NEN-ISO 15489)

49 Begrippenkader DUTO (ontleent aan NEN 2082)

4.4. Kwaliteit

Kwaliteit is de waarde van gegevens voor de politie en de strafrechtketen

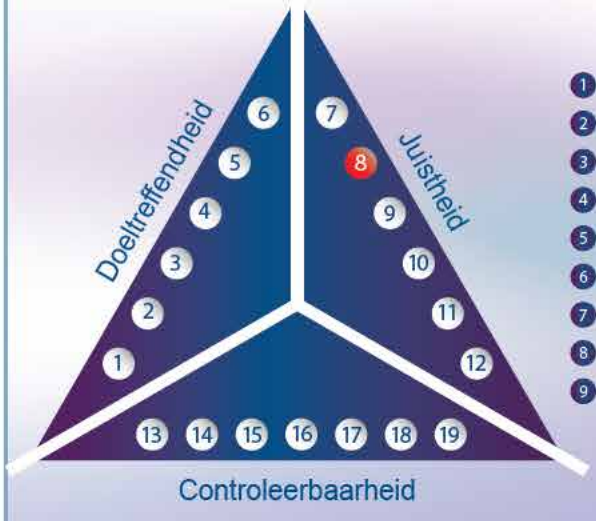
Ratio: Kwaliteit van gegevens gaat over de waarde van gegevens voor de politie en/of voor de strafrechtketen. Alleen gegevens van (enige) kwaliteit hebben ook waarde en kunnen waarde toevoegen. Maar wat goed genoeg is, is afhankelijk van het doel waar de gegevens voor worden gebruikt. De criteria voor verwerking van Big Data of gegevens van open bronnen kunnen andere zijn dan de criteria voor de kwaliteit van een proces-verbaal, of een zaaksdossier.

Gegevens kunnen directe waarde leveren in de vorm van een relaas, bewijs, een aanwijzing, etc. of indirect doordat verantwoording of beheer van overheidsinformatie mogelijk wordt. Alle soorten gegevens kunnen op een of andere wijze bijdragen aan kwaliteit.

Voor goede zorg voor kwaliteit is het van belang de gegevens te definiëren, criteria op te stellen waaraan gegevens (voor dat doel) moeten voldoen en de afweging te maken wat de gegevens waard zijn en hoeveel het (dus) waard is te investeren in de kwaliteit. Voor het formuleren van de kwaliteitseisen hanteert de politie het raamwerk van kwaliteitskenmerken[50] voor de strafrechtketen.

De criteria van het raamwerk vullen elkaar aan en concurreren in zekere zin ook met elkaar. Gegevens kunnen bijvoorbeeld niet volledig 12.actueel en direct 10.beschikbaar zijn en tegelijkertijd 1.100% correct. Immers: om de correctheid te controleren is wat tijd nodig, en daardoor zijn ze niet meer (allemaal) helemaal actueel zodra ze beschikbaar zijn. Die 'spanning' doet zich tussen andere criteria ook voor. Met andere woorden: Kwaliteit is een optimum – geen maximum – van kwaliteitskenmerken waar zo goed mogelijk aan is voldaan vanuit het belang voor het ***gebruik*** van de gegevens..

50 PM Raamwerk kwaliteitskenmerken van de strafrechtketen zoals opgesteld door het ministerie van V&J op basis van DAMA DM-BOK en IDQ. De IDQ-kenmerken die het DAMA-model niet onderkent, zijn veelal niet goed meetbaar of zijn een verzamelkenmerk. Derhalve is voor het raamwerk uitgegaan van de kenmerken van het DAMA-model aangevuld met enkele IDQ-kenmerken.



Het document[51] dat het raamwerk van kwaliteitskenmerken voor de strafrechtketen in detail beschrijft, bevat per kenmerk een nadere omschrijving en ook de mogelijke maatregelen waarmee betrokkenen (specifiek ontwikkelaars en gebruikers) de kwaliteitsrisico's kunnen verminderen. Hieronder wordt ingegaan op enkele specifieke kenmerken uit het kwaliteitsraamwerk

4.4.1. Correctheid (1), referentiële integriteit (2)

Correctheid en referentiële integriteit zijn de basis voor kwaliteit

Eén fout kan leiden tot een hele gegevensverzameling die is gekoppeld aan een verkeerde persoon, verkeerd voertuig etc. De fout 'sleept' als het ware de gegevenshuishouding rondom dat object met zich mee. Het voorkomen en opsporen van fouten in kernobjectgegevens is om deze reden ook essentieel voor **uniciteit (16)**. Voor elk kernobject kan een basisset van kenmerken – referentiegegevens dus – worden gedefinieerd die in combinatie met elkaar juiste identificatie van een persoon, voertuig, etc. mogelijk maken. Een basisset die werkbaar is maar voldoende uitgebreid om dubbelingen uit te sluiten. Referentiegegevens spelen een sleutelrol voor de kwaliteit van gegevens.

De kwaliteitszorg van **transactiegegevens**, waar de kwaliteit uiteindelijk zichtbaar in wordt, is dus van groot belang maar wordt beïnvloed door een goede gegevenshuishouding onder water.

4.4.2. Consistentie (14) en eenduidigheid (15)

Gegevens worden gedefinieerd

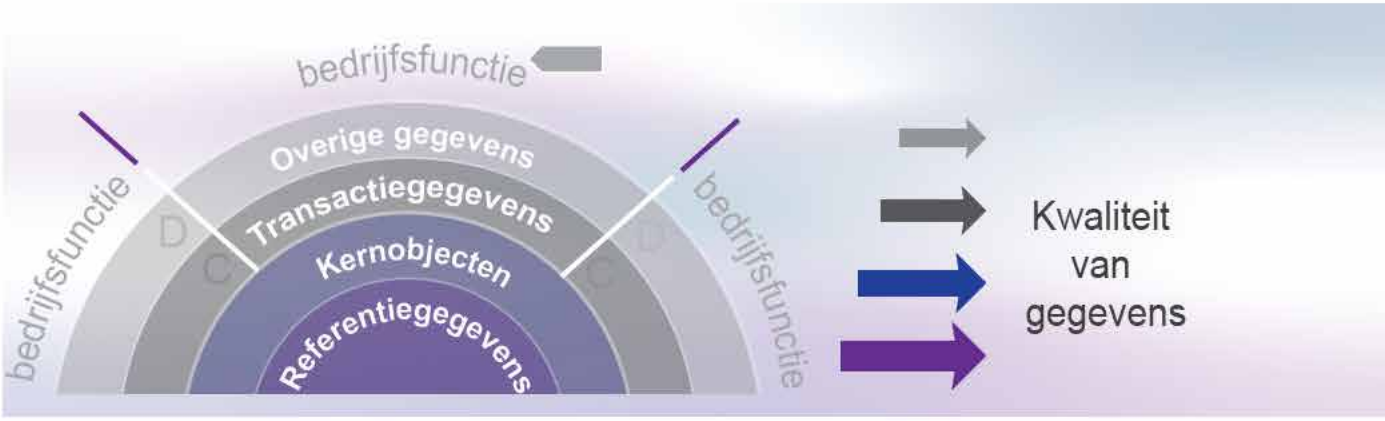
Definities zijn generieke beschrijvingen van een specifiek gegeven. Definities zijn geen metagegevens, want ze worden niet opgeslagen bij een gegeven en verwijzen ook niet naar een specifiek gegeven.

- Van bedrijfsobjecten stellen we een definitie op. Bedrijfsobjecten zijn de bedrijfsbegrippen waar de politie gegevens over verwerkt of wil verwerken. Het Bedrijfsobjectenmodel (BOM) geeft een opsomming van deze bedrijfsobjecten per business-domein (bijvoorbeeld jeugd of high impact crime) met de belangrijkste relaties hiertussen.[52]
- Referentiegegevens definiëren we om aan te geven wat we met dit specifieke kenmerk bedoelen (bijvoorbeeld 'maatschappelijke klasse') en elke mogelijke waarde van dat kenmerk (wat is een 'diefstal uit een voertuig' en wat is een 'woninginbraak').
- Metagegevens worden ook gedefinieerd, bijvoorbeeld in het toepassingsprofiel metagegevens (zie Toepassingsprofiel metadata op bladzijde 29). Het bestandtype en formaat van berichten worden ook gedefinieerd. Dit is een essentiële voorwaarde voor het zinvol en efficiënt uitwisselen van gegevens.
- Transacties worden meestal gedefinieerd aan de hand van een procesbeschrijving.

Definiëren lijkt triviaal maar het is van groot belang voor de kwaliteit van gegevens om alle bedrijfsbegrippen (kernobjecten en referentiegegevens) te definiëren. Daarmee wordt de betekenis uitgedrukt die ze voor het werk (operatie of bedrijfsvoering) hebben en kan

51 Raamwerk en stappenplan gegevenskwaliteit Strafrechtsketen, Ministerie van V&J, 11 november 2015

52 Het Politiegegevensmodel (PGM) kan worden gezien als een gegevensgerichte invulling van het BOM, waarbij bedrijfsobjecten uit het BOM geïmplementeerd worden in de logische onderdelen van het PGM.



worden bepaald of de gegevens voor een bepaald doel zinvol kunnen worden gebruikt, dus van waarde zijn.

4.4.3. Validiteit (6), relevantie (7) en universaliteit (8)

Gegevens zijn geldig en van toepassing voor het gebruik

De gegevensdefinities worden weer gebruikt in bedrijfsregels. Op basis van definities en afgeleid van het politiewerk worden afspraken gemaakt over het domein van waardes die gegevens kunnen hebben.[53] Validiteit is dus de mate waarin gegevens vallen binnen de verwachtingen die we op basis van definitie van hebben.

Gegevens die afwijken van die waardes zijn ongeldig en leiden tot uitval in het proces. Deze fouten moeten worden hersteld voor ze weer waarde kunnen toevoegen.

Aanverwante, maar lastiger waar te nemen aspecten zijn relevantie en universaliteit. Dat stelt dat gegevens geldig en ter zake dienend moeten zijn voor het doel waarvoor ze worden gebruikt. Niet in een rechtmatige zin, maar in de zin van representativiteit. Dat gaat niet altijd goed, vooral niet bij de toepassing van grote, ongestructureerde gegevensverzamelingen (Big data). Oververtegenwoordiging van een kenmerk in een bepaalde set gegevens kan voor een bepaalde toepassing geen probleem zijn en in een volgende toepassing problematisch. Gegevens die dus het ene moment nog van goede kwaliteit waren, zijn het voor de volgende toepassing niet, zonder dat er iets met die gegevens is gebeurd. De kwaliteitszorg voor *big data* vraagt dus aparte aandacht.

Gelet op het gebruik van *big data*-diensten is de individuele juistheid van bepaalde gegevens mogelijk minder van belang. Als de 'trend' die wordt gevonden er niet wezenlijk door wordt beïnvloed, kan er aardig wat tolerantie voor fouten in de dataset zitten. Aan de andere kant vraagt kwaliteitszorg veel aandacht voor de selectie van gegevens die wordt gemaakt en de wijze waarop hier (met bijvoorbeeld een algoritme) conclusies aan worden verbonden. Er moet oog zijn voor systematische fouten, selectie-bias en aandacht voor transparantie en uitlegbaarheid van de gekozen data en toegepaste analyse[54]

53 Voor zowel bedrijfsbegrippen als bedrijfsregels is een leidraad opgesteld Zie Leidraad opstellen begripsdefinities en Leidraad opstellen bedrijfsregels op Agora.

54 Zie hiervoor ook het kwaliteitskader *Big Data*

4.4.4. Volledigheid (3) en aannemelijkheid (5)

De mogelijkheid dat informatie niet (geheel) waar is wordt aanvaard, onderzocht en geregistreerd.

