Verbeterplan Wet politiegegevens en Informatiebeveiliging

Gegevensautoriteit

Status: definitief

Maart 2016

Rubricering: Openbaar

«waakzaam en dienstbaar»

POLITIE

Inhoudsopgave

1. Inleiding

Eind 2015 heeft de Auditdienst Rijk (ADR) aan de korpschef gerapporteerd over de in 2014 en 2015 uitgevoerde (externe) privacy audit. De ADR concludeert in dit rapport dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, naar de stand van ultimo december 2014, in opzet, bestaan en werking niet of niet geheel voldeed aan de vereisten van de Wet politiegegevens (Wpg).

De Minister van Veiligheid en Justitie heeft op 7 december 2015 de Tweede Kamer bij brief geïnformeerd over deze auditrapportage, over de uitkomsten van het onderzoek van het College bescherming persoonsgegevens naar de naleving door de politie van informatiebeveiligings- en gegevensbeschermingsvoorschriften van het Schengen Informatiesysteem (NSIS-II) en over het auditrapport van de ADR naar de beveiliging van het Europees Visum Informatiesysteem (EUVIS). De minister heeft in zijn brief aan de Tweede Kamer aangekondigd dat de korpschef, die een eigenstandige verantwoordelijkheid heeft op het gebied van de Wpg, aanvullende maatregelen zal nemen, uit te werken in een verbeterplan. De afspraken die de korpschef hierover met de minister heeft gemaakt zijn tevens in de brief aan de Tweede Kamer verwoord.

Dit verbeterplan bevat een overzicht van de maatregelen die de politie de komende jaren neemt om beter aan de Wpg te voldoen en bevat tevens de maatregelen op het gebied van informatiebeveiliging die moeten leiden tot het oplossen van de tekortkomingen die zijn geconstateerd in de onderzoeken naar EUVIS en NSIS-II. Met het uitvoeren van deze maatregelen zal de politie eind 2019 (de duur van het programma) grotendeels maar nog niet volledig de Wpg naleven. Het volledig kunnen naleven van de Wpg vergt onder andere aanpassingen in de huidige wetgeving en aanpassing of vervanging van bestaande (oudere) informatiesystemen. Dit zal niet allemaal binnen de looptijd van dit programma kunnen worden gerealiseerd. De verandering om tot de gewenste situatie te komen is dan wel in gang gezet.

2. Uitgangspunten verbeterplan

2.1. Analyse huidige situatie

De ADR geeft in haar rapportage aan dat de reorganisatie waar de politie zich in bevindt een continuïteitsrisico vormt voor de borging van de Wpg, ook omdat de Wpg op een aantal personen binnen de politie 'hangt'. De ADR overweegt verder dat de politie de Wpg nog te veel ziet als een 'losstaand project', terwijl dit onderdeel uit zou moeten maken van alle politiewerkprocessen. Tegelijkertijd ondersteunen de IV-systemen, zo stelt de ADR, de gebruikers onvoldoende, waardoor onevenredig veel inspanning is vereist om de Wpg-normen na te kunnen leven.

In de evaluatie van de Wpg uit 2013, uitgevoerd in opdracht van het WODC, wordt het beeld van een 'worstelende praktijk' geschetst. De minister heeft in reactie op deze evaluatie aangekondigd de Wpg en de eveneens geëvalueerde Wet justitiële en strafvorderlijke gegevens in onderlinge samenhang te zullen herzien. Deze herziening heeft ten doel de complexiteit van beide wetten voor de uitvoeringspraktijk terug te dringen en de toepasbaarheid ervan in de keten te vergroten. Bovendien zal de Wpg op korte termijn moeten worden aangepast als gevolg van de komende nieuwe algemene verordening gegevensbescherming en een nieuwe richtlijn gegevensbescherming voor het politie- en justitiedomein.

In de Herijkingsnota van 31 augustus 2015, die de herijking van de realisatie van de nationale politie beschrijft, wordt erkend dat de vorming van de nationale politie op een aantal gebieden nog niet de verwachte kwaliteitsimpuls geboden heeft. Als knelpunten bij de realisatie van de reorganisatie worden genoemd:

1. Er moet teveel tegelijkertijd.
2. Vertraging personele reorganisatie.
3. Meer ruimte voor lokaal maatwerk nodig.
4. Kennis en kunde voor verandering en functioneren als concern onvoldoende aanwezig.

