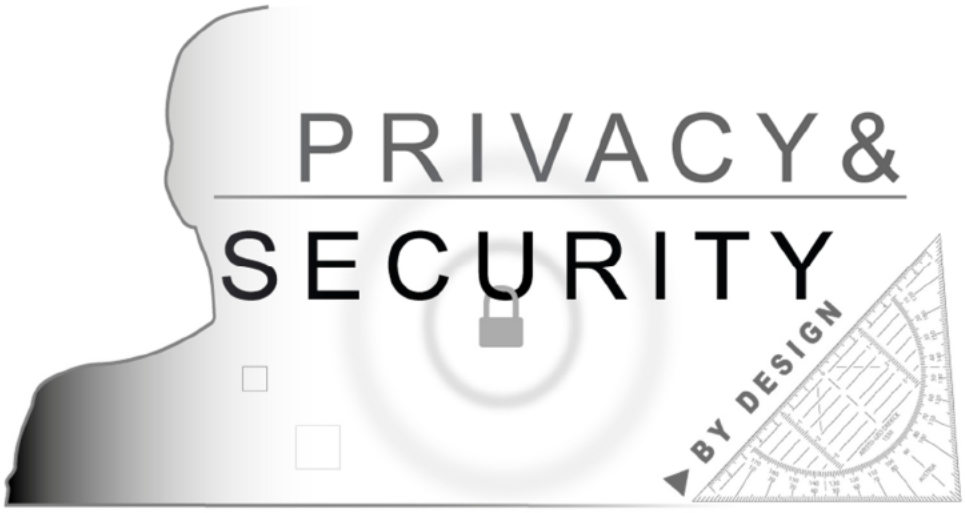
POLITIE



Uitvoerings-kader voor de omgang met gegevens

Definitief

Versie 2.0

Versiedatum 23 april 2018

Rubricering Niet Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	22-12-2016	Samenvoeging van verschillende tekstbijdragen.	
0.2	12-01-2017	Review van klankbordgroep verwerkt.	
0.3	23-01-2017	Versie gemaakt tbv reviewgroep.	
0.5	24-02-2017	Feedback van reviewgroep en nav ambassadeurssessie 31-1 verwerkt, laatste principes uitgewerkt.	
0.6	08-03-2017	Feedback van opdrachtgevers verwerkt.	
0.7	20-03-2017	Feedback laatste reviewronde verwerkt (, Nationaal Archief).	
0.71	22-03-2017	Toevoegen inhoudelijke normen bij het principe informatiebeveiliging op verzoek .	
0.72	18-05-2017	Positionering ten opzichte van IV-architectuur	
1.0	19-07-2017	Definitieve versie na vaststelling KMTO, paar kleine redactionele aanpassingen.	
1.02	07-08-2017	Nieuwe activiteiten a.g.v. de Richtlijn en de gevolgen van de AVG verwerkt.	
1.05	11-08-2017	Nieuw principe Privacy by Default toegevoegd.	
1.06	14-08-2017	Geüniformeerde en onderhoudbare figuren toegevoegd.	
1.1	16-08-2017	Publicatieversie herzien en aangepast aan AVG.	
1.98	26-03-2018	Aanpassingen a.g.v. het wetsvoorstel Wpg doorgevoerd.	
2.0	23-04-2018	Review op v1.98 van reviewgroep en klankbordgroep verwerkt.	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	29-12-2016		Directie IV,
0.3	23-01-2017		Reviewgroep: Dienst ICT, Dienst IM, Directie Operatien
0.3	23-01-2017		Ten behoeve van ambassadeurssessie 31-1-2017
0.5	24-02-2017		Ambassadeurs, opdrachtgevers, externe experts
0.6	9-3-2017	Alle personen genoemd onder versie 0.1 t/m 0.3, .	Reviewgroep en klankbordgroep
0.7	21-03-2017	Via .	
0.72	22-06-2017	Voor goedkeuring in	Leden
1.1	16-08-2017	Reviewgroep en klankbordgroep.	
1.98	27-03-2018	Opdrachtgevers, reviewgroep en klankbordgroep en ambassadeurs.	
2.0	Mei 2018	Publicatie op Agora Directie IV en betrokkenen per mail.	

Woord vooraf

Deze publicatie is tot stand gekomen dankzij de medewerking van vele collega's uit heel verschillende organisatieonderdelen van de politie. Dat is logisch want het werken met persoonsgegevens en politiegegevens en de daarbij behorende privacyvraagstukken raken alle haarvaten van de politieorganisatie. In bijlage 5 is een overzicht opgenomen van alle betrokkenen. Wij willen jullie van harte bedanken voor jullie inzet.

De samenleving digitaliseert en dat heeft grote gevolgen voor het politiewerk. Gedragingen van burgers (en ook criminaliteit) verplaatsen zich van de fysieke wereld naar het digitale domein. Alle politietaken krijgen steeds vaker ook een digitale component omdat meldingen en bewijsmaterialen in digitale vorm binnenkomen. Daarnaast ontstaan er nieuwe vormen van criminaliteit zoals cybercrime. Om de maatschappelijke veiligheid blijvend te kunnen waarborgen moet de politie mee-digitaliseren. Denk hierbij aan de aanwezigheid op internet, burgercommunicatie, het volgen van financiële transacties en communicatieverkeer, informatiestromen uit internet of things, et cetera. Dat betekent dat geautomatiseerde gegevensverwerking al lang niet meer een zaak is van de ondersteuning maar dat het integraal onderdeel vormt van het politiewerk. Voor de politie vormt dit een grote uitdaging omdat er een achterstand moet worden ingelopen. Het biedt daarnaast ook kansen omdat steeds meer veiligheidsrelevante informatie digitaal beschikbaar komt en nieuwe samenwerkingsvormen en allianties kunnen worden gesloten. Daarbij is de politie nadrukkelijk gebonden aan kaders voor zorgvuldige en rechtmatige omgang met persoonsgegevens. Dit uitvoeringskader Privacy & Security by Design geeft praktische handreikingen om de nieuwe informatiemogelijkheden effectief te kunnen benutten.

Onderstaande afbeelding laat goed zien hoe de rol van gegevens de afgelopen tien jaar veranderd is. Beide foto's zijn genomen bij de inauguratie van de paus. Ze geven een beeld hoe de technologische ontwikkelingen de maatschappelijke en sociale ontwikkelingen de afgelopen twaalf jaar hebben beïnvloed.

Figuur 1: inauguratie van de paus in 2005 en in 2013: technologische ontwikkelingen beïnvloeden het leven

Is Privacy & Security by Design het antwoord op alle hierboven genoemde ontwikkelingen en uitdagingen? Ja. Experts binnen dit domein zijn het hier al langer over eens. Zo zei Jacob Kohnstamm, voormalig voorzitter van de Autoriteit Persoonsgegevens dat het grootste risico is dat bij het ontwikkelen van nieuwe producten en diensten

iemand met gedegen kennis van privacywetgeving aan de ontwerptafel ontbreekt.[1] Marens Engelhard, Algemeen Rijksarchivaris, is van mening dat per 25 mei 2018 de privacy alleen gewaarborgd is als privacy van te voren in de architectuur wordt ingebed.[2] Ook Siebe Riedstra, secretaris-generaal van het ministerie van Veiligheid en Justitie, is die mening toegedaan. Dat blijkt uit zijn openingstoespraak op het symposium 'Grip op privacy' van 7 februari 2017.

In onze zoektocht naar kaders en richtlijnen, zowel binnen als buiten de politieorganisatie en de veiligheidsketen, stuitten we onder andere op de OECD-principes.[3] Een groot deel van deze acht principes hebben we verwerkt in dit uitvoeringskader. Wat betreft het 'openness'-principe willen we de relatie andersom leggen. Als de politie zorgvuldig is in het ontwerp van de omgang met persoonsgegevens, kan dit gebruikt worden in communicatie richting de maatschappij zodat dit de legitimiteit ten goede komt en de politie vertrouwen wint bij de burger. Privacy & Security by Design en het nog te ontwikkelen privacystatement dienen als instrumenten om de politie te positioneren als betrouwbare partij die werk maakt van gegevensbescherming.

Jaap-Henk Hoepman en Dimitri Tokmetzis verkondigden in 2014 al dat gegevens het beste beschermd kunnen worden door een goed ontwerp.[4] In 2017 erkent Hoepman dat 'by design' makkelijker ingang vindt bij juristen en organisatieadviseurs dan bij systeemarchitecten en techneuten. "Die vinden het vaak een vaag onderwerp. Het is meer informatiekunde dan informatica." Wij willen met dit uitvoeringskader niet alleen juristen en systeem- en procesarchitecten aanspreken, maar ook de bestuurder. "Privacybewustzijn begint bij de bestuurder, want het gaat om juridische interpretatie, goed ontwerp, ketensamenwerking, rapportage én beveiliging. Zoiets delegeer je dus niet simpelweg naar bijvoorbeeld een ICT-afdeling." aldus . Ook Frank van Vonderen en Renato Kuiper beargumenteren dat het om een business vraagstuk gaat, meer dan om een technische oplossing.[5]

"Als het gaat om de daadwerkelijke ICT, neem dan ook de broncode mee." Volgens , die voor de is de bron van een datalek vaak terug te voeren op dezelfde soort fouten. Privacy & Security by Design is volgens hem een belangrijke voorwaarde om de door hem geconstateerde fouten en datalekken te voorkomen.

Ontwikkelteams vinden in dit uitvoeringskader praktische handreikingen waar de systemen die ze ontwikkelen aan moeten voldoen. Omdat veel van de ontwerpkeuzes al gemaakt zijn, ondersteunt dit kader ook agile systeemontwikkeling. De vereisten liggen voor je en als leden van scrumteams deze kaders standaard in hun gereedschapskist hebben zitten, zijn de eerste ontwerpstappen al gezet. De politieorganisatie moet nog veel ervaring opdoen om het agile ontwikkelen goed in de vingers te krijgen. Dit uitvoeringskader kan product owners helpen in hun ontwikkeling om een goede omgang met gegevens te garanderen.

We zijn benieuwd naar de praktijkervaringen met dit uitvoeringskader en vragen dan ook om terugkoppeling. Op basis hiervan zullen wij als redactieteam ten minste jaarlijks een geactualiseerde uitgave uitbrengen. In deze herziene versie zijn de eerste reacties vanuit de organisatie verwerkt. Verder is het uitvoeringskader aangepast om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging die vanaf 25 mei 2018 van toepassing zijn. Dit heeft onder meer geleid tot de toevoeging van een nieuw principe over privacy by default.

Lever jouw tips en suggesties aan via e-mail en wij zorgen voor het actualiseren en actief distribueren van de volgende uitgave. Veel leesplezier en succes met het toepassen in de praktijk.

April 2018
, , en ,
Medewerkers van de Directie Informatievoorziening, staf korpsleiding

[1] Audit Magazine, 2016, nummer 1
[2] Toespraak iBestuur symposium 'Grip op privacy', 7 februari 2017
[3] https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[4] https://decorrespondent.nl/836/privacy-kun-je-beschermen-door-het-te-ontwerpen/40710692-2a05e113
[5] Informatiebeveiliging Magazine, nr. 6 2016. Frank van Vonderen is hoofddocent bij de tweedaagse praktijkcursus Privacy by Design: http://iir.nl/events/privacybydesign/

Managementsamenvatting

Het is inherent aan het politiewerk dat er op grote schaal gegevens over burgers worden verzameld en verwerkt. Het kleurrijke palet aan informatiesystemen, de toegenomen technologische mogelijkheden om gegevens op te slaan en te analyseren en de veranderende wet- en regelgeving rondom gegevensbescherming, dwingen de politie tot beleid rondom de omgang met gegevens. In 2015 heeft de politie een eerste versie van dit beleid ontwikkeld: Privacy By Design. Privacy by Design betekent dat al in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de informatievoorziening mechanismen worden ingebouwd voor de bescherming van persoonsgegevens. De eerste versie van dit beleidskader bevatte dertien principes om er vooral voor te zorgen dat privacywetgeving op eenduidige wijze geïnterpreteerd werd binnen het Aanvalsprogramma Informatievoorziening Politie 2013-2017 (AVP). Als snel bleek dat er behoefte was aan meer, want:

1. beleid over dit onderwerp is niet alleen voor het AVP nodig maar voor zowel bestaande als vernieuwingstrajecten;
2. behalve goede omgang met politiegegevens, dienen er ook regels te zijn over de omgang met persoonsgegevens (gegevens over bijvoorbeeld de medewerkers);
3. niet alleen privacy maar ook andere onderwerpen als security en duurzame toegankelijkheid dienen te worden meegenomen;
4. gegevensmanagement is niet een vakgebied voor alleen ICT'ers. Ook degenen die in de lijn verantwoordelijk zijn voor de gegevens hebben een rol;
5. in 2018 verandert het wetgevingslandschap: wat zijn daar de consequenties van?

Met deze vijf kanttekeningen is een nieuw uitvoeringskader opgesteld. De basis voor het uitvoeringskader wordt gevormd door de informatiearchitectuur en de informatiebeveiligingsarchitectuur die de kaders geven voor de omgang met gegevens. Daarbij worden tevens de kaders vanuit wet- en regelgeving en ketenstandaarden meegenomen. Deze kaders zijn verzameld in het document *Privacy & Security by Design - Architectuurprincipes voor de omgang met gegevens*. Dat document benoemt de principes die in dit uitvoeringskader verder zijn uitgewerkt in hoofdstuk vijf. Er zijn totaal twaalf principes waarvan drie principes betrekking hebben op de *besturing* van het gegevensmanagement, zoals de PDCA-cyclus en het beleggen van verantwoordelijkheden. De overige zijn inrichtingsprincipes: hoe moet de gegevenshuishouding ingericht worden? Elk principe bestaat uit een omschrijving en een ratio, inhoudelijke onderwerpen, met zoveel als mogelijk concrete handvatten en praktijkvoorbeelden, en tot slot een aantal handreikingen. De handreikingen beschrijven voor verschillende doelgroepen verschillende activiteiten en aandachtspunten. Met de komst van de nieuwe privacywetgeving in 2018 is versie 1.0 Uitvoeringskader Privacy & Security by Design geactualiseerd tot versie 2.0. Er zijn, net als in versie 1.0, nog steeds twaalf principes. Principe 'voldoen aan de wet' is komen te vervallen; de inhoud is verdeeld over een aantal andere principes. En er is een nieuw principe geïntroduceerd: 'privacy by default'

Voordat in hoofdstuk vijf de principes inhoudelijk aan bod komen, wordt een inleiding geboden en het wettelijk kader geschetst. Omdat de doelgroep gevarieerd is, is niet ieder hoofdstuk voor elke lezer noodzakelijke kost. Als de informatievoorziening van de politie en de vernieuwingsprojecten bekend zijn, dan kunnen hoofdstuk 2 en 3 worden overgeslagen. Voor alleen een overzicht van de principes wordt verwezen naar 'Principes en handreikingen', het document dat ook hard-copy verschijnt.

Inhoudsopgave

1. Inleiding

1.1. Achtergrond en aanleiding

Informatievergaring en -verwerking door politie en Openbaar Ministerie staat al vele jaren in de belangstelling. In de jaren negentig ontbrak hiervoor een duidelijke juridische grondslag en was er zelfs sprake van een heuse crisis: normen ontbraken en de politieorganisatie functioneerde niet goed. Sindsdien is er veel verbeterd en sinds 2008 heeft de wetgever een fijnmazig juridisch stelsel geschapen waarin de politiële gegevensverwerking aan strikte regels is gebonden. De huidige informatiesystemen ondersteunen dit juridisch stelsel nog onvoldoende. Dat is in het licht van de geschiedenis begrijpelijk.

In 2011 is de politie gestart met het omvangrijke Aanvalsprogramma Informatievoorziening Politie (AVP). Hiermee richtte de politie zich op het vervangen van de verouderde informatiesystemen door 'een landelijke informatievoorziening onder architectuur'. In dit kader zijn systemen gesaneerd en worden nieuwe voorzieningen opgeleverd voor de ondersteuning van het operationele politiewerk. Om te zorgen dat deze voorzieningen ontwikkeld worden met inachtneming van de privacywetgeving is in 2014 het boekje "Privacy by Design" geschreven.

De politie is met de ontwikkeling van zijn informatievoorziening aan een nieuwe fase toe. De ingezette vernieuwing moet worden afgerond zodat de informatievoorziening de solide basis kan vormen voor informatiegestuurd politiewerk. Daarnaast heeft de politie behoefte aan nieuwe voorzieningen om plaats- en tijdonafhankelijk te kunnen werken, om grote hoeveelheden data te kunnen analyseren en om effectief te kunnen optreden tegen cybercrime en andere nieuwe vormen van criminaliteit. Dat levert nieuwe uitdagingen op voor de zorgvuldige en rechtmatige verwerking van gegevens. Dit uitvoeringskader is bedoeld als opvolger van het boekje Privacy by Design om antwoord te geven op de vragen die voortvloeien uit de digitale transformatie van het politiewerk.

Versie 1.0 van het uitvoeringskader is gepubliceerd in juni 2017. In verband met de komst van de nieuwe privacywetgeving in 2018 is versie 2.0 ontwikkeld. Er zijn, net als in versie 1.0, nog steeds twaalf principes. Principe 'voldoen aan de wet' is komen te vervallen; de inhoud is verdeeld over een aantal andere principes. En er is een nieuw principe geïntroduceerd: 'privacy by default'

1.2. Onderwerp en reikwijdte: waar gaat het over?

Het onderwerp van dit uitvoeringskader is de informatievoorziening van de politie. Informatievoorziening wordt daarbij gedefinieerd als het geheel aan activiteiten dat voor een organisatie moet worden uitgevoerd om iedereen de informatie te geven die nodig is om toegewezen functies te vervullen[6]. De informatievoorziening omvat dus technische middelen zoals apparatuur en programmatuur maar ook de gegevensverzamelingen, mensen en procedures die nodig zijn bij het verstrekken van de benodigde informatie.

> *Informatievoorziening is het geheel aan activiteiten dat voor een organisatie moet worden uitgevoerd om iedereen de informatie te geven die nodig is om toegewezen functies te vervullen*

Het perspectief van waaruit het uitvoeringskader is geschreven is dat het gaat om een *kader voor de omgang met gegevens*. Dat is dus breder dan alleen privacy en informatiebeveiliging! Er zijn bijvoorbeeld ook principes opgenomen om het openbaar maken en archiveren van gegevens goed te laten verlopen. De omgang met gegevens betreft zowel geautomatiseerde gegevensverwerking als deels of niet geautomatiseerde gegevensverwerking. De focus van de kaders en de richtlijnen is echter gericht op geautomatiseerde gegevensverwerking. De titel van de publicatie gaat daarom vergezeld van de subtitel: *uitvoeringskader voor de omgang met gegevens*. De uitvoeringskaders die de IV-organisatie opstelt zijn primair gericht op de eigen informatievoorziening van de politie en hebben zowel betrekking op operationele- als bedrijfsvoeringprocessen. De gegevensverwerking in ketenverband wordt beschouwd voor zover daar kaders uit voortvloeien voor de informatievoorziening van de politie.

[6] Beheer van informatievoorziening, Guus Delen en Maarten Looijen (1992)

Bij het opstellen van dit uitvoeringskader hebben we geprobeerd om zo volledig mogelijk te zijn zodat het als checklist kan dienen. De principes uit hoofdstuk 5 zijn dus uitputtend maar niet limitatief, want als er nieuwe kaders ontstaan, kunnen de principes wijzigen of aangevuld worden.

1.3. Positionering uitvoeringskader

Dit uitvoeringskader is bedoeld om de geldende kaders voor de omgang met gegevens voor de uitvoeringspraktijk hanteerbaar en toepasbaar te maken. In het volgende schema wordt aangegeven hoe de verschillende kaders met elkaar samenhangen.

Figuur 2: de samenhang tussen de verschillende kaders en richtlijnen

De basis voor het uitvoeringskader bestaat uit de IV-architectuur. Deze architectuur geeft algemene ontwerpprincipes voor de inrichting van de informatievoorziening. De enterprise architectuur beschrijft de samenhang tussen de architectuuronderdelen en de samenhang met de organisatiestrategie. Het uitvoeringskader Privacy & Security by Design is gebaseerd op de onderdelen van de informatiebeveiligingsarchitectuur en de informatiearchitectuur die de kaders geven voor de omgang met gegevens. Daarbij worden tevens de kaders vanuit wet- en regelgeving en ketenstandaarden meegenomen. De architectuurprincipes worden vertaald naar uitvoeringskaders met praktisch toepasbare richtlijnen voor de uitvoeringspraktijk. In het schema worden verschillende van deze uitvoeringskaders genoemd. In het uitvoeringskader Privacy & Security by Design worden alle uitvoeringskaders voor de omgang met gegevens samengevat. Voor een overzicht van deze kaders zie Bijlage 7.

1.4. Wat is Privacy & Security by Design?

In steeds meer organisaties wordt invulling gegeven aan het principe ‘Privacy by Design’, zo ook binnen de politie. Privacy by Design betekent dat al in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de

informatievoorzieningen mechanismen worden ingebouwd voor informatiebeveiliging en de bescherming van persoonsgegevens[7]. Dit vereist dat er in een zo vroeg mogelijk stadium wordt nagedacht over het gebruik van persoonsgegevens binnen de organisatie, over de noodzaak van het gebruik van gegevens en over de bescherming ervan. De Autoriteit Persoonsgegevens hanteert de volgende toelichting:

> *Privacy by design houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.*

Dit uitvoeringskader heeft de titel Privacy & Security by Design omdat naast privacy ook informatiebeveiliging een belangrijke component vormt. Informatiebeveiliging is meer dan het naleven van de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG). Beide wetten schrijven echter wel voor dat gegevens goed beveiligd moeten worden, zowel organisatorisch als technisch. De principes die de politie voor gegevensmanagement heeft opgesteld hebben daarom zowel betrekking op privacy als op security.

"Privacywaarborgen moeten zo veel mogelijk ingebouwd worden in de informatievoorziening van politie en justitie. De visie van het kabinet is dat bij de bouw van systemen en het aanleggen van databestanden bescherming van persoonsgegevens uitgangspunt moet zijn ("privacy by design")".

aldus minister Opstelten in zijn brief aan de Tweede Kamer van 23 juni 2014

Het belang van een goede naleving van deze wetgeving is voor mij en voor de korpschef evident. De samenleving en internationale partners zijn niet alleen gebaat bij een veilige en goede taakuitvoering door de politie, maar ook bij een zorgvuldige omgang met politiegegevens die voor die taakuitvoering noodzakelijk is. Veiligheid en het respecteren van de privacy zijn onlosmakelijk met elkaar verbonden.

aldus minister van der Steur in zijn brief aan de Tweede Kamer van 7 december 2015

1.5. Mythes

Voor Privacy & Security by Design geldt dat veel mensen wel een idee hebben wat het is, maar dat deze beelden nogal kunnen verschillen. Daarom hieronder een viertal mythes over Privacy & Security by Design[8].

Mythe 1: Privacy & Security by Design is iets technisch
Hoewel de naam anders doet vermoeden, is Privacy & Security by Design niet technisch. Er wordt hoogstens techniek gebruikt om invulling te geven aan maatregelen. Het begint vooral bij organisatorische vragen als: hoe maak ik verstandig gebruik van persoonsgegevens? Dit doe je door niet meer te verzamelen dan nodig en door gegevens te verwijderen die niet (meer) noodzakelijk zijn. Wat overblijft, moet goed beschermd worden en slechts toegankelijk zijn voor personen die ze nodig hebben, en daar kan techniek bij helpen.
Mythe 2: Encryptie of anonimiseren is toch hetzelfde als Privacy & Security by Design?
Encryptie en anonimiseren kunnen helpen om persoonsgegevens netjes te beschermen. Maar voordat je deze technieken inzet, moet je de vraag stellen: welke gegevens heb ik echt nodig? Kan ik, door minder persoonsgegevens te verzamelen en deze slimmer te gebruiken voorkomen dat ik moet investeren in encryptie en anonimiseren?
Mythe 3: Privacy & Security by Design is alleen relevant voor nieuwe processen en systemen
De huidige systemen en gegevensverwerkingen van de politie voldoen niet aan alle eisen wat betreft gegevensbescherming. Naast de nieuwe, moeten ook de bestaande processen en systemen onderzocht en anders ingericht worden. Privacy & Security by Redesign zou voor bestaande processen en systemen dus een meer passende term zijn.

[7] In de bijlage worden zeven algemeen geaccepteerde uitgangspunten beschreven waarmee in de jaren negentig het begrip Privacy by Design geboren werd.
[8] Zie https://www.vka.nl/blog/9-mythes-privacy-by-design/

Mythe 4: Privacy & Security by Design is alleen iets voor specialisten
ICT-er's, procesontwerpers en informatieanalisten zijn de eerste groepen waar aan gedacht wordt als het gaat om het inbedden van maatregelen in het ontwerp. Echter, iedereen heeft het vermogen kritisch te kijken naar de eigen werkwijze en zichzelf vragen te stellen: waarom bewaar ik deze oude curricula vitae nog? Waar gebruiken we het Burgerservicenummer (BSN) nog voor? Waarom mailen we deze gevoelige gegevens? Dus ook bestuurders proceseigenaren, teamchefs en overige medewerkers dienen de principes actief toe te passen.

1.6. Value Sensitive Design

De normen en richtlijnen in dit uitvoeringskader hebben gemeen dat ze ontwerprichtlijnen geven om ervoor te zorgen dat 'by design' waarborgen worden ingebouwd voor de zorgvuldige en rechtmatige verwerking van gegevens. Op deze manier geven we invulling aan

1. de vereisten van *privacy* by design zoals die worden voorgeschreven door regelgeving voor de bescherming van persoonsgegevens en
2. beveiligingskaders die *security* by design voorschrijven: Informatiebeveiligingskader Nationale Politie (IBKP, 2014) en Informatiebeveiligingsarchitectuur Tactisch niveau, 2016.

Deze regelgeving en kaders geven echter niet aan wat die ontwerprichtlijnen (het design) moeten zijn. Die zijn namelijk niet in algemene zin voor te schrijven en moeten juist op maat, afhankelijk van de context en de kenmerken van de organisatie worden ingevuld. Om tot een goede set met ontwerprichtlijnen te komen kan de theorie van Value Sensitive Design worden toegepast. In Nederland wordt deze theorie ontwikkeld en toegepast door professor Jeroen van den Hoven van de TU Delft.[9] De theorie komt voort uit het besef dat de succesvolle inzet van informatietechnologie niet alleen afhankelijk is van de technische kwaliteit maar dat ook de sociale en gedragskundige aspecten bij het gebruik van informatietechnologie van belang zijn. Value Sensitive Design gaat over het realiseren van deze waarden in het ontwerp van informatiesystemen maar ook in andere toepassingen van technologie. Van den Hoven gaat ervan uit dat het ontwerp van technische oplossingen niet waardevrij is en dat mensen dit ontwerp kunnen maken of beïnvloeden. Een voorbeeld hiervan is dat we de aandrijftechnologie van motorvoertuigen kunnen kiezen en ontwerpen waarbij we rekening houden met de milieueffecten van de uitstoot die dat oplevert.

Dit uitvoeringskader geeft de ontwerprichtlijnen voor de informatievoorziening van de politie met waarborgen voor de zorgvuldige en rechtmatige verwerking van gegevens. Die waarborgen betreffen niet alleen privacy en security maar omvatten ook andere waarden die gelden voor zorgvuldige en rechtmatige gegevensverwerking zoals kwaliteitszorg, openbaarheid en verantwoording.

1.7. Doelgroep

Dit uitvoeringskader is in de eerste plaats bedoeld voor iedereen die op de een of andere wijze betrokken is bij de ontwikkeling van informatiesystemen, procesontwerp of informatiemanagement. Maar ook leidinggevenden in de operatiën vormen een belangrijke doelgroep. Daarnaast is het bedoeld voor andere geïnteresseerden binnen en buiten politie zoals de Vereniging Nederlandse Gemeenten (VNG), het Openbaar Ministerie (OM), de Rijksarchivaris, de Autoriteit Persoonsgegevens (AP) en de samenleving als geheel. Nu ICT een steeds groter deel uit van ons leven uitmaakt en daarmee ook van het politiewerk, raakt informatiebeveiliging en de bescherming van persoonsgegevens ons immers allen.

1.8. Leeswijzer

Aan dit uitvoeringskader ligt het document *Privacy & Security by Design - Architectuurprincipes voor de omgang met gegevens* ten grondslag. Dit document waarvan versie 1.1 op 14 november 2016 door de opdrachtgevers is vastgesteld, beschrijft de principes die in dit uitvoeringskader verder zijn uitgewerkt. Op 19 juli 2017 heeft het Korps Management Team de eerste versie van het uitvoeringskader vastgesteld. Deze tweede versie bevat eveneens de wijzigingen in verband met de veranderingen in de wetgeving (zie paragraaf 4.4).

Omdat de doelgroep gevarieerd is, is niet ieder hoofdstuk voor elke lezer noodzakelijke kost. Ben je goed bekend met de informatievoorziening van de politie en met de vernieuwingsprojecten, dan kun je hoofdstuk 2 en 3 wellicht overslaan.

---

[9] van den Hoven, J. (2013) Value Sensitive Design and Responsible Innovation, in Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society (eds R. Owen, J. Bessant and M. Heintz), John Wiley & Sons, Ltd, Chichester, UK.

Na de introductie van het onderwerp wordt in hoofdstuk 2 een terugblik geboden: de ontwikkeling van de informatievoorziening wordt beschreven waarbij de noodzaak wordt geschetst om de informatiehuishouding ingrijpend te vernieuwen. In hoofdstuk 3 wordt de vernieuwing van de informatievoorziening toegelicht. Dit gebeurt aan de hand van de drie plangebieden uit het Bestemmingsplan Informatievoorziening. Hoofdstuk 4 beschrijft het juridisch kader. In hoofdstuk 5 worden alle principes uitgewerkt. Deze zijn reeds benoemd in het document dat de architectuurprincipes bevat. Hier vindt de nadere invulling plaats, inclusief verwijzingen naar andere kaders en richtlijnen. Hoofdstuk 5 bevat de principes, dit hoofdstuk is dus waar het om draait. In de bijlagen vind je onder andere een nadere duiding van belangrijke concepten uit de Wpg en een overzicht van de kaders en richtlijnen waar we bij het schrijven van Privacy & Security by Design rekening mee hebben gehouden.

2. Ontwikkeling van de informatievoorziening politie

2.1. Nationale Politie en AVP

De actuele informatievoorziening van de politie is het product van drie belangrijke ontwikkelingen: de ontwikkeling van het regionale politiebestel, de daarop volgende vorming van de Nationale Politie en het Aanvalsprogramma Informatievoorziening. Door de vorming van de Nationale Politie zijn de regiokorpsen die tot 2013 hebben bestaan samengevoegd tot één landelijk politiekorps. De voornaamste reden daarvoor was om effectiever te kunnen optreden bij het aanpakken van landelijke veiligheidsproblemen. Het tweede doel was om de bedrijfsvoering van de politie efficiënter te organiseren in een landelijk politiedienstencentrum (PDC) waarbinnen ook ICT is opgenomen. Parallel aan deze reorganisatie is het Aanvalsprogramma Informatievoorziening (AVP) uitgevoerd met als doel om een aantal grote continuïteitsproblemen met de informatievoorziening op te lossen en de verouderde politiesystemen te vernieuwen. Dit AVP is als separaat programma naast de staande ICT-organisatie uitgevoerd en in 2017 vindt overdracht van de resultaten aan het PDC plaats. De politie heeft inmiddels de beschikking over een moderne en betrouwbare ICT infrastructuur. Ook de systemen voor de bedrijfsvoering zijn vernieuwd en landelijk georganiseerd. De vernieuwing van de operationele systemen is nog niet helemaal gerealiseerd. Met name de systemen voor registratie en transactieverwerking stammen nog uit de tijd van voor het AVP. Voor de komende tijd is de uitdaging om ook deze systemen te vernieuwen en om de nieuwe mogelijkheden van een geïntegreerde landelijke informatievoorziening te gaan benutten.

2.2. Het nieuwe Bestemmingsplan IV

De ontwikkeling van de informatievoorziening is de afgelopen jaren gestuurd op basis van de architectuur uit het Bestemmingsplan Informatievoorziening uit 2014. In dit bestemmingsplan zijn de strategische speerpunten voor de ontwikkeling van de informatievoorziening geformuleerd en wordt het hoofdontwerp van de toekomstige informatievoorziening beschreven. Het begrip bestemmingsplan is afkomstig uit de ruimtelijke ordening en brengt een ordening aan in de inrichting van het ICT landschap. Het bestemmingsplan vormt zodoende de basis voor de beleidslijnen en kaders voor de ontwikkeling van nieuwe systemen. Inmiddels is het plan herzien omdat de eerste doelen van het oude bestemmingsplan zijn gerealiseerd en omdat er nieuwe ontwikkelingen zijn die om aandacht vragen. Dit zijn zowel maatschappelijke als technologische ontwikkelingen die aanleiding vormen voor veranderingen in het politiewerk en voor de ondersteuning daarvan met informatievoorziening. We zien de volgende ontwikkelingen[10]:

- Virtuele wereld en fysieke wereld zijn één. Dit vraagt om nieuwe middelen om bijvoorbeeld cybercrime op te sporen en te bestrijden.
- Sociale-, eigendoms- en organisatiegrenzen vervagen. Er ontstaan allerlei netwerken, zoals combinaties van bedrijven in binnen- en buitenland, en ketens van onderaannemers.
- Burgers, bedrijven en overheid participeren in continu veranderende netwerken. De politie is daar een onderdeel van, of ze wil of niet.
- Burgers kunnen meer dan vroeger door de virtuele wereld. Ze handelen eigenstandig en kiezen zelf voor de manier waarop ze hun behoeften invullen. Burgers “bemoeien” zich ook steeds meer met politieprocessen (helpen meezoeken naar vermiste mensen, er ontstaan vormen van ‘eigenrichting’ bijv. via Twitter, en burgers gaan zelf opsporen of meehelpen met de opsporing, bijvoorbeeld via Bellingcat).
- De overheid loopt steeds verder achter op de samenleving. Organisatievormen en werkwijzen worden te langzaam aangepast.
- Mogelijkheden ontwikkelen zich snel en zijn moeilijk te voorspellen, iets waar je in investeert kan een half jaar later achterhaald zijn.
- De samenleving roept om een open en transparante overheid, de samenleving heeft behoefte aan steeds meer informatie, maar heeft ook moeite met het toenemende gebruik van persoonsgegevens door overheidsinstanties.

2.3. Hoofdlijnen IV-strategie

Deze ontwikkelingen vragen om een politie met een informatievoorziening die compact en wendbaar is en die flexibel kan worden gecombineerd met de informatievoorziening van anderen. Daartoe moet de politie kunnen meeliften op kennis van en investeringen door derden door slimme samenwerkingsverbanden aan te gaan. De politie houdt met de ontwikkeling van haar informatievoorziening vast aan de infrastructurele benadering. Deze benadering gaat uit van een zich ontwikkelend fundament dat zowel technologie omvat als gegevens- en applicatie-infrastructuur. Bij de

[10] IV-strategie en Bestemmingsplan Nationale Politie 2017

besturing van de informatievoorziening wordt veel ruimte geboden voor eigen initiatief dat in een gezonde balans is met een vorm van centrale regie.

2.4. Strategische speerpunten

De ontwikkelingen om ons heen zijn sneller gegaan dan bij het opstellen van het eerste bestemmingsplan in 2013 werd voorzien. De speerpunten van het Bestemmingsplan IV zijn daarom aangepast. Het heeft zo'n twee jaar geduurd voordat de betekenis van de speerpunten in de gehele organisatie waren doorgedrongen. Bij de nieuwe speerpunten is daarom gezorgd dat de formulering zo veel mogelijk herkenbaar is gebleven.

Het speerpunt 'Gegevens zijn de kern' blijft bestaan. Goede gegevens zijn randvoorwaardelijk voor de uitvoering van het politiewerk en voor een toekomstvaste informatievoorziening. Naast gestructureerde gegevens zijn dat ook steeds meer ongestructureerde en multimediale gegevens, zoals foto's en filmpjes die burgers met smartphones aanleveren en opnames van bodycams. De verwerking daarvan wordt onder architectuur georganiseerd en met metagegevens bestuurd. Er is een nieuw speerpunt toegevoegd 'Rechtmatigheid gewaarborgd' dat zeer relevant is voor het onderwerp van dit uitvoeringskader.[11] Hiermee geeft de politie aan de rechtmatigheid van de gegevensverwerking in het ontwerp van zijn informatievoorziening, 'by design', te willen borgen. Daarnaast gaat de politie ook open de dialoog aan over normatieve dilemma's. Wat (wettelijk) is toegestaan is niet altijd maatschappelijk geaccepteerd.

Figuur 3: de strategische speerpunten uit het Bestemmingsplan IV (versie 2017)

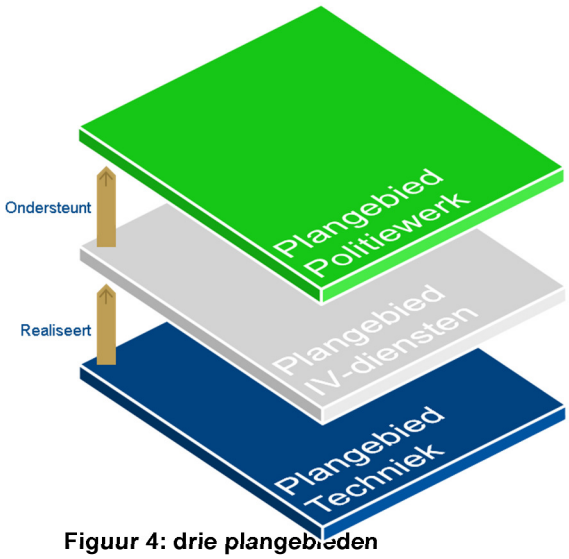
[11] Rechtmatigheid gewaarborgd' betekent dat de politie persoonsgegevens op een rechtmatige wijze verwerkt, dus volgens de wettelijke kaders van onder andere de Wpg en de AVG.