Het kwaliteitsaspect van volledigheid (de hele waarheid) en aannemelijkheid (de kans op waarheidsgetrouwheid) is voor elke organisatie relevant, maar voor de politie (en het OM) wel in bijzondere mate.De politie is 'in de business' van vermoedens, valse verklaringen, desinformatie, *deep fakes*, identiteitsfraude, voertuigfraude, etc. Gegevenskwaliteit is voor de politie een kwestie van zorgvuldig registreren van gegevens zoals die ons worden aangereikt, en tegelijkertijd een kwestie van het aanvaarden en onderzoeken van de kans ze de waarheid niet (geheel) weergeven. Door de aannemelijkheid van gegevens goed te onderzoeken en herleidbaar te registreren kan ook valse informatie heel goed waarde toevoegen.

Wanneer gegevens worden gecorrigeerd, moet dat onderscheid door de politie ook helder worden gemaakt.[55] Is het onderdeel van kwaliteitszorg, waarbij we gegevens zo veel mogelijk in overeenkomst met de werkelijkheid willen houden? Dan zijn het feitelijke gegevens. Of is hier sprake van waarheidsvinding in het kader van een vermoeden van misleiding of een (ander) strafbaar feit? Worden de gegevens (mogelijk) betwist door betrokkenen? Dan zijn het vermoedens – even waardevol, maar geen (gegevens)kwaliteitszorg.

4.4.5. Traceerbaarheid naar de bron (17) en gebruiker (18)

Kwaliteit is objectiveerbaar

Gegevenskwaliteit is een kwestie van zorgvuldig registreren van het feit, maar ook van de bron van de gegevens en de gebruiker die het heeft geregistreerd. Traceerbaarheid maakt kwalitieit objectiveerbaar en controleerbaar.

4.4.6. Legaliteit (9)

Rechtmatig verwerkte gegevens voegen meer waarde toe

Het legaliteitsaspect,- het rechtmatig verwerken van gegevens- is behalve een randvoorwaarde voor de omgang met gegevens ook een aspect van kwaliteit: rechtmatig verwerkte gegevens voegen meer waarde toe dan niet rechtmatig verwerkte gegevens, o.a. omdat ze als bewijslast kunnen worden meegenomen in een zaak en in de verdere rechtsgang niet terzijde worden geschoven. Het onrechtmatig verwerken van gegevens doet ook in meer algemene zin afbreuk aan (de waarde van) de politie doordat het de positie van betrouwbare partner en verwerker van gevoelige informatie verzwakt.

Dit aspect is bijvoorbeeld relevant voor gegevens die worden onttrokken aan publieke websites of andere openbare bronnen of multimedia-gegevens die door burgers worden aangereikt bij een incident. Omdat verwerking van deze gegevens niet valt binnen de bevoegdheden van art. 3 Politiewet en/of doordat de betrouwbaarheid van de bronnen veelal niet bekend is, moet deze met de nodige voorzichtigheid worden gebruikt.

55 Wpg artikel 4 lid 3: Voor zover mogelijk worden politiegegevens die op feiten zijn gebaseerd onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.

4.4.7. Beheerbaarheid (13)

Waar mogelijk wordt aangesloten op (keten)standaarden

Gegevens voegen waarde toe aan de politie of aan de strafrechtketen als ze zonder verlies door conversie of uitval kunnen worden verwerkt of uitgewisseld. Het gebruik van bestaande overheids- en ketenstandaarden bevordert deze uitwisseling en de interoperabiliteit van systemen, bijvoorbeeld in het berichtenverkeer. Het gebruik van overheids- en ketenstandaarden draagt tevens bij aan de ontwikkeling en het gebruik van ketenvoorzieningen. Dit vraagt om standaardisatie en uniformiteit in de informatievoorziening en ondersteunende processen. De organisatie hoeft minder zelf te ontwikkelen en het rendement van voorzieningen neemt toe. Daar waar de organisatie eigen keuzes maakt en in haar eigen informatievoorziening afwijkt van standaarden worden afspraken gemaakt over koppelvlakken bij gegevensuitwisseling met externe partijen.

Voor de rijksoverheid zijn vele standaarden gedefinieerd op het gebied van gegevensverwerking. Deze standaarden zijn niet allemaal automatisch op de politie van toepassing omdat de politie geen deel uitmaakt van de sector Rijk. Het kan niettemin toch verstandig zijn om zoveel mogelijk bij deze standaarden aan te sluiten omdat hiermee de samenwerkingsmogelijkheden met andere overheidsorganisaties worden vergroot.

Ketenstandaarden

Ten behoeve van samenwerking met organisaties in de strafrechtketen sluit de politie aan bij de standaarden voor elektronisch berichtenverkeer van de Justitiële Informatiedienst (Just-ID)[56]. De politie werkt mee aan de keuze voor een standaard voor biometrische gegevens in de veiligheidsketen om ervoor te zorgen dat biometrische gegevens kunnen worden uitgewisseld ten behoeve van identiteitsvaststelling. Zie ook de standaarden die gelden in de strafrechtketen[57] en in de vreemdelingenketen.[58]

Open standaarden

De Nederlandse overheid stimuleert het gebruik van open standaarden. Een open standaard (of norm) is publiekelijk beschikbaar. De specificaties van de standaard mogen vrij van licentierechten worden toegepast, gebruikt en gehanteerd. De term wordt vooral gebruikt bij hard- en software, omdat juist daar traditioneel ook veel gesloten standaarden worden gebruikt, waarbij men voor de inzage van de specificaties een licentie dient aan te vragen, of anders afhankelijk is van één leverancier. Het Forum Standaardisatie houdt een lijst bij van open standaarden[59] waarvoor in de publieke sector een in principe verplicht (*comply or explain*) gebruik geldt.

4.4.8. Andere aspecten van de informatievoorziening

De beschikbaarheid (10), tijdigheid (11) en actualiteit (12) van gegevens steunt op bovengenoemde aspecten maar wordt concreet gerealiseerd door een informatievoorziening die voldoet aan de eisen van informatiebeveiliging. Ook exclusiviteit (19) door autorisatie is een onderdeel van het stelsel van maatregelen voor informatiebeveiliging.

56 justid.nl/organisatie/ebv/ebv_standaarden.aspx

57 noraonline.nl/wiki/Standaarden_informatievoorziening_strafrechtsketen

58 digitaleoverheid.nl/document/architectuur-van-de-vreemdelingenketen/

59 forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

4.5. Informatiebeveiliging

Informatie wordt beveiligd met een adequaat stelsel van maatregelen

Ratio: informatiebeveiliging heeft een functie in de bescherming van persoonsgegevens en daarnaast een tactisch belang: de gerede uitvoering van de politietaak en de bedrijfsvoering is niet mogelijk zonder adequate beveiliging van informatie. Absolute beveiliging is doorgaans onbetaalbaar en ook onwenselijk: kenmerken van informatiebeveiliging staan onderling enigszins op gespannen voet met elkaar en er moet per risico voor een optimale beveiliging worden gekozen.

De informatiebeveiliging wordt onder meer geborgd op niveau van de infrastructuur, waar de afzonderlijke applicaties en voorzieningen deel van uitmaken. Voor alle **segmenten** van de infrastructuur worden maatregelen op basis van risicobeheersing genomen. Het stelsel van maatregelen omvat het voorgeschreven gebruik van **generieke voorzieningen** voor informatieveiligheid bij de ontwikkeling van gegevensverwerkende toepassingen, zoals voor **identificatie en authenticatie** en voor **logging**.

4.5.1. Segmentatie

De informatievoorziening wordt gesegmenteerd

De informatievoorziening wordt op basis van risicoprofielen georganiseerd in verschillende onderdelen met gecontroleerde koppelvlakken. De koppelvlakken worden systematisch beschreven en beheerd met specifieke beveiligingsmaatregelen. Deze maatregelen verschillen in type en werking zodat er meerdere, complementaire lagen van beveiliging ontstaan die de weerbaarheid verhogen tegen bedreigingen van verschillende aard.

4.5.2. Risicobeheersing

De benodigde risicobeheersing wordt bepaald op grond van kenmerken van gegevens

De informatiebeveiligingsarchitectuur biedt een methode voor risicobeheersing door middel van risicoanalyses op basis van beveiligingskenmerken. Naast de bekende beveiligingskenmerken als beschikbaarheid, integriteit en vertrouwelijkheid zijn dit ook andere kenmerken zoals de waarde van informatie, de oorsprong van informatie en het belang van informatie voor het proces.

De beschikbaarheid van informatiediensten dient te voldoen aan de met de verantwoordelijke gemaakte continuïteitsafspraken. Onderdeel van de risicobeheersing is het beschikbaar hebben van terugvalmogelijkheden voor zowel systemen als gegevens.

4.5.3. Logging

Elke verwerking van gegevens wordt gelogd

In de Wpg ziet art. 32a straks toe op logging. Uit de concepttekst van het wetsvoorstel [60] volgt dat gezorgd moet worden voor logging van tenminste de volgende verwerkingen van politiegegevens in geautomatiseerde systemen:

- verzameling;
- wijziging;
- raadpleging;
- verstrekking onder meer in de vorm van doorgiften;
- combinatie;
- het vernietigen.

Tevens moet de identificatie van de persoon die de persoonsgegevens heeft geraadpleegd of bekend gemaakt, worden geregistreerd.

60 Zie het beleidskader logging en de hierin als bijlage opgenomen concepttekst voor het wetsvoorstel.

Daarnaast de datum en het tijdstip van handelen en zo mogelijk de identiteit van de ontvangers (bij verstrekken en doorgiften).

De vastgelegde gegevens worden uitsluitend gebruikt voor:

1. de controle van de rechtmatigheid van de gegevensverwerking;
1. interne controles;
1. ter waarborging van de integriteit en de beveiliging van de politiegegevens;
1. strafrechtelijke procedures.

4.5.4. Generieke voorzieningen

Er zijn generieke diensten voor informatiebeveiliging

Dat de informatiebeveiliging, onder meer, is geregeld op het infrastructurele niveau brengt met zich mee dat er bij de ontwikkeling van applicaties en toepassingen gebruik wordt gemaakt van generieke voorzieningen voor informatiebeveiliging. Centrale autorisatie, *single sign-on*, compartimentering, etc. zijn immers niet te regelen binnen een applicatie zelf.

Identity- en access management

Toegang tot de informatievoorziening dient uniek herleidbaar te zijn tot een persoon, organisatie of geautomatiseerd systeem en dient uitsluitend te worden toegestaan op basis van de rechtmatige uitvoering van opgedragen werkzaamheden.

De 'toegang' tot (persoons)gegevens kent twee aspecten: toegang tot bepaalde verwerkingen enerzijds en toegang tot een bepaald gegevensdomein anderzijds. De verwerkingen op gegevens die in applicaties en voorzieningen mogelijk zijn, zijn terug te brengen tot een aantal basale verwerkingen waaronder lezen, schrijven, wissen, vernietigen en verlenen van toegangsrechten. Andere verwerkingen (bijv. het hernoemen van bestanden, verrichten van zoekslagen, etc.) zijn een vorm of combinatie van deze basisverwerkingen. De toegang tot gegevensdomeinen bepaalt op welk domein van gegevens de toegestane bewerkingen zijn toegestaan.

Single sign-on

Het gecentraliseerde beheer van identiteiten, met de hieraan verbonden toegangsrechten, biedt als voordeel voor de gebruiker dat hij of zij zich maar eenmaal uniek hoeft te identificeren om toegang te krijgen tot de relevante systemen en gegevens. De veiligheid hiervan vereist wel een adequate vorm van authenticatie, waarbij meerdere van de volgende factoren worden ingezet: unieke kennis van de gebruiker, een object dat de gebruiker bezit, biometrische gegevens van de gebruiker of de huidige locatie van de gebruiker.

Logging en monitoring

De loggingsverplichting wordt zoveel mogelijk vormgegeven door aan te haken op het LaaS-platform (Logging-as-a-Service). Dit stelt het Security Operations Center (SOC) in staat om aan de hand van indicatoren te monitoren op afwijkingen die duiden op compromittering.