Al deze knelpunten spelen, in meerdere of mindere mate, ook een rol bij het niet kunnen voldoen aan de eisen van de Wpg. Denk daarbij onder meer aan het gecompliceerde applicatielandschap als erfenis uit de voormalig korpsen, het uniformeren van vele politieprocessen (inclusief Wpg-aspecten) en onvoldoende personele capaciteit voor de inrichting van een Wpg-loket.

Ondanks deze knelpunten zijn sinds de vorming van de nationale politie grote stappen genomen in het ontwikkelen van de informatiebeveiliging van een maatregelgedreven aanpak naar een risicogeoriënteerde aanpak. Hiertoe zijn informatiebeveiligingsbeleid en -kaders opgesteld die de inhoudelijke normen beschrijven waarlangs de gehele organisatie dient te werken en die gebruikt worden voor het vormgeven van toezicht op de realisatie van informatiebeveiliging. Dit is een omvangrijke operatie die nog in volle gang is. Bevindingen over de aansluiting tussen strategisch, tactisch en operationeel niveau vinden hierin hun oorsprong. Dit betreft ook het in gang gezette proces van risicoafweging door lijnverantwoordelijkheden waarbij de lijn bepaalt, binnen de gestelde kaders, wat wel en wat niet op te lossen door maatregelen.

Al met al heeft het korps meer tijd nodig voor de veranderopgave en daarmee voor het volledig in werking brengen van de nieuwe organisatie. Dit geldt des te meer voor het voldoen aan de Wpg. Dit is namelijk – zoals de ADR ook opmerkt - tevens afhankelijk van de IT-ontwikkelingen. De herijking maakt inzichtelijk waarom de aandacht voor de Wpg de afgelopen jaren onvoldoende is geweest. Dit onderwerp moet namelijk concurreren met het op peil houden van de politieprestaties in een tijd waarin ook veel aandacht uitgaat naar de reorganisatie.

Aangezien bovengenoemde situatie voorlopig voortduurt wordt daar bij de formulering van de verbetermaatregelen, inclusief bijbehorend tijdspad en kosten, rekening mee gehouden.

2.2. Integrale aanpak

Dit verbeterplan gaat uit van een integrale aanpak waarbij verschillende maatregelen in samenhang worden ingevuld, zowel in de Operatiën als in de IV. Hoewel de aanpak zo complexer lijkt, is juist deze samenhang de sleutel tot duurzame borging. Hieronder volgt een schets van de elementen die in de aanpak in elk geval aan bod komen.

1: Wpg en informatiebeveiliging worden verankerd in de IV en IV-organisatie
De mogelijkheid van IT-ondersteuning bij de naleving van de wettelijke vereisten zal nadrukkelijk benut worden. Dit zal de naleving in de praktijk aanzienlijk vereenvoudigen, ook vanwege de reductie van administratieve lasten voor politieambtenaren.
De reden dat aanpassing van de informatievoorziening bij eerdere projecten geen prioritair onderwerp is geweest, ligt in het feit dat het de afgelopen jaren slechts beperkt mogelijk was verbetermaatregelen op applicatieniveau door te voeren. Binnen het Aanvalsprogramma Informatievoorziening Politie (AVP) lag de focus namelijk op het verbeteren van de continuïteit en stabiliteit van de informatievoorziening. Nu continuïteit en stabiliteit van de IV zijn gerealiseerd is er binnen het AVP meer aandacht voor verbetering en vernieuwing. Onderdeel van deze vernieuwing is dat ontwikkelaars bij het ontwerp van nieuwe applicaties deze zo vormgeven dat politiemedewerkers goed ondersteund worden in het naleven van de regels uit de Wpg; privacy & security by design is de norm. Dit wordt bereikt door gegevensbescherming een standaard en vast onderdeel te maken in het werk van de Dienst IM en in het verlengde daarvan ook de Dienst ICT.

Hierbij dienen de verwachtingen overigens realistisch te zijn. Door budgettaire beperkingen en een diversiteit aan prioriteiten bij systeemontwikkeling zal het programma primair inzetten op het inbrengen, borgen en monitoren van eisen ten aanzien van privacy en informatiebeveiliging bij nieuwe systemen. Verbeteren in de bestaande basispolitiesystemen zoals Summ-IT en BVH is een langdurig proces, dat stap voor stap verloopt.

2: De Wpg is onderdeel van werkprocessen:
Dat informatie in praktisch elk politieproces een rol speelt, zal voor elke politieman /-vrouw duidelijk zijn, maar of bij de verwerking van die gegevens overeenkomstig de Wpg wordt gehandeld niet. Het streven is dat deze naleving niet alleen geïntegreerd onderdeel uitmaakt van de IT-systemen, maar van het gehele werkproces. De Directie Operatiën krijgt dan ook een expliciete rol bij de actualisering van bestaande en ontwikkeling van nieuwe werkinstructies en –procedures ten behoeve van de naleving van de Wpg, maar ook bij de implementatie daarvan bij de eenheden.