3. Vernieuwing van de informatievoorziening

Het Bestemmingsplan IV beschrijft het toekomstbeeld en de veranderstrategie waarlangs de vernieuwing van de informatievoorziening van de politie plaatsvindt. Vernieuwing van de informatievoorziening gebeurt op vele manieren: in de politiepraktijk, in de ICT-organisatie, in projecten maar ook in de vorm van kleine experimenten en agile applicatieontwikkeling met directe betrokkenheid van politieagenten. Er is daarbij veel ruimte voor eigen initiatief maar er is wel centrale regie nodig op de ontwikkelrichting en de samenhang. Er moet ook een flexibele en wendbare infrastructuur aanwezig zijn om deze nieuwe ontwikkelingen mogelijk te maken en te ondersteunen. Het Bestemmingsplan IV is geen blauwdruk, maar geeft richting en kaders voor deze ontwikkeling met een hoofdontwerp van de informatievoorziening in de vorm van drie onderling verbonden plangebieden.

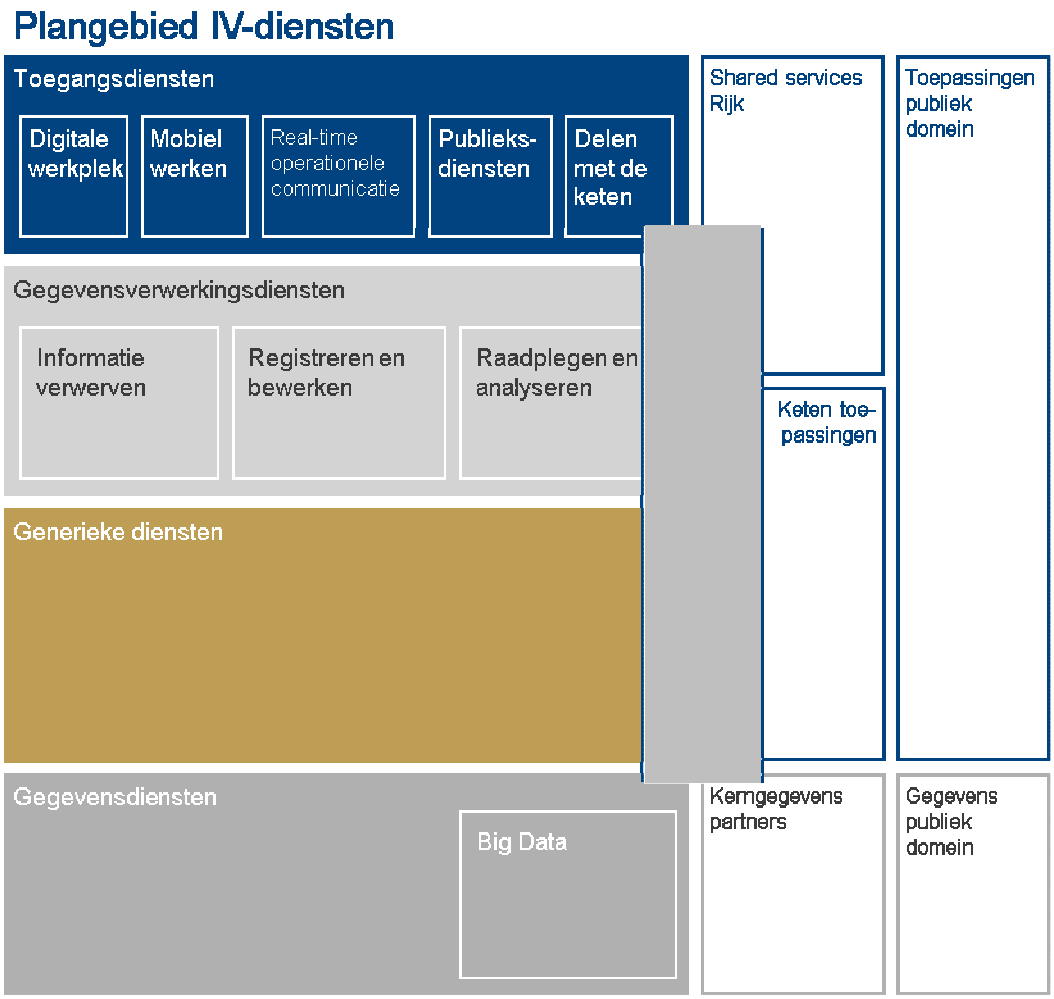
Het Bestemmingsplan gebruikt de analogie van de bouwwereld waarbij in plangebieden en kavels de functies en kaders voor de ruimtelijke ordening worden opgesteld. In dat verband kan dit uitvoeringskader gezien worden als een bouwbesluit of een plaatselijke verordening met uitvoeringsregels voor de inrichting en het gebruik van de aangewezen kavels. Dit uitvoeringskader geeft de ontwerprichtlijnen en de regels voor het gebruik van de aangewezen IV-diensten.

Het plangebied Politiewerk beschrijft de politieorganisatie in de vorm van doelen en werkzaamheden. De bedrijfsfuncties staan voor functionele bundelingen van competenties die bijdragen aan de werking en het behalen van de doelen van de organisatie.
Het plangebied IV-diensten beschrijft de informatievoorziening die het politiewerk ondersteunt. Een IV-dienst is een autonome eenheid van functionaliteiten die als bouwsteen kan worden ingezet voor het ondersteunen van een of meerdere bedrijfsfuncties.
Het plangebied Techniek levert de infrastructurele voorzieningen die nodig zijn om toepassingsdiensten te realiseren. Technische infrastructuurvoorzieningen omvatten apparatuur, netwerken en software-voorzieningen maar ook de voorzieningen voor de ontwikkeling en het beheer daarvan.



Figuur 4: drie plangebieden

De verwerking van gegevens maakt onderdeel uit van het plangebied IV-diensten. Voor dit uitvoeringskader is dus van belang wat de IV-strategie zegt over deze toepassingsdiensten en hoe de verschillende kavels van dit plangebied eruit zien.



Figuur 5: het plangebied IV-diensten, één van de drie plangebieden in het Bestemmingsplan IV

In het linkerdeel van het plangebied zijn de eigen IV-diensten van de politie weergegeven. In de twee rechterkolommen staan de IV-diensten van ketenpartners, van het rijk en het publieke domein. We voorzien dat de politie steeds meer gebruik gaat maken van externe IV-diensten. Overigens zijn de kavels zo gekozen dat de politie voor elke IV-dienst afzonderlijk sourcing-beslissingen kan nemen.

Bovenin het plangebied staan de IV-diensten die gebruikers toegang geven tot de informatievoorziening. De onderste rij bevat alle gegevensdiensten. Daar tussenin staan de IV-diensten waarin gegevens verwerkt worden. Er is een aparte tussenlaag gedefinieerd voor generieke diensten die voor meerdere toepassingen nodig zijn en die daarom als centrale voorziening geleverd worden. Naast standaard gegevensverwerkingsdiensten zijn er [redacted]. Daarbij wordt wél gebruik gemaakt van generieke diensten, gegevensdiensten en toegangsdiensten.

3.1. Toegangsdiensten

Bij de inrichting van toegangsdiensten geldt het IV-speerpunt ‘Mobiel werken is de norm’. Dat wil zeggen dat de informatievoorziening de politiepraktijk moet ondersteunen waarbij het werk steeds meer plaats- en tijdonafhankelijk georganiseerd is. Voor het mobiel werken op straat wordt daarbij ingezet op het gebruik van mobiele devices waarmee zo veel mogelijk informatie en hulpmiddelen voor agenten worden aangeboden. Er is daarnaast natuurlijk nog steeds werk dat op een digitale werkplek op kantoor plaatsvindt waarbij kantoorlocaties flexibel gebruikt worden en voor een deel van de werkzaamheden ook thuiswerken wordt toegestaan. In de praktijk betekent dit vooral dat functionaliteit van de informatievoorziening via meerdere kanalen of toegangsdiensten toegankelijk is.

Een bijzondere categorie van toegangsdiensten betreft de **Real-time operationele communicatie** van onder meer [redacted]. Hierbij worden bijzondere eisen gesteld aan de vertrouwelijkheid, de robuustheid en de real-time toegang tot de informatievoorziening. Voor deze categorie toegangsdiensten worden daar waar nodig bijzondere voorzieningen ingericht die al dan niet een gecontroleerde verbinding hebben met de rest van de informatievoorziening. Ten slotte zijn er nog toegangsdiensten voor externe partijen, waarbij we onderscheid maken tussen **diensten voor delen met de keten** en **publieksdiensten** voor het algemene publiek. De toegangsdiensten voor samenwerkingspartners voorzien in gecontroleerde gegevensuitwisseling tussen systemen en bevragingen van politiegegevens. De publieksdiensten ondersteunen de interactie met burgers en bedrijven met nieuws en meldingen maar ook met (elektronische) aangiftes. Bijvoorbeeld het doen van aangifte met DigiD.

3.2. Gegevensverwerkingsdiensten

Er zijn verschillende categorieën gegevensverwerkingsdiensten die tezamen de gehele levenscyclus van gegevensverwerking moeten omvatten en ondersteunen.

Toepassingsdiensten voor **informatie verwerven** bevatten veelal specifieke functionaliteit die is toegespitst op het type informatie, de aard van de bron of de bevoegdheid waarmee de informatie wordt ingewonnen. Door de digitalisering van de maatschappij wordt steeds meer informatie op digitale wijze ingewonnen en neemt de omvang en de diversiteit van de informatiestromen toe. Dit vereist dat diensten voor het verwerven van informatie gemakkelijk kunnen worden aangepast aan nieuwe informatiestromen en dat er gemakkelijk nieuwe diensten kunnen worden toegevoegd. Voorbeelden van informatieverwervingsdiensten zijn de elektronische aangifte en sollicitatieformulieren, (digitale) meldingen van burgers, interceptiefaciliteiten, bodycams, et cetera. Belangrijke kaders voor informatieverwerving zijn doelbinding en kwaliteitszorg. Met name als het gaat om persoonsgegevens moet duidelijk worden vastgesteld of de politie bevoegd is om de informatie verder te verwerken na verwerving en wat daarvoor de grondslag is. Bij het verwerven van informatie moeten ook de eerste waarborgen worden getroffen voor gegevenskwaliteit. Bijvoorbeeld door middel van [redacted].

Toepassingsdiensten voor het **registreren en bewerken** van gegevens vormen het hart van de gegevensverwerking door de politie. Deze toepassingsdiensten ondersteunen de werkprocessen, de dossiervorming en het samenwerken. Voorbeelden van registratie- en bewerkingsdiensten zijn de operationele systemen BVH, Summ-IT en [redacted], maar ook de bedrijfsvoeringssystemen Planon en BVCM. Er is op dit kavel van de informatievoorziening nog veel werk te doen om systemen te vernieuwen en legacy-toepassingen uit te faseren. Relevante kaders voor deze toepassingen zijn het beleggen van verantwoordelijkheden voor gegevensbeheer, het afleggen van verantwoording over de gegevensverwerking en ook het uiteindelijke bewaren of vernietigen van gegevens.

Bij de toepassingsdiensten voor het **raadplegen en analyseren** van informatie zijn grote vernieuwingen gaande die mogelijk worden gemaakt door de realisatie van landelijke verzamelingen van gegevens maar ook nieuwe technologische mogelijkheden. De landelijke verzamelingen van gegevens zijn het product van de vorming van de Nationale Politie en het Aanvalsprogramma Informatievoorziening. Deze gegevensverzamelingen bieden veel mogelijkheden om gegevens in onderlinge samenhang te doorzoeken en te analyseren. We staan pas aan de wieg van het benutten van deze mogelijkheden. Voorbeelden van systemen met raadplegings- of analysetoepassingen zijn [redacted]. Belangrijke principes voor raadplegen en analyseren zijn autorisatie, doelbinding en verantwoording. De mogelijkheden om gegevens in hun onderlinge samenhang te doorzoeken lijken welhaast onbeperkt maar dat betekent niet dat het altijd mag en wenselijk is. De toepassingsdiensten moeten waarborgen bevatten die ervoor zorgen dat de toegang wordt beperkt tot personen die daarvoor geautoriseerd zijn, dat analyses beperkt worden tot doelen waarvoor de gegevens gebruikt mogen worden en dat hierover verantwoording kan worden afgelegd.

[redacted]. De reden dat dit als afzonderlijk kavel is opgenomen, is dat nieuwe maatschappelijke ontwikkelingen om een grote dynamiek van de politie vragen met flexibele vormen van IV-ondersteuning. [redacted]

3.3. Generieke diensten

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. Hierdoor ontstaan generieke bouwstenen waarmee gemakkelijk nieuwe toepassingsdiensten gerealiseerd kunnen worden en waarmee vernieuwingen met een eenmalige implementatie gemakkelijk in de hele informatievoorziening kunnen worden doorgevoerd. Er zijn bijvoorbeeld verschillende toepassingen die gebruikmaken van landkaarten en luchtfoto's om geografische informatie op af te beelden. In plaats van verschillende toepassingen te bouwen wordt deze functionaliteit als generieke voorziening ingericht waar meerdere toepassingen gebruik van kunnen maken. Zodoende hoeft kaartmateriaal maar één keer te worden ingekocht en kunnen nieuwe kaarten gemakkelijk in alle toepassingen worden doorgevoerd. Andere voorbeelden van generieke toepassingsdiensten zijn: [redacted]. Veel van de normen en richtlijnen voor zorgvuldige en rechtmatige gegevensverwerking die in dit uitvoeringskader beschreven worden, kunnen het beste met voorzieningen in de vorm van generieke diensten worden ingericht.

3.4. Gegevensdiensten

3.4.1. Kerngegevens Politie

Het speerpunt 'Gegevens zijn de kern' wordt op het plangebied toepassingsdiensten doorgevoerd door de vastlegging en het beheer van gegevens te organiseren in de vorm van gegevensdiensten. Gegevens kunnen zodoende eenmalig worden vastgelegd en in verschillende toepassingsdiensten meervoudig worden gebruikt. Voor basisgegevens voor de uitvoering van politietaken die in meerdere werkprocessen voorkomen worden kernregisters gedefinieerd. Dit zijn bijvoorbeeld basisgegevens over personen, bedrijven, locaties en goederen. Door deze gegevensverzamelingen als kernregisters te behandelen kunnen generieke voorzieningen worden getroffen om de gegevenskwaliteit te waarborgen en het gegevensbeheer te organiseren. Dat wil overigens niet zeggen dat deze gegevensverzamelingen als centraal beheerde registraties worden ingericht.

Gegevensdiensten kunnen ook worden gerealiseerd in de vorm van generieke voorzieningen 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.

3.4.2. Bigdata-diensten

Een bijzondere categorie van gegevensdiensten wordt gevormd door big-datadiensten. Deze diensten hebben betrekking op gegevensverzamelingen die te groot zijn en die te veel in vorm en structuur van elkaar verschillen om in reguliere databases te kunnen worden opgeslagen. [redacted]. Deze gegevens worden benaderbaar gemaakt door middel van bigdata-diensten met indexeringsvoorzieningen die met deze omvang en diversiteit van de gegevens kunnen omgaan. Zodoende kunnen deze gegevens ook voor andere toepassingsdiensten beschikbaar worden gemaakt.

De politie heeft momenteel meerdere bigdata-diensten voor verschillende toepassingen en verschillende gegevensbronnen. [redacted] Vanwege de bijzondere toepassingsmogelijkheden is het van groot belang om hierbij de normen en ontwerprichtlijnen uit dit uitvoeringskader te betrekken. Zie ook paragraaf 5.3.5.

3.4.3. Kerngegevens Partners

De politie maakt gebruik van algemene overheidsinformatie die door andere overheidsinstanties beheerd wordt. Voor basisgegevens die door meerdere overheidsinstanties gebruikt worden zijn basisregistraties ingericht. Door al bekende gegevens binnen de overheid met elkaar te delen, kan de overheid efficiënter opereren en de dienstverlening verbeteren. Zo hoeft een burger of bedrijf bepaalde gegevens niet steeds opnieuw aan te leveren, maar volstaat één melding. Voorbeelden van basisregistraties zijn de basisregistratie personen (BRP), het handelsregister (HR), de basisregistratie voertuigen (BRV) en de basisregistratie inkomen (BRI). Voor het gebruik van de basisregistraties gelden spelregels voor gegevensbeheer en -gebruik waar de politie als afnemer dus ook aan

[redacted]

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.

3.4.4. Gegevens publiek domein

Voor de uitvoering van politietaken kunnen gegevens uit het publieke domein van groot belang zijn. Met de snelle digitalisering van de maatschappij is steeds meer van deze informatie via internet en via social media beschikbaar. Bij actuele gebeurtenissen zijn burgers vaak zelf sneller ter plaatse dan de politie en kunnen via hun smartphones live datastreams leveren en snel foto's en filmpjes op internet plaatsen met toepassingen zoals Twitter. Omdat voor deze gegevens de betrouwbaarheid van de bronnen veelal niet bekend is moet deze met de nodige voorzichtigheid worden gebruikt.

3.5. Ketentoepassingsdiensten

Voor ondersteuning van de samenwerking met ketenpartners gebruikt de politie ketentoepassingsdiensten die in veel gevallen door ketenpartners worden geleverd. Voorbeelden van zulke toepassingsdiensten zijn: de strafrechtsketendatabase (SKDB), het Justitieel Documentatiesysteem (JD online) en het Centraal Digitaal Depot (CDD+). 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 . Op die manier kunnen ook de normen voor zorgvuldig en rechtmatig gebruik het beste worden gehandhaafd. Ter verbetering van de ketensamenwerking is er behoefte aan meer van deze systeemkoppelingen. In plaats van rechtstreekse systeemkoppelingen streeft de politie naar gebruik van generieke voorzieningen voor gegevensuitwisseling met ketenpartners.

3.6. Shared services Rijk

Binnen de sector Rijk wordt de informatievoorziening steeds meer gecentraliseerd en in de vorm van gemeenschappelijke diensten aangeboden. De politie maakt geen deel uit van de sector Rijk maar kan op basis van eigen overwegingen wel besluiten om van zulke gemeenschappelijke diensten gebruik te maken.

3.7. Toepassingen publiek domein

In het publieke domein zijn veel toepassingen beschikbaar die een grote toegevoegde waarde leveren voor het politiewerk zoals de NS-reisplanner en Google Maps. Bij het gebruik hiervan moeten we ons bewust zijn van de gegevens die hiermee worden prijsgegeven aan de leveranciers van deze diensten en van gegevens die onbeveiligd over het internet worden verstuurd. Een belangrijk norm is dat er geen politiegegevens en overige persoonsgegevens die de politie verwerkt zonder noodzaak worden prijsgegeven. Dat betekent dat er geen persoons- of politiegegevens mogen worden verstuurd met publieke toepassingen zoals WhatsApp of verwerkt mogen worden met publieke opslagdiensten zoals Dropbox.

4. Juridisch kader

4.1. Inleiding

De politie heeft tot taak om de openbare orde te handhaven, hulp te verlenen en criminaliteit te bestrijden en heeft daartoe ruime bevoegdheden gekregen. Bij vrijwel al het politiewerk worden tal van gegevens over personen, goederen, locaties en gebeurtenissen geregistreerd en gebruikt. Al bij een eenvoudige verkeerscontrole, het uitschrijven van een boete of beslechten van een burenruzie worden grote hoeveelheden persoonsgegevens verwerkt. Vroeger gebeurde dat vooral met pen en papier, tegenwoordig worden gegevens opgeslagen in bestanden en kan dit dankzij nieuwe technologieën steeds eenvoudiger, sneller en goedkoper. Hierin schuilen ook risico's voor de betrokkenen en al snel is de privacy van het individu in het geding. Want mag de politie wel beschikken over persoonlijke gegevens van burgers en voor hoe lang dan? Zijn die gegevens wel juist, wie controleert dat? De spelregels hieromtrent zijn vastgelegd in met name de Wet politiegegevens en het Besluit politiegegevens, beide in werking getreden op 1 januari 2008. De wetgever probeert daarmee een evenwicht te creëren tussen het belang van de rechtsbescherming aan de ene kant en de informationele privacy van de burger aan de andere kant. Daarnaast verwerkt de politie gegevens over de eigen medewerkers, leveranciers en bezoekers. De persoonsgegevens die zij hiervoor verwerkt, vallen per 25 mei 2018 onder de Algemene Verordening Gegevensbescherming (AVG), daarvoor onder de Wet bescherming persoonsgegevens (zie paragraaf 4.4).

Figuur 6: koorddanser laat zien hoe de verschillende waarden met elkaar in balans dienen te zijn.

Informationele privacy: de aantasting van of inbreuk op persoonlijke vrijheden door het gebruik van persoonsgegevens.
Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit zijn zowel identificeerbare gegevens zoals een vingerafdruk, maar ook gegevens die zouden *kunnen* leiden tot identificatie van een persoon zoals initialen, leeftijd, een signalement, woonplaats en beroep.
Politiegegeven: elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt.
Verwerken van een persoonsgegeven: een handeling of het geheel van handelingen met betrekking tot een persoonsgegeven, waaronder het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van een persoonsgegeven.
Bestand: een gestructureerd geheel van politiegegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen. Een bestand kan zowel geautomatiseerde als niet-geautomatiseerde verwerkingen van persoonsgegevens bevatten.

De bescherming van deze informationele privacy is in verschillende wetten en verdragen geregeld. In beginsel is in Nederland de AVG van toepassing, maar zoals uit bovenstaande inleiding blijkt, is de Wpg bij de uitvoering van de politietaak de belangrijkste wet. Daarnaast geeft bijvoorbeeld de Telecommunicatiewet regels op het gebied van e-mail, spam en cookies bij het gebruik van internet en bevat de Wet justitiële en strafvorderlijke gegevens (Wjsg) regels specifiek voor het Openbaar Ministerie. Ook is er sectorale wetgeving die aan de politie taken en bevoegdheden toebedeelt voor de verwerking van gegevens. Die wetten worden niet behandeld; denk hierbij aan de wegenverkeerswet, belastingwetten en vreemdelingenwetgeving.

In deze publicatie ligt de nadruk op principes en regels voor de verwerking van politiegegevens, zoals deze in de Wpg zijn beschreven. De regels die gebaseerd zijn op de AVG zijn eveneens meegenomen en zijn terug te vinden in de verschillende principes. Wanneer er voor het AVG- en Wpg-domein sprake is van verschillende invulling, wordt dit in de tekst vermeld. Als er geen opmerking over gemaakt wordt, geldt een principe zowel bij de verwerking van politiegegevens als bij de verwerking van overige persoonsgegevens.

Beide privacywetten geven de burger bepaalde rechten, zoals het recht om te weten wat er met zijn persoonsgegevens gebeurt. De burger mag zijn gegevens inzien en mag ook verzoeken tot correctie van zijn gegevens.[13] Ook worden in beide domeinen bijvoorbeeld eisen gesteld met betrekking tot beveiliging, autorisaties, juistheid en actualiteit van gegevens.

In onderstaande paragrafen worden de AVG en Wpg geïntroduceerd. Elementen uit de Wpg die voor Privacy & Security by Design van speciaal belang zijn, worden verder uitgewerkt in bijlage 2. In paragraaf 4.4 komen de Europese ontwikkelingen aan bod. Als een verwerking stopt voor 25 mei 2018, is alleen de Wbp van toepassing. De tekst in deze versie van dit uitvoeringskader is geschreven uitgaande van de situatie na 25 mei 2018 en is gebaseerd op de concepttekst van de Wpg die op 16 februari 2018 naar de Tweede Kamer is verstuurd. In de laatste paragraaf wordt er een introductie verzorgd op de Archiefwet en de Wet hergebruik van overheidsinformatie.

4.2. Algemene Verordening Gegevensbescherming (AVG)

De AVG geldt voor alle personen, ondernemingen, organisaties en overheidsinstellingen die persoonsgegevens verwerken, dus ook voor de politie (voor zover het niet gaat om persoonsgegevens die voor de politietaak verwerkt worden).

Er is sprake van persoonsgegevens indien het gaat om informatie over een identificeerbaar natuurlijk persoon. Binnen de politie is de AVG in ieder geval van toepassing op alle verwerkingen bedoeld voor de interne bedrijfsvoering. De persoonsgegevens moeten op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt en mogen alleen verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Een verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Punt f, geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

De AVG is net als de voorgaande Wbp opgesteld aan de hand van open normen. Dit betekent dat in beginsel vrij veel mogelijk is op het gebied van het verwerken van persoonsgegevens, zolang er maar een gerechtvaardigd doel van toepassing is (zie hierboven). De aard van sommige persoonsgegevens brengt met zich mee dat de verwerking voor

[13] Voor inzage in politiegegevens bestaan uitzonderingsgronden (art. 27 Wpg)

een grote inbreuk op de persoonlijke levenssfeer van de betrokkene kan zorgen. Dit is de categorie bijzondere persoonsgegevens. Verwerking van de volgende persoons-gerelateerde gegevens is in beginsel verboden:

- ras of etnische afkomst
- politieke opvattingen
- religieuze of levensbeschouwelijke overtuigingen
- het lidmaatschap van een vakbond
- verwerking van genetische gegevens
- biometrische gegevens met het oog op de unieke identificatie van een persoon
- gegevens over gezondheid
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Ook persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen niet worden verwerkt. Het is niet toegestaan deze bijzondere persoonsgegevens te verwerken, tenzij hier een gegronde reden voor is. Een gegronde reden kan onder andere zijn:

- uitdrukkelijke (en uit vrije wil gegeven) toestemming van de betrokkene,
- duidelijk openbaar gemaakt door de betrokkene,
- een zwaarwegend algemeen belang (ook van de verantwoordelijke en/of betrokkene),
- gegevens zijn noodzakelijk tijdens een gerechtelijke procedure.

Een belangrijk onderdeel binnen de AVG zijn de rechten van betrokkenen. Een betrokkene heeft het recht op inzage, correctie en verzet. Verder stelt de AVG als eis dat er passende technische- en organisatorische maatregelen worden getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking. Vooruitlopend op de AVG is de politie begonnen met het opstellen van Gegevensbeschermingseffect-beoordelingen (GEB). Een zelfstandig onderdeel van de GEB is een risicoanalyse door PDC - Informatiebeveiliging, op basis waarvan genoemde beveiligingsmaatregelen moeten worden genomen. In het geval van een externe verwerker van persoonsgegevens zullen de te nemen maatregelen worden opgenomen in de (ook nieuwe) standaard politie verwerkersovereenkomst.

4.3. Wpg in vogelvlucht

In de Wpg en de daarbij behorende algemene maatregelen van bestuur[14] is geregeld hoe de politie dient om te gaan met politiegegevens. De Wpg geldt voor alle organisaties die politietaken uitvoeren, oftewel de:

- politie, inclusief de Rijksrecherche,
- Koninklijke Marechaussee,
- bijzondere opsporingsdiensten: FIOD-ECD, ISZW (voorheen SIOD), NVWA-IOD en ILT/IOD,

De Wpg heeft alleen betrekking op de uitvoering van de politietaak, oftewel op de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven (artikel 3 Politiewet 2012). De Wpg reguleert de verwerking van alle persoonsgegevens die de politie[15] in het kader van haar taakuitoefening verzamelt. In de kern gaat het erom dat de politie alleen persoonsgegevens verwerkt: [16]

- voorzover die noodzakelijk zijn voor een goede uitvoering van de politietaak,
- voor wettelijk geformuleerde doeleinden[17],
- die rechtmatig verkregen zijn,
- die accuraat zijn: gegevens die niet juist blijken te zijn, moeten gecorrigeerd worden of vernietigd,
- door daartoe geautoriseerde politiemedewerkers.

De Wpg stelt hiertoe voorwaarden aan de beveiliging, opslag, autorisaties, verwerkingstermijnen en ter beschikking stelling (binnen het Wpg-domein). Ook beschrijft de Wpg de regels voor het verstrekken van gegevens aan partners waarmee de politie samenwerkt zoals het Openbaar Ministerie (OM) de gemeente, de Raad voor de Kinderbescherming, de reclassering en buitenlandse (opsporings)organisaties. Tot slot beschrijft de wet de waarborgen voor de burger tegen ongerechtvaardigde inbreuken op zijn privacy en is het toezicht op naleving van de wettelijke regels geregeld. In bijlage 2 wordt een aantal onderdelen uit de Wpg toegelicht.

---

[14] Zie bijlage voor een overzicht van de gehele Wpg-wetsfamilie.

[15] In deze publicatie wordt met politie ook steeds gedoeld op de andere organisaties waar de Wpg voor geldt.

[16] Wpg regelt niet de bevoegdheid van de politie tot het verkrijgen van gegevens, die bevoegdheden zijn met name te vinden in het Wetboek van Strafvordering, de Politiewet 2012 en in bijzondere wetten.

[17] In de bijlage worden de verschillende verwerkingsgronden uitgewerkt.

De Wpg is niet van toepassing bij:

- toezichthoudende taken van de politie, bijvoorbeeld het uitvoeren van prostitutiecontroles ('burgemeesterstaken') vallen onder de AVG. Ook de vreemdelingentaak en wapenvergunningenadministratie wordt uitgevoerd onder de AVG[18].
- gegevens met betrekking tot een rechtspersoon die niet herleidbaar zijn tot een natuurlijke persoon,
- gegevens bedoeld voor persoonlijke doeleinden van de politiefunctionaris,
- gegevens bedoeld voor interne bedrijfsvoering van de politie,
- gegevens die de politie verwerkt over bezoekers en leveranciers (daarop is de AVG van toepassing).

4.4. Europese wetgeving

In mei 2016 zijn in de Europese Unie de Algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging in werking getreden. Deze regels zijn vanaf 25 mei 2018 in de gehele EU van toepassing. De AVG is rechtstreeks werkend en vervangt de Wbp. Daarnaast zal de AVG van toepassing zijn op de verwerking van persoonsgegevens in het kader van de Vreemdelingenwet en korpscheftaken. De Richtlijn is omgezet in nationale wet- en regelgeving. Dit betekent een wijziging van de Wpg en de Wjsg. Het wetsvoorstel en de bijbehorende Memorie van Toelichting zijn op 16 februari 2018 naar de Tweede Kamer verstuurd. Deze nieuwe Europese regels leiden onder meer tot een versterking van de rechten van de betrokkene, een zwaardere loggingsverplichting, een registerplicht voor alle verwerkingen en de aanstelling van een verplichte interne toezichthouder (Functionaris voor Gegevensbescherming) naast de Autoriteit Persoonsgegevens.

Per mei 2018 ziet de privacywetgeving (AVG en Wpg) er dus anders uit. Een aantal elementen uit de protocolplicht[19] is vervangen door loggingsverplichtingen, de registerplicht en de documentatieplicht. In hoofdstuk vijf en in bijlage twee wordt ditBIJLAGE 2: Onderdelen uit de Wpg toegelicht verder uitgewerkt. De gegevensverwerking voor de korpscheftaken (zoals jachtakten en wapenverloven) komen onder de AVG te vallen en dus niet meer onder de Wpg. Voor de vreemdelingentaak geldt dat een groot gedeelte van de gegevensverwerkingen onder de AVG komt te vallen en de strafrechtelijke onderdelen blijven onder de Wpg vallen.

Na 2018 zal de Wpg nog een keer worden aangepast en mogelijk worden samengevoegd met de Wjsg. Dan zullen ook zaken aangepast worden die uit bijvoorbeeld het knelpuntenonderzoek naar boven zijn gekomen of wensen vanuit de politieorganisatie.[20]

4.5. 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, Archiefbesluit 1995 en Archiefregeling 2009. 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 rijks-brede Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO[21]). Dit Normenkader is inmiddels onderdeel van de informatiear chitectuur van de politie.

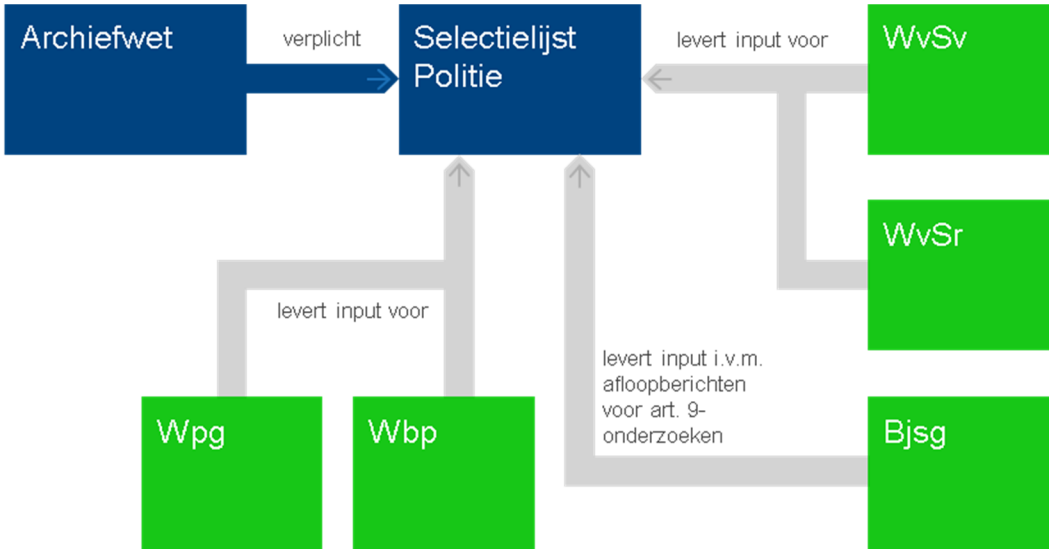
Op basis van deze algemene regels is een specifieke Beheerregeling Documentaire Informatie Politie 2017[22] opgesteld. De Beheerregeling geeft een nadere uitwerking van de taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeheer voor de politie en werkt een aantal nadere aspecten 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.

---

[18] In de toelichting op de nieuwe Wpg wordt onder artikel 23 lid 3 beschreven hoe voor de korpscheftaken gegevens van het Wpg-regime naar het AVG-regime verstrekt kunnen worden. Andersom biedt de AVG een mogelijkheid tot verstrekken aan de korpschef.
[19] Artikel 32 Wpg
[20] Zie het door het WODC uitgevoerde onderzoeksrapport 'Glazen privacy'
[21] Te vinden op: https://wiki.nationaalarchief.nl
[22] Zie Staatscourant 56416 van 9 oktober 2017

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 Wpg en het Wetboek van strafrecht en strafvordering (WvSr en WvSv). Ook het Besluit justitiële en strafvorderlijke gegevens bevat regels over verwijdertermijnen. De selectielijst beschrijft eveneens hoelang AVG-gegevens buiten de eigen vastgestelde bewaartermijnen bewaard moeten blijven. Dit zijn onder andere de gegevens die de politie verwerkt voor haar interne bedrijfsvoering. Bijvoorbeeld een personeelsdossier, schadezaak, gegevens over een leverancier of bezoeker, een veiligheidsonderzoek of de salarisadministratie.

De Wpg geeft invulling aan wat de Archiefwet vereist: de Wpg beschrijft welke gegevens hoe lang bewaard worden. Voor artikel 8-gegevens geldt in de Wpg 5 jaar verwerken, dan 5 jaar bewaren en daarna vernietigen. Voor artikel 9 eist de Wpg dat gegevens zolang 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. In onderstaand overzicht wordt dit verder uitgewerkt; het biedt geen uitputtende lijst maar geeft voor de meest voorkomende gegevensgroepen weer wat de Wpg en de selectielijst erover zeggen. De Gegevensautoriteit heeft een notitie opgesteld die beschrijft hoe de selectielijst, de Archiefwet en de Wpg zich tot elkaar verhouden.



Figuur 7: schematische weergave hoe Wpg en Archiefwet zich tot elkaar verhouden

4.6. Wet hergebruik van overheidsinformatie (Who)

De 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 als 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 (Wob) met de gedachte dat hergebruik uitgaat van reeds openbare informatie. Deze artikelen in de Wob zijn vervallen met de inwerkingtreding van de nieuwe Wet hergebruik.

Een Wob-verzoek biedt de burger de mogelijkheid om overheidsgegevens in te zien. De Wet hergebruik 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 overheidsorganisatie beschikt zelf over de intellectuele eigendomsrechten en het gaat om informatie waar geen wettelijke beperkingen op rusten of rechten van derden, zoals privacy- of auteursrecht.

Met de komst van de Who is het verplicht om een verzoek om hergebruik te honoreren, tenzij sprake is van één van de limitatief omschreven uitzonderingen. Verder moeten alle documenten zoveel mogelijk machineleesbaar zijn en in een open bestandsformaat beschikbaar worden gesteld. Zo'n formaat garandeert de toegankelijkheid van informatie en is ook van belang voor de digitale duurzaamheid. Ook na tien jaar dient een bestand nog verwerkt te kunnen worden.

De Who kent geen verplichting tot digitaliseren specifiek voor hergebruik, wel een inspanningsverplichting. Het is dus de bedoeling dat gevraagde informatie zoveel mogelijk via elektronische weg en in herbruikbaar formaat wordt

verstrekt. Hier dient dus in het ontwerp en de aanbesteding van informatiesystemen rekening mee gehouden te worden. De wet omvat nadrukkelijk geen verplichting tot het bijwerken van de kwaliteit van gegevens voordat ze verstrekt kunnen worden. De overheidsinstelling is zelf verantwoordelijk voor de kwaliteit van de gegevens en het uitgangspunt is dat de kwaliteit voldoende is om haar taak uit te voeren.

Het vrijgeven van data voor hergebruik vereist veel zorgvuldigheid. Het is namelijk niet uit te sluiten dat de hergebruiker de data vrijelijk kan koppelen aan andere data waardoor mogelijk persoonsgegevens ter beschikking komen. Het is daarom zinvol om de hergebruiker te informeren over de mogelijke risico's dat zijn handelingen kunnen leiden tot een inbreuk op de bescherming van persoonsgegevens.