5. Principes voor bescherming van persoons-gegevens

5.1. Doelbinding

Persoonsgegevens worden verwerkt voor een gerechtvaardigd doel

Ratio: er is sprake van rechtmatige verwerking van persoonsgegevens als er voor de verwerking een grondslag is die op zichzelf rechtmatig is en die een rechtvaardiging vormt voor de verwerking van de gegevens. Dit zogenaamde gerechtvaardigde **verwerkingsdoel** kan bij persoonsgegevens onder de AVG zelf worden gekozen en moet daarbij van een voorgeschreven categorie zijn. Bij de verwerking van politiegegevens onder de Wpg vormt de uitvoering van de politietaak de grondslag voor de verwerking, die is onderverdeeld in met name genoemde verwerkingsdoelen. In beide gevallen geldt: het doel biedt de grond voor verwerking en zodra het doel uit zicht verdwijnt, verdwijnt ook de grond voor de verwerking (**doelbinding**).

Alleen gegevens die rechtmatig zijn **verkregen** kunnen rechtmatig worden verwerkt. Gegevens die reeds worden verwerkt, mogen voor doelen worden verwerkt die **verenigbaar** zijn met het oorspronkelijke doel. Daarnaast mogen gegevens ook voor andere gerechtvaardigde doelen **verder** worden **verwerkt**.

5.1.1. Verkrijgen

Alleen gegevens die rechtmatig zijn verkregen kunnen rechtmatig worden verwerkt.

De verwerking van persoonsgegevens door een bevoegde autoriteit voor de uitvoering van de politietaak valt onder de werking van de Wpg. Maar het *verkrijgen* van politiegegevens niet. Daarvoor is een aparte grondslag nodig. Is die grond de uitvoering van de politietaak (dus Politiewet, artikel 3) of of een vordering op

grond van het Wetboek van Strafvordering dan valt de verwerking van deze persoonsgegevens vervolgens onder de Wpg.

De Wpg biedt ruimt om gegevens uit een samenwerking te verkrijgen via twee vormen;

1. Deelname aan een samenwerkingsverband[61], met nadere eisen over het belang en doel van de verwerking en grond voor de verwerking van alle deelnemers. Er wordt verstrekt aan elk van deelnemers afzonderlijk
2. Een gemeenschappelijke verwerkingsverantwoordelijkheid[62] waarbij wordt verstrekt aan het collectief van deelnemers.

Ook voor de AVG geldt dat gegevens rechtmatig moeten zijn verkregen, namelijk voor een doel dat behoort tot de categorieën van rechtmatige verwerking doelen. Het betreft hier niet de politietaak en het zal doorgaans gaan om situaties gaan waar de korpschef 'slechts' verwerkingsverantwoordelijke is:

3. als werkgever bij de verwerking van persoonsgegevens over personen werkzaam voor de politie. De grond is in dat geval de noodzaak te voldoen aan een wettelijke verplichting.[63]
4. als overheidsinstantie met een wettelijke taak, anders dan de politietaak, bijvoorbeeld Korpscheftaken of toezichtstaken. De grond is in dat geval de noodzaak tot vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag die aan de verwerkingsverantwoordelijke is opgedragen.[64]

Onder de AVG is een gemeenschappelijke verwerkingsverantwoordelijk ook mogelijk. [65]

Open bronnen

Voor de politie geldt dat gebruik van gegevens uit het publieke domein, net als *in real life*, alleen is toegestaan bij de uitvoering van de politietaak. Er moet dus sprake zijn van een redelijk vermoeden van een strafbaar feit (opsporing) of sprake zijn van één van de andere delen van de politietaak. Ongericht of stelselmatig rondstruinen op internet door de politie op zoek naar 'iets dat opvalt' leidt wellicht tot gegevens die interessant zouden kunnen zijn, maar waarvan zowel de betrouwbaarheid als de rechtmatigheid soms onvoldoende zullen zijn om er iets mee te mogen doen. Voor het verwerken van gegevens uit publieke bronnen (zoals bij open source intelligence, OSINT) heeft het OM richtlijnen opgesteld.

5.1.2. Verwerking en doelbinding

De grond voor verkrijging bepaalt de grond voor verwerking

Binnen het geldende wetsregime is de verwerking slechts toegestaan voor het doel dat als grond voor de verwerking is aangevoerd. De verwerking is 'gebonden' aan het doel; doelbinding. Voor persoonsgegevens (AVG) geldt dat verwerking voor 'verenigbare' doelen wel is toegestaan. De AVG noemt een aantal concrete overwegingen voor het beoordelen van de vraag of het ene doel verenigbaar is met het andere[66]. Voor politiegegevens (Wpg) is de ruimte door de wetgever zelf ingevuld: als de gegevens worden verkregen voor de uitvoering van de politietaak worden ze ook alleen voor dat doel (verder) verwerkt.

De verwerking van bijzondere categorieën van persoonsgegevens is alleen toegestaan in aanvulling op andere (rechtmatige) verwerkingen van persoonsgegevens en voor zover dat onvermijdelijk is.

61 Wpg artikel 20

62 Wpg artikel 1 onder f punt 4t

63 AVG, artikel 6 lid 1 onder c

64 AVG, artikel 6 lid 1 onder d

65 VG, artikel 26

66 AVG artikel 6, lid 4 onder a t/m f

5.1.3. Verder verwerken

Persoonsgegevens mogen verder worden verwerkt voor een nieuw doel

Verder verwerken van persoonsgegevens (AVG)

Persoonsgegevens verwerken voor een ander doel dan waarvoor de gegevens zijn verkregen is mogelijk, dit heet Verder verwerken. Dat kan voor een nieuw doel, met dezelfde of een nieuwe grondslag. Voor persoonsgegevens (AVG) geeft dit een zekere mate van flexibiliteit voor bedrijven en organisaties zoals de politie om persoonsgegevens te verwerken voor doelen die in elkaars verlengde liggen. Als de grond toestemming is, hoeft dan ook niet telkens toestemming te worden verkregen.

Het delen van informatie op basis van de AVG mag alleen plaatsvinden met een partij die ook iets met de gegevens moet doen (*need to know*) en een grondslag heeft om deze gegevens te verwerken.).

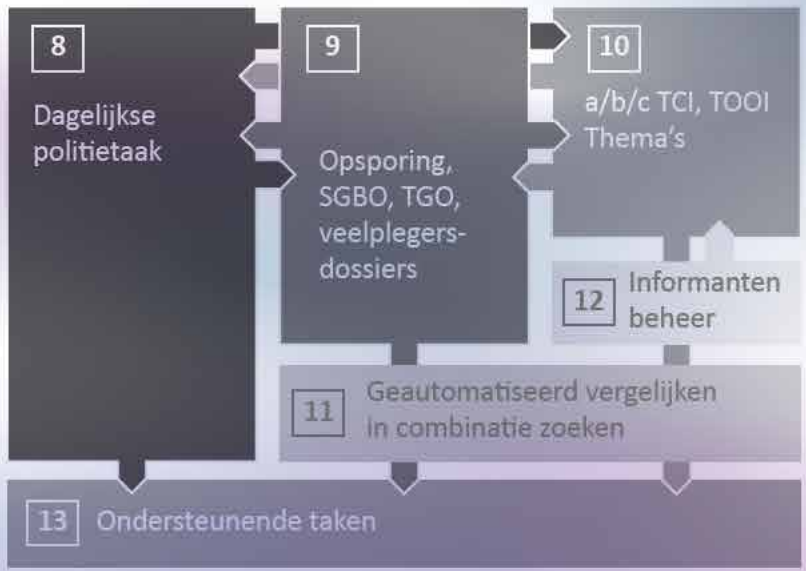
Verder verwerken met het oog op de politietaak (Wpg)

Politiegegevens mogen verder worden verwerkt, als het nieuwe doel geheel binnen de gestelde gerechtvaardigde doelen valt en ook verder aan alle rechtvaardigingsgronden is en blijft worden voldaan. Dat geldt voor verwerkingen met het oog op de uitvoering van de politietaak[67]. Gegevens verwerkt onder de Wpg mogen verder worden verwerkt voor een van de primaire verwerkingsgrondslagen 8, 9, 10 en 12. Deze gegevens mogen daarbij op grond van artikel 11 ook worden verwerkt in zoekslagen en gecombineerde vergelijkingen, waarbij wel een hiërarchie geldt van toegestane combinaties vanuit hun verwerkingsgrondslagen.

Politiegegevens zijn gedurende hun verwerking beschikbaar voor verdere verwerking door operatie en bedrijfsvoering. En in de periode daarna- de bewaartermijn- door specifiek aangewezen functionarissen. Gegevens worden bewaard – en vernietigd – op grond van Wpg artikel 14.

Politiegegevens mogen op grond van Wpg artikel 13 gedurende verwerking (inclusief de bewaartermijn) verder worden verwerkt ter *ondersteuning* van de politietaak; het gaat ook hier om een limitatieve lijst van mogelijke

67 Wpg § 2, artikelen 8 t/m 15a.



ondersteuningsvormen. Per categorie van verwerking dient het doel en de duur van deze verdere verwerking weer te zijn gespecificeerd en vastgelegd[68]. De politie heeft voor een aantal beschreven doelen een 'artikel 13-protocol' opgesteld[69].

Zo stimuleert de Wpg een voortdurende 'flow' van gegevensverwerking en dwingt af dat telkens, bij elke verdere verwerking, wordt verantwoord dat de gegevens voor een welbepaald, nauwkeurig omschreven gerechtvaardigd doel verder worden verwerkt. Het enkele feit dat persoonsgegevens rechtmatig zijn verkregen (en dus 'in huis' zijn), is dus geen voldoende grond voor rechtmatige (verdere) verwerking.

Big data

Het WRR[70]-rapport over *big data* in een veilige samenleving erkent dat het huidige juridische kader vooral betrekking heeft op de eerste verwerking. Voor een goede toepassing van big data-instrumenten en moderne manieren van informatie verwerken, is het nodig dat in toekomstige wetgeving ook aandacht wordt besteed aan de analysewerkzaamheden en gebruikstoepassingen.[71] In de tussentijd kan de politie het zich niet permitteren hier een voorschot op te nemen zonder dat dit rechtsstatelijk mogelijk is gemaakt

(Verder) verwerken met het oog op de plichten in de Wpg

Politiegegevens mogen (verder) worden verwerkt met het doel om invulling te geven aan een of meer van de plichten die in de Wpg zijn genoemd[72]. De invulling van de plichten van de Wpg vormt dus een gerechtvaardigd doelen voor verwerking, de politie verwerkt politiegegevens onder andere (verder) om te voldoen aan de volgende plichten:

1. Juistheid en volledigheid van politiegegevens (artikel 4). Bijvoorbeeld aanvulling of verwijdering van rollen van een betrokkene in een zaak op basis van ontvangen afloopberichten[73].
2. Bescherming van politiegegevens (artikel 4a). Bijvoorbeeld: het treffen van mitigerende maatregelen zoals pseudonimisering van politiegegevens;
3. Beveiligen van politiegegevens (artikel 4a en 6). Bijvoorbeeld:
    - het onderhouden van een systeem van autorisaties;
    - het beveiligen van berichtenverkeer en gegevens bij transport daarvan;[74]
    - het registreren van de verwerking van persoonsgegevens (artikel 32a);[75]
    - het maken en herstellen van data-backups;[76]
    - het testen, ontwikkelen, accepteren en in productie nemen van systemen.[77]

Het kan bij al deze verwerkingen gaan om grote verwerkingen, met grotere / veelvuldige inbreuk op de persoonlijke levenssfeer van betrokkenen. Bijvoorbeeld grote bestandsvergelijkingen en hiervoor noodzakelijke uitwisseling van persoonsgegevens tussen systemen van de politie, of in de vorm van verstrekkingen aan, of gezamenlijke verwerking met partners in de strafrechtketen. De politie moet bij het treffen van maatregelen rekening houden

68 Wpg artikel 13 lid 4.

69 Volgens de eisen die daaraan zijn gesteld in het Besluit politiegegevens 6:2

70 Wetenschappelijke Raad voor het Regeringsbeleid (WRR) zie www.wrr.nl

71 Zie het rapport Big Data in een vrije en veilige samenleving, Wetenschappelijke Raad voor het Regeringsbeleid, april 2016

72 Wpg § 1, artikelen 3 t/m 7a

73 De afloopberichten zelf zijn strafvorderlijke gegevens (Wjsg) die worden verwerkt onder de Wpg artikel 4.

74 Wpg artikel 4a lid 6 Jo Bpg Artikel 6:1a onder h

75 Treedt in werking op een nader te bepalen tijdstip en Bpg artikel 6:1a. lid 3 onder g en h

76 Wpg artikel 4a lid 6 Jo Bpg Artikel 6:1a onder i

77 Wpg artikel 4a lid 6 Jo Bpg Artikel 6:1a onder j

met "de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen"[78]. Bij het beoordelen van de rechtmatigheid van het verwerken van persoonsgegevens voor het voldoen aan een verplichting vanuit de Wpg, moet dus zwaarte van de risico's (zoals het niet kunnen invullen van deze plicht in de Wpg) worden afgewogen tegen de inbreuk op de privacy die gepaard gaat met de maatregelen. Met andere woorden; het middel moet niet erger zijn dan de kwaal.