3: De Wpg en informatiebeveiliging zijn onderdeel van sturing en control
De verbetermaatregelen van het programma zijn erop gericht de lijn in staat te stellen te sturen op de naleving van de Wpg en op aandacht voor informatiebeveiliging. Aan de hand van risico- en control matrices die per proces de belangrijkste risico's voor niet naleving van de Wpg en de bijbehorende controls in kaart brengen, worden overzichten gegenereerd. Met behulp van die overzichten zal de organisatie beter dan nu in staat gesteld worden te monitoren en bij te sturen op naleving van de Wpg. Hierdoor wordt ook actieve sturing mogelijk en kan iedere leidinggevende op zijn niveau zijn verantwoordelijkheid nemen voor het naleven van de Wpg. In managementgesprekken kan vervolgens de effectiviteit van de genomen sturingsmaatregelen worden besproken.

4: De Wpg en informatiebeveiliging zijn een vast onderdeel in basis- en vervolgopleidingen
Hoewel in de eenheden op uiteenlopende wijze aandacht is besteed aan opleiding & training en communicatie & awareness, moet het door de ADR geconstateerde gebrek aan kennis leiden tot het continueren van de lijn van het Wpg-project 2013-2015. Nu de Wpg en informatiebeveiliging in de IV en de IV-organisatie, in de werkprocessen en in de sturing en control zal worden verankerd, zal de inzet op opleiding & training en communicatie & awareness naar verwachting meer effect hebben dan in het eerdere traject. Dit betekent opnieuw grote inzet op opleiding & training en communicatie & awareness, waarbij de inzet van de Politieacademie onontbeerlijk is. Het is van belang dat dit onderwerp in alle geledingen van de eenheden en het PDC aandacht krijgt. Deze eis geldt nadrukkelijk niet alleen voor het uitvoerende, maar ook voor het leidinggevende niveau. De tijdens de vorige fase ontwikkelde werkinstructies zijn daarbij reeds beschikbaar, maar nog onvoldoende (korps)breed bekend.

Beseft moet worden dat het opleiden en trainen van medewerkers een doorlopend proces is. Dat de Wpg en informatiebeveiliging integraal verwerkt moet zijn in de basis- en vervolgopleidingen staat buiten kijf, maar de noodzaak om het onderwerp daarna continu aandacht te geven is nog onvoldoende onderkend en mag niet geïsoleerd benaderd worden. Een speciaal ontwikkeld communicatieprogramma zal ondersteunend aan de opleiding zorgdragen voor een voldoende niveau van awareness.

Speciaal daartoe opgeleide trainers in de eenheden hebben een grote bijdrage geleverd aan kennisvergroting en bewustwording, maar op den duur zal de Wpg onderdeel uit moeten maken van verplichte toetsmomenten. Omdat er niet altijd tijd en ruimte is om naar een opleiding te gaan, zijn de zogeheten profchecks ontwikkeld om snel juridische kennis up-to-date te houden. Omdat de Wpg samen met de Politiewet 2012 en het Wetboek van Strafvordering de belangrijkste wettelijke kaders vormt, dient ook de Wpg goed geïntegreerd te worden in de bestaande profchecks. Daarnaast wordt er een aparte profcheck ontwikkeld om de Wpg-kennis en het privacy bewustzijn goed te verankeren. Deze profchecks worden in de toekomst verplicht gesteld zodat daarmee is gewaarborgd dat alle medewerkers hun Wpg-kennis ontwikkelen.

2.3. Borging gegevensbescherming en informatiebeveiliging

Ondanks de omvangrijke reorganisatie staat er nu één korps dat beter dan tevoren operationeel kan samenwerken. Een korps dat de prestaties op peil heeft gehouden en verbeterd en dat tijdens een aantal grootschalige en complexe evenementen de veiligheid heeft gegarandeerd. Dit is, gezien de grote veranderingsoperatie die gaande is, een goede prestatie die niet onderschat mag worden. Ook op het gebied van gegevensbescherming en informatiebeveiliging is de politie positief over de toekomst. De aandacht voor gegevensbescherming is beter geborgd dan mogelijk was in het decentrale bestel. In 2013 is opdracht gegeven om te komen tot de inrichting van een Gegevensautoriteit en een Informatiebeveiligingsautoriteit, ondergebracht bij de Staf Korpsleiding en respectievelijk aangestuurd door een Chief Data Officer (CDO) en een Concern Information Security Officer (CISO). Beide rollen maken centrale regie mogelijk op de kwaliteit en beveiliging van informatie. Dit is een belangrijke maatregel om goed aan wet- en regelgeving te voldoen met betrekking tot de gegevensbescherming.