5. Principes voor de omgang met gegevens

5.1. Eenmalige vastlegging

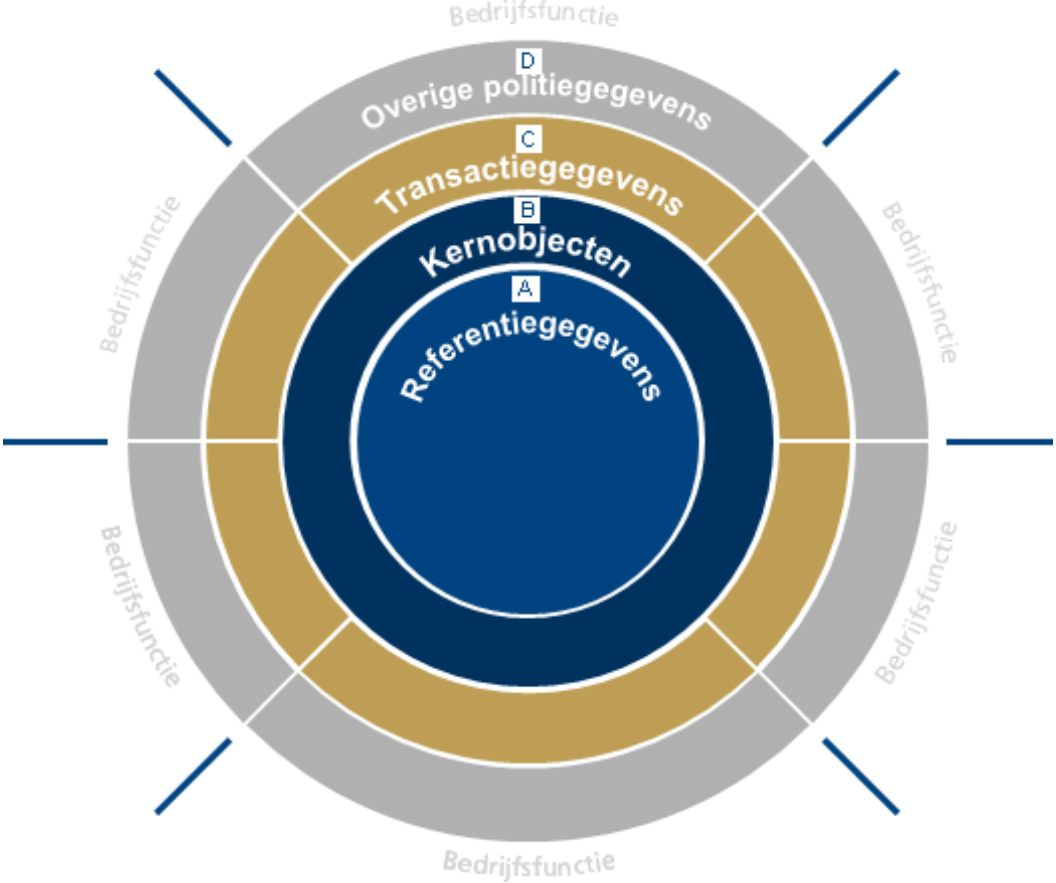
Principe

Gegevens worden eenmalig vastgelegd en meervoudig gebruikt.

Ratio: Het is efficiënter en goedkoper om gegevens te hergebruiken dan om gegevens opnieuw aan te maken of te verkrijgen. Daarbij leiden meerdere administraties van hetzelfde gegeven tot onduidelijkheid over het gebruik van de informatie. Bij de inzet van gegevens zal eerst gekeken moeten worden of er een authentieke bron is of dat al gegevens van eenzelfde of aantoonbaar ten minste gelijkwaardige kwaliteit en nauwkeurigheid beschikbaar zijn. In de gevallen waarin de politie met andere partijen samenwerkt, wordt bezien of de benodigde gegevens binnen de operationele en/of bedrijfsvoering keten kunnen worden verkregen.

5.1.1. Toelichting gegevenstypen

In onderstaand model wordt weergegeven dat de referentiegegevens (A) en de kernobjectgegevens (B) het fundament zijn van de gegevenshuishouding. 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.



Figuur 8: vier gegevenstypen

De transactiegegevens (C, de kern van het politiewerk) en de overige politiegegevens (D) bouwen voort op dat fundament. Ze bevatten de operationele aspecten van de informatiehuishouding van de politie. Deze gegevenstypen

maken gebruik van de kernobjectgegevens en de referentiegegevens. De kenmerken van de verschillende gegevenstypen worden nader beschreven in de beschrijving van het stelsel van kernobjecten[23].

Aangifte registratienr	Aangever	Locatie	Strafbaar feit	Goed	Maatschappelijke Klasse	Datum-tijd	Procesverbaal tekst
	B	B	C	B	A	A	

Aangifte is een construct dat voor de kwaliteit van de registratie sterk afhankelijk is van de kwaliteit van A (referentiegegevens) en B (kernobjectgegevens).

5.1.2. Eenmalige vastlegging per gegevenstype

Eenmalige vastlegging referentiegegevens
Een referentiegegeven is een verzameling waarden van één gegevenstype waarvan de betekenis, het gebruiksdoel en de inhoud vooraf is afgesproken. Het is met andere woorden een specifiek voorkomen van een referentie dat eenmalig wordt vastgelegd, meervoudig wordt gebruikt en niet door het operationele proces of het bedrijfsvoeringproces wordt gewijzigd. Voorbeelden van referentiegegevens zijn: de maatschappelijke klassen, de lijst van nationaliteiten en de lijst van typen goederen. Van ieder referentiegegeven wordt binnen de politie slechts één versie onderhouden.

Binnen de politieorganisatie is de afdeling GGB[24] 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, de mogelijke inhoud, de wijze van levering, de updatefrequentie en verzorgt de distributie van de ontwikkelde standaard. Een ingericht wijzigingsproces is één van de voorwaarden voor een op te leveren standaard. GGB ondersteunt de verantwoordelijken met het inrichten van het wijzigingsproces voor de referentiegegevens. De processen en de ondersteunende tooling voor het beheer van referenties moeten nog nader uitgewerkt worden.

Figuur 9: processen voor ontwikkeling en beheer van standaarden voor referentiegegevens

Eenmalige vastlegging kernobjectgegevens
Een kernobject is de verzameling gegevens van een bedrijfsobject dat een ankerpunt vormt voor vastlegging van transacties in de bedrijfsfuncties van de politie. Het is met andere woorden een gegevensweergave van tastbare objecten uit de wereld om ons heen, zoals personen, voertuigen, bedrijven of voorwerpen (goederen). Die objecten hebben in de buitenwereld hun eigen dynamiek en hun eigen levenscyclus waar de politie geen bijzondere invloed op heeft. Eén en hetzelfde object kan meerdere keren betrokken zijn bij verschillende operationele processen. De gegevens van die objecten blijven bij elk politieproces gelijk en deze zijn dus uitermate geschikt om opnieuw gebruikt te worden. Deze kernobjectgegevens kunnen worden opgeslagen in een kernregister. De gegevens van een kernobject worden één keer vastgelegd in zo'n kernregister, ongeacht hoe vaak hetzelfde object in verschillende processen geregistreerd is.

Daar waar mogelijk en toegestaan maakt de politie gebruik van de basisregistraties, een vorm van kernobjecten. De basisregistraties die voor de politie het meest van belang zijn, hebben betrekking op personen (Basisregistratie Personen), locaties (Basisregistratie Adressen en Gebouwen) en voertuigen (Basisregistratie Voertuigen).

[23] Informatiearchitectuur NP katern Stelsel van Kernobjecten
[24] De afdeling Gegevensgebruik en -beheer richt zich op een uniform kwaliteitsniveau van de gegevens rond vastlegging, beheer en gebruik. GGB beheert referentiestandaarden, formulieren en definities.

Onjuistheden in deze gegevensverzamelingen moeten worden teruggemeld aan de betreffende bronhouder (zie ook terugmelden bij het principe Kwaliteitszorg).

Eenmalige vastlegging transactiegegevens
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. Bij de uitvoering van die activiteiten wordt informatie verzameld en vastgelegd over de bedrijfsobjecten die tot de scope van de transactie behoren. Hiermee ontstaat niet alleen informatie over die bedrijfsobjecten zelf, maar ook over de redenen waarom een object relevant is voor het uit te voeren proces. Met deze informatie kan verantwoording afgelegd worden omtrent de registratie van bedrijfsobjecten. Bij de kernobjecten betekent dit dat zichtbaar is wat de hoedanigheid van een object is ten aanzien van een specifieke transactie.

> Bijvoorbeeld: de persoon [redacted] (kernobject) heeft bij een aangifte fietsdiefstal (specifieke transactie) de rol van aangever (zijn hoedanigheid bij deze transactie). Bij overige politiegegevens is dit terug te zien als de vastlegging van een relatie met de activiteit waar het object is geregistreerd.

Een transactiegegeven wordt in de regel in één applicatie vastgelegd. Het komt voor dat gegevens over transacties middels functionaliteit van meerdere applicaties worden verwerkt. In dat laatste geval is expliciete inrichting van een transactieregister met dataservices een vereiste.

Eenmalige vastlegging overige politiegegevens
Overige politiegegevens zijn ook een weergave van een feit of een gebeurtenis, maar het zijn informatieobjecten die 'bedacht' zijn door de politie of ketenpartners en waarvan de levenscyclus volledig beheerst wordt door de politie (dus niet vanwege veranderingen in de buitenwereld). De politie is verantwoordelijk voor het ontstaan, het beheer en de verwijdering van dit type gegevensobject. Voorbeelden zijn een signalement, spoor of antecedent.

Niet alle informatievoorzieningen binnen de politie zijn bestemd voor duurzame vastlegging van gegevens. Agora is bijvoorbeeld bestemd voor samenwerking en communicatie en niet voor registratie. Gegevens die hierin gedeeld worden, worden dan ook na korte tijd weer verwijderd. Voor duurzame beschikbaarheid dient dan ook gebruik gemaakt te worden van BVH, het daarvoor bestemde registratieve systeem.[25]

5.1.3. Eenmalige vastlegging versus Eenmalige opslag
Meervoudige vastlegging dient voorkomen te worden. Voor meervoudige opslag geldt dit eveneens, maar in mindere mate. Er zijn redenen om gegevens vaker op te slaan. Een voorbeeld hiervan is een datawarehouse-omgeving waarin gegevens worden geoptimaliseerd voor analysedoeleinden en opslag van historie. Andere voorbeelden zijn het maken van back-ups en borging van de beschikbaarheid van systemen (door 'on-the-fly' opgevragen bij de bron daalt de beschikbaarheid).

In geval van meervoudige opslag zijn de kaders voor zorgvuldige en rechtmatige gegevensverwerking zoals die gelden voor de bronsystemen onverkort van toepassing. Bovendien moeten extra waarborgen worden getroffen om de kwaliteit en de consistentie van de gegevensverwerking te waarborgen. [redacted]

5.1.4. Gegevensdiensten
De politie streeft ernaar om in de informatievoorziening gegevens te scheiden van functionaliteit. Gegevens moeten voor meerdere applicaties toegankelijk worden gemaakt via een gegevensdienstenlaag (los van de gegevensverwerkingsdiensten). De applicatiearchitectuur tezamen en de dynamische vormen van applicatieontwikkeling moeten het mogelijk maken om gegevens gemakkelijk te hergebruiken en in combinatie te analyseren.

---

[25] Zie de aansluitvoorwaarden waar een teamchef mee akkoord moet gaan bij gebruik van Agora voor politiegegevens

5.1.5. Handreikingen

In deze paragraaf wordt een aantal handreikingen geboden op basis van de bovenstaande tekst. De handreikingen zijn bedoeld als hulpmiddel om aan te geven waar rekening mee gehouden moet worden. Ze zijn dus niet als afvinklijst te gebruiken. De handreikingen beschrijven methoden en instrumenten die gebruikt kunnen worden om aan de principes te voldoen. Er kan ook op andere manieren invulling gegeven worden aan het principe.

Eenmalige vastlegging		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	Stuur bij IV wijzigingen aan op toepassing van kernregisters en centraal beheerde referentiegegevens. Hierbij hoort ook de ontsluiting van basisregistraties bij (via de kernregisters)
PDC	Sturing op IV ontwikkeling	Zorg voor inrichting en (door)ontwikkeling van kernregisters
	Requirements opstellen	Neem mee in de requirements: de koppeling aan kernregisters en de toepassing van centraal beheerde referentiegegevens

	Vaststellen gegevenstype	• Referentiegegevens
		  o Een verzameling waarden waarvan de betekenis, het gebruiksdoel en inhoud vooraf is afgesproken
		  o Vb. Nationaliteiten maatschappelijke klassen
		• Kernobjectgegevens
		  o Een verzameling waarden van tastbare objecten uit de wereld om ons heen zoals personen, voertuigen, bedrijven en voorwerpen
		  o Worden eenmalig vastgelegd in een kernregister en kunnen meervoudig worden gebruikt in verschillende processen
		• Transactiegegevens
		  o Een verzameling waarden over een feit of gebeurtenis. Het transactiegegeven kan binnen meerdere bedrijfsfuncties worden gebruikt en zijn veelal direct gerelateerd aan de wettelijke politietaak.
		  o Vb incident, aangifte, melding, zaak
		• Overige politiegegevens
		  o Een verzameling waarden over een feit of gebeurtenis waarbij levenscyclus is beheerst door de politie (niet onderhevig van veranderingen van de buitenwereld).
		  o Vb signalement, antecedent, spoor

	Ontwerpen	Neem vastlegging van gegevens van kernobjecten expliciet mee in ontwerp van processen en applicaties
	Analyse en ontwerpen BVI	Zoek de authentieke bron van gegevens en zorg dat de bron leidend is v.w.b. de beheerhandelingen
Uitvoering / Operatie	Registratie	Registreer gegevens (waar mogelijk) slechts eenmaal en wel in het daarvoor aangewezen registratieve systeem. Controleer voor invoer of gegevens niet al bestaan.

5.2. PDCA-cyclus

De werking van de informatievoorziening wordt bestuurd op basis van cyclische terugkoppeling.

Ratio: Informatiebeveiliging en gegevensmanagement zijn integraal onderdeel van de managementverantwoordelijkheid. De informatievoorziening levert daarom stuurinformatie aan de verantwoordelijke managers zodat zij zicht hebben op de stand van de gegevenskwaliteit en van de informatiebeveiliging en in staat zijn keuzes te maken.

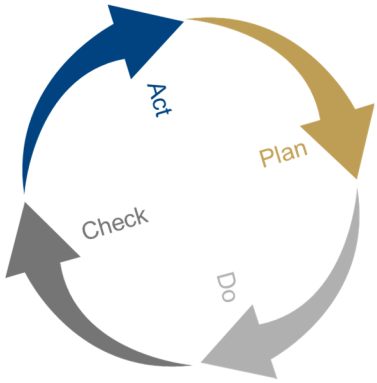
5.2.1. Besturing werkprocessen

Politiewerk bestaat voor een belangrijk deel uit het verwerken van gegevens. De informatievoorziening wordt daarom ook niet meer louter beschouwd als ondersteuning van politiewerk maar als onderdeel van het primaire proces. Voor besturing van de uitvoering moet de gegevensverwerking daarom een integraal onderdeel vormen van de besturingsprocessen. De politie kan alleen duurzaam haar doelstellingen realiseren wanneer de organisatie zijn processen continu aanpast aan de omstandigheden, zoals maatschappelijke ontwikkelingen, wijzigingen in de eigen middelen en wetgeving of tekortkomingen in geleverde diensten. Dit vereist een cyclische terugkoppeling of Plan-Do-Check-Act-cyclus (Deming-cirkel) in de besturingsprocessen met inbegrip van de gegevensverwerking.

De kwaliteitscirkel van Deming is een model voor kwaliteitsmanagement en organisatiebesturing ontwikkeld door William Edwards Deming. De cirkel beschrijft vier activiteiten die op alle verbeteringen in organisaties van toepassing zijn. De vier activiteiten zorgen voor een betere kwaliteit. Het cyclische karakter garandeert dat de kwaliteitsverbetering continu onder de aandacht is.

De vier activiteiten in de kwaliteitscirkel van Deming zijn:

- PLAN: Kijk naar huidige werkzaamheden en ontwerp een plan voor de verbetering van deze werkzaamheden. Stel voor deze verbetering doelstellingen vast.
- DO: Voer de geplande verbetering uit op een gecontroleerde en meetbare wijze.
- CHECK: Meet het resultaat van de verbetering en vergelijk deze met de oorspronkelijke situatie en toets deze aan de vastgestelde doelstellingen.
- ACT: Bijstellen aan de hand van de gevonden resultaten bij CHECK.



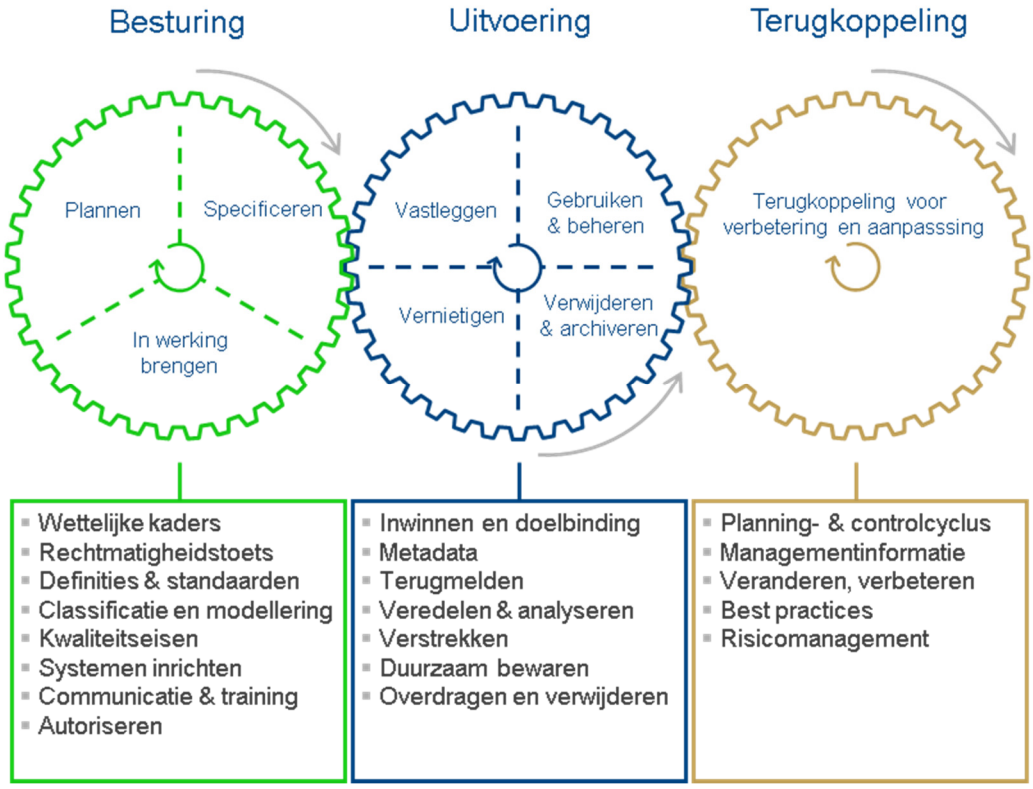
Figuur 10: vier activiteiten in de kwaliteitscirkel

De kern van dit model is dat de organisatie op deze manier in staat is om op ieder niveau haar werkzaamheden te beoordelen en te verbeteren. Het management dient de analyse te doen over de hoger gelegen processen, de korpsleiding voor de primaire bedrijfsprocessen.

5.2.2. Besturing gegevensverwerking

In dit uitvoeringskader worden de normen en richtlijnen voor de zorgvuldige en rechtmatige verwerking van gegevens opgesomd en toegelicht. Op elk van deze normen moet besturing worden georganiseerd in de vorm van de PDCA-cyclus. Dat geldt dus zowel voor de besturing op bijvoorbeeld autoriseren, kwaliteitszorg en privacy als op informatiebeveiliging. Het is onwenselijk om voor al deze verschillende normen en richtlijnen afzonderlijke besturingsprocessen in te richten met afzonderlijke plannen en rapportages. De besturing op de gegevensverwerking moet daarom worden ingericht als onderdeel van de besturing op het primaire proces.

Bij het inrichten van deze besturing moet de volledige levenscyclus van gegevensverwerking worden beschouwd vanaf de planning en het binnenhalen van gegevens tot en met het beheer en de uiteindelijke archivering of vernietiging daarvan. We gebruiken daarvoor het volgende referentiemodel waarmee wordt uitgedrukt dat de kaders en richtlijnen de gehele levenscyclus van gegevensverwerking moeten omvatten.



Figuur 11: levenscyclus van gegevensverwerking

Een belangrijk onderscheid is dat tussen de besturingscyclus (plannen – in werking brengen) en de uitvoeringscyclus (vastleggen – vernietigen). De principes voor omgang met gegevens komen tot uitdrukking of worden vertaald in de besturingscyclus en ze worden zichtbaar in de uitvoeringscyclus; daar waar daadwerkelijk gegevens worden *verwerkt*. Vanuit de uitvoeringscyclus vindt terugkoppeling plaats voor verbetering en aanpassing van de inrichting van zowel de besturingscyclus als de uitvoeringscyclus. In dit referentiemodel is de PDCA-cyclus herkenbaar van cyclische terugkoppeling in de besturing van de gegevensverwerking. Een belangrijke consequentie van dit uitgangspunt is dat gegevens gedurende hun gehele levenscyclus beheerd moeten worden.

> 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.

Vindt er gegevensverwerking plaats door een andere organisatie dan de politie (een externe verwerker)? Dan moet er een verwerkersovereenkomst zijn. Hierin worden onder andere afspraken opgesteld rondom geheimhouding, audits, opslag van de data en de beveiliging van de persoonsgegevens, het melden van datalekken en waar de persoonsgegevens voor mogen verwerkt. Zowel de AVG als de nieuwe Wpg vereisen dat er een dergelijke overeenkomst is.[26]

Het ontwerp van systemen moet worden getoetst en er moeten audits en onderzoeken op worden uitgevoerd. Daadwerkelijke controles op broncode zijn nodig om vast te stellen of aan de regels is voldaan. Tenslotte ligt in 75% van de IT-datalekken de oorzaak van het datalek in een fout in de broncode.[27]

5.2.3. Kennisontwikkeling medewerkers

Een politiemedewerker moet kennis hebben van de wet- en regelgeving die van toepassing is op zijn werkzaamheden. Dit betekent dat een teamchef moet zorgen dat zijn medewerkers voldoende kennis hebben en dat hij hier in de reguliere gesprekscyclus aandacht aan geeft. De profchecks van de Politieacademie bevatten vragen op het gebied van de Wpg en ook de nieuwe dilemma-game kent een categorie ‘omgang met gegevens’.

Privacywet- en regelgeving moet verankerd zijn in het opleidingsmateriaal- en in de diverse curricula. Dit geldt ten minste voor de elf basisopleidingen[28]. Alleen zo is gegarandeerd dat elke politiemedewerker de benodigde basiskennis heeft. Daarnaast zijn er vier specifieke Wpg-opleidingen: voor de bevoegd functionaris, de informatiemedewerker, de poortwachter en de privacyfunctionaris. Ook voor de overige aspecten inzake een zorgvuldige omgang met gegevens, dienen passende opleidingen te worden gevolgd, bijvoorbeeld op het gebied van de AVG en informatiebeveiliging.

De Wpg en de AVG dienen eveneens geïntegreerd te zijn in de werkinstructies en handboeken. Net zoals er geen werkinstructie of procesbeschrijving vastgesteld wordt zonder dat er gecontroleerd is of de Politiewet en het Wetboek van Strafvordering op de juiste wijze vertaald zijn, dient deze toets ook te worden gedaan voor de privacywetgeving. Distributie en het gebruik van het praktijkhandboek Wpg en de verstrekkingenwijzer dient door de teamchef gestimuleerd te worden zodat iedereen basiskennis heeft van de geldende wetgeving.

5.2.4. PDCA-voorzieningen en instrumenten

De besturing van de gegevensverwerking moet als onderdeel van de besturing van het politiewerk worden georganiseerd in een transparant proces met meetbare doelstellingen, rapportages, de resultaten van risicoanalyses en audits, registratie van risico’s en periodieke overzichten van incidenten. In de jaarplannen van de politie en al zijn onderdelen moeten daarom doelen worden opgenomen op het gebied van gegevensverwerking. Dat zijn doelen die

---

[26] Er is een sjabloon beschikbaar; dit is nog niet formeel vastgesteld, in verband met de nieuwe wetsteksten. Het sjabloon moet wel worden gebruikt bij nieuwe overeenkomsten waarbij er zaken worden uitbesteed bij derden, zoals externe hosting. Het document wordt op de Agora-site van de Gegevensautoriteit geplaatst

[27] Zie de toespraak van Rob van der Veer van de Software Improvement Group bij het iBestuur congres ‘Grip op privacy’

[28] Waaronder de MBO-opleiding voor agenten en de opleiding voor leidinggevenden (MTL/ LOS). Zie bijlage voor een compleet overzicht.

gaan over gegevenskwaliteit, informatiebeveiliging, autorisaties en alle andere aspecten van gegevensverwerking die in dit uitvoeringskader beschreven worden. Het is daarbij van belang om deze doelen meetbaar te maken zodat de uitvoering hiermee gestuurd en gecontroleerd kan worden. Op dezelfde manier moet over de uitvoering gerapporteerd worden. De managementrapportages moeten daarom ook een paragraaf bevatten over de gegevensverwerking zodat de verantwoordelijke managers kunnen (bij)sturen.

Gegevensbeschermingseffectbeoordeling (GEB)
Een belangrijk instrument bij de planning en het ontwerp van gegevensverwerking is de gegevensbeschermingseffectbeoordeling (GEB) die wordt voorgeschreven door de Algemene Verordening Gegevensbescherming (artikel 35) en de Wpg (artikel 4c). Dit is een voorafgaande toets op nieuwe of gewijzigde gegevensverwerkingen. 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. Aan de hand daarvan kunnen risico's worden ingeschat en benodigde maatregelen worden genomen. Het gebruik van de GEB is dus niet verplicht voor alle (bestaande) verwerkingen. Wanneer is het risico 'waarschijnlijk hoog'?[29] Bijvoorbeeld als er nieuwe technologieën worden gebruiken of als er bijzondere persoonsgegevens verwerkt worden. Er wordt door de Gegevensautoriteit een checklist ontwikkeld waarmee bepaald kan worden of het noodzakelijk is om een GEB uit te voeren. Zolang deze checklist nog niet beschikbaar is, kan gebruik worden gemaakt van onderstaand kwadrantenmodel uit de CIP-Handleiding Privacy by Design.[30]

[29] 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'.
[30] Zie Handleiding Privacy by Design, Centrum voor informatiebeveiliging en privacybescherming, 7 mei 2017, p. 17

Aard van de verwerking	conform of verenigbaar met oorspronkelijk doel	niet conform of verenigbaar met oorspronkelijk doel
structureel	Deze uitbreiding vormt geen eigen verwerking en vraagt dus niet om een eigen GEB. Indien deze uitbreiding op het proces nog niet is meegenomen in de GEB van dat werkproces c.q. de verwerking, dan kan de uitbreiding eenvoudig toegevoegd worden in de GEB op dat werkproces.	Deze uitbreiding vormt een eigen verwerking, omdat het een ander doel betreft dan de oorspronkelijke verwerking, waarvoor een GEB is uitgevoerd. Doordat deze uitbreiding structureel van aard is, is een GEB mogelijk en in dit geval dus een aparte, eigen GEB.
incidenteel	Door het incidentele karakter van deze verdere verwerking is het moeilijk of soms zelfs onmogelijk met enige trefzekerheid een GEB uit te voeren. Wel moet de individuele bewerker bepalen of de gegevensverwerking op zorgvuldige en rechtmatige wijze plaatsvindt. Als dat niet het geval is, bv door het ontbreken van een afdoende informatiebeveiliging, dan moet de bewerker afzien van de verdere verwerking.	De incidentele verdere verwerking vormt altijd een eigen verwerking, omdat zij een ander doel heeft dan de oorspronkelijke verwerking waarvoor een GEB is uitgevoerd. Door het incidentele karakter ervan verdere verwerking is het moeilijk of soms zelfs onmogelijk om trefzeker een GEB uit te voeren. Belangrijk verschil met hiernaast is dat er geen legitimering conform het doel van de oorspronkelijke verwerking is. Legitimering is door het incidentele karakter alleen mogelijk door aan te tonen dat het belang van de betrokkene wordt gediend en dit vast te leggen. Deze legitimering is vereist en kan het best worden bewerkstelligd door de verdere verwerking en het belang ervan met de betrokkene af te stemmen en vast te leggen, en dit voorafgaand te doen aan het gebruik van de resultaten van deze verdere verwerking. Daarnaast moet de individuele bewerker ook hier bepalen of de gegevensverwerking op zorgvuldige en rechtmatige wijze plaatsvindt. Als dat niet het geval is, bv door het ontbreken van een afdoende informatiebeveiliging, dan moet de bewerker afzien van de verdere verwerking.

Binnen de politie is een model voor deze toets beschikbaar voor de AVG-verwerkingen. Voor politiegegevens is het model in ontwikkeling. Het model en instructie is beschikbaar op de Agora-site van de Gegevensautoriteit.

Voorafgaande consultatie Autoriteit Persoonsgegevens
In bepaalde gevallen moet de AP door de verantwoordelijke geconsulteerd worden over de voorgenomen verwerking van persoonsgegevens, die in een nieuw bestand zullen worden opgenomen. Zie 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 meebrengt. Of de AP geconsulteerd moet worden, kan blijken uit een GEB (blijkt het risico inderdaad hoog?).

Register van verwerkingsactiviteiten
De AVG en de nieuwe Wpg vereisen dat elke verwerkingsactiviteit (dus elke informatievoorziening en elk gegevensbestand) wordt bijgehouden in een register. Zie artikel 31d Wpg en artikel 30 AVG. Dit is bedoeld om controle en toezicht op de gegevensverwerking mogelijk te maken. Daarbij moeten onder andere worden vastgelegd: de doelen van de verwerking, een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens en de beoogde verwijder- en vernietigingstermijnen. Ook de toekenning van autorisaties moet (conform artikel 31 d onder j) worden vastgelegd per verwerkingsactiviteit. Deze verplichting viel voorheen onder de protocolplicht (artikel 32 lid 1 onder c Wpg).

In de loop der jaren zijn verschillende overzichten gegenereerd van de applicaties bij de politie (zie onder andere maar er bestaat nog geen overzicht dat aan deze verplichting voldoet.[31] Bij een aanpassing of nieuwe informatievoorziening hoeft dus niet zelf een register te worden ontwikkeld maar er moet melding van gemaakt worden bij het register.

Niet alleen de verwerkingsverantwoordelijke heeft de plicht tot het aanleggen van een register, maar ook de verwerker heeft deze plicht. Dit staat beschreven in artikel 30 lid 2 AVG en artikel 31d lid 2 Wpg. In deze artikelen staat exact opgesomd welke gegevens over de verwerking in het register moeten worden opgenomen. Bij het afsluiten van een verwerkersovereenkomst is het verstandig hier expliciet op te wijzen richting de verwerker.

[31] De Gegevensautoriteit zorgt ervoor dat een register voor alle verwerkingsactiviteiten wordt ontwikkeld.

5.2.5. Handreikingen

PDCA-cyclus		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	• Neem de besturing op de gegevensverwerking op als onderdeel van de reguliere PDCA-cyclus. • Stel meetbare doelen voor gegevensverwerking. • Indien een gegevensverwerking plaatsvindt door een externe organisatie dan dient er een verwerkersovereenkomst te zijn. • Bij het besturen van de uitvoering moet gegevensverwerking een integraal onderdeel vormen van de besturingsprocessen. • Gegevensverwerking moet worden ingericht als onderdeel van de besturing van het primaire proces.
	Uitvoering rapportagecyclus	• Geef advies en ondersteuning bij planningen en rapportages.
PDC	Ontwikkelen	• Zorg dat gegevensverzamelingen beheerd worden; ook als een informatievoorziening wordt uitgefaseerd.
	Vernieuwing	• Processen moeten continu aangepast worden aan omstandigheden (maatschappelijke ontwikkelingen, wijzigingen in de eigen middelen, wetgeving of tekortkoming in geleverde diensten). • Voer samen met de privacyfunctionaris een GEB uit. • Als uit de GEB blijkt dat dit nodig is, consulteer dan de AP voorafgaand aan de verwerking. • Meld de verwerking aan bij het register van verwerkingsactiviteiten.
Uitvoering / Operatie	Besturen	• Het jaarplan bevat SMART-geformuleerde doelen ten aanzien van de gegevensverwerking. • Bijsturen van gegevensverwerking op basis van rapportages.
	Kennis op doen	• Een politiemedewerker heeft kennis van wet- en regelgeving die van toepassing is op zijn werkzaamheden • Privacywet- en regelgeving moeten verankerd zijn in het opleidingsmateriaal • De Wpg en AVG dienen eveneens geïntegreerd te zijn in de werkinstructies en handboeken.

5.3. Doelbinding

Persoonsgegevens worden alleen verwerkt als daar een gerechtvaardigd doel voor bestaat en ze worden niet verder verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel.

Ratio: Door de verwerking van gegevens te baseren op gerechtvaardigde doelen is de kans op inbreuken op de persoonlijke levenssfeer van betrokkenen beperkt en wordt misbruik van gegevens voorkomen. De realisering van een gerechtvaardigd doel moeten kunnen steunen op a) één of meer van de in de artikel 6 AVG genoemde gronden voor gegevensverwerking of b) de verwerkingsgronden zoals uit de Wpg. Bij de verdere verwerking van gegevens moet steeds worden beoordeeld of het doel niet onverenigbaar is met het doel waarvoor deze gegevens oorspronkelijk zijn verzameld. Hoe dichter die twee doelen bij elkaar liggen (of hoe meer ze verwant zijn), hoe groter de kans dat verder gebruik mogelijk is. Naast de doelbinding is ook het niveau van vertrouwelijkheid van gegevens (zie principe Informatiebeveiliging) in sterke mate bepalend voor het eventuele hergebruik.[32]

In het personeelssysteem is het BSN-nummer opgenomen voor fiscale verplichtingen. Dit mag dan alleen daarvoor gebruikt worden en dus niet voor verlofbriefjes of ziekmeldingen.

5.3.1. Systeemontwikkeling en -ontwerp

Voor persoonsgegevens die op basis van de AVG worden verwerkt, geldt dat deze alleen verzameld mogen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het kan bijvoorbeeld noodzakelijk zijn voor de uitvoering van een overeenkomst (de politie verwerkt facturen van zelfstandigen die voor de politie werkzaam zijn) of er is ondubbelzinnige toestemming van de betrokkene (bezoeker van de website politie.nl doet mee aan bezoekerspanel)[33]. De wetgever heeft hiervoor een zestal limitatieve verwerkingsgronden opgenomen in de AVG. In bepaalde gevallen kunnen gegevens die onder de AVG verwerkt worden, wel verder verwerkt worden op een wijze die onverenigbaar is met het oorspronkelijke doel.[34] Ook voor gegevens die onder de Wpg verwerkt worden, geldt dat er een limitatief aantal verwerkingsgronden bestaat.[35] Bij het ontwerp van een informatievoorziening dient ervoor gezorgd te worden dat elk gegeven van zo'n verwerkingsgrondslag wordt voorzien. Dat betekent dat duidelijk moet zijn of politiegegevens onder artikel 8, 9, 10, 12, 13 of 14 verwerkt worden. Als bijvoorbeeld bij een verkeerscontrole vastgelegd wordt dat het rijbewijs is verlopen, dan wordt dit opgeslagen op grond van artikel 8. Naast Wpg-classificatie zijn er nog andere vormen van classificatie, bijvoorbeeld de mate van betrouwbaarheid en vertrouwelijkheid van de gegevens (zie principe Informatiebeveiliging). De grondslag dient meegenomen te worden bij het maken van informatieanalyses en informatie-architecturen. Verwerkingsgrondslagen worden bij gegevens vastgelegd in de vorm van metagegevens (zie principe Metagegevens). In de ontwerpfase dient ook een gegevensbeschermingseffectbeoordeling (GEB) te worden uitgevoerd. Dit is verder uitgewerkt bij het principe PDCA.

Gegevens die verwerkt worden in informatiesystemen die de politietaak ondersteunen, moeten worden behandeld als zijnde politiegegevens (Wpg) tenzij de verwerking evident onder de AVG valt of geen persoonsgegevens betreft, zoals aantallen inbraken die niet tot personen te herleiden zijn. Ook gegevens over overleden personen en rechtspersonen worden als politiegegevens behandeld. Formeel vallen rechtspersonen niet onder de Wpg, maar als een bedrijf bijvoorbeeld afval dumpt, is het uiteindelijke doel een natuurlijk persoon te vervolgen. Ook gegevens over overleden personen vallen niet onder de Wpg of AVG. Echter, er is geen reden om op een andere wijze met deze gegevens om te gaan. Er zijn tenslotte ook nabestaanden.

Gegevens over de medewerkers van de politie vallen onder de AVG. Ook als deze medewerkers de politietaak uitvoeren. De Ondernemingsraad heeft op basis van de Wet op de ondernemingsraden (art. 27.1 onder k en l)

[32] Zie ook de Bedrijfsregels Wpg op Agora.

[33] Zie paragraaf 4.3 voor een volledige beschrijving van de verschillende mogelijkheden.

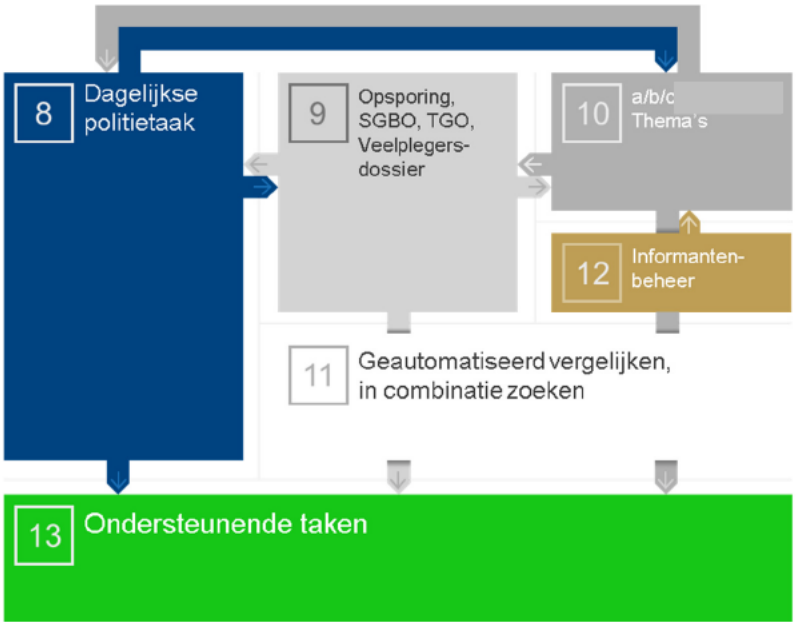
[34] deze uitzonderingsbepaling is beschreven in art. 6 lid 4 AVG (overweging 50). Als de verwerkingsverantwoordelijke een beroep wil doen op deze bepaling, dan moet hij onderbouwen en documenteren waarom hij meent dat hierop een beroep mogelijk is.

instemmingsrecht op een groot deel van deze verwerkingen. Gegevens van klanten, leveranciers en bezoekers vallen tevens onder de AVG.