5.1.4. Verstrekken

Overgang van wetsregime is mogelijk

De Wpg kent gronden voor verstrekking, waarbij de verwerkingsverantwoordelijkheid eindigt en de persoonsgegevens (het zijn dan geen politiegegevens meer) onder een ander regime worden verwerkt. Het verstrekken van gegevens binnen het Wpg-domein (delen) is mogelijk op grond van artikel 15: ter beschikking stellen van politiegegevens. Hiervoor is vereist dat de ontvanger is geautoriseerd voor de verwerking van politiegegevens en exact deze gegevens nodig heeft voor de rechtmatige uitvoering van diens taak.

Een veelvoorkomende verstrekking van de politie is die 'aan onszelf'. Ofwel de verstrekking van de politie als uitvoerder van de politietaak aan de politie in de rol van werkgever of organisatie met een bedrijfsdoel, of een taak buiten de politietaak. Om die reden wordt er verstrekt aan de korpschef en ook aan de Politieacademie.

Verstrekking is ook mogelijk aan andere met name genoemde instanties, diensten en gezagsdragers[79]. We spreken dan niet meer van beschikbaar stellen maar van bekend maken. De ontvanger verwerkt de gegevens verder onder eigen regime en de verwerking van de verstrekte gegevens door de politie blijft onder de Wpg vallen.

Publieke en commerciële gegevensdiensten

Aan het gebruik van publieke (commerciële) informatiediensten zoals Google, Dropbox, WhatsApp etc. zijn risico's verbonden voor de bescherming van persoonsgegevens en informatieveiligheid, onder meer door het onderliggende verdienmodel en door hun geografische locatie buiten Nederland. Als persoonsgegevens hiermee worden verwerkt is dit een verstrekking in de zin van de AVG en Wpg. Die is alleen rechtmatig als de politie de aanbieder van de informatiedienst als verwerker heeft aangewezen en voldaan wordt aan de zorgplicht van de verwerkingsverantwoordelijke. Voor de applicaties binnen de (eigen) beheerde omgeving van de politie is dit het geval en bij uitzondering (bijvoorbeeld MS Teams via BlauwOnline) is dit ook buiten de politie-omgeving het geval. In de andere gevallen niet.

Bepaalde verschijningsvormen van dienstverlening, met name waar cloudtechnologie wordt toegepast, zijn niet eenvoudig conform de AVG of Wpg uit te voeren[80].

5.1.5. Implicaties

1. De grond voor verkrijging (import) of verstrekking (export) wordt als kenmerk (metagegeven) aan persoonsgegevens verbonden. Dit moet als kenmerk van de transactie worden geregistreerd. De verkrijgingsgrond of verstrekkingsgrond heeft dus bijvoorbeeld betrekking op 'vermoedelijke betrokkenheid in de rol van a/b/c van persoon x bij delict y in zaak z' (Wpg), of 'dienstverband van medewerker x vanaf d.d. bij organisatieonderdeel y' (AVG).
2. Verwerkingsgronden worden als referentiegegevens geregistreerd. Het zijn generieke kenmerken die door de politie binnen de kaders van de AVG, of door de wetgever in de Wpg zijn bepaald;
3. De grond voor (verdere) verwerking wordt bij elke verwerking als kenmerk verbonden. De verwerkingsgrond is geen kenmerk van de

78 Wpg artikel 4a lid 3

79 Wpg Par. 3, De doorgifte of verstrekking van politiegegevens aan anderen dan de politie of Koninklijke Marechausseen

80 zie Cloudstrategie

personen zelf (kernobjecten) omdat daarvoor bij de politie nooit een zelfstandige grond bestaat. Alleen de verwerking voor een bepaald doel kan een grond hebben. Het doel (en daarmee de rechtmatige verwerking) moet daarom blijken uit de transactie. In de implementatie kan er praktisch wel voor gekozen worden om de grond(en) waarop de verwerking plaatsvindt, bij het persoonsgegeven op te slaan.

4. Bij een verdere verwerking wordt aan het persoonsgegeven volgens het principe van enkelvoudige vastlegging een nieuwe verwerking toegevoegd. Een verdere verwerking leidt dus niet tot een kopie van het kernobject.

5. Waar mogelijk moet de verwerkingsgrondslag geautomatiseerd worden afgeleid, als onderdeel van de gegevensregistratie- en bewerkende diensten (bestemmingsplan[81]). Dit kan op basis van kennis van het werkproces (uit de selectielijst de politie) dat door de betreffende locatie wordt ondersteund. Of, eventueel aanvullend op basis van de functie en rol van de medewerker en de locatie (op straat binnen of op het bureau, binnen of buiten het servicegebied van het basisteam of niet, etc.) waar deze zich bevindt.

81 In het (concept)bestemmingsplan wordt deze term gehanteerd om de systemen aan te duiden die bedoeld zijn voor invoer van gegevens (de registratieve / transactionele systemen). Dit is een gegevensverwerkingsdienst conform het (concept) bestemmingsplan.

5.2. Privacy by default

De verwerking van persoonsgegevens wordt standaard beperkt

Ratio: een rechtmatige verwerking (Doelbinding op bladzijde 42) moet zo veel mogelijk worden beperkt zodat ook de rechtmatige inbreuk op de persoonlijke levenssfeer wordt beperkt. De verwerking moet in alle gevallen **noodzakelijk** zijn voor het verwerkingsdoel, voor de bijzondere categorieën van persoonsgegevens moet de verwerking zelfs onvermijdelijk zijn (er bestaat dan dus geen alternatief).

Die beperking heeft in elk geval betrekking op de **hoeveelheid** verwerkte gegevens, de **mate** waarin zij worden verwerkt, de periode van opslag (**verwerkingstermijnen**), de toegankelijkheid van de politiegegevens (**autorisatie**) en de **groep** waaraan deze eventueel verstrekt worden. Het principe van *privacy by default* is opgenomen in de AVG (artikel 25) en in de Wpg (artikel 4b). De Wpg schrijft ook voor dat een **natuurlijk persoon** toestemming dient te geven voor de verstrekking aan meerdere personen.

5.2.1. Noodzaak

De verwerking moet noodzakelijk zijn voor het verwerkingsdoel

De noodzakelijkheid van de verwerking van persoonsgegevens kan worden beoordeeld aan de hand van een aantal aspecten:

- proportionaliteit: weegt het belang van de verwerking op tegen het belang van de bescherming van de persoonlijke levenssfeer van de betrokkene(n)
- subsidiariteit: maakt de (voorgenomen) verwerking ten opzichte van de voorhanden zijnde alternatieven de minste inbreuk op de persoonlijke levenssfeer?
- onvermijdelijkheid (in het geval van bijzondere categorieën van persoonsgegevens) van de verwerking van persoonsgegevens voor het doel van de verwerking.

De noodzakelijkheid moet er zijn in relatie tot het doel van de verwerking.

Voorbeeld

Een filmpje over een arrestatie van een persoon is soms noodzakelijk voor een opleiding. Gaat het om een instructiefilm over een procedure of over de-escalerend optreden? Het tonen van het gezicht en laten horen van de stem van een betrokkene is in het eerste geval waarschijnlijk niet noodzakelijk, in het tweede geval wellicht wel.

'Geslacht' moet worden ingevuld bij communicatie met de politie. Dat is misschien noodzakelijk voor de aanhef (mevrouw / meneer) maar is een dergelijke aanhef noodzakelijk voor het doel van de verwerking? Een andere vorm van aanspreken van de betrokkene kan volstaan.

Een geboortedatum is een te uitgebreide verwerking van gegevens voor het doel van vastellen van minderjarigheid of meerderjarigheid Een ja/nee of meerderjarig/minderjarig (op de dag van invullen) kan volstaan

5.2.2. Dataminimalisatie

De hoeveelheid gegevens die worden verwerkt wordt standaard beperkt

Bij de beperking van de hoeveelheid gegevens kan worden overwogen of het gegevensdomein wel beperkt genoeg is gekozen. Ten behoeve van de juistheid en volledigheid van gegevens worden bestandsvergelijkingen uitgevoerd of worden grote hoeveelheden persoonsgegevens in een systeemtest gebruikt. De overweging moet zijn of al deze gegevens noodzakelijk zijn. Welke deel

van de persoonsgegevens biedt een voldoende representatie van het gegevensbereik? Komen er gegevens mee die niet nodig zijn?

> **Voorbeeld**
>
> Een bestandsvergelijking die wordt uitgevoerd tussen twee systemen om verschillen tussen overleden personen te detecteren. De bestanden hoeven niet als geheel te worden uitgewisseld, alleen de overleden personen uit het ene bestand hoeven te worden vergeleken met de overleden personen uit het tweede bestand. Het doel van 'juistheid en volledigheid' wordt dan ook bereikt. Eigenlijk hoeven er dus helemaal geen persoonsgegevens te worden uitgewisseld

5.2.3. Privacy Enhancing Technologies

De mate van verwerking wordt standaard beperkt

De mate van verwerking kan worden beperkt door de identificeerbaarheid van personen te verminderen. Dit kan worden bereikt door toepassing van zogenaamde ***privacy enhancing technologies*** (PET). Dit zijn rekenkundige technieken die de identificeerbaarheid van natuurlijke personen op basis van de persoonsgegevens verminderen of geheel voorkomen.

Pseudonimiseren en anonimiseren

Pseudonimisering is het vervangen van de identificerende gegevens uit een bestand met een zogenaamd pseudoniem, dat niet zonder meer is terug te herleiden tot het origineel. Voor anonimiseren en pseudonimiseren worden informatica-technieken gebruikt waarmee een set gegevens met een bepaald bereik wordt herberekend. De gepseudonimiseerde data worden los van de identificerende gegevens en bijbehorend pseudoniem beheerd en technische en organisatorische maatregelen worden genomen om niet-koppeling aan een geïdentificeerd of identificeerbaar proces (of dito entiteit) te waarborgen. Pseudonimisering is dus een privacybevorderende maatregel, namelijk het beperken van de identificeerbaarheid van natuurlijke personen. Er zijn vormen van pseudonimisering waarbij de identificeerbaarheid van personen op wiskundige gronden als nihil mag worden verondersteld. De resterende gegevens vallen in dat geval niet meer onder de werking van de AVG of Wpg.

Het anonimiseren en pseudonimiseren is gericht op de identificeerbaarheid van de persoon. Als die onomkeerbaar wegvalt, is niet meer voldaan aan definitie van persoonsgegevens ex AVG artikel 4. De gegevens kunnen nog steeds andere persoonlijke details bevatten die maken dat zorgvuldige omgang is geboden.