Door een integrale aanpak, zoals beschreven in paragraaf 2.2., waarbij om te beginnen ingezet wordt op optimale ondersteuning door de IV bij de naleving van de Wpg en aandacht wordt besteed aan sturing en control, heeft dit programma een betere kans van slagen dan ooit.

3. Uitvoering verbeterplan door programma

3.1. Doel verbeterplan

Het verbeterplan heeft als doel inzichtelijk te maken hoe in de periode 2016 tot en met 2019 de overtredingen op de Wpg en de tekortkomingen in het stelsel van informatiebeveiliging aangepakt en uiteindelijk opgelost zullen worden. Daarnaast geeft het plan inzicht in hoe een instrumentarium ontwikkeld wordt dat de politie in staat stelt om beter dan nu het geval is te sturen op (dreigende) overtredingen van de Wpg of beveiligingsincidenten.

3.2. Realistisch en haalbaar

De minister heeft in zijn brief aan de voorzitter van de Tweede Kamer aangegeven dat het verbeterplan realistisch en haalbaar dient te zijn, met een ambitieus toekomstperspectief. Dit plan bevat de maatregelen die hieraan invulling geven. Gedurende de loop van het programma zullen deze maatregelen gaan leiden tot een voldoende naleving van de Wpg op de gebieden informatiebeveiliging, autoriseren, rechten van betrokkene, gevoelige gegevens, ter beschikking stellen, geautomatiseerd vergelijken en in combinatie verwerken, audit, de privacyfunctionaris en in control. Daarnaast zullen binnen de termijn van het programma de maatregelen worden ingevoerd voor de geconstateerde bevindingen in de EUVIS en NSIS-II audits.

Op de overige onderwerpen zoals bijvoorbeeld bewaartermijnen kunnen binnen het programma deeloplossingen worden ingevoerd, omdat huidige wetgeving, bestaande (oudere) informatiesystemen of complexiteit in de ketensamenwerking verhinderen dat een afdoende oplossing wordt gerealiseerd binnen de duur van het programma. De verwachting is dat op handen zijnde wijzigingen in wet- en regelgeving een oplossing naderbij brengt. Op deze onderwerpen zal in dat geval ook substantiële verbetering mogelijk blijken.

3.3. Lijn en programma

De eindverantwoordelijkheid voor een goede informatiebeveiliging en het naleven van de Wpg ligt bij de korpschef, welke deze voor de eenheden heeft gemandateerd naar de politiechefs. Deze worden hierbij ondersteund door de Informatiebeveiligingsautoriteit en de Gegevensautoriteit en dienen deze verantwoordelijkheid in te vullen binnen de kaders zoals vastgesteld door de Korpschef. Iedere politiechef heeft daarnaast nog een tweede (beleidsmatige) verantwoordelijkheid voor een goede informatiebeveiliging en het naleven van de Wpg. Namelijk voor de thema's waarvoor hij binnen de politie als portefeuillehouder verantwoordelijk is, zoals bijvoorbeeld Intelligence of Jeugd. Ook hier spelen informatiebeveiliging en privacy een belangrijke rol met name op het gebied van innovaties waarbij privacy by design en security by design de leidende kaders zijn.

Met de inrichting van een Gegevensautoriteit en een Informatiebeveiligingsautoriteit bij de vorming van de nationale politie is meer centrale regie mogelijk op de kwaliteit (privacy) en beveiliging van informatie door beleid en kaders. Door het aantal en de ernst van de bevindingen uit de audits is gekozen een programma in te stellen om in nauwe samenwerking met de operatie versneld een aantal doelen te realiseren en bevindingen op te lossen. Uitganspunt hierbij is dat de staande organisatie zo veel en zo snel mogelijk de regie op de naleving (her-)opneemt. Hiertoe zal het programma daar waar nodig in samenwerking met de eenheden aanvullend of nieuw beleid en kaders ontwikkelen en zorgdragen voor de invoering hiervan binnen de informatievoorziening of de operationele processen. Voor deze vorm is gekozen omdat de naleving van de Wpg en het opvolgen van de bevindingen uit de EUVIS en NSIS-II audits vraagt om een meerjarige aanpak die zorgt dat:

• operatie en IV samenwerken;
• op meerdere kennisgebieden;
• en meerdere plekken in de organisatie;
• soms met een interventie in de lijn, en
• soms met een project.