Als het gaat om bijzondere persoonsgegevens, dan mogen deze slechts worden verwerkt in aanvulling op de verwerking van andere persoonsgegevens en alleen als dit onvermijdelijk is voor het doel van de verwerking. Het gaat hierbij om godsdienst of levensovertuiging, ras, seksuele leven, maar ook genetische en biometrische gegevens. Dit betekent dat ook foto's waar gezichtsherkenning op kan worden toegepast onder deze bepaling vallen. Wat betreft informatiebeveiliging en autorisatie geldt voor de bijzondere persoonsgegevens een strikter regime. Omdat niet iedereen zich bewust is van deze restricties ten aanzien van de verwerking van bijzondere gegevens moet daar bij het ontwerp van informatievoorzieningen rekening mee worden gehouden. Gedacht kan worden aan het gebruik van kwaliteitsregels of een toelichting op het moment dat dit soort gegevens worden geregistreerd.

5.3.2. Dubbele verwerkingsgrondslag

Bij het toekennen van een nieuwe verwerkingsgrondslag aan gegevens die al een verwerkingsgrondslag hebben, blijft de oude ook bestaan. Een gegeven kan dus tegelijkertijd worden verwerkt op basis van zowel artikel 8, 9, 10, 12, 13 als 14. Zo kan een verlopen rijbewijs bijvoorbeeld in een opsporingsonderzoek gebruikt worden en dan zijn dit tegelijkertijd artikel 8 als 9-gegevens. Dit betekent dat het verlopen rijbewijs met het artikel 8-label na vijf jaar niet meer toegankelijk is. Het is dan verwijderd, komt in de bewaartermijn en krijgt dus een artikel 14-label in plaats van 8. Hetzelfde verlopen rijbewijs met het artikel 9-label zit nog in de verwerkingstermijn omdat er nog geen onherroepelijk vonnis is geweest. Of preciezer: het doel van de artikel 9-verwerking is nog niet bereikt en daarom hoeven de gegevens nog niet verwijderd te worden. Onderstaand schema toont de verschillende verwerkingsgrondslagen en hoe veelvoorkomende 'grondslagwisselingen' plaatsvinden.



Figuur 12: de verwerkingsgrondslagen die de Wpg biedt

5.3.3. Gegevensregistratie- en bewerkende diensten[36]

In registratieve systemen dient een mogelijkheid te zijn om de grondslag af te leiden (indien mogelijk) en vast te leggen. Afleiding kan plaatsvinden op basis van het werkproces (gebaseerd op de selectielijst politie) waarvoor de applicatie bedoeld is. Daarnaast kunnen ook de functie van de medewerker en de locatie waar hij zich bevindt gebruikt worden om de verwerkingsgrondslag af te leiden. Bijvoorbeeld een surveillant die op een MEOS-telefoon gegevens invoert op straat: deze combinatie maakt dat dit zeer waarschijnlijk een artikel 8-verwerking is. Dit sluit aan bij het Verbeterplan Wpg en Informatiebeveiliging waarin beschreven is dat oplossingen zoveel mogelijk geautomatiseerd moeten worden[37]. Een gebruiker dient af te kunnen wijken van de door het registratieve systeem afgeleide verwerkingsgrondslag.

[36] 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.
[37] Zie paragraaf 2.2 punt 1: Wpg en informatiebeveiliging worden verankerd in de IV en IV-organisatie.

Deze verwerkingsgrondslagen worden vervolgens aangeleverd door de IV-dienst / informatievoorziening. Als eerste moet bekend zijn of de gegevens onder de AVG of Wpg vallen. Bij AVG dient het doel en de grondslag te worden vastgelegd (zie hoofdstuk 4 voor een limitatieve lijst). Voor Wpg geldt dat het artikel moet worden vastgelegd: 8, 9, 10 lid 1a, 1b, 1c, 12, art. 13 lid 1, 2 of 3. En als het artikel 13 is, dan ook de datum einde verwerkingstermijn. Deze dient van tevoren bepaald te zijn en vastgelegd te zijn in het artikel 13-protocol dat de betreffende verwerking rechtvaardigt. Bijvoorbeeld voor gevarenclassificatie: als een persoon als vuurwapengevaarlijk aangemerkt wordt, dan dient bij de invoer van deze gegevens in BVH ook geregistreerd te worden tot wanneer dit label blijft bestaan. Binnen één artikel 13-protocol kunnen meerdere termijnen bestaan, zoals in het 'HKS-protocol' waarin beschreven is hoelang antecedentgegevens (de oude HKS-data) verwerkt mogen worden.

Deze metagegevens over de verwerkingsgrondslagen reizen mee naar de data-analyseomgeving zodat ook daar op de juiste wijze deze gegevens getoond of juist verwijderd kunnen worden.

5.3.4. Doel van samenwerkingsverband

Bij samenwerkingsverbanden bedoeld als in artikel 20 Wpg moet vooraf worden bepaald wat het doel van de samenwerking is en of alle deelnemers in het kader hiervan persoonsgegevens mogen verwerken. Bijvoorbeeld bij een samenwerking met de Belastingdienst om personen aan te pakken die over onverklaarbaar vermogen beschikken. De samenwerkingsafspraken worden schriftelijk vastgelegd in een convenant of een overeenkomst. Bij deze verstrekkingen dient er eveneens een artikel 20-beslissing te zijn. Er zijn twee mogelijkheden: er kan verstrekt worden aan de partners die deelnemen aan het samenwerkingsverband of er kan verstrekt worden aan het verband zelf indien dat zelfstandig gegevens verwerkt. In dat geval is er sprake van een gemeenschappelijke verwerking. Deze dient aangemeld te worden bij de Autoriteit Persoonsgegevens. Het delen van informatie op basis van de AVG mag alleen plaatsvinden aan een partij die ook iets met de gegevens moet doen ('need to know').

5.3.5. Big data, omgang met open bronnen en social media

Internet biedt vele mogelijkheden om informatie op te zoeken en binnen te halen vanuit open bronnen en social media. [redacted]. Net als bij andere bigdata-activiteiten is niet altijd op voorhand duidelijk wat het doel is van de gegevensverzameling. De meerwaarde van deze gegevens ligt vaak in het secundair gebruik en hoe meer gegevens verzameld worden ten aanzien van een bepaald vraagstuk, hoe beter voor de kwaliteit van de analyse of de te ontwikkelen modellen. Echter, bij het verzamelen van gegevens dient altijd duidelijk te zijn met welk doel de gegevens verzameld zijn. Omdat hierover nog geen jurisprudentie of toelichting op wetgeving bestaat, zijn er geen concrete voorbeelden of adviezen mogelijk. Het principe van doelbinding is bij het verzamelen van gegevens uit open bronnen en social media in ieder geval onverkort van toepassing!

Het WRR-rapport over big data in een veilige samenleving erkent dat het huidige juridisch kader vooral betrekking heeft op de eerste verwerking. Voor een goede toepassing van bigdata-instrumenten en moderne manieren van informatie verwerken, is het nodig dat in toekomstige wetgeving ook aandacht wordt besteed aan de analysewerkzaamheden en gebruikstoepassingen.[38]

Om de rechtmatigheid van de opsporingshandelingen op social media te kunnen beoordelen, is het noodzakelijk dat in het procesdossier wordt verantwoord op welke wijze dit onderzoek heeft plaatsgevonden. Daarbij komt dat in open bronnen en op social media gegevens continu kunnen wijzigen. De politie zowel als het Openbaar Ministerie moeten daarom de onderzoekshandelingen in open bronnen en social media gedetailleerd verantwoorden met duidelijke verwijzing naar het doel van de gegevensverwerking. Gegevens die onrechtmatig verzameld zijn, mogen namelijk überhaupt niet verder worden verwerkt.[39] Soms is het ook niet nodig om zelf gegevens te verzamelen omdat deze reeds elders beschikbaar zijn.[40]

> Een kenteken dat vanwege een openstaande boete of een lopend onderzoek van belang is voor de politie wordt op een referentielijst gezet en levert bij passage van een ANPR-camera een hit op. Deze hits worden door de politie verder verwerkt. Het verder verwerken van no hits is zonder expliciete wettelijke regeling niet toegestaan. Omdat het bewaren van no hits van belang is voor de opsporing is zo'n regeling in de maak. De proportionaliteit van het bewaren van de no hits wordt onderbouwd doordat er een beperkte set gegevens voor een

[38] Zie het rapport *Big Data in een vrije en veilige samenleving*, Wetenschappelijke Raad voor het Regeringsbeleid, april 2016
[39] Artikel 3 lid 2 Wpg.
[40] Zie paragraaf 5.10.1 en bijlage 2 voor een toelichting op het begrip dataminimalisatie.

beperkte tijd wordt bewaard, de toegang tot de bewaarde gegevens beperkt is en er alleen vergeleken wordt op basis van hit/no hit. Verwerken van gegevens uit andere bronnen of internet, moet op dezelfde manier worden bekeken. De set verzamelde gegevens zal daarbij vaak groter zijn dan bij ANPR, en mogelijk bijzondere persoonsgegevens bevatten. Als er datamining toegepast wordt in plaats van hit/no hit vergelijken moet het gebruik daarvan zorgvuldig onderbouwd worden, onder andere door data-minimalisatie, wetenschappelijke validatie van de analyses en verplichte interpretatie en weging van de uitkomsten door een persoon.[41]

5.3.6. Geautomatiseerde individuele besluitvorming

Artikel 7 a lid 1 van de Wpg stelt het volgende: Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij het besluit voorziet in het recht op menselijke tussenkomst van de zijde van de verwerkingsverantwoordelijke en wordt voorzien in specifieke voorlichting aan de betrokkene. Artikel 22 lid 1 van de AVG kent een vergelijkbare bepaling.

Hiermee wordt bedoeld dat er in de totstandkoming van een besluit altijd sprake moet zijn van menselijke tussenkomst. Een voorbeeld waarbij geen sprake is van menselijke tussenkomst, zijn flitspaalboetes. Een flitspaalboete is een besluit dat volledig gebaseerd is op geautomatiseerde verwerking. Deze verwerking werd in het verleden door de politie uitgevoerd.

Een voorbeeld van een verwerking waarbij er (dus op de juiste wijze) sprake is van menselijke tussenkomst, is het risicotaxatie-instrument. Dit model kent betrokkenen op basis van een algoritme een kleur toe en alle ‘rode betrokkenen’ worden bijvoorbeeld naar de wijkagent doorgestuurd. Hij dient vervolgens een toets te doen of hij deze risicowaarde herkent bij de betrokkene en pas dan kunnen er consequenties aan verbonden worden. In dit geval bijvoorbeeld extra toezicht of maatregelen om (verder) crimineel gedrag te voorkomen.

[41] NRC van 24 februari beschrijft dat het gebruik van ANPR door de Belastingdienst door de Hoge Raad wordt verworpen.

5.3.7. Handreikingen

Doelbinding		
	**Activiteit**	**Aandachtspunten**
Beleid	Beleid vormen en strategie bepalen	Beschrijf (in de bedrijfsarchitectuur) welke informatievoorzieningen bestemd zijn voor welk soort gegevensverwerking (AVG en Wpg, inclusief verwerkingsgrondslag).
PDC	Requirements	• Beschrijf welke typen gegevens verwerkt worden (AVG en Wpg, inclusief verwerkingsgrondslag). • Ga uit van afgeleide verwerkingsgrondslag als requirement bij systeemontwikkeling. Geef aan hoe de controle op de juistheid van deze afleiding verloopt. • Neem voor het verwerken van bijzondere persoonsgegevens strikte vereisten op voor autorisatie en informatiebeveiliging.
	Ontwerpen	• De registratieve systemen zouden waar mogelijk de verwerkingsgrondslagen automatisch moeten herleiden. • Neem in het ontwerp mee dat er tegelijk verschillende verwerkingsgrondslagen kunnen zijn. • Bij een besluit dat op geautomatiseerde verwerking is gebaseerd, moet sprake zijn van menselijke tussenkomst. • Gebruik metagegevens voor het bijhouden van de ”levenscyclus”. Biedt de gebruiker de mogelijkheid af te wijken van de afgeleide verwerkingsgrondslag.
Uitvoering / Operatie	Training & sturing	Train medewerkers in het vastleggen van de doelbinding door instructies te geven over welke criteria afgewogen moeten worden om tot een keuze te komen.
	Registratie	• Stel voor elke nieuwe verwerking vast dat er sprake is van een gerechtvaardigd doel.
	Gebruik	• Het doel waarvoor politiegegevens verwerkt worden, moet worden vastgelegd.

5.4. Verantwoording

De politie moet verantwoording kunnen afleggen over zijn taakuitvoering en over de gegevensverwerking die daarbij plaatsvindt.

Ratio: De politie moet over zijn taakuitvoering verantwoording kunnen afleggen. Dit is met name van belang voor gegevensverwerking in strafzaken en de inzet van opsporings- en geweldsbevoegdheden maar het geldt ook voor de bedrijfsvoering in brede zin. De informatievoorziening moet het daarom mogelijk maken dat de politie verantwoording aflegt over handelingen en de totstandkoming van besluiten. Verder zijn het gegevensmanagement en de kwaliteit van de informatievoorziening gebaseerd op een stelsel van werkprocessen met gedefinieerde taken en verantwoordelijkheden. De verantwoording ten aanzien van gegevensverwerking vormt het sluitstuk van de besturing van de informatievoorziening. De verantwoording zorgt tevens dat invulling gegeven kan worden aan de rechten van betrokkenen wiens persoonsgegevens verwerkt worden.

5.4.1. Verantwoordingseisen

Er zijn verschillende politietaken en –processen waarvoor verantwoordingseisen gelden. Het meest nadrukkelijk zijn deze eisen geformuleerd in het Wetboek van Strafvordering waarin de dossiervorming in strafzaken beschreven wordt. Alle opsporingshandelingen en –besluiten moeten daarin worden vastgelegd om in strafzaken de totstandkoming van rechterlijke beslissingen te kunnen verantwoorden.

Ook voor de handhaving en hulpverlening gelden verantwoordingseisen waar de politie gebruik maakt van zijn bevoegdheden om personen staande te houden, te onderzoeken en in noodzakelijke gevallen geweld toe te passen. Bij de registratie van deze gevallen moet worden aangegeven in welke omstandigheden en met welke reden de bevoegdheden zijn toegepast.

Er zijn verder ook verantwoordingseisen die gelden voor de besturing van de organisatie en voor de bedrijfsvoering. Deze verantwoordingseisen vloeien voort uit de verantwoordelijkheden voor het openbaar bestuur en het gebruik van publieke middelen. De handelingen en besluiten zowel als de verwerking van persoonsgegevens moeten op een controleerbare manier worden vastgelegd zodat voor controlerende instanties de zorgvuldigheid en de rechtmatigheid daarvan kan worden aangetoond.

Verantwoording hangt ook samen met de PDCA-cyclus. Daarbij gaat het echter om de besturing van de informatievoorziening als geheel. Bijvoorbeeld het register van verwerkingsactiviteiten kan daarbij behulpzaam zijn.[42] Bij verantwoording gaat het om de individuele handelingen en besluiten.

5.4.2. Vastleggen van handelingen en besluiten: documentatieplicht en logging

Om verantwoording te kunnen afleggen over de gegevensverwerking moeten handelingen en besluiten worden vastgelegd in de vorm van een audittrail. Een audittrail maakt het mogelijk voor een controlerende instantie om vast te stellen wie, wanneer welke handelingen heeft verricht en hoe besluiten tot stand zijn gekomen. In de Wpg werd hiervoor een ondergrens gedefinieerd in de protocolplicht (artikel 32). In de aangepaste Wpg is de protocolplicht vervangen door de documentatieplicht. De volgende zaken moeten in het kader van de documentatieplicht worden vastgelegd:

- Doelen van de onderzoeken, bedoeld in artikel 9 lid 2.
- De verstrekking of doorgifte van politiegegevens op grond van paragraaf 3 Wpg,
- De feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, 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 nadrukkelijk wel onder het principe van verantwoording. Hoe de logging van gebruikershandelingen moet worden ingericht, is beschreven in het beleidskader logging.

Bij het aanleggen van logging van gebruikershandelingen (audittrails) gaat het om de keten van handelingen en beslissingen die tot een bepaalde conclusie of besluit geleid hebben. De werkprocessen waarin deze

[42] Zie Principe PDCA-cyclus voor de uitwerking van het register van verwerkingsactiviteiten.

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.

Wpg artikel 32 a bevat de nieuwe loggingsverplichting. Hierin staat dat ten minste de volgende verwerkingen gelogd moeten worden: verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of 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 vastgesteld.[43] Dus met de datum, het tijdstip, de identiteit van de bevrager en die van ontvanger(s) moet de reden achterhaald kunnen worden. Dit betekent dat met behulp van deze logging-gegevens een opsporingsambtenaar na bijvoorbeeld een klacht moet kunnen uitleggen waarom hij een bevraging gedaan heeft. Het is dus niet noodzakelijk om bij elke bevraging vast te leggen waarom deze gedaan wordt.

> In MEOS of BVI-IB is het niet noodzakelijk om bij elke bevraging vast te leggen waarom een bevraging wordt uitgevoerd. Ook is het niet noodzakelijk dat het systeem de reden van bevraging afleidt en registreert.

De richtlijn gegevensbescherming opsporing en vervolging bevat geen bewaartermijn voor de logging, gelet op het doel van de gegevensverwerking is de verordening gegevensbescherming op die gegevens van toepassing.

De vastlegging van verantwoordingsinformatie is op zich ook weer een verwerking onder de AVG, waar tevens de Wet op de Ondernemingsraden op van toepassing is. De gegevens kunnen immers ook 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 27.1 lid L 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.

5.4.3. Verantwoordingsproces

Met de registratie van handelingen en besluiten leveren individuele functionarissen verantwoordingsinformatie over de uitvoering van hun werkzaamheden. Deze informatie kan gebruikt worden in de lijnorganisatie in de cyclus van besturing en controle van werkzaamheden. De registratie is daarnaast nadrukkelijk bedoeld voor auditdoeleinden om achteraf aan controlerende instanties bewijs te kunnen leveren over de zorgvuldigheid en rechtmatigheid van de taakuitvoering. Hierbij kan onder andere gebruik worden gemaakt van het nog te ontwikkelen register van verwerkingsactiviteiten.[44]

> Ieder over wie persoonsgegevens verwerkt worden, heeft het recht op inzage (rechten van betrokkenen). Het feit dat een burger dit recht uit kan oefenen, betekent dat er functionele eisen over opgenomen moeten worden in het ontwerp. En dat deze ook getoetst moeten worden. Op eenvoudige wijze moeten alle persoonsgegevens te ontsluiten zijn binnen de politieorganisatie. Het kunnen uitoefenen van de rechten van betrokkenen, geeft op indirecte wijze invulling aan het afleggen van verantwoording.

> Gerrit-Jan Zwenne, hoogleraar recht en de informatiemaatschappij bij de afdeling eLaw van de Universiteit Leiden, schat dat 80 procent van de AVG ongeveer hetzelfde is als de Wbp. Het verschil zit vooral in accountability. “Daar ligt in de AVG veel meer nadruk op. Je moet kunnen aantonen dat je voldoet aan wat in de Verordening staat. Om dat te kunnen, moet je precies weten welke gegevensverzamelingen je waar in je organisatie hebt en voor welke doelen je de gegevens inzet. Op dit moment hebben te veel overheden daar een te onbepaald beeld van.”[45]

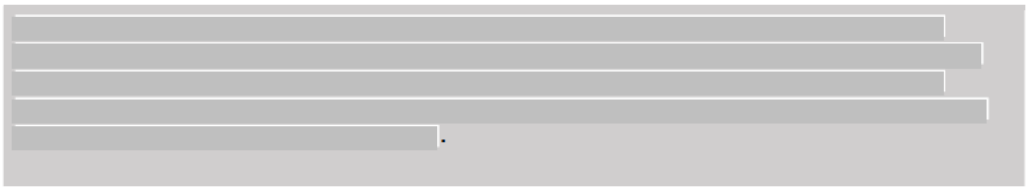
---

[43] Zie memorie van toelichting artikel 32 a en overweging 57 van de Richtlijn opsporing en vervolging.
[44] Zie Principe PDCA-cyclus.
[45] iBestuur magazine “Grip op Privacy”, nummer 21, januari 2017

5.4.4. Actieve informatie aan betrokkene

De nieuwe 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 verantwoordelijke 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.

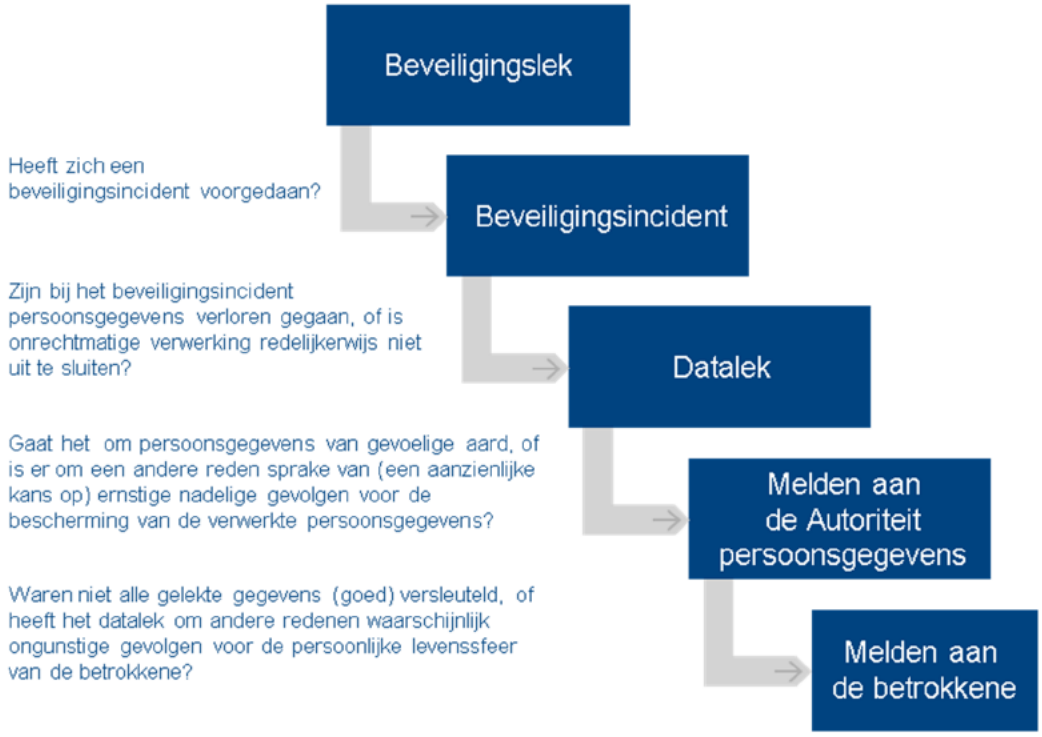
Specifieke informatie kan ook via de website beschikbaar worden gesteld; dit gebeurt bijvoorbeeld in reactie op een aangifte of een ander contact met de betrokkene. Het gaat daarbij onder andere om de verwerkingsgrondslag, de bewaartermijn, de categorieën van de ontvangers van de politiegegevens en het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



5.4.5. Datalekken

Met de komst van de nieuwe Wpg is ook het melden van een datalek bij politiegegevens verplicht gesteld (dit was al verplicht voor verwerkingen onder de Wbp). Dit betekent dat een datalek moeten worden gemeld bij de Autoriteit Persoonsgegevens. Dit geldt zowel voor verwerkingen onder de AVG als de Wpg. Een datalek is bijvoorbeeld een verloren USB stick, gestolen laptop, een succesvolle hack, brand in het datacenter of een malware infectie.

Niet ieder informatiebeveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het incident persoonsgegevens verloren zijn gegaan, of als er onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uit te sluiten is. Een factor die hierbij ook een rol speelt is de aard van de gelekte persoonsgegevens. De consequentie van mogelijk onrechtmatige verwerking is ernstiger als er bijzondere persoonsgegevens (medisch, financieel) zijn gelekt. In sommige gevallen moet een datalek ook aan betrokkene worden gemeld. Onderstaand schema toont hoe het beoordelingsproces plaatsvindt.



Figuur 13: processtroomschema voor het melden van een datalek

Er is politiebeleid dat beschrijft wat er gedaan moet worden bij een datalek. Dit dient mee te worden genomen in proces- en systeemontwerp zodat –wanneer daar sprake van is- een datalek daadwerkelijk gemeld kan worden.

Tevens bestaat er een meldplicht cybersecurity. De Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) stelt een meldplicht in voor ernstige ICT-inbreuken en geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving. Het meldpunt wordt belegd bij het nationaal cyber security center (NCSC) van het Ministerie van Justitie. Het NCSC de meldingen gebruiken om organisaties te informeren over cyberdreigingen en biedt waar nodig ondersteuning. Het Besluit meldplicht cybersecurity beschrijft voor welke instanties de meldplicht gaat gelden. Op 11 juli 2017 heeft de Eerste Kamer het wetsvoorstel en het besluit aangenomen. Daarmee kan de wet op afzienbare termijn in werking treden.

Voor wat betreft de overheid heeft de meldplicht betrekking op aanbieders van digitale overheidsdiensten. Om welke aanbieders en diensten dit gaat is afhankelijk van een beoordeling die wordt uitgevoerd door het Nationaal Beraad Digitale Overheid. Op basis van de uitkomst daarvan zal het Besluit meldplicht cybersecurity bij de eerstvolgende gelegenheid worden aangevuld. Voor de politie geldt intern de procedure dat ernstige ICT-inbreuken altijd dienen te worden gemeld bij de CISO. De CISO heeft ook nu al de mogelijkheid om hierover contact op te nemen met het NCSC.

5.4.6. Handreikingen

Verantwoording		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	• Maak een inventarisatie van wettelijke en wenselijke verantwoordingseisen per proces.
	N.a.v. issues	• Organiseer audits op verantwoordingsinformatie
PDC	Ontwerpen	• Specificeer registratiefuncties voor verantwoordingsinformatie bij voorkeur als generieke voorziening. • Beoordeel of actieve informatie aan betrokkene nodig is.
	Ontwikkelen	• Opnemen van registratiefuncties in processen en systemen • Opname van het politiebeleid betreffende een datalek in de gebruikers- en/of beheerhandleiding of bijbehorend protocol bij beheer van het systeem
	Ondersteuning	• Beheren van verantwoordingsinformatie • De audittrail moet beveiligd zijn tegen manipulatie.
	Incident	• Rapportage leveren op basis van audittrail
Uitvoering / Operatie	Ontwikkelen	• Ontwikkel werkinstructies voor het protocolleren
	Registratie	• De handelingen en besluiten moeten worden vastgelegd in de vorm van een audittrail. • Meld een datalek bij de AP.
	Incidenten/vragen	• Lever verantwoordingsinformatie

5.5. Autorisatie

Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van noodzaak voor de uitvoering van de hen opgedragen werkzaamheden.

Ratio: Door de toegang en het gebruik van informatie en systemen te koppelen aan de werkzaamheden waarvoor deze nodig zijn, hoeven autorisaties niet meer op de persoon of het systeem te worden toegekend en wordt het mogelijk om de rechten vanuit de registratie van functies en werkzaamheden te organiseren en te beheren. Dit levert een reductie in beheerslast op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren. Het principe geldt zowel voor interne gebruikers als 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.

5.5.1. Autorisatiebeleid

Op 21 april 2016 is een nieuw autorisatiebeleid vastgesteld.[46] Dit autorisatiebeleid geeft een actuele invulling aan de visie op een landelijk autorisatiemodel dat in juli 2011 door de toenmalige Raad van Korpschefs is vastgesteld.[47] De kernpunten uit de visie zijn:

- 'politiemedewerkers delen gegevens tenzij de wet dat niet toestaat' en delen 'by the book' waarbij een evenwicht wordt gekozen tussen informatie delen en het voorkomen van afbreukrisico's;
- professionaliteit van en vertrouwen in medewerkers staan centraal;
- de combinatie LFNP-functie, werkzaamheden en organisatorische plaats geven op rollen gebaseerde autorisaties, waarbij de autorisatieprofielen voor dezelfde 'combinatie' landelijk gelijk zijn;
- toegang tot informatie is in principe landelijk, de fysieke werklocatie is daarbij niet relevant;
- ten aanzien van autorisaties wordt een eenduidig, landelijk, eenvoudig en transparant proces gehanteerd;
- daar waar dat mogelijk is worden toe te kennen autorisaties geautomatiseerd opgeleverd;
- de toegang tot systemen wordt verleend op basis van gebleken 'noodzakelijkheid'.

De inhoud van het autorisatiebeleid wordt mogelijk gemaakt door het autorisatieprincipe. In het autorisatie*beleid* wordt de balans gedefinieerd tussen het risico enerzijds dat gebruikers onbevoegd toegang krijgen tot vertrouwelijke informatie en het risico anderzijds dat bij de uitvoering van taken belangrijke aanwezige informatie wordt gemist. Het autorisatie*principe* zorgt ervoor dat de organisatie zijn autorisatiebeleid kan veranderen zonder dat de processen en systemen voor autorisatie hoeven te worden aangepast.

Voor effectief politiewerk is het cruciaal dat politiegegevens zo veel mogelijk gedeeld worden. De wetgever verplicht daartoe in artikel 15 lid 1 Wpg. Dit wordt wel 'delen tenzij' of free flow of information genoemd. Dit 'delen tenzij' geldt voor de politie, de KMar en de BOD'en. Uit het wetsvoorstel Wpg blijkt dat ook de boa's door middel van een besluit onder de Wpg gaan werken, dus het Wpg-domein wordt nog verder uitgebreid. Het is nog niet duidelijk hoe dit praktisch ingevuld wordt, maar het betekent onder andere dat boa's, als zij bezig zijn met opsporingswerk, toegang kunnen krijgen tot politiegegevens die door de politie verwerkt worden.

De term 'delen tenzij' is een afgeleide van artikel 15 Wpg: delen binnen het Wpg-domein is verplicht. Het begrip houdt in dat elke politiemedewerker gebruik moet maken van de politiesystemen en onnodig afschermen van gegevens is niet toegestaan. Een belangrijke afweging in de Wpg is de vraag of een politiemedewerker gegevens nodig heeft voor zijn taak. Alleen dan mogen gegevens worden geraadpleegd. Het is niet toegestaan om voor privédoeleinden gegevens te raadplegen. En als iets niet tot de eigen werkzaamheden behoort, mogen deze gegevens niet worden verwerkt. Bijvoorbeeld als er 's nachts collega's werkzaam zijn geweest in de straat van een medewerker, mag hij niet vanuit zijn privébelang bekijken welke registraties daarover zijn aangemaakt.

5.5.2. Rolgebaseerde toegang en attribuutgebaseerde toegang

Om ervoor te zorgen dat gebruikers worden geautoriseerd op basis van de noodzaak voor hun werkzaamheden moet de informatievoorziening faciliteiten leveren voor de ondersteuning van autorisatiebeheer volgens de volgende ontwerprichtlijnen (by design). Het autorisatiebeheer moet eenvoudig en efficiënt worden ingericht en zo veel mogelijk

[46] Autorisatiebeleid 2016 – 2020, 21 april 2016
[47] 'Autoriseren: zo doen we dat hier!', visie op een landelijk autorisatiemodel voor de Nederlandse Politie, juli 2011

gebruik maken van geautomatiseerde procedures. We moeten dus zoveel mogelijk voorkomen dat autorisaties op ad hoc basis aan individuen worden toegekend. Noodzakelijke ad hoc autorisaties worden centraal vastgelegd en zijn van tijdelijke aard. In het verleden werden autorisaties nog veelal per applicatie georganiseerd waardoor het totaaloverzicht op uitstaande autorisaties ontbrak. Voor nieuwe applicaties geldt daarom de richtlijn om gebruik te maken van een generieke voorziening die autorisaties toekent op basis van de rollen van gebruikers en de kenmerken van de verwerkte gegevens. We noemen dit rolgebaseerde- en attribuutgebaseerde toegang.

In het verleden was het beheer van autorisaties versnipperd, regionaal verschillend, chaotisch, het vond handmatig plaats zonder dat er sprake was van toezicht en sturing. Om deze problemen op te lossen en een systeem van autorisaties te realiseren dat zou gaan voldoen aan de vereisten van zorgvuldigheid en evenredigheid en de mogelijkheid daar een actueel overzicht van te genereren is eraan gewerkt om te zorgen dat:

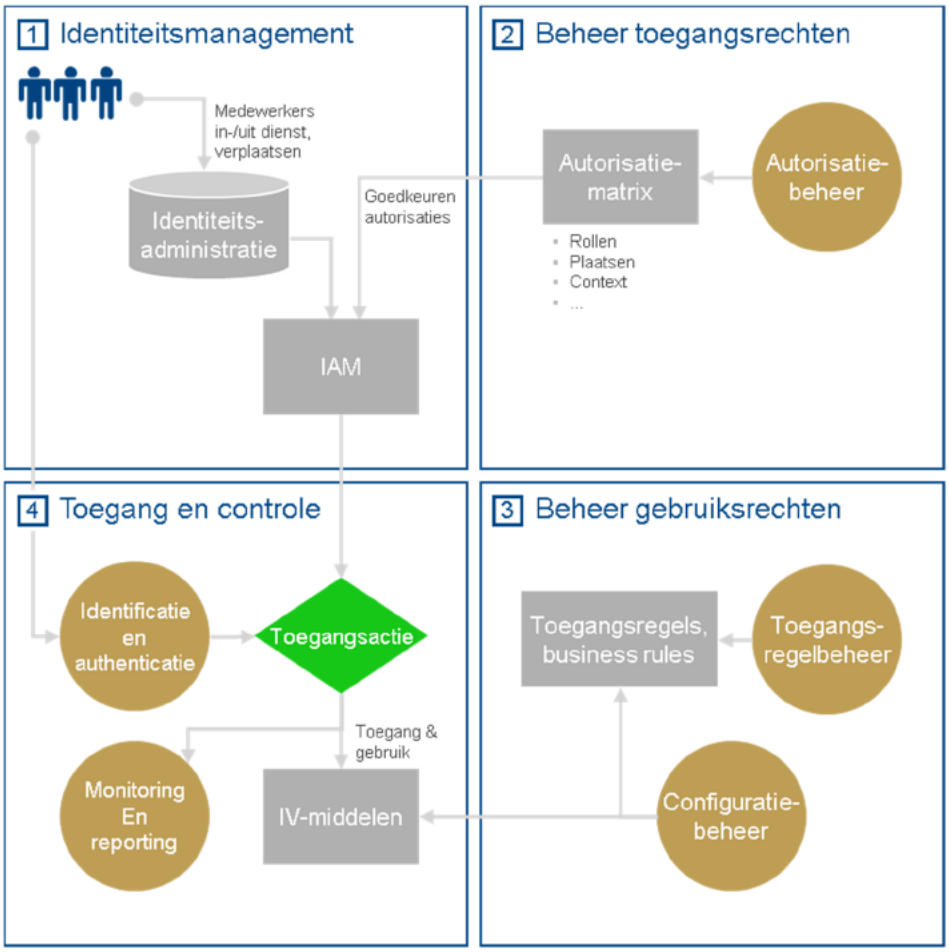
- de registratie van medewerkers en dienstverbanden uniform, eenduidig en actueel is. Autorisaties komen bij voorkeur geautomatiseerd via het personeelssysteem tot stand. Zodra daar een functie, rol of taak wordt toegekend, gewijzigd of ingetrokken zal dit automatisch tot een autorisatiewijziging leiden. Dit vereist een goede, tijdige registratie van medewerkers, dienstverbanden, opleidingen et cetera. 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 een landelijk autorisatiebeheersysteem is waarin autorisaties centraal zijn vastgelegd en decentraal kunnen worden beheerd. Dit autorisatiebeheersysteem krijgt geautomatiseerd signalen van het HRM-systeem (zoals uitdiensttreding en schorsing).

5.5.3. Autorisatiebeheer

Autorisatiebeheer is niet één werkproces maar een combinatie van vier groepen werkstromen die tezamen waarborgen leveren voor zorgvuldige en rechtmatige toegang tot gegevens:

1. Beheer van identiteiten van subjecten (Identiteitsmanagement, IdM);
2. Beheer van de toegangsrechten / regels voor toegang (Access Management, AM);
3. Beheer van toe te wijzen gebruiksrechten op IV-middelen (behorend bij functioneel applicatiebeheer);
4. Gebruik en monitoring van toegangsrechten.

Alleen als alle vier werkstromen zijn ingericht, is er een sluitend autorisatiestelsel. De werkstromen ten aanzien van autorisatiebeheer worden organisatorisch gescheiden uitgevoerd, bij voorkeur geautomatiseerd afgedwongen en bij verschillende medewerkers belegd.



Figuur 14: verschillende werkstromen voor goed autorisatiebeheer

5.5.4. Autorisatie op gegevens

In het verleden zijn autorisaties aan gebruikers toegekend per applicatie. Dat wil zeggen dat de toegang tot gegevens afhankelijk is gemaakt van de toegang tot de applicaties waarin deze gegevens verwerkt worden. Met de ontwikkeling van kernregisters en gegevensdiensten komt het echter steeds vaker voor dat dezelfde gegevens via meerdere applicaties geraadpleegd en verwerkt kunnen worden. Het is daarbij van belang dat gebruikers die niet geautoriseerd zijn voor het raadplegen en verwerken van gegevens via de ene applicatie ook niet onbedoeld via een andere applicatie bij dezelfde gegevens kunnen. Dat kan worden gewaarborgd door de autorisaties voor verschillende applicaties te baseren op dezelfde autorisatieregels. Het zou echter beter zijn om de autorisaties niet per applicatie te verstrekken en te beheren maar om dat op het niveau van de gegevens te regelen. Bij de ontwikkeling van kernregisters en gegevensdiensten moet ook de autorisatie op gegevens worden ingericht. Vervolgens moeten ook de applicaties die daar gebruik van maken worden aangepast om met deze autorisaties te kunnen werken.