NB. De genoemde technieken hebben doorgaans zwakheden waarmee afbreuk kan worden gedaan aan de mate waarin ze de herleidbaarheid verminderen. Deze zijn beschreven in de factsheet Anonimiseren en Pseudonimiseren. (PM)

Hashing

Hashing is een wiskundige berekening op een oorspronkelijk gegevensbereik naar een tweede gegevensbereik, de hashwaarde. Voor deze 'vingerafdruk' wordt een aantal principes toegepast (zie kader Principes voor hashing op bladzijde 50) om te zorgen dat de hash uniek is en niet prijsgeeft van welk oorspronkelijk gegevensbereik het is afgeleid. Het is niet zonder meer mogelijk om vanuit de hashwaarde terug te keren bij het origineel, al is het wel denkbaar dit dat wordt herleid

Hashing is een vorm van pseudonimisering. Als naar de stand van de techniek ruimschoots wordt voldaan aan bovengenoemde voorwaarden, wordt gesproken van cryptografische hashing. De herleidbaarheid is dan (nagenoeg) nihil en de hash van persoonsgegevens valt in dat geval niet onder de werking van de AVG en Wpg. Dit is ook het standpunt van de Autoriteit Persoonsgegevens.[82] (Het is van belang te beseffen dat deze status in theorie eindig is, doordat de cryptografische kracht van algoritmes en computersystemen voortschrijdt.)

82 9 januari 2019: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#wat-is-pseudonimiseren-6129

Principes voor hashing

De berekening is deterministisch (zonder random functies) en kan dus telkens door iedereen worden herhaald met dezelfde uitkomst voor dezelfde gegevens.

De hashwaarde verspringt sterk van waarde bij de kleinste verandering van de oorspronkelijke gegevens. Gegeven één hash kunnen de oorspronkelijke gegevens dus niet 'bij benadering' worden gevonden.

De lengte van de hashwaarde is voldoende om in de praktijk te voorkomen dat verschillende gegevens tot eenzelfde hashwaarde leiden (hash collision).

Er zijn vormen van hashing die niet voldoen aan (al) deze voorwaarden:

- een *checksum* is een vorm van hashing waarbij de 'hash' zeer kort is. Te kort om uniek te zijn, maar voldoende om meer zekerheid te geven dat een verwachte waarde ook echt correct is overgenomen. (De *checksum* van de verwachte waarde wordt vergeleken met die van de ingevoerde waarde.)
- een KENO-sleutel is een bekend voorbeeld in de politiecontext, waarbij de oorspronkelijke gegevens tot een vaste lengte (de eerste vier letters van de achternaam, de eerste letter van de eerste voornaam en de laatste twee cijfers van het geboortejaar) worden teruggebracht. Dit is een zeer zwakke vorm van pseudonimiseren en kenosleutels zijn zeker persoonsgegevens. Het wordt wel nuttig toegepast als manier om effectief te zoeken in een verzameling met een grote hoeveelheid personen, vanuit een toepassing die uit de aard van de voorziene werkzaamheden vereenvoudigde bediening vereist, bijvoorbeeld een smartphoneapplicatie voor gebruik op straat.

Datacompressie, vervorming en blurren

Hoewel datacompressie op het eerste gezicht geen pseudonimisering lijkt, is dit het wel. Bij data-compressie wordt voor de herberekening een gemiddelde of trend van de oorspronkelijke gegevensset berekend. Compressie wordt zowel toegepast met verlies van oorspronkelijke gegevens (bijvoorbeeld bij audio of afbeeldingen) als zonder verlies van gegevens (bij tekst, maar soms ook bij andere media). Gecomprimeerde persoonsgegevens zijn voor AVG en Wpg ook persoonsgegevens.

Het *blurren* van beelden of het vervormen stemmen of andere (audio)signalen kan ook worden bereikt door toepassing van compressietechnieken, soms in combinatie met het toevoegen van (willekeurige) gegevens. Toepassen van deze technieken vermindert de herleidbaarheid, maar er is doorgaans nog steeds sprake van informatie over een identificeerbare persoon. De huidskleur, vorm van het hoofd, of de manier van praten blijven immers deels herleidbaar. Valt dit geheel weg, dan is sprake van anonimisering. In plaats van blurren zal de informatie dan vaak geheel verwijderd zijn.

Encryptie

Encryptie is versleuteling van de gegevens. Het gehele gegevensbereik wordt versleuteld en bij decryptie – het omgekeerde proces – komen alle gegevens weer beschikbaar. Ge-encrypte persoonsgegevens zijn voor de AVG en Wpg nog steeds persoonsgegevens. Bij het versleutelen van gegevens is het van belang zich rekenschap te geven van de verwachte ontwikkelingen in de cryptografie en meer in het bijzonder ***quantum computing***. De opkomst van quantumcomputers zal ervoor zorgen dat sommige encryptiealgoritmen 'waardeloos' worden en het nut van andere algoritmen ernstig wordt verzwakt. Hiermee moet ook nu rekening worden gehouden, zeker met oog op duurzame vertrouwelijkheid van gegevens.

Differential Privacy

Differential Privacy is een statistische techniek waarbij in een gegevensverzameling met micro- informatie aanpassingen kunnen worden gemaakt, zodat op persoonsniveau geen conclusies meer kunnen worden getrokken. De aanpassingen maken die conclusies te

onzeker. Tegelijkertijd blijven de eigenschappen voor statistische doeleinden (variëteit, aantal waarnemingen, gemiddelde, etc.) intact. Het is geen vorm van pseudonimiseren maar is wel een privacy-bevorderende techniek. Na toepassing ervan blijven de persoonsgegevens onder de werking van de AVG en Wpg.

5.2.4. Bewaartermijnen

Gegevevens worden voor een beperkte tijd verwerkt

Ratio: bewaartermijnen zijn een (wets)instrument waarmee de verwerking van persoonsgegevens wordt beperkt en daarmee ook de inbreuk op de persoonlijke levenssfeer. De duur van de verwerking voor een bepaald doel wordt beperkt, alsmede de periode dat de gegevens daarna worden bewaard en vervolgens moeten worden vernietigd. Net als het beperken van de toegang middels autorisatie wordt het doel van de verwerking als aangrijpingspunt genomen voor de (mate van) beperking van de bewaarduur. Een doel met een groter belang rechtvaardigt doorgaans een langere verwerking dan een doel met een minder groot belang.

De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden. Voor de termijn dat de gegevens verwerkt worden, moet de informatievoorziening waarborgen treffen voor duurzame toegankelijkheid. Deze waarborgen worden uitgewerkt in het Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO) van de politie.

Toegankelijkheid van overheidsinformatie

Het beheer van overheidsinformatie binnen de politie is geregeld in de Beheerregeling Documentaire Informatie Politie 2017. De termijnen voor bewaren en vernietigen zijn verzameld in de generieke selectielijst voor de Nationale Politie[83]. Hierin zijn de kaders voor het bewaren en vernietigen van politiegegevens (Wpg) en bedrijfsvoeringsgegevens (AVG etc.) in één instrument gecombineerd.

Hierin vind je dus zowel de wettelijke termijnen voor het bewaren en vernietigen van persoonsgegevens volgens de Wpg als de termijnen voor het bewaren en vernietigen

83 De selectielijst is door het Nationaal Archief goedgekeurd en vastgesteld bij besluit in de Staatscourant.

Afbeelding: processtappen en termijnen voor de verschillende verwerkingsgrondslagen van de Wpg

van andere (persoons)gegevens op basis van hun waarde voor het bedrijfsvoerings-, verantwoordings- en cultuurhistorisch belang.

De selectielijst is opgesteld aan de hand van de taken en bedrijfsprocessen van de politie[84]. De processen zijn daarin ingedeeld in drie hoofdcategorieën: besturen, uitvoeren en ondersteunen. In de selectielijst wordt per proces een waardering toegekend aan de informatie die uit dat proces voortvloeit in de zin van bewaren (B) of (op termijn) vernietigen (V). Bij de met een V gewaardeerde processen wordt een bewaartermijn weergegeven op grond van de waarde van de inhoud vanuit het oogpunt van verantwoording, bewijslevering, bedrijfsvoering of een wettelijke plicht (zoals de Wpg). Met een B gewaardeerde informatie wordt overgebracht naar het Nationaal Archief ten behoeve van mogelijk toekomstig historisch onderzoek.

Verwerkingstermijn en bewaartermijn

De verwerking van persoonsgegevens onder de AVG vindt plaats voor de termijn waarbinnen het doel de verwerking rechtvaardigt. De korpschef is als verwerkingsverantwoordelijke verplicht om na te gaan of er termijnen gelden voor de specifieke persoonsgegevens. Voor fiscale gegevens is de bewaarplicht bijvoorbeeld op 7 jaar vastgesteld[85] en voor medische gegevens in beginsel op 15 jaar[86]. Wanneer er geen wettelijk vastgestelde termijn is, dient de politie de termijn zelf vast te stellen. Daarbij bieden de vragen die gesteld worden bij een GEB goede aanknopingspunten voor een zorgvuldige motivering van de bewaartermijnen. Het ministerie van J&V heeft een stappenplan opgesteld voor het bepalen van bewaartermijnen[87].

De verwerking van politiegegevens onder de Wpg vindt plaats voor de termijn die gesteld is bij het specifieke verwerkingsdoel. Voor de primaire verwerkingsgrondslagen in artikel 8, 9, 10 en 12 is de termijn (of: zijn de criteria) voor verwerken en bewaren aangegeven. De bewaartermijn voor verdere verwerking op grond van artikel 13 (ondersteunende taken) is vastgelegd in een artikel 13-protocol, waarin ook de categorieen van personen (de betrokkenen) en het doel van de verwerking is gemotiveerd en toegelicht.

84 Deze zijn ontleend aan het Referentiemodel Bedrijfsprocessen Politie RBP 2008/2012 en de inrichting van het capaciteitsmanagementsysteem BVCM.

85 artikel 52, lid 4, AwrAwrArchiefwet

86 artikel 7:454 BW

87 2 november 2018 | Bewaartermijn persoonsgegevens in de AVG, F. Makhloufi V.D.W. van Dijk, Justid (voorbeelden aangepast)

Toelichting op het schema:

- De verwerking (groen) vind plaats voor zover en zolang als gerechtvaardigd voor het doel waarvoor de gegevens worden verwerkt. De implementatie binnen de politie is zo, dat voor verwerkingen onder artikel 8 gegevens tot vijf jaar mogen worden verwerkt, tenzij evident is dat kan worden volstaan met één jaar terugkijken, of zelfs nog korter, afhankelijk van het doel van de verwerking.[88] In artikel 8 lid 1 is geregeld dat gedurende het eerste jaar na vastlegging elke geautoriseerde vrijwel alles mag doen met artikel 8-gegevens: vergelijken, kijken of er verbanden bestaan tussen gebeurtenissen, combineren, et cetera. In artikel 8 lid 2 is geregeld dat gegevens over een periode van vijf jaar met elkaar vergeleken kunnen worden. Zo kan een gebruiker bijvoorbeeld nagaan of een persoon, adres of voertuig al in de systemen voorkomt en wat zich daar de afgelopen vijf jaar heeft voorgedaan.
- Verwerkingen onder artikel 9 en 10 mogen slechts voortduren voor zover en zolang het doel van de verwerking niet is bereikt. De 'voor zover' vereiste wordt geïmplementeerd door gegevens die niet aan een zaak worden toegevoegd, te vernietigen of eventueel in een 'rest PV' weg te zetten. De 'voor zolang' vereiste wordt concreet geïmplementeerd door het bekend worden van een onherroepelijke beslissing door OM of Rechtspraak[89] te beschouwen als het moment waarop het doel van het onderzoek op grond van artikel 9 is bereikt..
- Na afloop van de termijn van verwerking op grond van artikel 9 volgt een periode van maximaal een half jaar waarin mag worden beoordeeld of verdere verwerking voor een ander doel noodzakelijk is;
- Verder verwerken ter ondersteuning van de politietaak is mogelijk zo lang als noodzakelijk voor dat doel;
- Als het doel van de verwerkingen op grond van artikel 8, 9 danwel 10 is bereikt, worden gegevens verwijderd; verwerking door de operatie is dan niet meer mogelijk. De gegevens zijn nog wel beschikbaar voor hernieuwde verwerking. Binnen de politie wordt dit organisatorisch geïmplementeerd door het toestaan van de verwerking te beleggen bij een poortwachter. Deze functionaris kan gegevens beschikbaar stellen voor zowel hernieuwde verwerkingen als voor audits, toezicht, inzageverzoeken en klachtafhandeling.[90]
- Nadat gegevens de bewaartermijn hebben bereikt, wordt het belang van duurzame toegankelijkheid van overheidsinformatie gewogen en worden de gegevens eventueel separaat gearchiveerd. Ze zijn niet meer beschikbaar.