Als een gebruiker niet geautoriseerd is voor het verwerken van gegevens via de ene applicatie, kan hij alleen geautoriseerd worden voor deze gegevens via een andere applicatie als daar bewust voor gekozen wordt.

Identificatie en authenticatie van een gebruiker wordt verzorgd door Deze functie identificeert de gebruiker, controleert of deze toegang heeft, en met welke autorisatierol. Bij het starten van een applicatie wordt vanuit contact opgenomen met geeft vervolgens de rol van de geautoriseerde gebruiker door aan . Daarnaast kan 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 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 worden toegepast. Als een medewerker iets in [redacted] niet kan zien, kan hij of zij dat ook niet via [redacted] zien. De regels gaan afwijken als het gaat om informatie die niet als zodanig in een bronsysteem is vastgelegd, bijvoorbeeld als het ontstaat na integratie van gegevens uit verschillende bronsystemen.

De toegangsregels worden per [redacted] vooraf vastgesteld. [redacted] voorziet in het beheer van de regels die de rechten binnen autorisatierollen verder differentiëren.

5.5.5. Autorisatiematrix

De autorisatiematrix met de actueel geldende autorisatie wordt actief beheerd en wordt daarom ook regelmatig bijgewerkt en aangepast. De hier opgenomen autorisatiematrix is een concept van 27 januari 2017. Voor de actuele autorisaties verwijzen we naar de publicaties van de portefeuillehouder Intelligence op intranet.

	Gegevenskenmerk	Medewerker Dagelijkse politietaak	Informatie-Coördinator Dagelijkse politietaak	Medewerker rechtsorde	Informatie-Coördinator Rechtsorde Algemeen	Informatie-Coördinator Rechtsorde + Algemeen	Medewerker [redacted]	Medewerker	Medewerker	[redacted]	Chef [redacted]	Chef [redacted]	Chef	[redacted]
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		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		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	

Figuur 15: concept-autorisatiematrix voor BVI

Toelichting:

Ja	Vrij doorzoeken: dit is het doorzoeken van grote hoeveelheden politiegegevens met vrije zoeksleutels. Als de gebruiker besloten gegevens mag zien, dan ziet de gebruiker ook dat de gegevens besloten zijn. Wie vrij mag doorzoeken, mag ook hit/no hit zoeken.
Hit/no-hit	Hit/no hit zoeken is het zoeken binnen gegevens op een beperkt aantal vaste kenmerken (bijvoorbeeld op kenteken, kenosleutel of postcode), waarbij uitsluitend wordt aangegeven of een gegeven voorkomt of niet
For Intell. Only	De gebruiker ziet dat de gegevens 'For Intelligence Only' zijn.
BL	De gebruiker ziet het registratienummer, een melding dat de registratie besloten is, plus de naam en de OE van de eigenaar.
BM	De gebruiker ziet het registratienummer en een melding dat de registratie besloten is.
BV&F	De gebruiker ziet wat hij op basis van de niet-V&F-beslotenheid mag zien, maar kan het veld verklaring en de formulieren niet inzien, op basis van de van toepassing zijde maatschappelijke klassen.
Signaal	De gebruiker ziet geen gegevens, maar de betreffende bevoegd functionaris krijgt een signaal dat iemand naar de betreffende gegevens heeft gezocht. [redacted] reageert voor de gebruiker alsof de gegevens waarnaar gezocht wordt niet bestaan.

5.5.6. Handreikingen

Autorisatie		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	• Richt autorisatie in op basis van het autorisatiebeleid en de informatiebehoefte bij de uitvoering van politiewerk
	N.a.v. issues	• Beoordeel rapportages en organiseer audits op autorisatiebeheer

PDC	Ontwerpen	• Richt autorisatiebeheer in volgens het autorisatiestelsel van de volgende vier werkstromen
		  o Beheer van identiteiten van subjecten (IdM)
		  o Beheer van toegangsrechten/regels voor toegang (AM)
		  o Beheer van toe te wijzen gebruiksrechten op IV-middelen
		  o Gebruik en monitoring van toegangsrechten.
		• Neem voor het verwerken van bijzondere persoonsgegevens strikte vereisten op voor autoriseren. Denk hierbij aan training of een beperkte groep personen.

	Ontwikkelen	• Laat systemen aansluiten op de generieke voorzieningen voor identificatie, authenticatie en autorisatie • Geef gebruikers toegang op gegevensniveau in plaats van op applicatieniveau
	Ondersteuning	• Zorg voor functioneel rechtenbeheer in applicaties in aanvulling op de generieke autorisatievoorziening. • Zorg ervoor dat de gebruikers ten alle tijden geïnstrueerd zijn mbt de voor hen geldende autorisatieregels
	Incident	• Lever rapportages over het gebruik van autorisaties
Uitvoering / Operatie	Registratie	• Autorisatie moeten worden toegekend op basis van rollen van gebruikers en de kenmerken van de verwerkte gegevens.
	Controleren	• Voer ten minste jaarlijks controles uit op toegangs- en gebruiksrechten van medewerkers
	Incidenten/vragen	• Lever ondersteuning bij het beheren van autorisaties

5.6. Metagegevens

Gegevens worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de juistheid en de rechtmatigheid van de gegevensverwerking te waarborgen.

Ratio: De gegevensverwerking door de politie gaat uit van eenmalige vastlegging en meervoudig gebruik, waarbij gegevens en toepassingen worden gescheiden. Om de juistheid en de rechtmatigheid van het gebruik te kunnen waarborgen worden metagegevens vastgelegd over bijvoorbeeld de context, inhoud, structuur, vorm en gedrag evenals het beheer en gebruik. Deze metagegevens bepalen de wijze waarop deze gegevens (mogen) worden verwerkt. Ze maken het mogelijk om daar waar nodig en toegestaan:

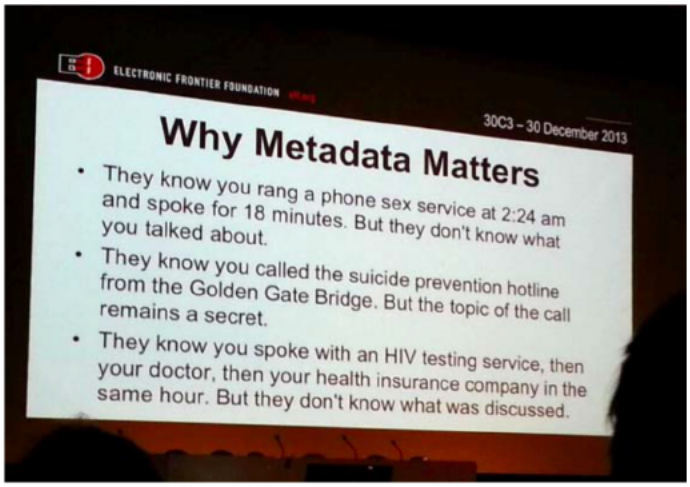
- gegevens binnen wet- en regelgeving te hergebruiken en te vernietigen;
- gegevens uit te wisselen tussen organisaties;

- de toegangsrechten te bepalen en de vertrouwelijkheid van informatie te garanderen;
- kwaliteit van gegevens te waarborgen in termen van authenticiteit, betrouwbaarheid, volledigheid, integriteit, bruikbaarheid en duurzaamheid;
- waarborgen te bieden voor vindbaarheid, identificatie en toegankelijkheid;
- beheer en reproductie mogelijk te maken;
- het doel en de context van de inwinning te herleiden.

5.6.1. Het belang van metagegevens

In juni 2013 onthulde Edward Snowden, een medewerker die voor de Amerikaanse geheime dienst (NSA) werkte, dat er grootschalige spionageactiviteiten plaatsvonden en wereldwijd communicatie in de gaten werd gehouden. In een poging om het publiek gerust te stellen reageerde de staf van president Obama: "It's just Metadata", "The information acquired does not include the content of any communications"[48]. Zonder stelling te nemen in deze casus kunnen we stellen dat deze reactie alles behalve geruststellend is. Iets waar organisaties die burgerrechten en privacy in de digitale wereld verdedigen, dan ook gretig op inspelen.

De afbeelding: "Why Metadata Matters" van Electronic Frontier Foundation, geeft de (latente) angst of argwaan weer, die (Amerikaanse) burgers voelen. Het laat anderzijds ook zien hoe waardevol en rijk metagegevens zijn. Metagegevens zijn van belang om context te geven aan gegevens en kunnen zo van gegevens informatie maken. Aan de andere kant zijn metagegevens essentieel om juist zorgvuldig om te gaan met persoonsgegevens.



Figuur 16: het belang van metagegevens

5.6.2. Typen metagegevens

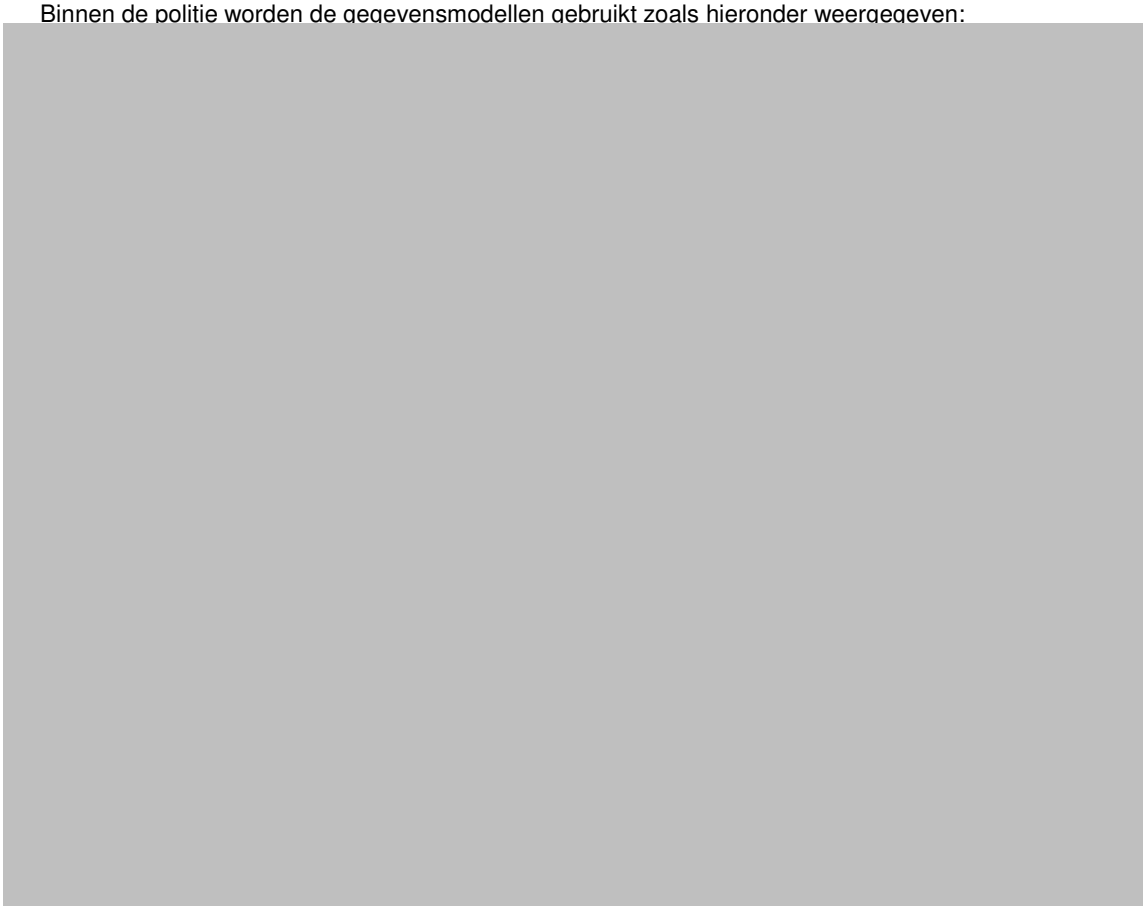
Metagegevens zijn gegevens die nodig zijn voor de ontsluiting en het beheer van andere gegevens. Metagegevens beschrijven verschillende facetten van een informatie-object om de bruikbaarheid te vergroten gedurende de levenscyclus. Metagegevens zijn nodig om van gegevens betekenisvolle informatie te maken. Het zijn in feite gegevens over gegevens. Er zijn beschrijvende metagegevens, zoals gegevensmodellen, die gebruikt worden voor onder meer de juiste vastlegging en interpretatie van informatieobjecten voordat verwerking in bedrijfsprocessen plaatsvindt. De gegevensmodellen zoals gebruikt binnen de politie zijn weergegeven in paragraaf 5.6.3 en nader toegelicht in de bijlage. Er zijn ook 'administratieve' metagegevens die ontstaan bij de uitvoering van bedrijfsprocessen en die gebruikt worden voor onder meer beheer, terugvindbaarheid en archivering[49]. Denk hierbij aan kenmerken zoals de herkomst, de wijze van verkrijging (artikel 3 lid 5 Wpg) en de verwerkingsgrondslag. Deze kenmerken komen in paragraaf 5.6.5 aan bod.

Voorbeeld metagegevens : Geboortedatum
Definitie: de datum van de bevalling waarop hij/zij geboren is.
Bron: In Nederland wordt deze datum geregistreerd in de basisregistratie personen, de BRP.
Lengte: 8 karakters
Formaat: mmddjjjj
Dit staat dus los van de inhoud van het veld "Geboortedatum"

[48] Metadata en metagegevens zijn synoniemen; binnen de politie heeft metagegevens de voorkeur.
[49] De administratieve metagegevens worden in de beschrijvende metagegevens al gedefinieerd (zoals de gegevens zelf ook gedefinieerd worden), maar inhoud ervan ontstaat pas bij de uitvoering van het proces.

5.6.3. Gegevensmodellen

Binnen de politie worden de gegevensmodellen gebruikt zoals hieronder weergegeven:



Figuur 17 Samenhang gegevensmodellen

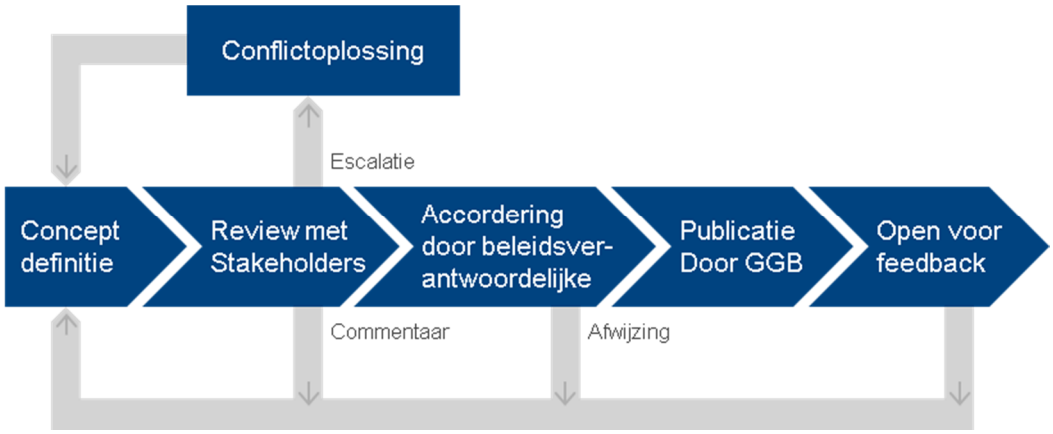
Bedrijfsbegrippen worden gedefinieerd zodat de betekenis van de woorden die gebruikt worden bij de uitvoering van het werk, eenduidig beschreven is. Voorbeelden van begrippen zijn ‘verdachte’ en ‘slachtoffer’. De bedrijfsbegrippen worden gebruikt in bedrijfsregels. Dit zijn ondubbelzinnige afspraken over de wijze waarop het werk uitgevoerd moet worden. Voor zowel bedrijfsbegrippen als bedrijfsregels is een leidraad opgesteld[50]. 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). Tevens geeft het aan wat de belangrijkste relaties tussen de objecten zijn. Ten slotte zijn er bedrijfsregels van kracht op de objecten. Voor artikel 1 tot en met 10 van de Wpg zijn er bedrijfsregels beschikbaar die vastgesteld zijn door de Gegevensautoriteit.

Bespreken

[50] Zie Leidraad opstellen begripsdefinities en Leidraad opstellen bedrijfsregels op Agora.

5.6.4. Metagegevensproces

Het opstellen en onderhouden van definities wordt procesmatig ondersteund vanuit GGB[24] (proces en tooling moet nog nader uitgewerkt worden). Op hoofdlijnen omvat dit proces de stappen zoals weergegeven in Figuur 18.



Figuur 18 Proces opstellen en onderhouden van definities

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. Een voorbeeld van die implementatie is de entiteit 'persoon' die een generalisatie is voor bedrijfsobjecten 'verdachte' en 'slachtoffer'. De conceptuele modellen PGM en het dossiermodel zijn geïmplementeerd in fysieke databasemodellen en specificaties voor berichtuitwisseling. Het dossiermodel is bijvoorbeeld geïmplementeerd in . Een ander voorbeeld is de toepassing van het PGM voor de specificatie van gegevensuitwisseling in ketenverband (via het Canonical Data Model, afgekort CDM) en ook voor het . Deze gegevensmodellen worden nader toegelicht in bijlage 4.

5.6.5. Metadateringkenmerken

Door eisen vanuit wet- en regelgeving en ten behoeve van verantwoording wordt het steeds belangrijker om kenmerken aan gegevensobjecten toe te voegen. Specifiek ook door het aandeel semi-gestructureerde en ongestructureerde gegevens, waarvan verwacht wordt dat dit een vlucht zal nemen. Denk aan het beeldmateriaal dat geüpload wordt door burgers en vastgelegd door agenten (MEOS), de verwerking van multimedia-opnames van verhoren, telecom-data, gegevens van internet (websites, social media, twitter) of ANPR-data. Bovendien is de politie een organisatie waar veel gewerkt wordt met zachte gegevens, bijvoorbeeld een signaal of vermoeden, en niet altijd met harde gegevens, feitelijke waarneming. De behandeling van deze gegevens verschilt van elkaar. Om de juiste behandeling voor te staan dienen kenmerken te worden toegekend.

Ontwerpkader Toepassingsprofiel Metagegevens Politie

Het Ontwerpkader Toepassingsprofiel Metagegevens Politie dat vastgesteld is in het MTCIO van 24 november 2016, beschrijft hoe het gegevensmodel Toepassingsprofiel Metagegevens Politie (TMP) opgezet moet worden. De afdeling GGB stelt dit gegevensmodel TMP op. Het TMP zal gebaseerd worden op het Toepassingsprofiel Metagegevens Rijk (TMR)[51]. Het uiteindelijke doel is dat de geformuleerde beleidsuitgangspunten en constructie-eisen opgenomen worden in de referentiearchitectuur van de politie. Het geformuleerde ontwerpkader is in lijn met de Informatiearchitectuur en het Bestemmingsplan IV. Zo lang het gegevensmodel nog niet beschikbaar is, is het ontwerpkader het document dat de contouren bepaalt. In het ontwerpkader wordt onder andere beschreven wat de functies zijn van metagegevens en waarom ze noodzakelijk zijn (zie ook de opsomming onder de ratio aan het begin van deze paragraaf 5.6).

Specifieke gegevensmodelleringeisen vanuit privacywetgeving

Voor zover mogelijk moet duidelijk onderscheid gemaakt worden tussen politiegegevens betreffende verschillende categorieën van betrokkenen. Dit betekent dat in de gegevensverwerking duidelijk moet blijken of een persoon verdachte, slachtoffer of getuige is of dat het om een derde gaat die contact heeft met een verdachte of veroordeelde.

[51] Zolang het TMP nog niet beschikbaar is kan teruggevallen worden op het TMR.

Dit is een nieuwe eis die terug te vinden is in artikel 6b Wpg. In de huidige systemen wordt hier voor een groot deel reeds in voorzien. Zowel in ontwerp van processen als systemen dient dit metagegeven vastgelegd en gewijzigd te kunnen worden.

Een andere nieuwe eis (artikel 4 lid 3) luidt dat politiegegevens die op feiten zijn gebaseerd onderscheiden moeten worden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd (voor zover dit mogelijk is). Net als bij verschillende categorieën van betrokkenen geldt ook hier dat er in het huidige werkproces voor een groot deel reeds in wordt voorzien. Bijvoorbeeld bij de vastlegging van politiegegevens in mutaties en processen-verbaal. Indien mogelijk moet in metagegevens terug te vinden zijn of een gegeven een feit betreft of een persoonlijk oordeel.

Naast deze twee wettelijke vereisten, dienen ook de volgende metagegevens te worden gehanteerd:

- wettelijke verwerkingsgrondslag (zie Principe doelbinding),
- de herkomst van de gegevens (voor artikel 9 en 10-gegevens is dit verplicht)[52],
- de wijze van verkrijging (voor artikel 9 en 10-gegevens is dit verplicht),
- logginggegevens, zoals tijd en datum en wie is ingelogd, noodzakelijk voor onder andere de nieuwe loggingsplicht (artikel 32a Wpg).

Het is van belang dat deze metagegevens op het juiste niveau worden vastgelegd. Voor de verwerkingsgrondslag geldt bijvoorbeeld dat de combinatie van naam en adres van een persoon met een strafbaar feit maakt dat het strafbare feit een persoonsgegeven is. Alleen het strafbare feit is dat niet (en heeft dan ook geen verwerkingsgrondslag). In combinatie met een locatie kan het strafbare feit weer wel een persoonsgegeven zijn.

Welke metagegevens?
Naast de specifieke gegevensmodelleringeisen vanuit privacywetgeving moeten de kenmerken onder andere de volgende onderdelen kunnen bevatten:

- identificatiekenmerken,
- kenmerken die noodzakelijk zijn voor het verwerken van gegevens binnen het politieproces en/of binnen de keten, voorbeelden zijn transactie/event, datum, status, vorm,
- kenmerken die noodzakelijk zijn voor het verwerken van gegevens in de keten,

Verder geldt:

- De systemen die gebruikt worden voor de gegevensverwerking (de toepassingsdiensten) moeten voorzieningen bieden om de vereiste gegevenskenmerken zo veel mogelijk geautomatiseerd af te leiden uit het object of de transactie.
- Bij aanpassingen in informatiesystemen en nieuwe functionaliteit dient in het ontwerp gebruik te worden gemaakt van metagegevens.
- Eerder toegekende metagegevens dienen te worden gebruikt, in plaats van bijvoorbeeld opnieuw af te leiden.

[52] Zie Wpg Bedrijfsregels op Agora voor bedrijfsregels over onder andere de herkomst en de wijze van verkrijgen.

5.6.6. Handreikingen

Metagegevens		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	Stel definities op voor te verwerken gegevens en gebruik hierbij de leidraad.

	Sturing	• Richt een proces op voor het opstellen en onderhouden van definities
		  ○ Zijn definities volledig
		  ○ Worden definities toegepast
		  ○ Zijn de definities gepubliceerd
		  ○ Zijn de definities geëvalueerd
		  ○ Wordt er gereageerd op advies en wijzigingsverzoeken

PDC	Requirements opstellen	• Neem toepassingsprofiel metagegevens mee in requirements. Zolang het TMP nog niet beschikbaar is kan teruggevallen worden op het TMR. • Maak gebruik van de Wpg bedrijfsregels voor zover beschikbaar. • Neem de specifieke gegevensmodelleringeisen vanuit privacywetgeving mee. • Een informatiesysteem, nieuw en na aanpassing, moet gebruik maken van metagegevens
	Ontwerpen	• Pas de relevante gegevensmodellen aan, waarbij ook de relaties tussen de modellen wordt beheerd. • Zorg dat IV-toepassingen de vereiste metagegevens zoveel mogelijk geautomatiseerd vastleggen. • Maak gebruik van de standaard invoer- en verwerkingsmethoden (waarbij metagegevens geautomatiseerd worden vastgelegd).
Uitvoering / Operatie	Registratie	• Zorg dat de geldende definities bekend zijn.

5.7. Kwaliteitszorg

De informatievoorziening waarborgt de kwaliteit van de gegevensverwerking.

Ratio: Van gegevens die door de politie verwerkt worden moeten de kwaliteitseisen (bijvoorbeeld juistheid, actualiteit en nauwkeurigheid) bekend zijn. Waarborgen voor gegevenskwaliteit zijn onmisbaar om de juiste werking van systemen en de integriteit van de informatievoorziening als geheel te waarborgen. Geprogrammeerde, automatische controles bieden efficiënte en effectieve waarborgen zodat de integriteit van de informatievoorziening gehandhaafd kan worden[53]. Daarnaast zijn aanvullende handmatige controles vereist. Controles hebben betrekking op verschillende kwaliteitsaspecten zoals juistheid, volledigheid en tijdigheid. Bij ketensamenwerking moeten afspraken gemaakt worden over waarborgen voor gegevenskwaliteit. Wanneer de kwaliteitseisen van gegevens bekend zijn en hierover afspraken met alle betrokkenen partijen zijn gemaakt, kan de politie deze kwaliteit bewaken en zorgen dat deze in orde is en in orde blijft.

[53] Bij data-integriteit gaat het om de mate waarin relaties tussen de data-elementen te allen tijde stand houden. De geldigheid van gegevens die naar elkaar verwijzen. Het gaat dus niet om de persoonlijke integriteit.

Figuur 19 Waarom is de kwaliteit van gegevens cruciaal voor goede uitvoering van de politietaak?

5.7.1. Uitgangspunten en activiteiten

Voor de uitwerking van het principe Kwaliteitszorg hanteren we onderstaande uitgangspunten. Deze zijn nog niet (allemaal) uitgewerkt in bestaand politiebeleid of in richtlijnen maar ze bieden context om datgene wat bij dit principe beschreven wordt, goed te interpreteren:

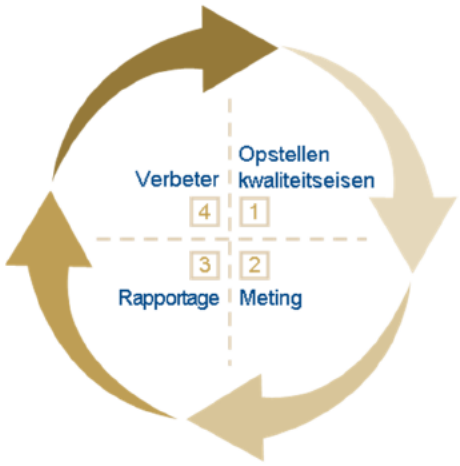
- Gegevens worden (afhankelijk van afnemerseisen) zoveel mogelijk in één keer goed (First Time Right/FTR) vastgelegd; dit in plaats van controles en gegevensherstel achteraf.
- Gegevenskwaliteitseisen van gebruikers (processen of ketenpartners) worden opgesteld en beheerd. De eisen worden gebruikt in IV-voortbrengingsprocessen om FTR mogelijk te maken.
- Gegevenskwaliteitsmanagement is een doorlopend proces en wordt uitgevoerd zo dicht mogelijk bij de processen die de gegevens verwerken. Terugkoppeling van de afnemers helpt kwaliteit te verbeteren.
- Medewerkers krijgen opleiding en coaching op het gebied van gegevenskwaliteit en kwaliteitszorg.
- De operatien en projecten worden niet alleen op tijd en kosten gestuurd maar ook op kwaliteit.
- Beleidsverantwoordelijkheid en uitvoeringsverantwoordelijkheid zijn belegd (zie principe Verantwoordelijkheden belegd).
- De verantwoordelijken worden ondersteund op het gebied van datamanagement en gegevenskwaliteitsanalyse.
- Gegevenskwaliteit van kritische gegevenselementen wordt actief gemonitord.
- Issues met de kwaliteit van gegevens worden gemeld en centraal beheerd.

Opmerking: voor de verantwoordelijkheden ten aanzien van taken genoemd in bovenstaande uitgangspunten zie principe Verantwoordelijkheden belegd. Bij de zorg voor kwaliteit van gegevens kunnen de volgende continue doorlopende activiteiten worden onderscheiden. Nog niet voor al deze activiteiten zijn kaders of richtlijnen beschikbaar. Ook middelen, zoals tools en procedures zijn nog niet overal beschikbaar en uitgewerkt. Voor zover mogelijk worden de activiteiten hieronder toegelicht.

Gegevenskwaliteitsmonitoring en -rapportage	• Opstellen kwaliteitseisen • Opstellen en beheren gegevenskwaliteit(kennis)regels • Gegevenskwaliteitsmeting en -rapportage
Gegevenskwaliteit-issuemanagement	• Terugmelden incident (en behandelen) • Melden issue • Gegevenskwaliteitanalyse • Gegevenskwaliteitherstel
Verbetering gegevenskwaliteit bewustzijn en competenties	• Vergroting bewustzijn van waarde van gegevens en belang van kwaliteit • Gegevenskwaliteit: opleiding en coaching • Vergroting begrip hoe gegevenskwaliteit bereikt kan worden door continue en integrale verbetering (PDCA) van mensen, processen en systemen (First Time Right)

5.7.2. Gegevenskwaliteitsmonitoring en -rapportage

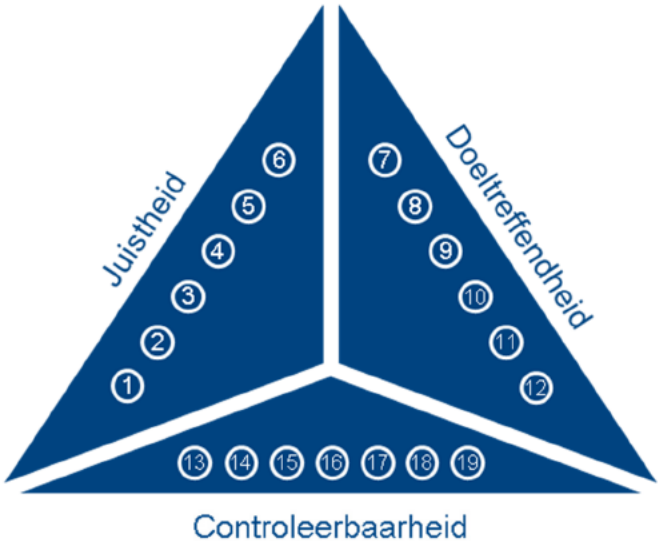
Het proces voor monitoring en rapportage is hiernaast weergegeven. Dit proces start al bij requirements-, ontwerp- en teststappen van een IV project. Door in de testfase al te meten op de geformuleerde eisen is de kwaliteit van gegevens in een vroegtijdig stadium inzichtelijk. Dit monitoringproces kan ook gestart worden n.a.v. geconstateerde problemen of n.a.v. een risicoanalyse.



Figuur 20 Proces gegevenskwaliteits-monitoring

Opstellen kwaliteitseisen

Voorafgaand aan de gegevensverwerking worden de kwaliteitseisen vastgesteld door de beleidsverantwoordelijke voor de gegevens. Voor het formuleren van de kwaliteitseisen kan de politie gebruik maken van onderstaand raamwerk van kwaliteitskenmerken[54]. Gegevenskwaliteit wordt in dit raamwerk ingedeeld in de groepen juistheid, doeltreffendheid en controleerbaarheid.



Figuur 21 Raamwerk kwaliteitskenmerken

Voorbeelden kwaliteitseisen proces-verbaal

- In ieder pv dient zich een ID-staat van verdachte te bevinden waarop de gegevens staan die in SKDB zijn vastgelegd (referentiële integriteit)

[54] 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.

- Bij verdachte met alleen een buitenlands paspoort dient in het pv een V-(RIS)-nummer vermeld te staan (volledigheid)

De kenmerken van het raamwerk staan min of meer op gespannen voet met elkaar. Bestaan er veel maatregelen op doeltreffendheid, dan zal de Juistheid afnemen. Tenzij daar ook maatregelen op getroffen worden, maar dan daalt de Controleerbaarheid. Gegevens kunnen bijvoorbeeld niet volledig 12.actueel en 10.beschikbaar zijn en tegelijkertijd 3. correct (want controle kost tijd) en 14.exclusief (want dan is het niet meer openbaar). Kortom: Kwaliteit is een optimum – geen maximum - van kenmerken waar in bepaalde mate aan is voldaan. Het document[55] dat het raamwerk van kwaliteitskenmerken Strafrechtsketen in detail beschrijft, bevat per kenmerk een omschrijving en ook de mogelijke maatregelen waarmee betrokkenen (specifiek ontwikkelaars en gebruikers) de kwaliteitsrisico's kunnen verminderen.

Waargenomen waarheid
Bij een aantal kenmerken van juistheid (correctheid, volledigheid, nauwkeurigheid, et cetera) moet niet uit het oog worden verloren dat deze kenmerken in het kader van waarheidsvinding een tweede betekenis hebben. Is bijvoorbeeld een valse aangifte die netjes is opgetekend in de betekenis van dit raamwerk correct (want goed opgetekend) of niet (want moedwillig van valse informatie voorzien)? Is een gedeeltelijk signalement 'volledig' te noemen? Voor de eenvoud: De kwaliteitskenmerken in dit kader gaan over de kwaliteit van gegevens zoals de politie die waarneemt. Een gedeeltelijk signalement is dus 'volledig' als het volledig is overgenomen van de getuigenverklaring. Dat daarna een onderzoek start dat de werkelijke toedracht onderzoekt, doet aan de kwaliteit van de gegevensvastlegging niets af.

Opstellen en beheren gegevenskwaliteit(kennis)regels
Het vooronderzoek TrueBlue[56] beschrijft op welke wijze gegevenskwaliteitscontroles uitgevoerd dienen te worden. Het gaat daarbij om functionaliteit voor:
- het signaleren op basis van kennisregels: geautomatiseerd en handmatig;
- het bewaken van geconstateerde fouten: door opslag van controles, persoonlijk benadering naar gebruikers en ruimte geven om af te wijken;
- het monitoren door middel van dashboards en rapportages.

Naar aanleiding van het vooronderzoek wordt geadviseerd om als 'eenvoudig' bestempelde kennisregels te implementeren in het bronsysteem. Het is bijvoorbeeld verplicht om bij het invoeren van een adres een huisnummer toe te voegen, net als een modus operandi bij een incident. Volg de aanwijzingen uit het vooronderzoek op voor wat betreft het opstellen en beheren van kennisregels voor gegevenskwaliteit.

Gegevenskwaliteitsmeting en rapportage
Het vooronderzoek TrueBlue[56] beschrijft eveneens op welke wijze meting en rapportages plaats dienen te vinden. Naast monitoring op individueel recordniveau en terugkoppeling aan collega's in de uitvoering dient er ook monitoring plaats te vinden door de beleidsverantwoordelijke: in hoeverre wordt aan kwaliteitseisen voldaan om invulling te geven aan de doelstellingen van de portefeuille?

Rechten van betrokkene en kwaliteit van gegevens
Kwaliteitsmaatregelen dragen bij aan een goed proces. Een extra argument om kwaliteit hoog in het vaandel te hebben, zijn de rechten van betrokkenen die zowel in de AVG als de Wpg voorkomen. De betrokkene heeft het recht op inzage, het recht op correctie en het recht op verwijdering. Onder de AVG ook het recht op beperking en het recht op overdraagbaarheid. Verklaringen van agenten, bijvoorbeeld uit BVH-registraties zijn dus inzichtelijk voor de burger. Er is een mogelijkheid tot weigeren van geregistreerde informatie, maar dat moet per gegeven worden gemotiveerd. Er dienen dus maatregelen te worden getroffen zodat er professioneel gemuteerd wordt en dat stigmatiserende opmerkingen vermeden worden. De volgende regels kunnen daarbij helpen:
- ontdoe een mutatie van eigen emoties;
- muteer kort, zakelijk en objectief. Onthoud je van stigmatiserende en beledigende opmerkingen;
- vermeld de bron en hoe de informatie is verkregen;
- als er 'slechts' een vermoeden is, dan moet dit duidelijk kenbaar worden gemaakt dat het om een vermoeden gaat.[57]

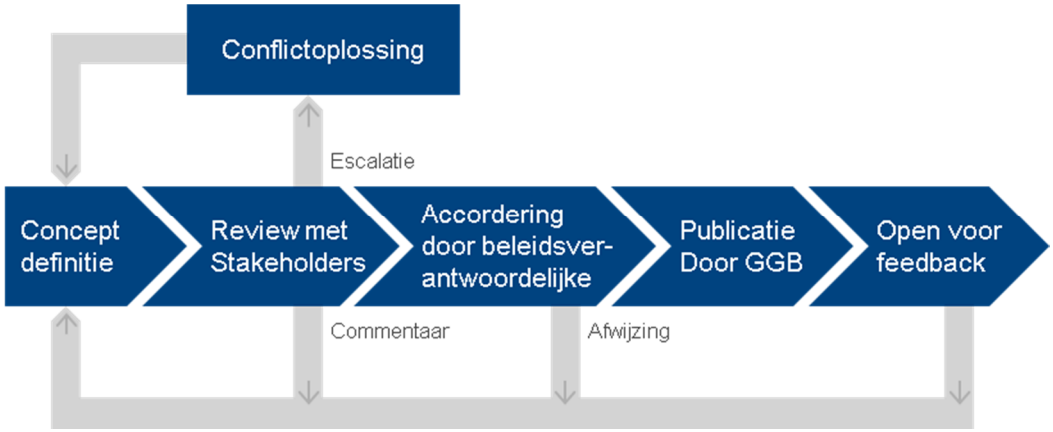
Door transparant te zijn - elke burger het recht heeft op inzage-, kan de politie laten zien dat aan bovenstaande regels gehoor wordt gegeven. Neem deze ten minste mee in opleiding en training.

---

[55] Raamwerk en stappenplan gegevenskwaliteit Strafrechtsketen, Ministerie van V&J, 11 november 2015
[56] Vooronderzoek uitfaseren TrueBlue en realisatie vervangende functionaliteit, AVP,11 April 2016
Advies hieruit: TrueBlue functionaliteit "Signaleren" wordt verplaatst naar BVH en hiermee wordt direct bij gegevensinvoer gecontroleerd op fouten. Trueblue wordt tot nader orde gehandhaafd voor nieuwe kennisregels en kennisregels die nog niet of lastig te realiseren zijn in BVH. (dit advies is overgenomen)
[57] In de nieuwe Wpg, artikel 4 lid 3, wordt expliciet vereist dat feiten en persoonlijke oordelen onderscheiden moeten worden.

5.7.3. Gegevenskwaliteit-issuemanagement

Structurele verbetering van gegevenskwaliteit wordt bereikt door procesverbetering en de omgang met gegevens hierin. Het gaat hierbij zowel om bedrijfsprocessen als om de IV-voortbrengingsprocessen (ontwikkeling en beheer). In de figuur hieronder zijn de stappen in de gegevenskwaliteit-issuemanagementprocessen weergegeven. Het proces van het melden van een issue tot het afhandelen daarvan is een specifieke invulling van het generieke verbeterproces (zie Principe PDCA-cyclus).



Figuur 22 Gegevenskwaliteit-issuemanagementprocessen

Terugmelden incident (en behandelen)

Incidenten met de kwaliteit van gegevens (kwaliteitsissues) worden zo veel mogelijk gemeld door de gebruikers. Het begrip 'terugmelden' komt uit de regelgeving omtrent het gebruik van basisregistraties. Afnemers van basisregistraties zijn wettelijk verplicht, indien zij 'gerede twijfel' hebben bij een gegeven afkomstig uit een basisregistratie, dit te melden bij de bronhouder van de betreffende registratie. De politie heeft dus niet alleen een wettelijke afnameplicht van gegevens uit basisregistraties, maar ook een wettelijke terugmeldplicht. Terugmelden is een belangrijk middel om de kwaliteit van deze basisregistraties te verbeteren. Tevens is het een middel om de kwaliteit van de overige gegevens binnen het politiedomein te verhogen en daarmee draagt terugmelden bij aan de veiligheid, ook aan die van de politiemedewerker. Het begrip terugmelden wordt binnen de politie ook breder geïnterpreteerd. Immers, de politie maakt naast Basisregistraties ook gebruik van veel andere externe registraties, waarin eveneens fouten kunnen worden geconstateerd die 'teruggemeld' moeten worden. Een praktijkvoorbeeld hiervan is de terugmeldvoorziening die gerealiseerd is in de vreemdelingenketen.

Ook in de gegevens die de politie zelf beheert en registreert kunnen fouten aanwezig zijn, die aangepast moeten worden. In de Visie op Terugmelden is uitgewerkt hoe dit proces plaats dient te vinden en welke processtappen daarin onderscheiden worden[58]. Middelen voor terugmelden moeten nog grotendeels ontwikkeld worden. Zowel in de 'legacyomgeving' als in de 'vernieuwing'. In de legacyomgeving zal een aantal processtappen handmatig moeten worden uitgevoerd, hetgeen de efficiency van het proces vermindert. In de 'vernieuwing' is het mogelijk om veel meer te sturen op het inbedden van terugmelden in de primaire processen.

Melden issue

Incidenten kunnen opgelost worden door correctie van de brongegevens. Als incidenten zich herhalen en daarmee structureel van aard zijn, dan is een verbeterproces nodig. Hiervoor is het nodig om naast de registratie van incidenten ook een administratie van issues te onderhouden met daarbij onder andere de omschrijving van het issue, aangemeld door, aangemeld datum, proces en omgeving oorzaak, processen en omgevingen die impact ondervinden, urgentie, frequentie, status. Een dergelijke administratie bestaat nog niet. Bij (her)ontwerp dient hiermee rekening te worden gehouden. Issues kunnen ook actief geïnventariseerd worden waarbij gebruik gemaakt wordt van een aanpak analoog aan die bij risicoanalyse (zie Principe Informatiebeveiliging).

Gegevenskwaliteitsanalyse

Gegevenskwaliteitsanalyse bestaat uit de analyse van de beschikbaarheid en kwaliteit van de metagegevens, de kwaliteit van de gegevens zelf en de impact en oorzaak van een gegevenskwaliteit-issue. Op basis van de analyse kan een herstelplan opgesteld worden, ervan uitgaande dat hier een noodzaak en/of een business case voor bestaat. Zowel bij de analyse als bij het herstelplan dient integraal aandacht besteed te worden aan de factoren mens, proces

[58] Visie op terugmelden, GGB, 13 oktober 2015

en systeem. Beleid, werkwijze en middelen voor de analye van gegevenskwaliteit moeten binnen de politie nog verder uitgewerkt worden.

Gegevenskwaliteitherstel
Bij herstel van gegevens kan onderscheid gemaakt worden naar dweilen (gegevensherstel/correctie) en het dichtdraaien van de kraan (structureel). Gegevenskwaliteitherstel is binnen de politie georganiseerd voor BVH vanuit de controles in Trueblue. Herstel in andere omgevingen is meer incidenteel en reactief van aard. Denk bij structureel herstel aan het doorvoeren van verbeteringen in applicaties en procedures. Verbetering van de omgang met gegevens kan ook bereikt worden door opleiding. Uitvoering van structureel herstel is onderdeel van het generieke verbeterproces (zie Principe PDCA-cyclus).

5.7.4. Verbetering gegevenskwaliteit bewustzijn en competenties

De meest essentiële factor voor duurzaam succesvol functioneren van de gegevenskwaliteit verbeteractiviteiten is de mens. De laatste activiteit richt zich daarom op de vergroting van het bewustzijn van waarde van gegevens en het belang van kwaliteit, en op opleiding en coaching op het gebied van gegevenskwaliteit. Deze activiteit vergroot het begrip hoe gegevenskwaliteit bereikt kan worden door continue en integrale verbetering (PDCA). Houd bij opleiding en coaching rekening met de uitgangspunten uit dit hoofdstuk, maar ook met bijvoorbeeld artikel 4 lid 3 Wpg waarin vereist wordt dat feiten en persoonlijke oordelen van elkaar gescheiden moeten worden, en met het onderscheid tussen bijzondere persoonsgegevens en overige persoonsgegevens. De partijen die actief zijn in de gegevenskolom (Gegevensautoriteit, GGB en KvI) zijn trekker voor deze activiteit.

5.7.5. Handreikingen

Kwaliteitszorg		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	• Stel gegevenskwaliteitseisen op bij proces
	Issuebehandeling	• Starten van analyse en structureel herstel
PDC		
	Opstellen requirements	• Zorg voor eisen rondom het terugmelden aan een basisregistratie. • Het opstellen van kwaliteitseisen moet gedaan worden volgens het raamwerk ingedeeld in juistheid, doeltreffendheid en controleerbaarheid.
	Ontwerpen	• Specificeer gegevenskwaliteits- (kennis)regels. Het gaat daarbij om: o Het signaleren op basis van kennisregels (geautomatiseerd en handmatig) o Het bewaken van geconstateerde fouten o Het monitoren doormiddel van dashboards en rapportages
	Ontwikkelen	• Voorzie in geautomatiseerde kwaliteitscontroles bij registratie (t.b.v. in één keer goed) en verdere verwerking van gegevens (bijvoorbeeld postcode niet goed ingevuld) . • Lever geautomatiseerde controle op kwaliteit (hoe vaak is een pv volledig ingevuld?)
	Testen	• Test de gegevenskwaliteit zoveel mogelijk met realistische gegevens[59]; gebruik makend van opgestelde gegevenskwaliteitseisen.
	Change uitwerken	• Pas gegevenskwaliteitseisen en controles aan waar nodig.
	Incident oplossen	• Analyseer structurele problemen door middel van gegevenskwaliteitsanalyse.
Uitvoering / Operatie	Training & sturing	• Creëer bewustzijn voor de kwaliteit van registraties in ketenprocessen.
	Registratie gegevens	• Registreer volledig volgens definities en toelichting • Meld onduidelijkheid bij registratie. • Definieer kwaliteitscontroles en laat ze implementeren.
	Incident vaststellen bij gebruik gegevens	• Meld twijfel over de kwaliteit van een politiegegeven afkomstig uit een basisregistratie terug aan de basisregistratie.

[59] Houd bij gebruik van productiegegevens voor testen rekening met de hiervoor geldende kaders

5.8. Bewaren en vernietigen

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

Ratio: De politie mag alleen gegevens verwerken indien en voor zolang daar een wettelijke grondslag voor bestaat. Als die grondslag komt te vervallen moeten de gegevens worden verwijderd of vernietigd. Ook voor gegevens waarvan blijkt dat ze onjuist zijn geldt dat ze moeten worden vernietigd of gecorrigeerd. De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden. Voor de termijn waarbinnen de gegevens bewaard moeten worden, moet de informatievoorziening waarborgen treffen voor duurzame beschikbaarheid en toegankelijkheid. Deze waarborgen worden uitgewerkt in het Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO). De 'spelregels' voor gegevensbeheer zijn vastgelegd in de Beheerregeling Documentaire Informatie Politie 2017 en de termijnen voor bewaren en vernietigen zijn verzameld in de Generieke Selectielijst voor de Nationale Politie (concept).

5.8.1. Selectielijst

In de nieuwe Generieke Selectielijst voor de Nationale Politie (concept, v 0.12, voortaan 'selectielijst')[60] worden de kaders voor het bewaren en vernietigen van politiegegevens en bedrijfsvoeringsgegevens 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 van andere (persoons)gegevens op basis van hun waarde voor het bedrijfsvoerings-, verantwoordings- en cultuur-historisch belang.

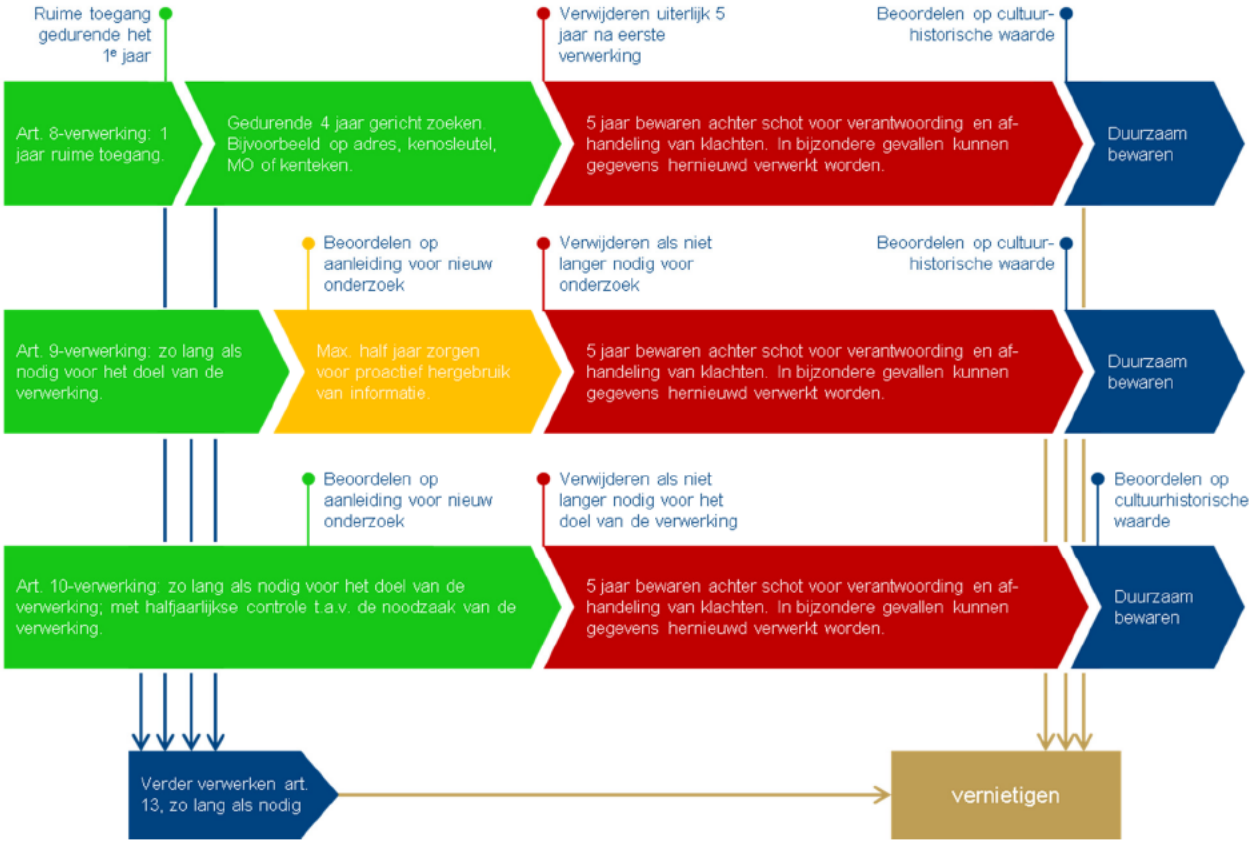
Uit de titel en de toelichting blijkt dat de selectielijst betrekking heeft op documentaire informatie. Hoewel deze benaming misschien anders doet vermoeden gaat het hierbij om alle informatie, ongeacht de vorm, die door de politie bij de taakuitvoering wordt opgemaakt of ontvangen. Dit omvat naast documenten ook gestructureerde gegevens en naast tekstinformatie ook multimedia-informatie.

In dit uitvoeringskader worden de voorschriften en termijnen voor bewaren en vernietigen niet gespecificeerd, daarvoor verwijzen we naar de selectielijst. We geven hier alleen een toelichting op de systematiek en het gebruik van de selectielijst. De selectielijst is opgesteld aan de hand van de taak- en bedrijfsprocessen van de politie[61]. De processen zijn daarin ingedeeld naar een drietal 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 content 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 historisch onderzoek.

[60] Ten tijde van de publicatie van versie 2.0 van dit uitvoeringskader is de selectielijst door het Nationaal Archief goedgekeurd maar nog niet officieel vastgesteld bij besluit in de Staatscourant.
[61] Deze zijn ontleend aan het Referentiemodel Bedrijfsprocessen Politie RBP 2008/2012 en de inrichting van het capaciteitsmanagementsysteem BVCM.

5.8.2. Wpg-processtappen en termijnen

De termijnen voor het verwerken, bewaren en vernietigen van politiegegevens zijn afhankelijk van de verwerkingsgrondslag. Het volgende schema geeft de processtappen en termijnen voor de verschillende verwerkingsgrondslagen volgens de Wpg.



Figuur 23: Wpg-termijnen voor de verschillende verwerkingsgrondslagen

De Wpg maakt onderscheid tussen 'verwijderen' en 'vernietigen'. Onder verwijderen wordt verstaan dat de gegevens 'achter een schot' worden geplaatst en niet meer voor operationele doeleinden beschikbaar zijn. Alleen met toestemming van het bevoegd gezag mag in specifieke gevallen een hernieuwde verwerking van de gegevens plaats hebben. Vernietigen betekent dat een gegeven daadwerkelijk niet meer bestaat. Ook back-ups, hard-copyarchieven et cetera dienen dan dus vernietigd te zijn. Gegevens die verwijderd zijn maar nog niet vernietigd, kunnen ontsloten worden door een poortwachter. Deze persoon kan zowel gegevens beschikbaar stellen voor hernieuwde verwerkingen als voor audits, toezicht, inzageverzoeken en klachtafhandeling.[62]

> Voor cold cases geldt dat als een zaak niet is opgelost, deze gegevens als artikel 9-gegevens beschikbaar blijven (in de verwerkingstermijn) zolang het feit niet is verjaard. Het doel is tenslotte nog niet bereikt. Als er nieuwe aanknopingspunten zijn, kan er dus gewoon verder worden gewerkt aan de zaak. Vaak echter blijkt voor het oplossen van cold cases dat gegevens die destijds niet relevant leken voor de zaak en binnen artikel 8 verwerkt werden, nu toch relevant zijn. Ook voor deze gegevens gelden echter de reguliere verwijder- en vernietigingstermijn.

Wat betreft artikel 8-gegevens geldt dat een gebruiker toegang moet hebben tot alle artikel 8-gegevens tot vijf jaar terug, tenzij evident is dat dit voor het werk niet nodig is en er volstaan kan worden met één jaar terugkijken, of zelfs nog korter, afhankelijk van het doel van de verwerking.[63] 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

---

[62] Zie ook de werkinstructie poortwachter voor een beschrijving van de werkzaamheden:
[63] Zie ook de Agora-afspraken die voorschrijven dat gegevens op de tijdslijn van een basisteam na twee weken geautomatiseerd verwijderd worden.

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. Omdat de Memorie van Toelichting zegt dat 'ook een zeer ruime kring personen' geautoriseerd mag worden voor deze periode van vijf jaar, hanteren we het standpunt dat vijf jaar vergelijken de norm is. De informatievoorziening is gewijzigd sinds in 2006 de contouren voor de Wpg helder werden; er is nu meer mogelijk en het past ook meer bij de wijze waarop de politieprocessen zijn georganiseerd om elke geautoriseerde zelfstandig tot vijf jaar terug artikel 8-gegevens met elkaar te laten vergelijken.

Op het juiste moment verwijderen en vernietigen betekent onder andere dat er afloopberichten verwerkt moeten worden. Dit zijn berichten over de afloop van een strafrechtelijke procedure bij het OM of na een dagvaarding bij de rechter. Een afloopbericht is bijvoorbeeld een strafbeschikking, sepot of een HALT-afdoening. Als het OM besluit tot een sepot omdat een persoon onterecht als verdachte is aangemerkt, moeten de gegevens in onder andere worden aangepast. Hij mag niet meer als verdachte worden aangemerkt. De Wpg schrijft tenslotte voor dat gegevens altijd juist, actueel en volledig moeten zijn. En zodra voor alle verdachten van een strafbaar feit een afloopbericht is ontvangen, moeten artikel 8- en 9-gegevens achter een schot worden geplaatst.

Ten aanzien van verwerkingen onder de AVG moet de verantwoordelijke voor de verwerking zelf aangeven wat de rechtvaardiging is om de gegevens uit die verwerking een bepaalde termijn te bewaren. Ook dit moet weer een gerechtvaardigd doel dienen. Over het algemeen is een termijn van twee jaar acceptabel, tenzij wetgeving een langere termijn verplicht of de verantwoordelijke kan motiveren waarom de gegevens langer moeten worden bewaard.

5.8.3. Voorzieningen voor bewaren en vernietigen

De basissystemen van de politie moeten voorzieningen bevatten voor beheersprocessen en het bewaken van termijnen voor bewaren en vernietigen. Deze beheerhandelingen moeten op één plaats in de informatievoorziening worden uitgevoerd. Als dezelfde gegevens ook in andere systemen gebruikt worden, dan volgen die andere systemen het gegevensbeheer van het bronsysteem. Op deze manier zorgen we er voor dat er maar één versie van de waarheid bestaat zoals het principe Eenmalige vastlegging vereist. Er zijn ook specifieke kaders die richting geven aan het verwijderen en vernietigen van gegevens in de registratieve politiesystemen.[64] BV maakt als raadpleegsysteem van de politie een grote hoeveelheid politiegegevens toegankelijk. Het beleid dat in BVI ten aanzien van bewaren en vernietigen wordt gehanteerd is dat BVI hierin altijd de bron volgt. De implicatie hiervan is dat de Wpg-verwerkingsgrondslag en daarbij bijbehorende termijnen van de bron ook in BVI wordt gerespecteerd.

BVH-registraties worden conform artikel 8* Wpg na vijf jaar achter een schot geplaatst. Hierdoor zijn deze registraties in BVH niet meer toegankelijk voor verwerking. Binnen BVH vindt dit plaats door deze registraties te geven.

[64] 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

Voor de termijnen waarop gegevens duurzaam bewaard moeten worden, moet de informatievoorziening waarborgen bieden voor duurzame beschikbaarheid en toegankelijkheid. De daarbij geldende kwaliteitseisen zijn te vinden in de DUTO standaard[65]. De basissystemen van de politie zijn geen archiefsystemen en bevatten doorgaans ook geen voorzieningen voor duurzaam bewaren. De gegevens die voor langere tijd bewaard moeten worden, moeten dus worden overgebracht naar een archiefsysteem dat daarvoor is toegerust. Voor bedrijfsvoeringsgegevens kan de politie hiervoor gebruik maken van zijn content managementsysteem (Documentum).

5.8.4. Handreikingen

Bewaren en vernietigen		
	**Activiteit**	**Aandachtspunten**
Beleid	Beleid vormen en strategie bepalen	• Ontwikkel en beheer de selectielijst. • Ontwikkel beleid om richting te geven aan verwijder- en vernietigingsmechanismen.
PDC	Ontwerpen	• De basissystemen moeten voorzieningen bevatten voor beheersprocessen en het bewaken van termijnen voor bewaren en vernietigen. • Als dezelfde gegevens ook in andere systemen gebruikt worden, volg het gegevensbeheer van het bronsysteem.
	Ontwikkelen	• Voorzieningen moet waarborgen bieden voor duurzame beschikbaarheid en toegankelijkheid (DUTO-standaard)
	Ondersteuning	• Advies bij selectiebeslissingen m.b.t. bewaren (B) en/of vernietigen (V).
	Incident	• Leg selectiebeslissingen voor aan de eigenaren van processen/dossiers.
Uitvoering / Operatie	Registratie	• Maak dossiers compleet met waardering en selectie ten behoeve van bewaren en vernietigen.
	Incidenten/vragen	• Maak tijdig selectiebeslissingen ten aanzien van bewaren en vernietigen van dossiers.
	Gebruik	• Zorg dat er poortwachters zijn aangewezen om gegevens te ontsluiten

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

5.9. Informatiebeveiliging

De informatievoorziening wordt beveiligd met een adequaat stelsel van maatregelen op basis van risicobeheersing.

Ratio: De bedoeling van informatiebeveiliging op basis van risicobeheersing is dat mogelijke schadelijke gevolgen door bedreigingen van de informatievoorziening bewust worden afgewogen tegen de kosten en de belemmeringen van beveiligingsmaatregelen. Op voorhand hoeft niet ieder risico te worden afgedekt. Wanneer de lasten van de maatregelen om een risico te beperken hoger zijn dan de mogelijke schade, dan kan ook besloten worden tot lichtere maatregelen en om resterende risico's te accepteren. In ieder geval houdt de politie rekening met de verantwoordelijkheid en de verplichting om de gegevens van burgers te beschermen.

5.9.1. Informatiebeveiligingsarchitectuur

De aanpak van informatiebeveiliging op basis van risicobeheersing wordt beschreven in de Informatiebeveiligingsarchitectuur.[66] Deze manier van informatiebeveiliging is gebaseerd op het uitgangspunt dat 100% veiligheid niet bestaat en dat bewust moet worden afgewogen op welke wijze de risico's afgedekt kunnen worden of teruggebracht tot een aanvaardbaar niveau. Hiermee neemt de politie afstand van de oude baseline-benadering waarbij een standaard set met maatregelen voor informatiebeveiliging wordt gehanteerd die over de gehele informatievoorziening uniform wordt toegepast. Door de nieuwe benadering wordt een direct verband gelegd tussen informatiebeveiligingsmaatregelen en de risico's die hiermee worden afgedekt. Dat maakt het mogelijk om gericht te beveiligen waar dat nodig is en afgewogen risico's te nemen waar dat kan. Risicogebaseerde informatiebeveiliging is een wisselwerking tussen de operatie en de ondersteunende diensten. Naast de Dienst IM en de Dienst ICT zijn dat nadrukkelijk ook de Dienst Facility Management voor de fysieke beveiliging en de Dienst HRM voor beveiliging ten aanzien van personeel.

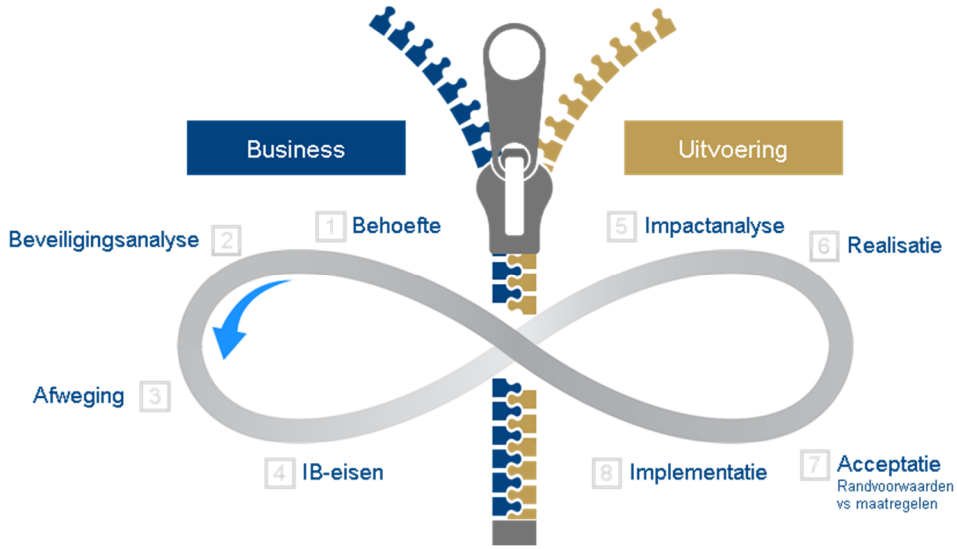
5.9.2. Risicoanalyses

De risicogebaseerde benadering houdt in dat informatiebeveiliging integraal onderdeel is van de verantwoordelijkheid van het lijnmanagement. De verantwoordelijke voor een werkproces of voor een systeem moet de risico's voor informatiebeveiliging in kaart brengen en op basis daarvan eisen stellen aan de ondersteunende diensten. De informatiebeveiligingsarchitectuur biedt hiervoor een methode voor 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. Hieronder valt tevens de wettelijke verplichting tot bescherming van persoonsgegevens.

Voor zowel AVG als Wpg-verwerkingen geldt een registerplicht. In BIJLAGE 2: Onderdelen uit de Wpg toegelicht is beschreven wat daaronder wordt verstaan. Als uit de informatie in het register blijkt dat een verwerking een hoog risico heeft, bijvoorbeeld omdat er gebruik gemaakt wordt van nieuwe technologieën, dan is het noodzakelijk om er een gegevensbeschermingseffectbeoordeling (in de volksmond ook wel PIA of Privacy Impact Assessment geheten) voor op te stellen. Als uit de GEB blijkt dat het een verwerking met een hoog risico betreft, moet mogelijk de Autoriteit Persoonsgegevens worden geraadpleegd voordat de gegevensverwerking in gebruik wordt genomen. Het uitvoeren van een goede risicoanalyse is daarom cruciaal. Zeker waar het een verwerking betreft die door een derde partij wordt uitgevoerd (verwerker) en/of extern wordt gehost. Op basis van de risicoanalyse zullen de te nemen beveiligingsmaatregelen aan deze derde partij worden opgelegd door middel van een verwerkersovereenkomst.

Bij het maken van een risicoanalyse voor een proces of een systeem wordt de verantwoordelijke manager ondersteund door een informatiebeveiligingsexpert van de Dienst IM. In een beperkt aantal interviews wordt de behoefte aan informatiebeveiliging bepaald. De informatiebeveiligingsexpert vult deze behoefte aan met mogelijke risico's, dreigingen en consequenties zodat de manager een afweging kan maken welke risico's acceptabel zijn en welke niet en welke maatregelen moeten worden genomen om deze risico's te mitigeren.

[66] Informatiebeveiligingsarchitectuur versie 1.0, september 2016

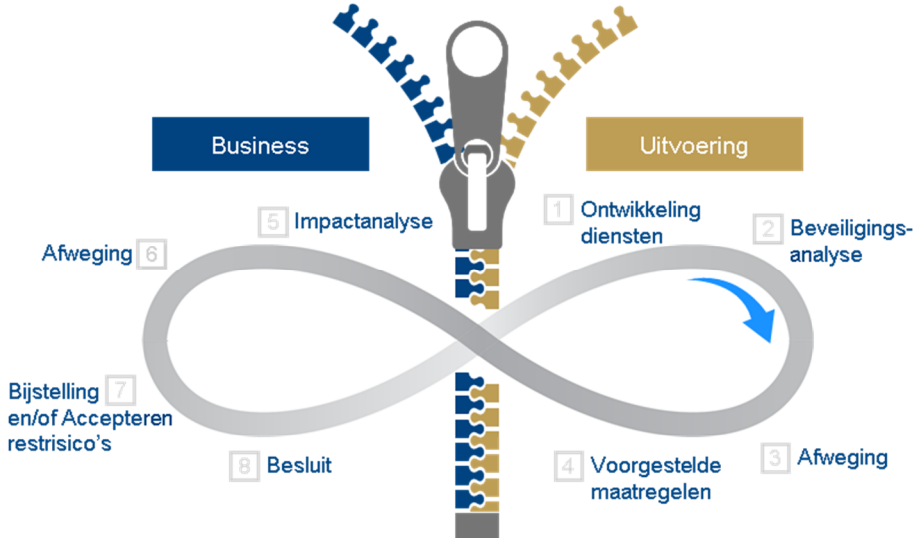


Figuur 24 Vraagprocessen Informatiebeveiligingseisen

Het resultaat is een pakket van informatiebeveiligingseisen. De ondersteunende diensten beoordelen deze eisen op de impact, dat wil zeggen of en hoe deze eisen gerealiseerd kunnen worden en of dit de beveiliging van andere dienstverlening beïnvloed. Bij het realiseren van de eisen wordt door de ondersteunende diensten samengewerkt om te komen tot een optimale mix van maatregelen op de terreinen ICT, Fysiek, Personeel en Organisatie.

5.9.3. Informatiebeveiligingsdiensten

Vanuit de ondersteunende diensten van het PDC worden informatiebeveiligingsdiensten ontwikkeld.[67] Deze diensten worden in eerste aanleg door het PDC zelf beoordeeld op risico's en impact op de totale dienstverlening. Het PDC voorziet de nieuwe diensten met voorgestelde maatregelen om deze risico's te reduceren. De verantwoordelijke lijnmanager zal, ondersteund door de Dienst IM, de impact van de nieuwe dienst en de consequenties daarvan beoordelen. De lijnmanager maakt een afweging over de diensten en de mogelijke risico's/consequenties. Deze verantwoordelijke maakt vervolgens een keuze over de diensten, de risico's en eventueel aanvullende maatregelen.



Figuur 25 Aanbodprocessen Informatiebeveiligingsmaatregelen

Bij het samenstellen van informatiebeveiligingsdiensten moet het PDC gebruik maken van de ontwerprichtlijnen en beveiligingsconcepten die worden voorgeschreven door de informatiebeveiligingsarchitectuur. Een aantal van die beveiligingsconcepten zijn als principe in dit uitvoeringskader opgenomen:

[67] Zie bijvoorbeeld de Uitvoeringsregeling Informatiebeveiliging Dienst ICT Politie Intern versie 1.0.

- **Autorisatie.** Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van noodzaak voor de uitvoering van de hen opgedragen werkzaamheden.
- **Metagegevens.** Gegevens worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de juistheid en de rechtmatigheid van de gegevensverwerking te waarborgen.
- **Kwaliteitszorg.** De informatievoorziening waarborgt de juistheid, doeltreffendheid en controleerbaarheid van de gegevensverwerking.

Daarnaast is er nog een aantal informatiebeveiligingsprincipes met specifieke ontwerprichtlijnen die in de informatievoorziening van de politie moeten worden toegepast:

- **Gelaagde beveiliging.** De informatievoorziening wordt beschermd door meerdere lagen van verschillende complementaire beveiligingsmaatregelen.
- **Segmentering.** De informatievoorziening wordt op basis van risicoprofielen georganiseerd in verschillende onderdelen met gecontroleerde koppelvlakken.
- **Koppelvlakken.** De koppelvlakken tussen onderdelen van de informatievoorziening worden systematisch beschreven en beheerd met specifieke beveiligingswaarborgen.
- **Identificatie en authenticatie.** Toegang tot de informatievoorziening is uniek herleidbaar tot een persoon, organisatie of geautomatiseerd systeem.
- **Registratie en controle.** De informatievoorziening voorziet in de registratie en monitoring van handelingen van gebruikers.
- **Beschikbaarheidsfuncties.** De beschikbaarheid van informatiediensten voldoet aan de met de verantwoordelijke gemaakte continuïteitsafspraken.

De meeste van deze ontwerprichtlijnen gelden niet voor individuele systemen maar moeten generiek in de infrastructuur en de werkprocessen van de organisatie worden georganiseerd. Het is wel van belang om te zorgen dat deze systemen ook daadwerkelijk gebruik maken van deze generieke voorzieningen voor informatiebeveiliging. Voor nadere toelichting op de toepassing van de informatiebeveiligingsprincipes verwijzen we naar de Informatiebeveiligingsarchitectuur en de Uitvoeringsregelingen Informatiebeveiliging van de Dienst ICT.

5.9.4. Risicomanagement

Bij een beveiligingsanalyse wordt er een match gemaakt tussen de beveiligingseisen van de business en de beveiligingsdienstverlening van de uitvoerende diensten. Wanneer beveiligingseisen niet door de standaard informatiebeveiligingsdiensten worden gerealiseerd moet een afweging worden gemaakt om tegen extra kosten aanvullende maatregelen te nemen of om restrisico's te accepteren. Deze restrisico's moeten vervolgens worden beheerst door de verantwoordelijke lijnmanager. Hij moet de risico's periodiek monitoren en evalueren. In de reguliere planning- en rapportagecyclus moet daartoe een informatiebeveiligingsparagraaf worden opgenomen.

5.9.5. Handreikingen

Informatiebeveiliging		
	**Activiteit**	**Aandachtspunten**
Beleid	Inrichten	Lijnmanagers zijn verantwoordelijk voor de informatiebeveiliging van primaire en bedrijfsvoeringsprocessen
	Kaderstellen	• Het korps heeft een door de korpsleiding vastgesteld informatiebeveiligingsbeleid. Het beleid moet actief worden uitgedragen aan de medewerkers. • Lijnmanagers moeten voor hun processen risicoanalyses (laten) uitvoeren. • Stel beveiligingseisen aan systemen en processen.
	Sturen	• Maak informatiebeveiliging onderdeel van de integrale sturing en managementrapportages. • Restrisico's moeten worden beheersd door de verantwoordelijke lijnmanager
	Controleren	Organiseer audits op informatiebeveiliging.
PDC	Ontwerpen	Ontwikkel informatiebeveiligingsdiensten conform informatiebeveiligingsarchitectuur met: • Gelaagde beveiliging

		• Segmentering op basis van risicoprofielen • Gecontroleerde koppelvlakken • Identificatie en authenticatie van gebruikers • Registratie en monitoring van handelingen • Continuïteitswaarborgen
	Ontwikkelen	• Maak gebruik van generieke voorzieningen voor informatiebeveiliging waaronder identity- en access management, logging en monitoring.
	Ondersteuning	• Geef medewerkers de beschikking over middelen die het mogelijk maken om veilig om te gaan met gegevens. • Lever ondersteuning bij risicoanalyses.
Uitvoering/ operatie	Voorlichting	Leidinggevende moeten veilig gedrag stimuleren door instructies en werkafspraken.
	Gebruik middelen	• Maar voor de verwerking van gegevens gebruik van veilige middelen die door de organisatie worden verstrekt. • Neem voor het verwerken van bijzondere persoonsgegevens strikte vereisten op voor autoriseren.
	Registratie	Houd een register van alle verwerkingen bij, inclusief risico-analyses en verwerkingsovereenkomsten en voer actief risicomanagement conform de PDCA cyclus.
	Incidenten/vragen	Houd een registratie bij van informatiebeveiligingsincidenten en rapporteer over informatiebeveiligingsrisico's.

5.10. Privacy by default

De verwerking van persoonsgegevens is standaard zo beperkt mogelijk ingericht

Ratio: Zowel de AVG als de Wpg bevatten privacy by default en privacy by design als verplichte principes. Deze dienen ertoe om gegevensbescherming vanaf het moment van ontwikkeling van informatiediensten tot aan het laatste gebruik zoveel mogelijk in de gegevensverwerking te integreren. Daar waar privacy by design vooral toeziet op ontwerpkeuzes bij de *ontwikkeling* van informatiediensten is privacy by default van belang bij keuzemomenten tijdens *gebruik* van de informatiediensten. Dit principe verplicht organisaties om de privacy van betrokkenen zo veel mogelijk te beschermen door de verwerking van persoonsgegevens standaard (by default) op de meest privacyvriendelijke stand te zetten.

5.10.1. 'Standaardinstellingen'

Het principe van privacy by default is opgenomen in de algemene verordening gegevensbescherming (art. 25 AVG) en in de aangepaste Wpg (art. 4b Wpg). De Nederlandse vertaling van privacy by default is 'gegevensbescherming door standaardinstellingen'. Dit zou de indruk kunnen wekken dat het volstaat om in geautomatiseerde systemen de instellingen standaard op de meest privacybeschermende waarden te zetten. De bedoeling is echter breder: het gaat erom dat betrokkenen ervan uit moeten kunnen gaan dat de verwerking van persoonsgegevens zo beperkt mogelijk is ingericht (gegeven het specifieke doel van de verwerking). Dat geldt voor:

- de hoeveelheid verzamelde persoonsgegevens,
- de mate waarin zij worden verwerkt,
- de termijn waarvoor zij worden opgeslagen en
- de toegankelijkheid daarvan.

Het 'pas toe of leg uit'-principe is hierbij van toepassing: afwijkingen kunnen worden toegestaan als daar een dwingende reden voor is.

Verzamel alléén die gegevens die voor het betreffende doel nodig zijn: als een (persoons)gegeven niet nodig is, vraag dit dan niet. De afweging die dit concept verlangt, dient voor elke verwerking opnieuw gemaakt te worden. Adresgegevens van een getuige kunnen bijvoorbeeld nodig zijn in het opsporingsproces maar niet noodzakelijk voor het strafproces; deze mogen dan ook niet aan het OM verstrekt te worden.

> Theo Hooghiemstra geeft in iBestuur magazine een mooi voorbeeld van dataminimalisatie: "een gemeente liet burgers 106 vragen beantwoorden bij het aanvragen van huursubsidie. Achteraf bleken 6 vragen voldoende om de beoordeling te maken."

Een andere belangrijke vuistregel is dat bij toetsvragen altijd de vraag gesteld moet worden: is het inhoudelijk antwoord noodzakelijk of is het voldoende om vast te leggen of aan de toetsvraag wordt voldaan?