Er is ook onder de Wpg verwerking mogelijk van politiegegevens met het oog op invulling van plichten uit de Wpg[91]. Onder andere voor de juistheid en volledigheid, de bescherming en de beveiliging van persoonsgegevens. (zie (Verder) verwerken met het oog op de plichten in de Wpg op bladzijde 45). De termijn voor verwerken – inclusief bewaren en verwijderen – wordt door de politie bepaald volgens dezelfde beginselen als de andere verwerkingen.

88 Zie ook de Agora-afspraken die voorschrijven dat gegevens op de tijdslijn van een basisteam na twee weken geautomatiseerd verwijderd worden.

89 it wordt in de praktijk bekend gemaakt middels een afloopbericht.

90 Zie ook de werkinstructie poortwachter voor een beschrijving van de werkzaamheden:

91 Wpg, artikel 3

Referentieproces (beslisboom) voor gegevensdragers

Als persoonsgegevens naar gegevensdragers worden gekopieerd, moeten deze nog steeds worden beheerd als persoonsgegevens. In projecten waar een systeem wordt gemigreerd en de gegevens van het achterblijvende systeem worden 'weggezet' verdient dit extra aandacht. De verantwoordelijkheid voor het vernietigen van de gegevens valt binnen de reikwijdte van een migratietraject en dient dus onder de aandacht en sturing van de opdrachtgever te worden gebracht. Voorkomen moet worden, dat persoonsgegeven op gegevensdragers belanden, onbeheerd, ergens in een kluis.

Losse datadragers buiten de beheerde omgeving van de politie vormen niet alleen een risicio op gegevensverlies maar ook op onrechtmatigheid. Er is een Referentieproces vernietigen van gegevensdragers opgesteld en als onderdeel van het beleid Bewaartermijnen vastgesteld[92]. Dit proces moet worden gevolgd om gegevens weer in beheer te nemen en te bepalen of verdere bewaring rechtmatig is.

Implicaties voor ontwerp

De applicaties en voorzieningen waarmee persoonsgegevens worden beheerd, moeten termijnen voor bewaren en vernietigen kunnen afleiden uit het doel van de verwerking (oftewel het proces waarvoor de gegevens worden verwerkt). De consequentie van het principe van enkelvoudige vastlegging is daarbij, dat verwerking voor verschillende doelen dus leidt tot verschillende bewaartermijnen die simultaan moeten worden beheerd. Bewaartermijnen moeten kunnen worden 'opgestapeld' bij transacties waar persoonsgegevens worden verwerkt, waarbij elke applicatie en voorziening de persoonsgegevens voor het eigen doel en voor de duur van de eigen termijn kan verwerken. En omgekeerd moeten bewaartermijnen weer worden 'afgestapeld', telkens wanneer een doel van de verwerking is bereikt, of is vervallen. Vanuit het perspectief van die betreffende applicatie of voorziening is het gegeven vanaf dat moment verwijderd. Als de langste bewaartermijn is verstreken worden de persoonsgegevens vernietigd. Er zijn specifieke kaders die richting geven aan het verwijderen en vernietigen van gegevens in de registratieve politiesystemen.[93]

Voor de termijnen waarop gegevens duurzaam bewaard moeten worden, moet de informatievoorziening waarborgen bieden voor separate, duurzame beschikbaarheid en toegankelijkheid. De daarbij geldende kwaliteitseisen zijn te vinden in de DUTO-standaard[94]. De primaire registratieve systemen zijn geen archiefsystemen en hebben- zoals het hoort- ook geen archieffunctionaliteit.Een DUTO vereiste is wel dat systemen zijn te.koppelen met een archiefsysteem. De gegevens die voor langere tijd bewaard moeten worden, moeten exclusief worden overgebracht naar een archiefsysteem dat daarvoor is toegerust. Voor bedrijfsvoeringsgegevens kan de politie hiervoor ook gebruik maken van een contentdocument-managementsysteem Voor het bewaren van gegevens die de politie verwerkt ten behoeve van de politietaak ligt het meer voor de hand om aan te sluiten bij de standaard ketenvoorziening voor de strafrechtketen.

92 Besluit BBVO (Lid KL) op 13 februari.

93 Onder andere de volgende kaders zijn vastgesteld: 1. Beschrijving vernietigen van gegevens in BVH, versie 1.0, 26 juli 2016 2. Uitgangspunten en principes voor de schoning van onderzoeksgegevens uit Summ-IT conform de Wpg, versie 1.1, 9 september 2015 3. Inrichting poortwachtersorganisatie n.a.v. Wpg-schoning BVH, 9 juni 2015 4. Uitgangspunten en principes voor de schoning van BVH, 21 januari 2015, Beleid Bewaartermijnen, 13 februari 2020

94 DUTO standaard van kwaliteitseisen voor de duurzame toegankelijkheid van overheidsinformatie, http://wiki.nationaalarchief.nl

5.2.5. Autorisatie

De toegang tot verwerking wordt standaard beperkt

Autorisatie is een instrument ter beheer van toegang. Met autorisatie wordt de exclusieve bevoegdheid gecreëerd om als 'geautoriseerde' gebruiker van een applicatie of gegevensvoorziening (persoons)gegevens te verwerken. De rest van de gebruikers heeft deze bevoegdheid niet. De toegang tot persoonsgegevens kan ten behoeve van gegevensbescherming worden beperkt door:

1. toegang te beperken. De persoonsgegevens zijn wel vindbaar, maar de toegang ertoe is beperkt doordat ze niet kunnen worden ingezien. De toegangsbeperking werpt een barrière op, om vanuit het doel van de verwerking eerst de noodzakelijke toegang te motiveren.
2. Aanvullend toegang tot *verwijzingen* naar de gegevens te beperken: verwijderen. De persoonsgegevens zijn niet langer vindbaar met zoekslagen. De toegang tot persoonsgegevens is beperkt tot beheerders (van systemen) of poortwachters (van data). Toegang tot informatie *dat* een persoon voorkomt in een onderzoek, bekend is bij de politie, in het verleden bekend was bij de politie, etc. wordt beperkt. Dat is immers al ee inbreuk op de privacy., De beoordeling of toegang moet worden verleend tot de (verwijzing naar) persoonsgegevens ligt bij een beperkte groep personen.

Autorisatiebeleid

Het autorisatiebeleid van de politie brengt een balans aan tussen het belang enerzijds om gegevens te delen met geautoriseerden voor wie dat noodzakelijk is (of zou kunnen zijn) voor de uitvoering van hun taken en het belang van de betrokkenen anderzijds om de toegang te beperken. Autorisatie creëert daarin een optimale situatie waarin wordt vertrouwd op de professionaliteit van de eigen medewerkers, die zich ook indien geautoriseerd dienen te houden aan het principe van *need-to-know*. Het autorisatiebeleid van de politie[95] geeft invulling aan de visie op een landelijk autorisatiemodel dat in juli 2011 door de Raad van Korpschefs is vastgesteld.[96]

Autorisatie op gegevensniveau

Het autorisatiebeleid moet worden geïmplementeerd op gegevensniveau. Niet de toegang tot een applicatie moet 'als consequentie' leiden tot toegang tot gegevens, maar de toegang tot de verwerking van gegevens moet een consequentie zijn van de kenmerken van die gegevens zelf. Dat betekent, dat autorisatie voor een applicatie los staat van de toegang tot persoonsgegevens die daarmee worden verwerkt. De applicatie is zo ontworpen dat zij geen directe toegang tot gegevens geeft, maar in plaats daarvan toegang tot gegevens 'aanvraagt' op basis van invoer van de gebruiker via het autorisatiesysteem. Voor de eindgebruiker is deze tussenstap transparant (niet merkbaar).

Toegang tot informatie is in beginsel landelijk en overal volgens eenzelfde transparant proces geregeld. Uit de combinatie LFNP-functie, werkzaamheden en organisatorische eenheid wordt – waar mogelijk geautomatiseerd- een rol afgeleid. Aan deze rol wordt een autorisatie toegekend. De autorisatieprofielen voor dezelfde combinatie van kenmerken zijn landelijk gelijk. Door de toegang tot de verwerking van persoonsgegevens op deze wijze te koppelen aan de werkzaamheden waarvoor deze nodig zijn, worden rechten vanuit de registratie van functies en werkzaamheden beheerd: zodra in het personeelssysteem een functie, rol of taak wordt toegekend, gewijzigd of ingetrokken zal dit automatisch tot een autorisatiewijziging leiden. Dit vereist een goede, tijdige registratie van onder meer medewerkers, dienstverbanden en opleidingen op een centrale plaats, op landelijk niveau. Het personeelssysteem moet het *single point of truth* zijn rond de status van de medewerker. Bovendien moet een gebruiker een uniek landelijk personeelsnummer hebben. Er moet een landelijk autorisatiebeheersysteem zijn waarin autorisaties centraal zijn vastgelegd en decentraal kunnen worden beheerd. Dit

95 Autorisatiebeleid 2016 – 2020, 21 april 2016

96 'Autoriseren: zo doen we dat hier!', visie op een landelijk autorisatiemodel voor de Nederlandse Politie, juli 2011

autorisatiebeheersysteem krijgt geautomatiseerd signalen van het HRM-systeem (zoals uitdiensttreding en schorsing).