> Vraag je bij een inkomenstoets naar het inkomen en toets je of dit een drempel overschrijdt, of vraag je of iemand meer of minder verdient dan de drempelwaarde? In het laatste geval leg je weliswaar een persoonsgegeven vast, maar minder gegevens dan het inkomen. Ook dit is een vorm van dataminimalisatie.

5.10.2. Informatiediensten

Het principe van privacy by default is in de nieuwe privacywetgeving onder andere opgenomen met het oog op informatiediensten waarbij gebruikers zelf de mogelijkheid wordt geboden om hun persoonsgegevens te delen of af te staan. Denk hierbij aan sociale netwerken of webwinkels die persoonsgegevens gebruiken voor gepersonaliseerde aanbiedingen en om automatisch te koppelen met andere websites. Denk aan apps voor tablets en smartphones die standaard toegang vragen tot je adressenboek, locatie en identiteitsgegevens. Andere voorbeelden zijn (online) contactformulieren met vooraf aangevinkte opties zoals "ik wil op de hoogte gehouden worden". In al deze gevallen wordt niet voldaan aan privacy by default.

Ook zaken als algemene voorwaarden moeten privacyvriendelijk zijn. Er mogen geen privacy-aspecten voorkomen op een plek waar ze niet thuishoren. Geen opt-out regime, maar opt-in: pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), niet het automatisch ontvangen totdat het wordt stopgezet (opt-out).

> Op politie.nl kunnen burgers meldingen doorgeven of aangifte doen van een misdrijf. In de formulieren die daarbij gebruikt worden kunnen afhankelijk van de gebeurtenis of de delictsoort verschillende gegevens worden ingevuld. Op de formulieren wordt duidelijk aangegeven welke gegevens verplicht zijn om de melding of de aangifte in behandeling te kunnen nemen. Burgers kunnen er zo zelf voor kiezen welke persoonsgegevens ze door de politie willen laten verwerken. Als dat nodig is kan de politie bij de verdere behandeling altijd contact opnemen om aanvullende gegevens op te vragen.

Dit principe kan ook worden toegepast bij de verwerking van persoonsgegevens waarbij de gebruikers politiemensen zijn. Bij de verwerking is het gebruik van persoonsgegevens zo minimaal mogelijk ingesteld (de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan). Politiemensen moeten expliciet kiezen voor ruimere verwerkingen en dit kunnen beargumenteren, als dat noodzakelijk is voor hun taak op dat moment.

> Met kunnen hotspots gemaakt worden van bijvoorbeeld woningovervallen. Bij dergelijke kaarten dient de standaardinstelling te zijn dat een kaart wordt opgebouwd op postcode-4-niveau. Indien een gebruiker meer detailinformatie nodig heeft, kan hij doorklikken tot bijvoorbeeld postcode-6-niveau.

> .

5.10.3. Pseudonimisering

In de memorie van toelichting op het wetsvoorstel Wpg en in artikel 25 AVG wordt expliciet pseudonimisering genoemd. Hiermee wordt gedoeld op het verwerken van persoonsgegevens op zodanige wijze dat de gegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om niet-koppeling aan een geïdentificeerd of identificeerbaar proces te waarborgen. Zo'n maatregel kan getroffen worden voor gegevens in het datawarehouse van de politie als het gaat om het maken van trendrapportages die zichtbaar maken hoe criminaliteit zich over de jaren heen ontwikkelt. Pseudonimisering is een technisch hulpmiddel om privacy by default mogelijk te maken. Dit wordt wel een Privacy Enhancement Technology (PET) genoemd. Andere PET's zijn anonimiseren en versleutelen.[68]

Bij data-analyses en intelligence-toepassingen moet een heldere scheiding worden gehanteerd tussen persoonsgegevens en andere gegevens. Het maken van trendrapporten over typen misdrijven en modus operandi kan uitstekend over decennia heen gedaan worden, als de persoonsgegevens uit de dataset verwijderd zijn. Bij de analyses moeten alleen persoonsgegevens worden betrokken als dat voor het doel van de analyse noodzakelijk is. Pseudonimisering is een technisch hulpmiddel dat uitermate geschikt is om representatieve testsets te creëren bij systeemontwikkeling en –tests.

---

[68] Het witboek PET voor beslissers van de Autoriteit Persoonsgegevens beschrijft diverse technologieën en maatregelen

[redacted] leveren belangrijke managementinformatie over bijvoorbeeld aantallen medewerkers en ziekteverzuim. Deze worden standaard aangeboden op afdelingsniveau en er zou doorgeklikt kunnen worden tot bijvoorbeeld het niveau van groepen bestaande uit tien of twintig personen. Op deze manier kan managementinformatie worden geleverd zonder dat daarbij persoonsgegevens worden verwerkt.

5.10.4. Handreikingen

Privacy by default		
	**Activiteit**	**Aandachtspunten**
Beleid	Inrichten	Lijnmanagers moeten zich bewust zijn van hun verantwoordelijkheden bij de verwerking van persoonsgegevens en hun medewerkers daarop aanspreken.
	Kaderstellen	De kaders voor gegevensverwerking bevatten het uitgangspunt dat informatievragen worden beantwoord met een standaard zo beperkt mogelijk gebruik van persoonsgegevens. Onnodige en bovenmatige verwerkingen van persoonsgegevens moeten worden gesignaleerd en worden afgewezen.
PDC	Ontwerpen	Ontwerp de voorzieningen waarmee gegevens worden opgevraagd zodanig dat gebruikers expliciet moeten kiezen om aanvullende persoonsgegevens te verwerken: geen opt-out maar opt-in.
	Ondersteuning	Zorg dat business experts en systeemontwikkelaars kunnen adviseren over methoden en technieken om informatievragen te beantwoorden met gebruik van zo min mogelijk persoonsgegevens. Deze medewerkers moeten kennis hebben van privacy enhancing technologies zoals pseudonimisering, anonimiseren en encryptie.
	Data-analyse	Persoonsgegevens en andere gegevens moeten als dataset van elkaar worden gescheiden. • Analyse in de basis maken zonder dataset persoonsgegevens • Persoonsgegevens alleen bij analyse gebruiken indien noodzakelijk voor het doel
	Testen	Gebruik gegenereerde testgegevens tenzij het echt niet anders kan. Als het echt nodig is, gebruik je voor het ontwikkelen, testen en opleiden een zo minimaal noodzakelijke set. Dat houdt in dat niet strikt relevante gegevens worden uitgesloten of geanonimiseerd.
Uitvoering/ operatie	Voorlichting	Alle instructies op het gebied van gegevensverwerking moeten uitgaan van een zo beperkt mogelijk gebruik van persoonsgegevens. • Politiemedewerkers moeten methoden, technieken en voorzieningen aangereikt krijgen om het gebruik van persoonsgegevens te beperken. • Bij een verzoek voor ruimere verwerking is dit een expliciete keuze die beargumenteerd moet worden.
	Incidenten/vragen	Vraag je altijd eerst af of het mogelijk is om het probleem op te lossen zonder persoonsgegevens te gebruiken. Gebruik vervolgens alleen die persoonsgegevens die je nodig hebt voor je taakuitvoering.

5.11. Toepassing standaarden

Bij de gegevensverwerking wordt gebruik gemaakt van bestaande overheids- en ketenstandaarden.

Ratio: Het gebruik van bestaande overheids- en ketenstandaarden bevordert de samenwerking tussen organisaties 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.

5.11.1. Gebruik van standaarden

Een standaard is een document dat een set van regels bevat die beschrijven hoe materialen, producten, diensten, technologieën, taken, processen en systemen dienen te worden ontwikkeld en beheerd. (NORA)-standaarden worden vastgelegd binnen een organisatie, de partijen binnen een samenwerkingsverband of via een erkende standaardisatie-organisatie (zoals ISO of NEN). Verder kennen standaarden doorgaans een proces waarmee ze ontwikkeld, erkend en beheerd worden. Standaarden kunnen door wet- en regelgeving verplicht worden gesteld. Daarbij wordt doorgaans het 'pas toe of leg uit'-principe gehanteerd waardoor afwijkingen kunnen worden toegestaan als daar een dwingende reden voor is. De politie moet ook actief deelnemen aan interdepartementale en internationale fora waarin standaarden voor gegevensverwerking worden ontwikkeld en vastgesteld.

In dit uitvoeringskader willen we projecten helpen bij het vinden van de juiste standaarden (en herbruikbare bouwstenen) voor gegevensverwerking. Dat doen we allereerst door te verwijzen naar de diverse plaatsen waar overzichten worden beheerd van standaarden, zodat we inzicht krijgen in alle beschikbare standaarden. Daarnaast proberen we inzicht te geven in welke situaties, welke standaarden bij voorkeur worden toegepast.

5.11.2. Rijks- en overheidsstandaarden

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. Een voorbeeld waarbij de politie afwijkt van rijksstandaarden is het Besluit Informatiebeveiliging Rijksdienst (BIR). Omdat de voorgeschreven maatregelen niet passen op de uitvoeringstaken van de politie hebben we hiervoor een eigen informatiebeveiligingsarchitectuur op basis van risicobeheersing.[69]

5.11.3. Ketenstandaarden

Ten behoeve van samenwerking met organisaties in de strafrechtsketen sluit de politie aan bij de standaarden voor elektronisch berichtenverkeer van de Justitiële Informatiedienst (JustID).

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 strafrechtsketen en in de vreemdelingenketen.

5.11.4. 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 ook veel gesloten standaarden worden gebruikt, waarbij men voor de inzage van de specificaties, een licentie dient aan te vragen. Het Forum Standaardisatie houdt een lijst bij van open standaarden waarvoor in de publieke sector een verplicht gebruik geldt.

[69] Zie Rijksregister Standaarden

5.11.5. Handreikingen

Toepassing standaarden		
	**Activiteit**	**Aandachtspunten**
Beleid	Vernieuwing	Neem deel aan fora waarin standaarden voor gegevensverwerking worden ontwikkeld
	N.a.v. issues	Organiseer compliance toetsen
PDC	Ontwerpen/ ontwikkelen	• Maak indien mogelijk bij ontwerpen en ontwikkelen zo veel mogelijk gebruik van beschikbare standaarden • Maak gebruik van standaarden die door wet- en regelgeving verplicht worden gesteld. Hiervan kan afgeweken worden door de pas toe of leg uit-procedure.
	Ondersteuning	Maak en beheer het overzicht van toepasselijke standaarden
Uitvoering / Operatie	Registratie	Maak gebruik van afgesproken standaarden voor gegevensverwerking bijvoorbeeld referentiegegevens.

5.12. Verantwoordelijkheden belegd

De verantwoordelijkheden voor de zorgvuldige en rechtmatige verwerking van gegevens zijn eenduidig belegd.

Ratio: 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, realiseren van gegevensuitwisseling of het doorvoeren van verbeteringen. Wat betreft de verdeling van verantwoordelijkheden dienen onderstaande rollen daarvoor te zijn ingevuld.

De verantwoordelijkheid voor gegevens en de wijze waarop de verantwoordelijkheden worden belegd in de organisatie is beschreven in het document Verantwoordelijkheid voor gegevens. Onderstaande tekst geeft een inleiding op dit beleid en een toelichting op proces van beleggen van de verantwoordelijkheden.

5.12.1. 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 de beleid, koers en strategie voor de verwerking van gegevens. Denk bij strategie aan kwaliteitsverbetering of 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 het belang van kwaliteit naar het eigen team en de omgeving. Tot slot hoort ook het laten benutten van gegevens in de uitvoering van de politietaak tot de uitvoeringsverantwoordelijkheid.

	Beleidsverantwoordelijkheid	**Uitvoeringsverantwoordelijkheid**

Voorbeeld: **Proces-verbaal**	De definities, richtlijnen en kwaliteitseisen waaraan het proces-verbaal moet voldoen worden centraal opgesteld en onderhouden in afstemming met alle afnemers en informatiemanagement.	De collega is verantwoordelijk voor de kwaliteit van het proces-verbaal. De leidinggevende stuurt zijn medewerkers op de vastlegging van het pv volgens de definities, richtlijnen en kwaliteitseisen.

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. Een blauwdruk voor de taken van deze rollen is hieronder weergegeven.

Rollen beleidsverantwoordelijkheid
De rol van *beleidsverantwoordelijke* is belegd bij directeuren en portefeuillehouders (politiechefs). 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. De rol van *adviseur met proces- en beleidskennis* brengt kennis in voor definitie, classificatie en kwaliteitseisen. Deze rol ligt bij één of meer beleidsadviseur(s) vanuit het team van de beleidsverantwoordelijke (portefeuille, directie). De rol van *adviseur vanuit informatiemanagement* ondersteunt bij het opstellen en onderhouden van definities en richtlijnen voor gegevens en de verwerking daarvan. Daarnaast verzorgt deze rol de vraagarticulatie aan GGB en andere uitvoeringsorganisaties voor het doen van aanpassingen en verbeteringen aan de gegevenshuishouding. Deze rol bewaakt ook de integraliteit van de IV in totaal en de gegevenshuishouding specifiek. Binnen de afdeling IM zijn verschillende functionarissen die hier een rol in hebben. Het eerste aanspreekpunt van een beleidsverantwoordelijke is de coördinerend business expert. Daarnaast hebben de IV-experts een rol in de uitvoering van onderstaande taken.

Rollen uitvoeringsverantwoordelijkheid
De rol van *uitvoeringsverantwoordelijke* is belegd bij leidinggevenden in de operatie en PDC, bijvoorbeeld een teamchef van een basisteam. Voor politiechefs betekent dit een dubbele rol: zij hebben de uitvoerings-verantwoordelijkheid als lijnchef, maar zij hebben ook een beleidsverantwoordelijkheid in hun rol als landelijk portefeuillehouder. Binnen de operatie worden specifieke taken en bevoegdheden die behoren bij de uitvoeringsverantwoordelijke belegd bij rollen zoals de poortwachter, de privacyfunctionaris (adviseur), de taakaccenthouder (onder andere kwaliteit en bijzondere persoonsgegevens) en de bevoegd functionaris (hieronder nog kort toegelicht). Iedere individuele politiemedewerker heeft in zijn rol als *gegevensverwerker* de taak om gegevens juist te verwerken volgens kaders en richtlijnen. Denk hierbij onder andere aan terugmelden, vastlegging van de verwerkingsgrondslag, verwijderen, archiveren en vernietigen. Verder valt hier ook onder de ontsluiting, interpretatie, het gebruik en mogelijk verstrekken van gegevens met afweging van noodzaak, grondslag en toepassing van beschikbare metagegevens. Specifiek voor artikel 9- en 10-verwerkingen vereist de Wpg dat een bevoegd functionaris aangewezen wordt door de uitvoeringsverantwoordelijke (in naam van 'de verantwoordelijke'). Kern van deze rol is dat zorgvuldig wordt omgegaan met doelafwijkend gebruik van politiegegevens. De bevoegd functionaris besluit onder andere welke gegevens uit een art. 9- of 10-verwerking mogen worden gebruikt binnen een andere verwerking en wie geautoriseerd mag zijn voor gegevens uit 'zijn' onderzoek.

De uitvoeringsverantwoordelijke dient invulling te geven aan de actieve informatieplicht aan betrokkenen. Zie paragraaf 5.4.4 voor meer informatie. Hij moet betrokkenen ongevraagd informeren over de verwerkingen:

- Algemeen: via de website en brochures. Hierin wordt onder andere vermeld: de contactgegevens van de verantwoordelijke en functionaris gegevensverwerking, de verwerkingsdoelen, de procedures voor het uitoefenen van de rechten van betrokkenen en het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Specifiek: kan via de website, maar ook in reactie op een aangifte of een ander contact met de betrokkene. Geef onder andere informatie over de rechtsgrondslag van de verwerking, de verwerkings- en bewaartermijnen, de categorieën van ontvangers van de politiegegevens en het bestaan van geautomatiseerde besluitvorming (waaronder profilering).

Randvoorwaarden en middelen
Voor de uitoefening van de gegevensverantwoordelijkheid in alle facetten is het van belang dat enkele randvoorwaarden zijn ingevuld en specifieke middelen beschikbaar zijn. Denk hierbij aan beschikbaarheid van beleid en richtlijnen, en aan datamanagementprocessen en ondersteunende systemen. Daarnaast zijn organisatie- en overlegstructuren nodig, training en afdoende capaciteit ondersteunende functionarissen en afdelingen.

5.12.2. Afdelingen met een speciale functie voor de gegevenshuishouding

Er zijn afdelingen binnen de politie die een specifieke rol hebben voor de gegevenshuishouding. De IM-organisatie heeft bijvoorbeeld een sleutelrol in het sturen op verbeteringen vanuit integraliteit[19]. GGB geeft advies over- en voert regie op het behandelen van gegevens als de kern. De Gegevensautoriteit (GA), CISO en Documentaire Informatievoorziening (DIV) stellen kaders op en zien toe op de naleving daarvan. De privacyfunctionarissen, samen met de Gegevensautoriteit en het team Juridische Zaken (Bestuurszaken Korpsstaf) verenigd in het Privacyplatform, adviseren over naleving van de Wpg en AVG. De teams KvI ondersteunen de uitvoering met monitoring, signalering en advies op het vlak van kwaliteit van gegevens. Database-administrators bij DICT dragen zorg voor de continuïteit en prestatie van gegevensvoorzieningen. Politieprofessie zorgt voor het in werking brengen van procedures en richtlijnen, de Politieacademie voor opleiding en de Directie HRM voor competenties en de juiste cultuur.

De politie is verplicht om een functionaris gegevensbescherming (FG) aan te stellen. Dit is zowel verplicht op basis van de AVG (artikel 37) als de Wpg (artikel 36). Voor de politiegegevens is dit nieuw; in het verleden was het een vrije keuze van de verwerkingsverantwoordelijke om deze onafhankelijke functionaris aan te stellen. De politie stelt twee FG's aan. Zij worden aangesteld op grond van hun professionele kwaliteiten en hun deskundigheid op het gebied van de wetgeving en hun kennis van de praktijk. Er mag geen belangenverstrengeling zijn tussen de FG-taken en de eventuele andere taken of functies van de FG. De FG:

- is verplicht op basis van de AVG en Wpg;
- heeft (wettelijk) mandaat;
- rapporteert rechtstreeks aan de korpschef en is eerste aanspreekpunt voor de AP
- voert toezicht uit in samenwerking met de auditors en de privacyfunctionarissen;
- stelt jaarlijks een verslag op met zijn bevindingen;
- mag geen instructies krijgen hoe hij zijn taken als FG moet uitvoeren;
- heeft ontslagbescherming.

Een zeer cruciale persoon voor het bewaken van de continuïteit van de gegevenshuishoudiung, is degene die de sleutelfunctie van een applicatie vervult. Vaak is er een persoon die vanaf het begin bij een informatievoorziening betrokken is geweest, zowel in de rol van ontwerper als in die van ontwikkelaar.

Zowel bij projecten en programma's in de operatiën als in de informatievoorziening moet privacywetgeving binnen de scope van een project vallen. Een projectleider mag geen decharge krijgen als dit onderwerp onvoldoende in het project is verwerkt. Hierbij kan gebruik worden gemaakt van instrumenten als de gegevensbeschermingseffectbeoordeling; deze komt aan de orde in paragraaf 5.2.4.

5.12.3. Proces van beleggen van verantwoordelijkheid

Als de vraag om de verantwoordelijkheid voor specifieke gegevens te beleggen zich aandient, dan worden de stappen van het datamanagement-verbeterproces doorlopen met de activiteiten zoals hieronder beschreven.

Figuur 26 Datamanagement-verbeterproces

Verbeter-processtap	Activiteiten
Definieer verbetering	• Scope van initiatief voor beleggen van verantwoordelijkheid voor gegevens wordt bepaald; • IM start met een analyse van hoe de beleids- en uitvoeringsverantwoordelijkheden o worden belegd gezien vanuit het beleid; o in de huidige situatie (mogelijk al impliciet) al belegd zijn;
Ontwerp	• Op basis van de analyseresultaten worden verantwoordelijken (in concept) geïdentificeerd door IM [redacted]; • Iedere beoogd verantwoordelijke wordt benaderd door een vertegenwoordiger vanuit IM voor het informeren en afstemmen: wat wordt er van ze verwacht, voelt de betrokkene zich verantwoordelijk vanuit zijn functie en in hoeverre zijn de taken, verantwoordelijkheden en bevoegdheden werkbaar? Hierbij wordt besproken welke datamanagement processen aandacht nodig hebben en wat eventueel te treffen voorzieningen (capaciteit, middelen) zijn; • In geval van vragen, onduidelijkheden of conflicten kan de Gegevensautoriteit benaderd worden voor verheldering, bemiddeling en waar nodig escalatie
Voorbereiden verandering	Als de verantwoordelijke akkoord is, dan wordt • samen met de verantwoordelijke een draaiboek opgesteld voor het in werking brengen (op basis van een blauwdruk); • onderdeel van het plan is communicatie en training;
Doorvoeren verbetering	• Uitvoer van de geplande activiteiten voor in werking brengen; • De verantwoordelijkheid wordt vastgelegd in de gegevenscatalogus; • Er is regulier overleg tussen de gegevensondersteunende partijen en de verantwoordelijke over het succes in de uitoefening van de verantwoordelijkheid en over de kwaliteit van de gegevenshuishouding.

De ‘gegevenscatalogus’ bestaat begin 2017 uit lijsten per gegevenstype. Zo wordt bij GGB voor referentiegegevens de lijst met verantwoordelijken opgebouwd.

5.12.4. Handreikingen

Verantwoordelijkheden belegd		
	**Activiteit**	**Aandachtspunten**
Beleid	Beleid, koers en strategie vormen	Vertaal strategie voor de eigen beleidsscope ook naar een strategie op gegevens: Denk bij strategie aan kwaliteitsverbetering of verwerven van extra gegevens
	Prioritering voor portfolio	Geef afdoende prioriteit aan de integraliteit van de gegevenshuishouding; denk hierbij aan toepassing van kernregisters en centraal beheerde referentiegegevens
	Uitwerken vernieuwing en verbetering	Stel (ontbrekende) definities op en inventariseer welke kwaliteitseisen gelden vanuit verschillende afnemers
PDC	(agile/anders)	
	IV Projectleiding	Neem beleggen van gegevensverantwoordelijkheid mee in projectactiviteiten.
	Adviseren en ondersteunen portefeuillehouder	Taken van business experts IM in domein/portefeuilleteams onder meer: • Opstellen en onderhouden van definitie en classificatie van gegevens. • Formulering van kaders en richtlijnen voor verwerking van gegevens. • Definiëren en onderhouden van kwaliteitseisen op basis van gebruiksdoelen. • Laten creëren van inzicht in kwaliteit van gegevens ten behoeve van toezicht. • Bewaken van de integraliteit van de IV in totaal en de gegevenshuishouding specifiek.
Uitvoering / Operatie	Verwerking: registratie	Let bij verkrijgen en vastleggen van gegevens in de werkprocessen op de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid.
	Verwerking: beheer	Zorg voor terugmelden in geval van kwaliteitsproblemen. Zorg verder voor veredelen, verbeteren en evalueren van de beslotenheid.
	Verwerking: gebruik	Houd bij ontsluiting, interpretatie en gebruik van gegevens rekening met de geldende privacy-en securitywet- en regelgeving. Maak hierbij gebruik van de beschikbare metagegevens.
	Verwerking: verwijderen, bewaren en vernietigen	Zorg voor verwijderen, bewaren en vernietigen van gegevens, hierbij waar mogelijk gebruik makend van de ondersteunende automatisering
	Gegevenskwaliteitincident opvolging	• Herstel proactief • Rapporteer aan de uitvoeringsverantwoordelijke. Leg indien nodig besluiten voor aan de uitvoeringsverantwoordelijk en zorg voor rapportage
	Gegevensprobleemanalyse (door KvI)	Betrek de adviseurs van de beleidsverantwoordelijke voor de gegevens

Bijlagen

BIJLAGE 1: het concept privacy by design

Het concept Privacy by Design werd in de jaren negentig ontwikkeld door de Information & Privacy Commissioner van Canada. Dit was het antwoord op de constant groeiende informatie- en communicatietechnologieën en grootschalige datasystemen. Aanvankelijk werd de ontwikkeling van wetgeving en de toepassing van Privacy-Enhancing Technologies (PETs) gezien als oplossingen. Vandaag de dag is duidelijk dat een meer fundamentele benadering nodig is. Privacy by Design vereist een nauwe afstemming tussen informatiesystemen, werkprocessen (werkwijzen en gebruik van informatiesystemen) en het fysieke ontwerp van de techniek en infrastructuur. Dit kan worden weergegeven in de volgende, algemeen geaccepteerde, uitgangspunten:[70]

1. Proactief in plaats van reactief; preventief in plaats van herstellend
   De Privacy by Design-benadering wordt gekarakteriseerd door het nemen van proactieve maatregelen in plaats van reactieve. Het anticipeert op en voorkomt inbreuken op iemands privacy voordat deze feitelijk plaatsvinden. PbD wacht niet totdat privacyrisico's een feit zijn noch biedt zij oplossingen voor privacyschendingen die reeds hebben plaatsgevonden. Het doel is om te voorkomen dat zij gebeuren. Het vindt dus vooraf plaats, niet achteraf.
2. Privacy als standaard
   Privacy by Design streeft naar een maximale privacy door te verzekeren dat persoonlijke gegevens in een informatiesysteem of werkproces automatisch afdoende beveiligd zijn. Ook als het individu zelf niets onderneemt zal zo toch zijn privacy zijn gewaarborgd. Dit concept wordt in de nieuwe Europese wetgeving aangeduid met de term 'privacy by default'.
3. Privacy geïntegreerd in het ontwerp
   Privacy by Design is geïntegreerd in het ontwerp en de architectuur van informatiesystemen en werkprocessen. Het is geen los onderdeel dat ergens aan vast geplakt zit. Privacy vormt een essentieel onderdeel van de kernfunctionaliteit van informatiesystemen en werkprocessen. Er is aandacht voor in een vooronderzoek of uitwerking van een business case.
4. Volledige functionaliteit
   Privacy by Design streeft ernaar om alle legitieme belangen en doelstellingen op de wijze van een 'win-win' te faciliteren. Dus in plaats van privacy tegenover veiligheid te stellen (een benadering die in het verleden gebruikelijk was) juist te bewijzen dat een combinatie van beide mogelijk is.
5. Veiligheid van begin tot eind, gedurende de volledige levenscyclus
   Privacy by Design van begin tot eind geïntegreerd in een informatiesysteem nog voordat er enige informatie is verzameld, verspreidt zich over de gehele levenscyclus van de betrokken gegevens. Krachtige veiligheidsmaatregelen van begin tot eind zijn essentieel voor het behoud van privacy. Dit geeft de garantie dat alle gegevens op een veilige wijze zijn verkregen en tijdig en op veilige wijze worden vernietigd aan het eind van het proces. Zodoende verzorgt Privacy by Design een juiste behandeling van gegevens en een veilige omgang met informatie, van begin tot eind.
6. Zichtbaarheid en transparantie
   Privacy by Design streeft er naar om alle belanghebbenden ervan te verzekeren dat alle betrokkenen inzicht hebben in welke maatregelen worden getroffen voor gegevensbescherming. De technische componenten en het operationeel handelen blijven zichtbaar en transparant voor gebruikers en dienstverleners. Vertrouwen is de basis, maar nooit zonder controle.
7. Respect voor privacy, laat de gebruiker centraal staan
   Privacy by Design vereist architecten en exploitanten die de belangen van het individu als hoogste prioriteit beschouwen en daarvoor maatregelen nemen zoals het instellen van krachtige privacy instellingen, passende informatievoorzieningen en gebruikersvriendelijke opties.

BIJLAGE 2: Onderdelen uit de Wpg toegelicht

In hoofdstuk 4 zijn de AVG en Wpg op hoofdlijnen beschreven. Een aantal belangrijke Wpg-onderdelen met het oog op het toepassen van Privacy & Security by Design worden in deze bijlage toegelicht. Begrip van deze concepten is noodzakelijk om de principes uit hoofdstuk 5 op de juiste wijze te interpreteren. Verder luidt het advies om ook de wettekst zelf te lezen (zie bijlage 3).

Autoriseren

De politie is verplicht om passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen verlies of vormen van onrechtmatige verwerking (art. 4 a lid 2, 3 en 4 Wpg). Een van die maatregelen is het vooraf aanwijzen van personen die bevoegd zijn om de politiegegevens te verwerken; oftewel hen daartoe te autoriseren. Bij het invullen van het autorisatieregime heeft de politie een zekere vrijheid maar de

[70] Ann Cavoukian. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada, 2009.

hoofdregel is dat naarmate de politiegegevens 'gevoeliger' worden en specialistisch, er minder geautoriseerden mogen zijn. In artikel 6 Wpg staan de algemene eisen opgesomd waaraan autorisaties moeten voldoen.

Voor het invullen van het autorisatieregime betekent dit dat politiemedewerkers gericht geautoriseerd moeten worden om politiegegevens te mogen verwerken.[71] Ook moet de autorisatie expliciet maken voor welke taken van de politiemedewerker de autorisatie geldt en voor welke handelingen hij precies geautoriseerd wordt. Een algemene bevoegdheid tot "het verrichten van handelingen" is onvoldoende specifiek.

Verwerken
Uitgangspunt van de Wpg is dat politiegegevens slechts worden verwerkt voor zover zij rechtmatig zijn verkregen en dit noodzakelijk is voor door de wetgever geformuleerde doeleinden. Daarbij komt dat de gegevens ten opzichte van dat doel toereikend moeten zijn, ter zake dienend en niet bovenmatig mogen zijn (art. 3 lid 1 en 2 Wpg). Daarnaast kunnen politiegegevens onder voorwaarden worden verwerkt voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verkregen.

Verwerkingsdoeleinden
De wet kent vier initiële verwerkingsdoeleinden (ook wel verwerkingsgrondslagen genoemd):

- Art. 8 lid 1 Wpg: verwerking met het oog op de uitvoering van de dagelijkse politietaak;
- Art. 9 lid 1 Wpg: gerichte verwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval;
- Art. 10 lid 1 Wpg: gerichte verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde;
- Art. 12 lid 1 Wpg: verwerking met het oog op de controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens.

Daarnaast staat de Wpg toe dat politiegegevens mogen worden verwerkt voor een ander doel dan waarvoor oorspronkelijk verkregen maar alleen indien de Wpg daar uitdrukkelijk in voorziet. Dat doet de wet in deze artikelen:

- Art. 13 Wpg: de politiegegevens van artikel 8, 9 en 10 Wpg mogen verder worden verwerkt ten behoeve van de ondersteuning van de politietaak;
- Art. 11 Wpg: de mogelijkheid om verbanden te leggen tussen gegevens (geautomatiseerd vergelijken en in combinatie zoeken; zie verderop voor een uitgebreide toelichting);
- Art. 14 Wpg: het bewaren van verwijderde politiegegevens voor de afhandeling van klachten en verantwoording van verrichtingen en voor het onder voorwaarden hernieuwd verwerken.

Verwerkingstermijnen
Voor iedere verwerkingsgrondslag heeft de wetgever tevens bepaald binnen welke termijn een gegeven verwerkt mag worden en wanneer het verwijderd en vernietigd moet worden. Verwerkingen nadat deze termijnen verstreken zijn, zijn per definitie onrechtmatig.

Delen van politiegegevens
Voor effectief informatiegestuurd politiewerk is het cruciaal dat gegevens daadwerkelijk gedeeld worden. De Wpg stimuleert dit doordat er een *plicht* is opgenomen om informatie ter beschikking te stellen.[72] Het motto binnen de Wpg is 'delen, tenzij'; er bestaat een 'free flow of information' binnen het *volledige* Wpg-domein.[73] Dit betekent naast de politie ook de Koninklijke Marechaussee, Rijksrecherche, opsporingsambtenaren van de bijzondere opsporingsdiensten (BOD'en) en overige boa's. De BOD'en zijn de FIOD-ECD, ISZW (voorheen SIOD), NVWA-IOD en ILT/IOD. Door deze plicht om te delen maakt de wetgever beter informatiegestuurd werken mogelijk. Zo kunnen politiegegevens die bijvoorbeeld verkregen zijn bij een verkeerscontrole (artikel 8-gegevens) verder worden verwerkt in een drugsonderzoek (artikel 9-gegevens). Alleen op deze wijze voorkom je dat er bijvoorbeeld twee observatieteams hetzelfde subject volgen zonder dat van elkaar te weten.

> "…Het is voor een adequate criminaliteitsbestrijding van essentieel belang dat politiegegevens beschikbaar zijn voor de politieambtenaren die deze voor hun taak nodig hebben."
>
> aldus de Nota van Toelichting op het Bpg

[71] In het Besluit Politiegegevens zijn nadere regels opgenomen over specifieke categorieën van personen en gegevensverwerkingen die vanwege hun karakter beperkt moeten worden tot daartoe gespecialiseerde personen (met soms specifieke deskundigheidseisen).
[72] Artikel 15 lid 1 Wpg
[73] Dit concept bestaat in de AVG niet. Daar geldt: 'niet delen, tenzij'.

Een groot deel van deze ter beschikking stellingen verloopt geautomatiseerd, bijvoorbeeld doordat de gegevens uit de BVH's landelijk kunnen worden bevraagd met [redacted]. Of door [redacted] zodat opsporingsinformatie wordt gedeeld met iedereen die dat nodig heeft voor zijn werk. Dit werkt vooral binnen het politiedomein en nog niet binnen het volledige Wpg-domein zoals met de BOD'en. Voor het ter beschikking stellen (zowel binnen politie als daarbuiten, bijvoorbeeld met een BOD) gelden de volgende voorwaarden:

1. Er wordt gedeeld met een collega binnen het Wpg-domein die geautoriseerd is;
2. Deze medewerker heeft het gegeven nodig voor een goede uitvoering van de politietaak;
3. Die (verdere) verwerking is expliciet toegestaan door de wetgever;
4. Als het gaat om artikel 9-of 10-gegevens: er is instemming van de bevoegd functionaris en er is geen weigeringsgrond van toepassing (artikel 2:13 Bpg).[74]

Een tweede manier van delen, is met organisaties buiten het Wpg-domein en met burgers. Dit kan alleen als de Wpg het expliciet mogelijk maakt[75]. Denk aan gemeenten, de Belastingdienst, de Stichting Processen Verbaal en de AIVD. In een samenwerkingsverband kan onder voorwaarden ook verstrekt worden aan partners zoals een woningbouwvereniging en winkeliers. In de Verstrekkingenwijzer[76] is het totaaloverzicht van instanties opgenomen met de daarbij behorende voorwaarden. Deze instanties kunnen politiegegevens nodig hebben voor het verrichten van hun eigen taken, maar ze kunnen ook bijdragen aan de politietaak. Zij kunnen bijvoorbeeld hulp verlenen of strafbare feiten voorkomen doordat ze beschikken over politiegegevens.

Verstrekken heeft betrekking op iedere vorm van bekendmaken: zowel mondeling als schriftelijk meedelen maar ook online toegang tot systemen, het geven van een printuitdraai, het laten meekijken op een beeldscherm of bevestigend antwoorden op een vraag. Bij verstrekken dient de identiteit en de functie van een partner te worden gecontroleerd.

Personen en instanties	Welke politiegegevens	Speciale aandachtspunten	Wordt verstrekt door (KMar)	Wordt verstrekt door (politie)
Autoriteit financiële markten (AFM) *art. 18 Wpg en art. 4:3 tweede lid, onder c Bpg*	Alle politiegegevens	Nodig voor een betrouwbaarheidsonderzoek in het kader van: • de Wet financieel toezicht; • de Wet toezicht accountantsorganisaties. De verstrekking wordt eerst afgestemd met het OM.	Infodesk	Teammedewerker, [redacted]
Belastingdienst *art. 18 Wpg en art. 4:2 derde lid Bpg*	Art. 8 en art. 13 eerste lid	1. Nodig voor het inschatten van de veiligheidsrisico's (agressie & geweld) met betrekking tot het toezicht houden op naleving van: • Invorderingswet 1990; • Algemene wet inzake rijksbelastingen; • Wet arbeid vreemdelingen.	[redacted]	Teammedewerker Teammedewerker Teammedewerker [redacted]
art. 20 Wpg	Art. 8 en art. 13 eerste lid	2. Voor andere doeleinden dan bij 1, zoals samen structureel fraude voorkomen of de 'patseraanpak', moet er sprake zijn van een samenwerkingsverband/convenant (art. 20 Wpg).	Medewerker genoemd in convenant [redacted]	Medewerker genoemd in convenant
art. 16 eerste lid, onder a Wpg	Alle politiegegevens	3. Bij een opsporingsonderzoek van de Belastingdienst kan de BOA politiegegevens verstrekt krijgen. Voor haar toezichtstaken kan ze gegevens ontvangen via de FIOD (artikel 15).	[redacted] Infodesk	Teammedewerker, [redacted]

Figuur 27: fragment uit de verstrekkingenwijzer Wpg

Ook als politiegegevens aan een andere partij worden verstrekt, die ze op haar beurt verwerkt onder de AVG, blijven het voor de politie politiegegevens. Ofwel, de politie gaat de verstrekte gegevens niet opeens onder de AVG verwerken. Ook niet in samenwerkingsverbanden.

Verder verwerken onder artikel 13

Zoals reeds aangegeven mogen politiegegevens in beginsel slechts verwerkt worden voor het doel waarvoor zij initieel zijn verwerkt. Als de Wpg daarin uitdrukkelijk voorziet, mogen zij ook worden verwerkt voor een ander doel. Zoals eerder benoemd voorziet onder andere artikel 13 daarin. Voor de effectieve uitvoering van het politiewerk is artikel 13 heel belangrijk.[77] Op grond van artikel 13 kunnen artikel 8, 9 en 10-gegevens breed beschikbaar komen:

- Lid 1: als landelijk raadpleegbare politiegegevens; dit zijn onder andere antecedenten,[78] modus operandi, signaleringen vanwege vuurwapengevaarlijkheid en arrestatiebevelen, maar ook foto's en vingerafdrukken om personen of goederen te identificeren en verificeren.
- Lid 2: om landelijk inzicht te verwerven in specialistische onderwerpen zoals levens- en zedendelicten, kinderporno, mensenhandel en mensensmokkel.