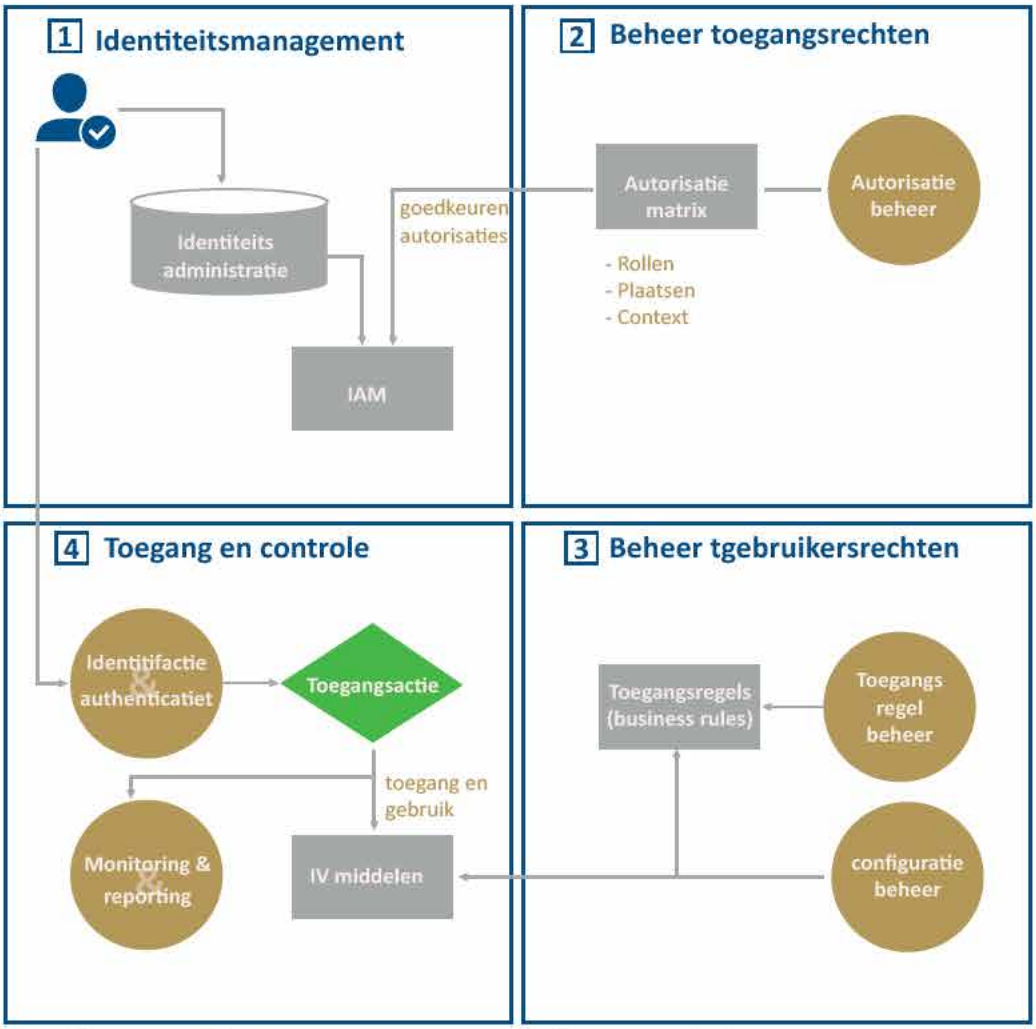
Dit levert een lage beheerlast op en beter overzicht op uitstaande gebruiksrechten. Het wordt mogelijk om op basis van de landelijke standaard geautomatiseerd rol-gebaseerde toegang door te voeren en aan te passen. Dit werkt voor interne gebruikers en voor externe gebruikers zoals ketenpartners, stagiaires, externe inhuur en tolken en het geldt zowel voor eindgebruikers als voor overige gebruikers zoals beheerders, ontwikkelaars en testers. Zo krijgt ook de medewerker zelf de gelegenheid om kennis te nemen van de voor haar of hem geldende autorisaties en om het initiatief te nemen om deze in te perken waar de eigen *need to know* is vervallen.

5.2.6. Implicaties voor ontwerp

In het autorisatiebeheer moet een aantal werkstromen organisatorisch van elkaar worden gescheiden:

- beheer van identiteiten van subjecten;
- beheer van de toegangsrechten / regels voor toegang;
- beheer van toe te wijzen gebruiksrechten op IV-middelen (behorend bij functioneel applicatiebeheer);
- gebruik en monitoring van toegangsrechten.

Het autorisatiebeheer moet eenvoudig en efficiënt worden ingericht en zo veel mogelijk gebruikmaken van geautomatiseerde procedures, om zo het aantal handmatige ad hoc-autorisaties te beperken. Noodzakelijke ad hoc-autorisaties worden centraal vastgelegd en zijn van tijdelijke



Afbeelding: verschillende werkstromen voor goed autorisatiebeheer

Afbeelding: autorisatiematrix zoals in gebruik voor een van de applicaties van de politie

		Medewerker Dagelijkse politietaak	Informatie-Coördinator Dagelijkse politietaak	Medewerker rechtsorde	Informatie-Coördinator Rechtsorde		Informatie-Coördinator Rechtsorde +		Medewerker TCI	Medewerker Thema	Medewerker TOOI	Informatie-Coördinator TCI/Thema/TOOI	Chef TCI	Chef Thema	Chef TOOI	Poortwachter
					Algemeer	IRC	Algemeer	IRC								
Dagelijkse Politietaak (Wpg artikel 8)	1e jaar	Ja	Ja	Ja	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	2e t/m 5e jaar	Ja	Ja	Ja	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Na het 5e jaar															Ja
	Geen beslotenheid	Ja	Ja	Ja	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Beslotenheid 0															Ja
	Beslotenheid 1	BM	Ja	BM	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Beslotenheid 2	BL	Ja	BL	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Beslotenheid V&F	BV&F	Ja	BV&F	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
	Beslotenheid Wpg (Wpg-verwijderd)															Ja
Onderzoek bepaald geval (Wpg artikel 9)	Afhandelcode bruikbaar		hit/no hit t/m niveau 3	hit/no hit t/m niveau 3	t/m niveau 4		t/m niveau 4		t/m niveau 4	t/m niveau 4	t/m niveau 4	t/m niveau 4	Ja	Ja	Ja	
	Afhandelcode For Intelligence Only				t/m niveau 5		t/m niveau 6		t/m niveau 7	t/m niveau 7	t/m niveau 7	t/m niveau 7	Ja	Ja	Ja	
	Weigeringsgrond	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris		Signaal naar bevoegd functionaris		Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris
	Wpg-verwijderd															Ja
Inzicht dreiging rechtsorde (Wpg artikel 9)	Afhandelcode bruikbaar		Hit/no hit t/m niveau 3	Hit/no hit t/m niveau 3	t/m niveau 5		t/m niveau 5		t/m niveau 5	t/m niveau 5	t/m niveau 5	t/m niveau 5	Ja	Ja	Ja	
	Afhandelcode For Intelligence Only						t/m niveau 6		t/m niveau 7	t/m niveau 7	t/m niveau 7	t/m niveau 7	Ja	Ja	Ja	
	Weigeringsgrond	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris		Signaal naar bevoegd functionaris		Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris	Signaal naar bevoegd functionaris
	Wpg-verwijderd															Ja
Ondersteunende taken (Wpg artikel 13)	Bruikbaar voor dagelijkse politietaak	Hit/no hit	Ja	Hit/no hit	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	
	Bruikbaar voor rechtsorde			Hit/no hit	Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	
	Alleen voor intell. gericht				Ja		Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	
	Alleen voor intell. dreiging rechtsorde						Ja		Ja	Ja	Ja	Ja	Ja	Ja	Ja	
	IRC				Hit/no hit	Ja	Hit/no hit	Ja	Hit/no hit	Hit/no hit	Hit/no hit	Hit/no hit	Hit/no hit	Hit/no hit	Hit/no hit	

aard. Voor nieuwe applicaties wordt gebruik gemaakt van een generieke voorziening voor autorisatiebeheer.

Identity & Access Management

Identificatie en authenticatie van een gebruiker wordt binnen BVI verzorgd door het Identity & Access Management-systeem (IAM). Deze functie identificeert de gebruiker, controleert of deze toegang heeft, en met welke autorisatierol. Bij het starten van een applicatie wordt vanuit BVI geautomatiseerd contact opgenomen met IAM. IAM geeft vervolgens de rol van de geautoriseerde gebruiker door aan BVI. Daarnaast kan IAM ook andere gegevens doorgeven die relevant zijn bij het verlenen van toegang tot specifieke data, zoals plaats, functie, rol in de organisatie en rol in het proces. Deze informatie wordt in BVI mede gebruikt om de gebruiker rechten te verlenen. Dit gebeurt aan de hand van regels.

De regels voor toegang zijn in principe dezelfde regels als in de bronsystemen. Als een medewerker iets in BVH niet kan zien, kan hij of zij dat ook niet via BVI zien. De regels gaan afwijken als het gaat om informatie die niet als zodanig in een bronsysteem is vastgelegd, bijvoorbeeld als gegevens ontstaan door integratie van gegevens uit verschillende bronsystemen.

De toegangsregels worden per BI-informatieproduct vooraf vastgesteld. Het BI-systeem voorziet in het beheer van de regels die de rechten binnen autorisatierollen verder differentiëren.

Bijzondere aandacht dient er te zijn voor de entiteiten die toegangsrechten kunnen manipuleren; hiervoor wordt dit decennium korpsbreed een systeem van Privileged Access Management (PAM) ingericht, waarop alle applicaties en infrastructuren worden aangesloten. (zie Generieke voorzieningen op bladzijde 41)

Autorisatiematrix

De autorisatiematrix met de actueel geldende autorisatie wordt actief beheerd en wordt daarom ook regelmatig bijgewerkt en aangepast. Kijk op bladzijde 65voor de link naar de versie op intranet

5.2.7. Beperkende applicatie-instellingen

De verwerking wordt door de applicatie-instellingen standaard beperkt

Privacy by default applicatie-instellingen houden in dat de gebruiker de meest privacy-vriendelijke optie als standaardoptie wordt aangeboden. Het *default* slaat op de 'standaard'-waarde of uitgangssituatie waarbij alleen gegevens worden verwerkt voor zover noodzakelijk voor het doel, voor de termijn noodzakelijk voor het doel en door de personen voor wie dat vanuit de aard van het werk noodzakelijk is. Afhankelijk van de invoer van de gebruiker kan de verwerking van gegevens worden uitgebreid (meer gegevens, een langere termijn of door meer geautoriseerden), mits het doel dat rechtvaardigt. Met andere woorden,

Privacy by design omvat de principes van privacy by default, alsmede principes voor rechtmatige verkrijging van gegevens en het waarborgen van de rechten van betrokkenen. Beheerders en eindgebruikers stellen de applicatie of voorziening standaard zo in, dat deze de verwerking van persoonsgegevens tot het minimum beperkt. Op basis van de invoer van de gebruiker kan die verwerking worden uitgebreid tot een verwerking van meer persoonsgegevens.

Dit principe kan worden toegepast op de dienstverlening door de politie, door de toestemming voor 'extra' verwerking van gegevens (zoals het plaatsen van adresgegevens op een distributielijst of het bewaren van gegevens die zijn ingevuld op een website) standaard uit te zetten. De gebruiker moet zelf de moeite doen – en de overweging maken – om hier toch voor te kiezen.

Hierbij moet ook altijd rekening gehouden worden met het principe van 'vrij gegeven toestemming': toestemming gegeven in een gezags- of afhankelijkheidsrelatie is geen geldige toestemming.

Het principe kan ook in operationele systemen worden toegepast, door bijvoorbeeld het zoeken op persoonsgegevens standaard globaal uit te voeren (op postcodegebied) en pas in tweede instantie preciezer (straat of adresniveau), of door persoonsgegevens niet allemaal in beeld te zetten, maar bijvoorbeeld bijzondere categorieën van persoonsgegevens achter een knop (">> meer informatie"). Bij smartphone- en tablet-apps die voor de politie worden ontwikkeld, of waarvan het gebruik wordt toegestaan, moet de vereiste toegang tot camera, adressenboek, locatie, etc. minimaal zijn en kan deze op basis van het gebruik worden uitgebreid. Denk ook aan groepscommunicatieapps die in gebruik zijn, waar de berichten standaard na een week worden verwijderd (tenzij gebruikers dit anders kiezen).

Beperkende applicatie-instellingen moeten wel zinvol zijn. Een standaardinstelling die op den duur als routine wordt omzeild of uitgebreid, kan een obstakel vormen voor functionaliteit en verliest zo haar betekenis.

5.3. Verantwoording

Persoonsgegevens worden zo verwerkt dat verantwoording mogelijk is

Ratio: Dat gegevens rechtmatig worden verwerkt en *privacy by default* wordt toegepast (zie hiervoor), moet te allen tijde aantoonbaar en navolgbaar zijn. Daarmee krijgt bescherming van persoonsgegevens bekendheid en betekenis voor betrokkenen: door de **verantwoordelijkheid voor** (persoons)**gegevens** te beleggen in de organisatie, verwerkingen vast te leggen in een **register** en een **gegevensbeschermingseffectbeoordeling** uit te voeren. Er zijn daarnaast specifieke **rechten van betrokkenen** waar alleen invulling aan kan worden gegeven als we hier bij de omgang met gegevens de voorwaarden voor naleven.