---

[74] Zie voor aanwijzing van de bevoegd functionarissen artikel 2:10 Bpg. Hierbij speelt ook de zaaksofficier een rol.
[75] Dit wordt wel een 'gesloten verstrekkingenregime' genoemd.
[76] https://agora.portal.politie.local/sites/staven/1503111105/Onze%20documenten/2016-08-01_verstrekkingenwijzer_Wpg.pdf
[77] Muijen 2012: "… kan artikel 13 worden beschouwd als U-bocht om ervoor te zorgen dat politiekorpsen verplichtend informatie delen voor een effectiever optreden."
[78] Antecedenten geven aan dat jegens iemand een proces-verbaal is opgemaakt als verdachte van een strafbaar feit en de beslissing van het OM of de rechter daarover.

- Lid 3: ten behoeve van de afstemming van verschillende verwerkingen binnen de politie jegens eenzelfde persoon .

In de Wpg 2008 was in de protocolplicht opgenomen dat voor artikel 13-verwerkingen het noodzakelijk is dat de korpschef van tevoren bij elke artikel 13-verwerking een reglement verzorgt waarin beschreven is voor welk doel deze gegevens verder verwerkt worden, om wat voor gegevens het gaat en hoe lang de gegevens verwerkt worden. Met de nieuwe Wpg is deze eis teruggekomen in de vorm van de registerplicht; zie artikel 31d.

De mogelijkheid om verbanden te leggen tussen gegevens (artikel 11)

Bij het (actief) ter beschikking stellen van politiegegevens is verdere verwerking voor andere doelen afhankelijk van degene die de gegevens oorspronkelijk verwerkt. Alleen als deze weet dat ze nodig zijn voor een ander doel, zal hij de gegevens daarvoor ter beschikking stellen. Dit brengt het risico met zich mee dat gegevens die wel voor een ander doel van belang zijn, daarvoor niet beschikbaar komen. De Wpg bevat daarom nog twee zoekmogelijkheden. Daarmee kan rechtstreeks worden gezocht in politiegegevens die voor andere doeleinden zijn verwerkt: geautomatiseerd vergelijken en in combinatie verwerken (zie artikel 8 lid 2 en 3 en artikel 11). Hierbij maakt niet degene die de gegevens oorspronkelijk verwerkt ze voor andere doeleinden beschikbaar. Maar het is degene die voor dat andere doel gegevens nodig heeft, die zoekt in gegevens die voor andere doeleinden zijn verwerkt.

Geautomatiseerd vergelijken is de meest toegepaste vorm van zoeken in gegevens. Je wilt vaststellen of bepaalde gegevens uit de ene gegevensverzameling ook voorkomen in andere gegevensverzamelingen binnen het Wpg-domein. Alleen gegevens die al beschikbaar zijn voor het doel van je huidige verwerking, mogen daarvoor gebruikt worden.[79] De gevonden gegevens kunnen verder verwerkt worden in de eigen verwerking voor zover deze noodzakelijk zijn. Denk aan hits na een bevraging in [redacted] of [redacted]. Het Besluit politiegegevens regelt in de artikelen 2:11 en 2:12 hoe de resultaten van een geautomatiseerde vergelijking zichtbaar worden.

Artikel 11 lid 5: vergelijken met niet-politiegegevens

Politiegegevens mogen ook geautomatiseerd worden vergeleken met andere persoonsgegevens dan politiegegevens. Dit is uitgewerkt in artikel 11 lid 5. Dit kan alleen ten behoeve van een artikel 9 en 10-verwerking. Het is daarbij van belang of gegevens zijn binnengehaald (bijvoorbeeld na vordering door de officier) of niet. Zijn de gegevens het politiedomein binnengehaald, dan is er géén sprake van een 11 lid 5-verwerking. De gevorderde of op andere wijze (bijvoorbeeld van internet of andere openbare bronnen) verkregen gegevens worden dan gewoon verwerkt op basis van art. 8, 9, 10 of 13. Blijft het gegevensbestand extern (buiten de gegevensverzameling die valt onder de Wpg), dan vindt er een vergelijking plaats zoals dit bedoeld is in art. 11 lid 5 Wpg. De vergelijking wordt dus extern, door of onder toezicht van de politie en op haar verzoek uitgevoerd. De politie ontvangt en verwerkt vervolgens de resultaten in de bestaande gegevensverwerking.

Bij een gewelddadige verkrachting van een drieënzestigjarige vrouw vermoedt het opsporingsteam dat de dader een band heeft met de buurt waar het misdrijf gepleegd is. Er wordt een extract uit [redacted] opgevraagd met speciale aandacht voor [redacted]. Hoe maakt de Wpg zo'n vergelijking mogelijk en welke voorwaarden zijn daaraan gebonden?

Artikel 11 lid 5 biedt de mogelijkheid om politiebestanden te vergelijken met bestanden van partners. De bevoegd functionaris zorgt ervoor dat aan de voorwaarden wordt voldaan. De vergelijking moet in elk geval schriftelijk worden vastgelegd. Dit betekent dat een aanmeldformulier verstuurd moet worden naar de privacyfunctionaris met daarin beschreven welke gegevens gebruikt zijn in de zoekvraag en welke gegevens verder worden verwerkt.

Je bent bezig met een artikel 9-analyse rondom woonfraude. Daarbij combineer je een extract uit het [redacted] met gegevens uit [redacted]. Is dat toegestaan?

Artikel 11 lid 5 biedt de mogelijkheid om politiebestanden te vergelijken met bestanden van partners. De bevoegd functionaris, leider van het onderzoek, zorgt ervoor dat aan de voorwaarden wordt voldaan.

[79] Memorie van Toelichting bij de Wpg, pagina 52-53.

Alle artikel 11-verwerkingen moeten conform de protocolplicht schriftelijk worden vastgelegd. Dit betekent dat de privacyfunctionaris een overzicht dient te hebben dat beschrijft welke gegevens gebruikt zijn in de zoekvraag en welke gegevens verder worden verwerkt. Een deel hiervan wordt automatisch ingevuld door loggingsfunctionaliteit.

Artikel 11 lid 4 : in combinatie verwerken

Wat onder in combinatie verwerken van politiegegevens dient te worden verstaan is niet in de Wpg gedefinieerd. Het is ruimer dan geautomatiseerd vergelijken, want alle beschikbare politiegegevens kunnen worden geraadpleegd, doorzocht en gecombineerd, bijvoorbeeld door het stellen van samengestelde zoekvragen of analyseren aan de hand van bepaalde profielen van daders, slachtoffers of feiten. Dit is een verstrekkende bevoegdheid waarbij onbeperkt geanalyseerd wordt en zeer geavanceerde zoekmethoden kunnen worden toegepast, bijvoorbeeld [redacted]. Als gebeurt in het kader van een artikel 9-of 10-verwerking, zijn daar voorwaarden aan verbonden: het mag alleen worden gedaan door daartoe aangewezen en opgeleide informatiemedewerkers, er moet sprake zijn van een bijzonder geval en het bevoegd gezag moet er opdracht voor geven. Verder geldt dat –als er verbanden blijken te bestaan – de bevoegd functionaris van het oorspronkelijke onderzoek instemming moet verlenen om de gerelateerde gegevens verder te verwerken.[80]

[redacted]. Wat voor soort verwerking is dit en wat zijn de voorwaarden?

Dit is een artikel 11 lid 4 verwerking. Dit omdat bestanden worden samengevoegd en in combinatie worden verwerkt. Hiervoor geldt dat dit alleen mag 'in bijzondere gevallen', door daartoe bevoegde informatiemedewerkers. Het bevoegd gezag toetst van tevoren de aanvraag voor deze verwerking.

Bovenmatigheid en dataminimalisatie

De Wpg schrijft in artikel 3 lid 2 voor dat gegevens niet bovenmatig mogen zijn; er mogen dus niet 'te veel' gegevens verwerkt worden. Dataminimalisatie betekent dat er zo min mogelijk persoonsgegevens verwerkt moeten worden; alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.[81]Het gemak van digitale communicatie en de grote hoeveelheden gegevens die we als politie voorhanden hebben, maakt niet dat we alles klakkeloos kunnen gebruiken en delen. Zo is het berekenen en opslaan van een geweldsindicator voor alle personen die [redacted] voorkomen, een bovenmatige verwerking. Het doet er niet aan af dat een persoon een score 'niets aan de hand' krijgt. Voor personen die aangehouden zijn geweest, verdachten en veroordeelden, is het uit te leggen dat we een dergelijke indicator standaard berekenen. Dat is noodzakelijke informatie voor een juiste bejegening bij een toekomstig contact. Voor een aangever of getuige is dit echter niet goed uit te leggen. Dus mag een dergelijke indicator niet voor iedere persoon die [redacted] voorkomt, standaard berekend worden.

Toezicht en verantwoording

Een belangrijk beginsel van gegevensbescherming is transparantie. De politie moet zich kunnen verantwoorden voor al haar handelingen: vooraf bijvoorbeeld door een zorgvuldige autorisatieregistratie, achteraf doordat handelingen inzichtelijk en controleerbaar zijn. In de Wpg is op verschillende manieren voorzien in toezicht op de naleving van de wet. Zo moeten diverse verwerkingen gelogd worden, er moet een register worden aangelegd waarin alle verwerkingen beschreven zijn, er moeten periodiek audits worden uitgevoerd en er is voorzien in intern en extern toezicht.[82]

---

[80] Zie ook de Aanwijzing Wet politiegegevens en de rol van de Officier van Justitie
[81] De Autoriteit Persoonsgegevens beschouwt dataminimalisatie als een belangrijk concept voor Privacy by Design.
[82] In paragraaf vijf van de Wpg zijn deze maatregelen uitgewerkt.

Documentatieplicht en logging
De Wpg verplicht in artikel 32 tot de schriftelijke vastlegging van een aantal zaken. Voorheen heette dit de protocolplicht, nu de documentatieplicht. Door dit te doen, wordt het mogelijk na te gaan of de politie zich aan de spelregels houdt. Zo moeten de doelomschrijvingen van de artikel 9-verwerkingen worden vastgelegd, maar ook de datalekken die zich hebben voorgedaan, de redenen om inzage te weigeren (artikel 27 lid 1) en de handmatige verstrekkingen. Artikel 32 a bevat de plicht tot logging.

Herkomst en wijze van verkrijging
In verband met de vereiste juistheid en nauwkeurigheid van politiegegevens verplicht de Wpg (art. 3 lid 5) dat voor artikel 9, 10 en 12-gegevens de herkomst en wijze van verkrijging worden vastgelegd. Mocht een rechter of advocaat verzoeken om duidelijkheid hierover, moet de politie in staat zijn die meteen te verschaffen.

Rechten betrokkene
Voor personen over wie gegevens in de politiesystemen staat (betrokkene) bestaat het recht om kennis te nemen van de gegevens die over hem verwerkt worden. Ook heeft hij recht op correctie van gegevens en 'het recht vergeten te worden'. Een ieder kan schriftelijk verzoeken of er, en zo ja welke, politiegegevens over hem of haar verwerkt worden en in welke gevallen deze gegevens de afgelopen vier jaar verstrekt zijn (artikel 25 lid 1 Wpg). Hieronder vallen dus ook de gegevens die niet meer beschikbaar zijn voor de operatiën. Aan een verzoek om kennisneming hoeft niet altijd voldaan te worden. Een verzoek kan worden afgewezen als dat noodzakelijk is in het belang van de goede uitvoering van de politietaak, de bescherming van de rechten van de betrokkene of van de rechten en vrijheden van derden of de veiligheid van de staat (art. 27 lid 1).

Registerplicht
Ten aanzien van elke verwerkingsactiviteit (bijvoorbeeld applicaties en gegevensbestanden) moet een schriftelijk register worden bijgehouden (art. 31 d Wpg en artikel 30 AVG). Dit is een nieuwe verplichting met de komst van de gewijzigde Wpg. Daarbij moeten onder andere het volgende worden vastgelegd:
- de doelen van de verwerking;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van verstrekkingen;
- de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;
- een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging;
- de toekenning van de autorisaties.

BIJLAGE 3: de Wpg-wetsfamilie
Geldig op 1 januari 2016

Regelgeving die op deze regeling is gebaseerd (gedelegeerde regelgeving)

1. Aanpassingsbesluit basisregistratie personen
2. Aanpassingsbesluit openbare lichamen Bonaire, Sint Eustatius en Saba
3. Aanpassingsbesluit Politiewet 2012
4. Beleidsregels CBP handhaving protocolplicht Wet politiegegevens
5. Besluit beheer politie
6. Besluit ex artikel 18, tweede lid, Wet politiegegevens, houdende opdracht en toestemming aan korpschef landelijk politiekorps tot verstrekken politiegegevens aan colleges van B&W
7. Besluit gegevensverstrekking ongebruikelijke transacties BES
8. Besluit Jeugdwet
9. Besluit modern migratiebeleid
10. Besluit politiegegevens
11. Besluit politiegegevens bijzondere opsporingsdiensten
12. Besluit ter voorkoming van witwassen en financieren van terrorisme BES
13. Besluit verplichte politiegegevens
14. Mandaatbesluit Wet Politiegegevens FIOD-ECD
15. Regeling team criminele inlichtingen FIOD
16. Regeling team criminele inlichtingen Inspectie SZW-DO

17. Regeling toezichtsbevoegdheden functionaris voor de gegevensbescherming EL&I
18. Uitvoeringsbesluit Wet ter voorkoming van witwassen en financieren van terrorisme
19. Verlenging Wpg-machtigingsbesluit RIEC's/werkproces integrale casusanalyse
20. Verzamelbesluit evaluatie en uitbreiding Wet Bibob
21. Wijzigingsbesluit Vreemdelingenbesluit 2000 (meldingsformaliteiten schepen die aankomen in en/of vertrekken uit havens en tot intrekking Richtlijn 2002/6/EG)

Beleidsregels en circulaires die betrekking hebben op deze regeling

1. Aanwijzing Wet politiegegevens en de rol van de Officier van Justitie
2. Aanwijzing afstemmingsprotocol onderzoeksraad voor de veiligheid - openbaar ministerie

Artikelen of vergelijkbare tekst die verwijzen naar deze regeling

1. Aanwijzing Opsporingsberichtgeving, beleidsregel 2017A007 Tekst
2. Aanwijzing Wet politiegegevens en de rol van de Officier van Justitie: tekst
3. Aanwijzing auditief en audiovisueel registreren van verhoren van aangevers, getuigen en verdachten Bijlagen: 2, 3
4. Aanwijzing inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken (552i Sv.)Tekst: tekst
5. Aanwijzing opsporingsbevoegdheden: tekst
6. Aanwijzing uitbreiding identificatieplicht: tekst
7. Aanwijzingen voor de regelgeving artikel: 162b
8. Algemene wet bestuursrechtBijlage: 1
9. Beleidsregel CBP richtsnoeren ANPRTekst: tekst
10. Beleidsregels CBP handhaving protocolplicht Wet politiegegevens: tekst
11. Beleidsregels actieve openbaarmaking door het CBP, artikel: 1
12. Besluit bewaren en vernietigen niet-gevoegde stukken, artikel: 3
13. Besluit instelling criminele-inlichtingeneenheid ILT-IOD 2012Artikelen: 2, 3, 5, 9
14. Besluit politiegegevens
15. Besluit politiegegevens bijzondere opsporingsdiensten Artikelen: 1, 2
16. Besluit verplichte politiegegevensArtikelen: 5, 9
17. Circulaire bewaking en beveiliging van personen, objecten en diensten 2015Tekst: tekst
18. Gemeentewet Artikel: 151c
19. Luchtvaartwet Artikel: 37s
20. Mandaatbesluit Wet Politiegegevens FIOD-ECD Artikelen: 2, 3
21. Organisatie-, mandaat- en volmacht besluit directie Opsporing 2012Artikel: 6
22. Politiewet 2012 Artikelen: 24, 54
23. Regeling beheer politiekorps BES Artikel: 4
24. Regeling instelling criminele-inlichtingeneenheid NVWA-IOD Artikelen: 2, 3, 5, 9
25. Regeling periodieke audit politiegegevens Artikelen: 1, 2, 3, 4, 5, 6
26. Regeling team criminele inlichtingen FIOD Artikelen: 2, 3, 8
27. Regeling team criminele inlichtingen Inspectie SZW-DO Artikelen: 2, 3, 8
28. Regeling toezichtsbevoegdheden functionaris voor de gegevensbescherming EL&I Artikel: 1
29. Regels verzoek om zienswijze CBP inzake verwerking persoonsgegevens: tekst
30. Reglement verwerking gegevens kentekenregister 2009 Artikel: 3
31. Veiligheidswet BES Artikel: 14
32. Voorschrift Vreemdelingen 2000Artikel: 7.1e
33. Algemene Verordening Gegevensbescherming
34. Wet bevordering integriteitsbeoordelingen door het openbaar bestuur Artikel: 27
35. Wet openbare lichamen Bonaire, Sint Eustatius en Saba Artikel: 156

36. Wet ter voorkoming van witwassen en financieren van terrorisme Artikel: 13
37. Wet ter voorkoming van witwassen en financieren van terrorisme BES Artikel: 3.2
38. Wet veiligheidsonderzoeken Artikelen: 7, 9, 13
39. Wetboek van Strafvordering Artikelen: 125n, 126dd, 126hh

BIJLAGE 4: Toelichting gegevensmodellen

Bedrijfsbegrippen

Een bedrijfsbegrip is een woord dat gebruikt wordt in de uitvoering van het politiewerk. Een bedrijfsbegrip is een equivalent dan een begripsdefinitie: het gaat het om een woord of een samenstel van woorden die een eenheid van kennis vormen omtrent een concept in een bepaalde context. Een begripsdefinitie is een omschrijving van wat in een bepaalde context met een begrip wordt bedoeld, zodat het begrip eenduidig te onderscheiden is van gerelateerde begrippen. Eenduidige begripsdefinities vormen een hulpmiddel om te komen tot één gemeenschappelijke taal. Met goed geformuleerde definities is het voor iedereen duidelijk wat onder een bepaald begrip wordt verstaan.
Het doel van de Leidraad opstellen begripsdefinities is:

- Het bieden van een gemeenschappelijke taal waarmee medewerkers met elkaar de bedrijfsprocessen en informatieprocessen kunnen bespreken en verder kunnen ontwikkelen.
- Het voorkomen van interpretatieverschillen bij het toepassen van de gemeenschappelijke taal bij het opstellen van bedrijfsregels.

Bedrijfsbegrippen worden gebruikt bij het opstellen van bedrijfsregels. De IM-organisatie ondersteunt bij het opstellen en onderhouden van begripsdefinities. Borging en delen van bedrijfsbegrippen wordt gefaciliteerd door de afdeling Gegevensgebruik en -beheer.

Bedrijfsregels

Bedrijfsregels zijn regels die specifiek voor het politiewerk gelden. Alleen al vanuit de wet zijn dit er nogal wat. Het gaat dan om verwerkingstermijnen of om de vraag wanneer een bijzondere opsporingsbevoegdheid gehanteerd mag worden of wanneer terugkoppeling gegeven moet worden over een aangifte. Maar ook een beperking, bijvoorbeeld dat van een zelfde incident maar één keer aangifte gedaan mag worden, is een bedrijfsregel. [redacted] De Leidraad opstellen bedrijfsregels[83] beschrijft hoe op een eenduidige wijze werkbare aanwijzingen opgesteld kunnen worden op basis van een gemeenschappelijke vocabulaire. Het doel van deze leidraad is:

- Het bieden van een gemeenschappelijke taal waarmee business experts en IV-experts met elkaar de bedrijfsprocessen kunnen bespreken en inzichtelijk maken.
- Hanteren van ondubbelzinnige bedrijfsregels en bedrijfsadviezen die begrijpelijk zijn voor de werkvloer en welke als basis kunnen dienen voor de inrichting van de bedrijfsprocessen.
- Eenvoudige vertaling mogelijk maken naar implementeerbare aanwijzingen voor de ontwikkeling van geautomatiseerde hulpmiddelen.
- Deze leidraad is vooral bestemd voor bedrijfsanalisten, informatieanalisten en architecten.

Bedrijfs Objecten Model (BOM)

Het BOM biedt een taal voor afstemming tussen business en IV en business onderling. Deze taal komt met name terug in user-interfaces en in informatieproducten. Hoger gelegen doelen waaraan het BOM bijdraagt, zijn eenduidige informatiedeling binnen de politie en met de keten, eenduidige en betrouwbare intelligence (door het scherp krijgen van de informatiebehoefte), minder dubbele invoer en een hogere kwaliteit van gegevens.

De bedrijfsbegrippen en het BOM zijn een onderdeel van de informatiearchitectuur in Project Start Architectuur-documenten (PSA's), waarbij het als kader maar tevens als vliegende start dient voor het project. Begrips- en objectendefinities, relaties en regels hoeven immers niet elke keer opnieuw geïnventariseerd, bediscussieerd en beschreven te worden omdat dit al gebeurd is. Als er binnen een project nieuwe inzichten komen op het model, worden deze door de beheerder van het BOM weer in het model verwerkt. Het BOM is gepubliceerd en voor alle belanghebbenden toegankelijk[84].

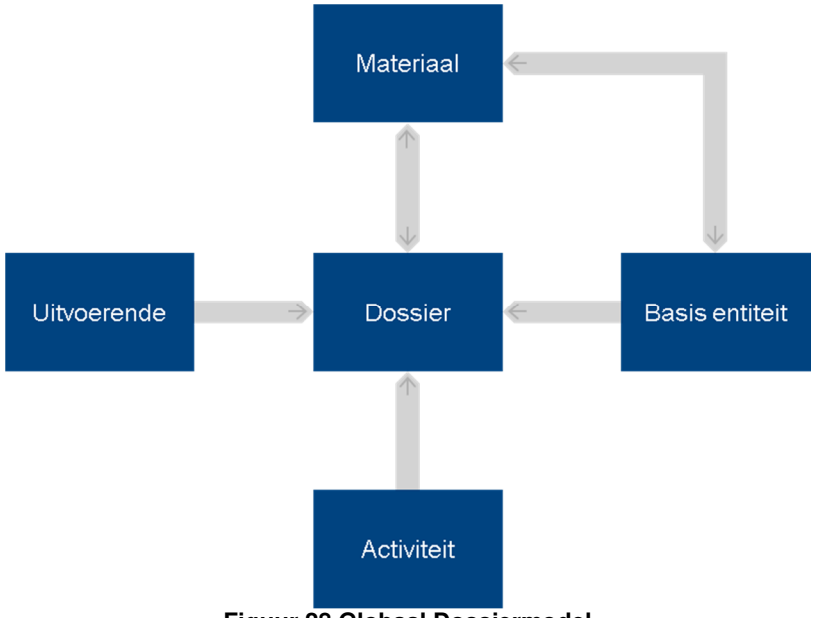
Politie Gegevens Model (PGM)

In het BOM is de basis gelegd voor een gemeenschappelijke taal met de executieve politiecollega's. Er is echter een wezenlijk verschil tussen de natuurlijke taal waarmee mensen met elkaar communiceren en de taal waarmee

[83] Zie Leidraad opstellen bedrijfsregels op Agora
[84] Zie [redacted]/Gegevensmodellen.aspx

systemen met elkaar 'praten' en interacteren met eindgebruikers van dat systeem. Omdat computers geen betekenis kunnen verlenen aan de symbolen die ze verwerken, moet er noodgedwongen een grote versimpeling plaatsvinden van de rijkdom en ambiguïteit van de menselijke taal. Een andere reden is dat door formalisering de software en algoritmiek, die op de ingevoerde gegevens wordt toegepast, veel eenvoudiger en functioneel rijker te maken is. Het PGM heeft tot doel de informatievoorzieningen voor het operationeel proces te voorzien van een gemeenschappelijke structurele basis voor de vastlegging en uitwisseling van gegevens. Alle informatievoorzieningen voor het operationele proces "praten" in deze taal met elkaar. Het PGM dient zowel om structuur te geven aan de vastlegging van gegevens als aan het uitwisselen en verstrekken van de gegevens. Zo is het PGM ook de basis voor de gegevensuitwisseling met [redacted] Het verband tussen het BOM en het PGM bestaat uit het leggen van verbanden van bedrijfsobjecten naar hun implementaties in PGM-klassen (met attributen), associaties daartussen en bijhorende bedrijfsregels. Hierdoor wordt gerealiseerd dat er een consistentie- en volledigheidsvalidatie plaatsvindt tussen de informatiebehoefte uit de business en de IV-ondersteuning daarvan. Uitbreiding en onderhoud van het PGM wordt uitgevoerd door de IM-afdeling GGB (Gegevensgebruik en -beheer). Het PGM is gepubliceerd en voor alle belanghebbenden toegankelijk[85].

Dossiermodel
De kennis vanuit het PGM wordt hergebruikt bij de (door)ontwikkeling van het dossiermodel en wordt daarin overgenomen. Het dossiermodel is (net als PGM) object-georiënteerd en is in het kader van [redacted] opgesteld om het operationele werk van de politie met ICT te ondersteunen[86]. Dit werk wordt uitgevoerd door politiemedewerkers en teams. In onderstaand schema is dat weergegeven door “Uitvoerende”. Een dossier is “een samenhangend geheel van gegevens en gedrag betrekking hebbende op één onderwerp ten behoeve van regie, uitvoering of overzicht”[87].



Figuur 28 Globaal Dossiermodel

Andere beschrijvende metagegevens

Naast gegevensmodellen worden van informatieobjecten de (uitvoering van) gegevensverwerking ook andere metagegevens vastgelegd, zoals rubricering en kwaliteitseisen.

Rubricering (IB) betreft de classificatie met betrekking tot betrouwbaarheid en vertrouwelijkheid; dit wordt verder uitgewerkt bij het principe Informatiebeveiliging.

Kwaliteitseisen worden gedefinieerd vanuit de gebruiksdoelen van de gegevens. Voor het formuleren van de kwaliteitseisen maakt de politie gebruik van een raamwerk van kwaliteitskenmerken. Voor meer informatie zie het principe Kwaliteitszorg. Het opstellen en onderhouden van het raamwerk is een verantwoordelijkheid van de beleidsverantwoordelijke die daarbij ondersteund wordt door de Dienst IM en de teams Kwaliteit van Informatie (KvI).

---

[85] [redacted]/Gegevensmodellen.aspx
[86] Wikipedia beschrijft wat object-georiënteerd inhoudt: https://nl.wikipedia.org/wiki/Objectgeorienteerd
[87] Informatiemodel [redacted]

BIJLAGE 5: Betrokkenen

Bij de totstandkoming van versie 2.0 van deze publicatie zijn de volgende personen betrokken geweest:

Rol	Naam	Functie
Opdrachtgever		
Schrijver/ opdrachtnemer		
Klankbordgroep		
Reviewgroep		
Ambassadeur		

Bij de totstandkoming van versie 1.0 (juni 2017) van deze publicatie zijn de volgende personen betrokken geweest:

Rol	Naam	Functie
Opdrachtgever		
Schrijver/ opdrachtnemer		
Klankbordgroep		
Reviewgroep		
Ambassadeur		

BIJLAGE 6: Basisopleidingen waar Wpg in verankerd wordt

Initiële opleidingen:

- (assistent) politiemedewerker (N2 en 3)
- PO 2.0
- Bachelor Politiekunde
- Master Recherchekunde
- AOPV/BOA

Intelligence:

- Verzamelen en verwerken van informatie
- Analyseren van informatie
- Het heimelijk inwinnen van informatie

Leidinggevende opleidingen:

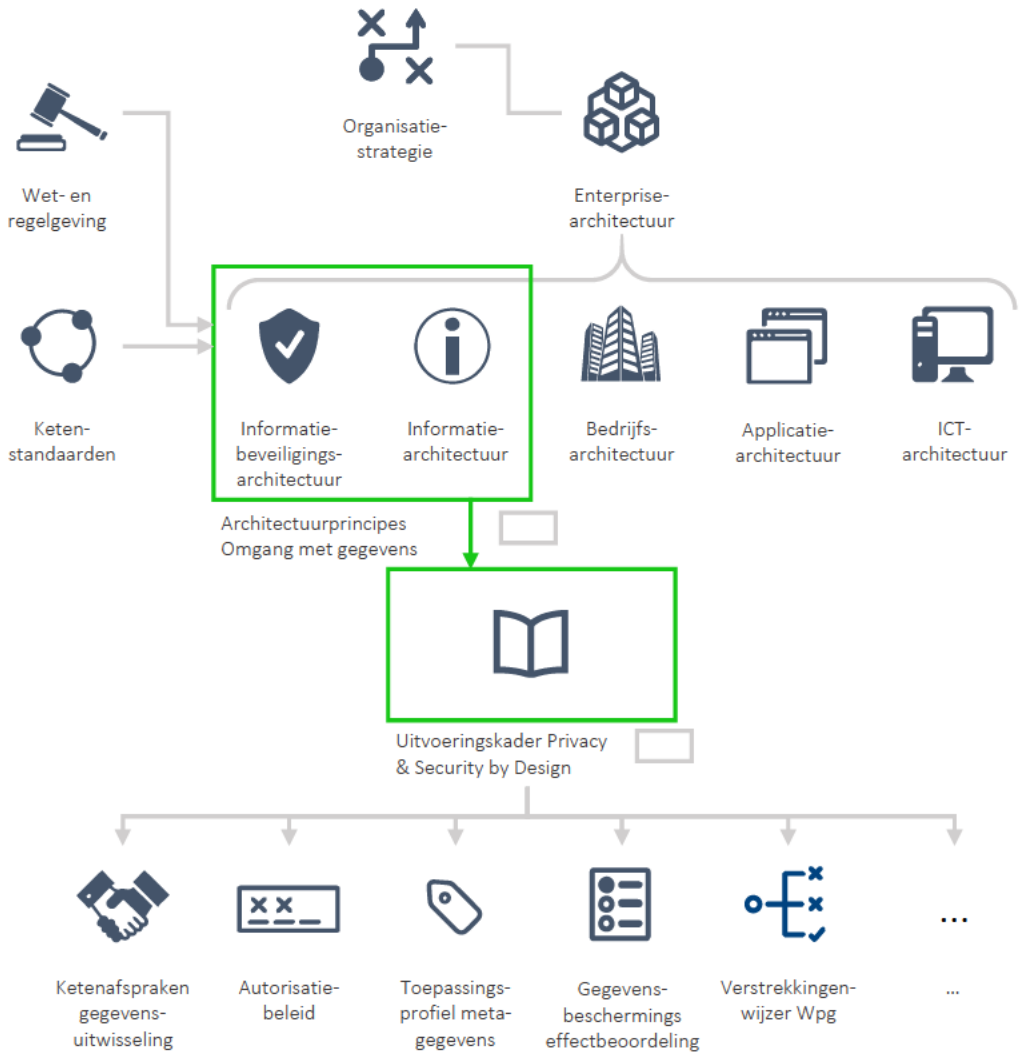
- Leergang Operationele Sturing
- Master Tactisch Leidinggeven

Overige opleidingen:

- Generalist Meldkamer
- Rechercheren in een meeromvattende zaak
- SGBO
- Leergang Wijkagent

BIJLAGE 7: Overzicht kaders en richtlijnen

In deze bijlage wordt een overzicht gegeven van alle kaders en richtlijnen die bij het schrijven van dit uitvoeringskader gebruikt zijn. De kaders en richtlijnen zijn geordend volgens het positioneringsschema dat in hoofdstuk is toegelicht.



Figuur 29 Positionering van kaders en richtlijnen voor Privacy & Security by Design

In het uitvoeringskader Privacy & Security by Design worden alle uitvoeringskaders voor de omgang met gegevens samengevat.

Enterprise Architectuur

1. EA VenJ De Afspraken, m.n. Domein 3: gegevens

Informatiebeveiligingsarchitectuur

2. Informatiebeveiliging – Architectuur tactisch niveau, versie 1.0, juni 2016
3. Rubriceringsregeling Politie, versie 1.0, 23 maart 2015
4. Autorisatiebeleid, 27 januari 2016

Informatiearchitectuur

5. Informatiearchitectuur, versie 2.1, 21 februari 2018
6. Definitie en criteria voor kernregisters, versie 1.0, 26 januari 2016
7. Ontwerpkader Toepassingsprofiel Metagegevens Politie, versie 1.1, 29 september 2016
8. Leidraad opstellen begripsdefinities, versie 1.6, oktober 2016
9. Leidraad opstellen bedrijfsregels, 10-2-2016.

Wet- en regelgeving

10. Algemene verordening gegevensbescherming (AVG) en de Richtlijn,
11. De Wpg 2008 en het Bpg

12. Het wetsvoorstel Wpg en de Memorie van Toelichting.

Ketenstandaarden

13. Nederlandse Overheid Referentie Architectuur, NORA versie 3.0
14. Kwaliteitseisen voor de duurzame toegankelijkheid van overheidsinformatie (DUTO), versie 1.0
15. CBP Richtsnoeren Beveiliging van Persoonsgegevens 2013
16. Standaarden Informatievoorziening Strafrechtsketen, 1 februari 2014
17. Architectuur van de Vreemdelingenketen, februari 2013

Uitvoeringskaders

18. Generieke selectielijst voor de documentaire informatie van de politie vanaf 1 januari 2013, versie 0.12
19. Kaders die richting geven aan het verwijderen en vernietigen van gegevens in de registratieve politiesystemen:
    a. Beschrijving vernietigen van gegevens in BVH, versie 1.0, 26 juli 2016
    b. Uitgangspunten en principes voor de schoning van onderzoeksgegevens uit Summ-IT conform de Wpg, versie 1.1, 9 september 2015
    c. Inrichting poortwachtersorganisatie nav Wpg-schoning BVH, 9 juni 2015
    d. Uitgangspunten en principes voor de schoning van BVH, 21 januari 2015
    e. Notitie relatie Wpg, Archiefwet en Selectielijst Politie
20. Uitvoeringsregeling Informatiebeveiliging Dienst-ICT Politie Intern en Politie Confidentieel, 2016.
21. Gebruik productiedata voor testen, ontwikkelen en/of opleiden, versie 2.0, augustus 2016
22. Eindrapport Autorisatiemodel, juni 2013
23. Uitvoeringskader: Verantwoordelijkheid voor gegevens februari 2018
24. Visie op terugmelden, 13-10-2015
25. Verstrekkingenwijzer, versie 2.0, 1 augustus 2016 2016-08-01_verstrekkingenwijzer_Wpg.
26. Praktijkhandboek Wpg, 08-05-2017
27. Beleidskader voor security en Wpg-compliancy in BVI: BVI Inrichting voor Security en Wpg-Compliancy V1.02
28. GEB, sjabloon GEB
29. Wpg Bedrijfsregels (pdf)
30. Handleiding Privacy by Design – CIP, Centrum Informatiebeveiliging en privacybescherming, 7-5-2017
31. Proces meldplicht datalekken, 15-03-2016

Projectstartarchitecturen

De applicatiearchitecturen OPP en BVI zijn beschikbaar als PSA's. De rol van PSA's bij de kaderstelling voor gegevensverwerking zullen we behandelen in hoofdstuk 1 van het uitvoeringskader. Daarnaast kunnen we bezien om de kaders op te nemen van thema-architecturen, zoals de thema-architectuur Business Intelligence of de thema-architectuur multimedia.

BIJLAGE 8: Afkortingen

ANPR	Automatic NumberPlate Recognition
Art.	(wets)artikel
AT	Arrestatieteam
AVG	Algemene Verordening Gegevensbescherming
AVP	Aanvalsprogramma informatievoorziening Politie
BAG	Basisregistraties Adressen en Gebouwen
BF	Bevoegd functionaris
BGT	Basisregistratie Grootschalige Topografie
BI	Business Intelligence
Bjsg	Besluit justitiële en strafvorderlijke gegevens
BLAU	Basisregistratie voor Lonen, Arbeidsverhoudingen en Uitkeringen
BOB	Bijzondere opsporingsbevoegdheden
BOD'en	Bijzondere opsporingsdiensten
BOM	Bedrijfsobjectenmodel Nederlandse Politie
Bpg	Besluit politiegegevens
Bpgbo	Besluit politiegegevens bijzondere opsporingsdiensten
Bpgbo	Besluit politiegegevens bijzondere opsporingsdiensten
BRP	Basisregistratie personen
BRV	Basisregistratie Voertuigen (kentekenregister)

BSN	Burger Service Nummer
BVI	Basisvoorziening Informatie
CDD+	Centraal Digitaal Depot
CDO	Chief Data Officer/Gegevensautoriteit
CISO	Chief Information Security Officer
DICT	Dienst ICT
DIV	Documentaire Informatievoorziening
EDP	Electronic Data Processing
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst - Economische Controle Dienst
GA	Gegevensautoriteit
GGB	Gegevensgebruik- en beheer
IAM	Identity & Access Management
ICT	Informatie en Communicatie Technologie
ILT-IOD	Inspectie Leefomgeving en Transport – Inlichtingen en Opsporingsdienst
IM	Informatiemanagement
IMDM	Programma Integraal Mediabeleid en Digitale Media
ISZW	Inspectie Sociale Zaken en Werkgelegenheid
IT	Informatietechnologie
IV	Informatievoorziening(en)
JD online	Justitieel Documentatiesysteem
JustID	Justitiële Informatiedienst
KMar	Koninklijke Marechaussee
KvI	Kwaliteit van Informatie
LFNP	Landelijk Functiehuis Nederlandse Politie
MvT	Memorie van Toelichting
NHR	Nederlands Handelsregister
NvT	Nota van Toelichting
NVWA-IOD	Nederlandse Voedsel- en Warenautoriteit Inlichtingen- en Opsporingsdienst
OPP	Operationeel Politie Platform
PGM	Politie Gegevens Model
RBP	Referentiemodel Bedrijfsprocessen Politie
SKDB	Strafrechtketen Database
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
[redacted]	[redacted]
[redacted]	[redacted]
Wbp	Wet bescherming persoonsgegevens
Wjsg	Wet Justitiële en strafvordelijke gegevens
Wob	Wet openbaarheid bestuur
WODC	Wetenschappelijk Onderzoeks- en Documentatiecentrum
Wpg	Wet politiegegevens
Wpolr	Wet politieregisters
WvSr	Wetboek van Strafrecht
WvSv	Wetboek van Strafvordering