5.3.1. Verantwoordelijkheid voor verwerking van gegevens

De verantwoordelijkheid voor verwerking van persoonsgegevens wordt belegd

Om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen is vereist dat de verantwoordelijkheden voor de verwerking van gegevens eenduidig zijn belegd. Dat betekent dat de rollen, taken en bevoegdheden ten aanzien van alle gegevensverwerkingsstappen duidelijk en eenduidig aan verantwoordelijke functionarissen zijn toegewezen. Deze functionarissen zijn aanspreekbaar op de rechtmatigheid en de kwaliteit van de gegevensverwerking en moeten daarover desgevraagd verantwoording kunnen afleggen. Bij ieder initiatief dat de gegevenshuishouding en/of gegevensverwerking raakt, is het voor de verankering van privacy en security van belang dat de verantwoordelijkheden goed belegd zijn. Het kan bij deze initiatieven gaan om IV-projecten, het realiseren van gegevensuitwisseling of het doorvoeren van verbeteringen. Wat betreft de verdeling van verantwoordelijkheden dienen ten minste onderstaande rollen daarvoor te zijn ingevuld.

De verantwoordelijkheid voor gegevens en de wijze waarop de verantwoordelijkheden worden belegd in de organisatie zijn vastgelegd in het privacybeleid. De verantwoordelijkheid voor beheer van metagegevens en referentiegegevens is beschreven in het document Verantwoordelijkheid voor gegevens[97].

Beleids- en uitvoeringsverantwoordelijkheid

Bij de verantwoordelijkheid die een collega heeft in de organisatie hoort ook de verantwoordelijkheid voor de betrokken gegevens. De scheiding tussen beleid en uitvoering zoals beschreven in het Inrichtingsplan Nationale Politie is hierbij ook van toepassing op gegevens.

De **beleidsverantwoordelijkheid** omvat het vaststellen van definities, richtlijnen en kwaliteitseisen. Deze worden, in afstemming met eventuele afnemers, opgesteld door adviseurs. De beleidsverantwoordelijke gaat ook over beleid, koers en strategie voor de verwerking van gegevens. Denk bij een strategie aan kwaliteitsverbetering of het verwerven van extra gegevens.

De **uitvoeringsverantwoordelijkheid** betreft het volledig, actueel en juist laten verwerken van gegevens. Van belang hierbij is het uitdragen van de waarde van gegevens en de noodzaak van gegevenskwaliteit naar het eigen team en de omgeving. Tot slot hoort ook het correct (laten) benutten van gegevens in de uitvoering van de politietaak tot de uitvoeringsverantwoordelijkheid.

De beleidsverantwoordelijke zal zich voor de uitoefening van de verantwoordelijkheden in de regel laten ondersteunen. Het gaat hierbij om ondersteuning op grond van proces- en beleidskennis en informatiemanagement.

97 PM op Agora

5.3.2. Gegegevensbeschermings-effectbeoordeling

De risico's van verwerking van gegevens wordt vooraf beoordeeld

Een belangrijk instrument bij de planning en het ontwerp van gegevensverwerking is de gegevensbeschermingseffectbeoordeling (GEB) die wordt voorgeschreven in de AVG (artikel 35) en de Wpg (artikel 4c). Dit is een voorafgaande toets op nieuwe of gewijzigde gegevensverwerkingen. Daarbij moeten onder andere worden vastgelegd: de doelen van de verwerking, een beschrijving van de categorieën van betrokkenen en persoonsgegevens en de beoogde verwijder- en vernietigingstermijnen. Ook de toekenning van autorisaties moet worden vastgelegd per verwerkingsactiviteit[98]. Het doel van de GEB is om al bij de totstandkoming (het ontwerp) van een verwerking waarbij het risico waarschijnlijk hoog is, te beoordelen welk effect de verwerkingsactiviteiten op de gegevensbescherming hebben. In de Wpg is toegelicht: Het risico is waarschijnlijk hoog[99] als er nieuwe technologieën worden gebruikt of als er bijzondere categorieën van persoonsgegevens worden verwerkt. Er is een checklist ontwikkeld (PM) waarmee bepaald kan worden of het noodzakelijk is om een GEB uit te voeren. Aan de hand daarvan kunnen risico's worden ingeschat en kan de verwerking zo worden ingericht dat de risico's aanvaardbaar zijn. Het gebruik van de GEB is niet verplicht voor alle (bestaande) verwerkingen.

Voorafgaande consultatie Autoriteit Persoonsgegevens

In bepaalde gevallen moet de Autoriteit Persoonsgegevens (AP) door de verantwoordelijke (de politie) geconsulteerd worden over de voorgenomen verwerking van persoonsgegevens die in een nieuw bestand worden opgenomen. (artikel 33b Wpg en Artikel 36 AVG). Daarbij moet gedacht worden aan gebruikmaking van nieuwe technologieën, mechanismen of procedures die een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengen. Of de AP geconsulteerd moet worden, kan blijken uit een GEB (blijkt het risico inderdaad – waarschijnlijk – hoog?).

5.3.3. Documentatieplicht en logging

Verwerkingshandelingen worden vastgelegd

Om verantwoording te kunnen afleggen over de gegevensverwerking, moeten handelingen en besluiten worden vastgelegd in de vorm van een *audit trail*. Dit maakt het voor een controlerende instantie mogelijk om vast te stellen wie wanneer welke handelingen heeft verricht en hoe eventuele besluiten tot stand zijn gekomen. De volgende zaken moeten in het kader van de documentatieplicht worden vastgelegd:

- doelen van de onderzoeken, zoals bedoeld in artikel 9 lid 2;
- de verstrekking of doorgifte van politiegegevens aan anderen dan de Koninklijke Marechaussee, op grond van paragraaf 3 Wpg;
- de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, zoals bedoeld in artikel 27, lid 1 (de zogenaamde verzoeken om inzage).
- de datalekken zoals bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.

Deze vorm van vastlegging verschilt van technische logging die bedoeld is om de correcte werking van systemen te controleren en om bij storingen te kunnen analyseren wat er is misgegaan. De logging van gebruikershandelingen ten behoeve van informatiebeveiliging valt

98 Wpg artikel 31d onder j

99 Het document WP 248 van de artikel 29-werkgroep van de EU beschrijft van pagina 7 tot 11 criteria en voorbeelden waaruit blijkt wanneer er sprake is van een 'waarschijnlijk hoog risico'.

nadrukkelijk wel onder het principe van verantwoording (zie Logging op bladzijde 40). Hoe de logging van gebruikershandelingen moet worden ingericht, is beschreven in het Beleidskader Logging (Bronnen op bladzijde 65).

Bij het aanleggen van logging[100] van gebruikershandelingen – de ***audit trails*** – gaat het om de keten van handelingen en beslissingen die tot een conclusie of besluit hebben geleid. De werkprocessen waarin deze werkzaamheden georganiseerd zijn, kunnen over meerdere personen en afdelingen heen lopen. Het is ook mogelijk dat de handelingen en besluiten met behulp van verschillende instrumenten of systemen worden vastgelegd. Omwille van de controleerbaarheid en het goede beheer van de verantwoordingsinformatie heeft het de voorkeur om voor de vastlegging van handelingen en besluiten één registratie te gebruiken. Vanuit die registratie kan wel worden doorverwezen naar andere registraties of systemen voor inhoudelijke of achtergrondinformatie.

De registratie van verantwoordingsinformatie richt de politie bij voorkeur in als generieke voorziening met verplicht gebruik. Daarbij worden ten minste de volgende verwerkingen gelogd: verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren en vernietigen van politiegegevens.

Deze logging-gegevens mogen alleen worden gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, voor het waarborgen van de integriteit en de beveiliging van de politiegegevens en voor strafrechtelijke procedures. De identificatie van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, moet worden geregistreerd en ***op basis daarvan*** moeten de redenen voor de verwerkingsactiviteiten kunnen worden gemotiveerd.[101] Ook de handelingen die worden gedaan met de logging-gegevens, moeten zelf weer herleidbaar tot de persoon zelf worden gelogd, onder meer om de integriteit van de logging zelf te kunnen aantonen.

Verwijzing atypisch, PM

Gelet op het doel van de gegevensverwerking is logging een verwerking van persoonsgegevens op grond van de AVG, waar tevens de Wet op de Ondernemingsraden op van toepassing is. De gegevens kunnen immers worden gebruikt voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen. Daarmee is het op basis van WOR artikel 27, lid1 onder l mogelijk instemmingsplichtig. De registratie van handelingen moet beveiligd worden tegen manipulatie en waarborgen bieden voor bewaring en goede toegankelijkheid, om ervoor te zorgen dat de bewijskracht voor het verantwoordingsdoel niet in gevaar komt

100 Wpg artikel 32 a beschrijft de loggingsverplichting.

101 Zie memorie van toelichting artikel 32 a en overweging 57 van de Richtlijn opsporing en vervolging.

5.3.4. Rechten van betrokkenen

De uitoefening van rechten van betrokkenen wordt ondersteund

Actief informeren van betrokkenen

De Wpg vereist dat betrokkenen ongevraagd actief geïnformeerd worden over bepaalde onderwerpen. Het gaat daarbij zowel om algemene informatie als om meer specifieke informatie. Algemene informatie wordt reeds via de website en brochures beschikbaar gesteld. Het gaat daarbij om contactgegevens van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming, de verwerkingsdoelen van de politiegegevens, de rechten van betrokkene, en het recht een klacht in te dienen bij de AP.

Specifieke informatie kan ook via de website beschikbaar worden gesteld; dit gebeurt bijvoorbeeld in reactie op een aangifte of een ander contact met de betrokkene. Het gaat daarbij onder andere om de verwerkingsgrondslag, de bewaartermijn, de categorieën van de ontvangers van de politiegegevens en het bestaan van geautomatiseerde besluitvorming. Deze plicht om aan betrokkenen van te voren zowel algemene als specifieke informatie beschikbaar te stellen, bestaat eveneens in de AVG.

Bijvangst

Het verstrekken van informatie aan de betrokkene kan worden uitgesteld, beperkt of achterwege worden gelaten in het belang van onder andere de opsporing en het onderzoek[102]. In de praktijk blijkt dat de actieve informatieplicht in het geval van 'bijvangst' van politiegegevens bij het plaatsen van telefoon – of internettaps in het geheel achterwege wordt gelaten.

Inzage en correctierecht

Betrokkenen hebben recht op inzage in de persoonsgegevens die over hen worden verwerkt. Het feit dat een burger dit recht uit kan oefenen, betekent dat er functionele eisen over opgenomen moeten worden in het ontwerp. Het houdt ook in dat deze getoetst moeten worden. Op eenvoudige wijze moeten alle persoonsgegevens te ontsluiten zijn binnen de politieorganisatie. Het kunnen uitoefenen van hun rechten door betrokkenen, geeft op indirecte wijze invulling aan het afleggen van verantwoording door de politie.

Verklaringen van opsporingsambtenaren zijn doorgaans inzichtelijk voor de burger. Onder de AVG is ook het recht op beperking van de verwerking en het recht op overdraagbaarheid geregeld. Er is een mogelijkheid tot weigeren van het verstrekken van geregistreerde informatie, maar dat moet per gegeven worden gemotiveerd. Mutaties moeten dus worden genoteerd op een professionele wijze die ook de 'externe' toets der kritiek kan doorstaan.

102 Artikel 27 Wpg (Uitzonderingen)

Bronnen

Brondocument	vindplaats	versie
Architectuurkader IB;		
Korpsstrategie: Agora		
Vernieuwde IV strategie		concept mei 2021
Datavisie en strategie, Comissie Digitalisering en Intelligence		(concept opdracht april 2021)
Enterprise Architectuur		
Beheerregeling Documentaire Informatie Poltie:	Staatscourant 56416 van 9 oktober 2017	
Archiefwet en Wpg,	Agora	
Beleidskader vakmanschap en security,	Intranet Privacypagina	
Visie op terugmelden		
Beleid Bewaartermijnen		
Rubriceringsregeling Politie	Intranet https://intranet.de politie.local/downloads/1206/rubriceringsregeling.html	
Cloudstrategie		