Het programma zal zich daarbij richten op die activiteiten die niet regulier door de staande organisatie worden uitgevoerd. Daarbij krijgen de ernstige bevindingen prioriteit en wordt de invoering van de meer complexe oplossingen ook in het programma belegd.

3.4. Programma governance

Met de vaststelling van het verbeterplan door de Korpsleiding krijgt de stuurgroep de opdracht om het verbeterplan uit te werken in deelplannen. Deze deelplannen worden waar nodig vastgesteld in het Breed Operationeel Overleg (BOO) of het Breed Bedrijfsvoeringsoverleg (BBVO) en daarna verwerkt in het bestaande planning & control instrumentarium.

De realisatie van de deelplannen is de verantwoordelijkheid van de stuurgroep die hiertoe de programmamanager opdracht geeft. Deze stuurt op het bereiken van de voorgestelde oplossingen.

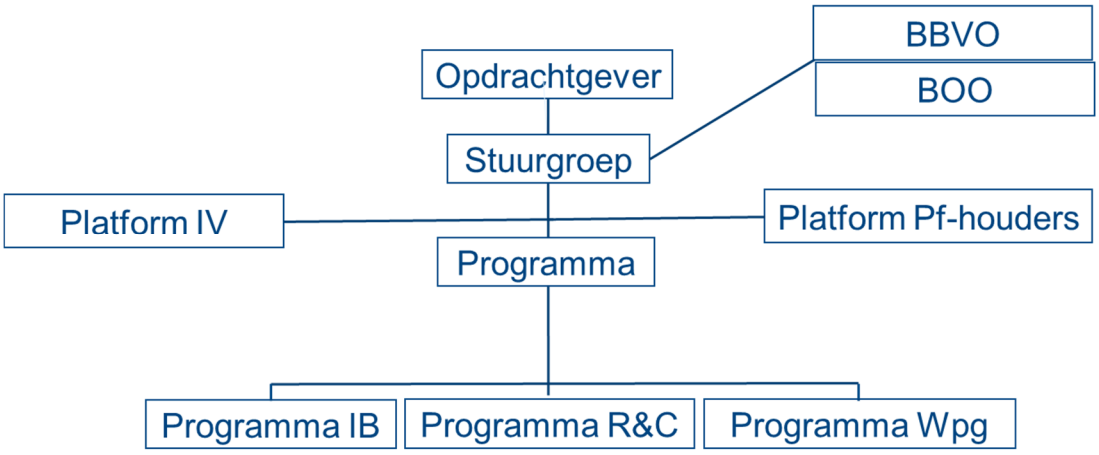
Opdrachtgever voor het verbeterplan is de directeur Informatievoorziening. Voor kwesties waarvoor de besluitvorming ontoereikend verloopt, zal de opdrachtgever verdere benodigde actie ondernemen in lijn met het besturingsmodel.

Voor de besturing van het programma is gekozen voor een samenstelling van de stuurgroep die een evenwichtige representatie geeft van de betrokken partijen en de integrale aanpak. Voorzitter van de stuurgroep is een hoofd Operatiën, welke tevens lid is van een eenheidsleiding. Verder maken een hoofd Bedrijfsvoering van een andere eenheid, ook lid van een eenheidsleiding, de CDO, de CISO en de landelijke programmamanager deel uit van de stuurgroep.

Het hoofd Operatiën vertegenwoordigt tevens de personen binnen de organisatie die binnen de eenheden verantwoordelijk zijn voor de correcte naleving van de Wpg. Via zijn deelname aan het Breed Operationeel Overleg is geborgd dat alle strategisch verantwoordelijken in de eenheden op dit gebied op de hoogte blijven en hun invloed hebben op de besluitvorming. Evenzo kan het programma kwesties in de programma-uitvoering in dit overleg via deze lijn aan de orde stellen.

Het hoofd Bedrijfsvoering vertegenwoordigt de deelnemers aan het Breed Bedrijfsvoeringsoverleg waar Informatiebeveiliging in portefeuille is. Via zijn deelname aan dit overleg is geborgd dat alle verantwoordelijken in de eenheden op dit gebied op de hoogte blijven en hun invloed kunnen hebben op de besluitvorming. Evenzo kan het programma kwesties in de programma-uitvoering in dit overleg via deze lijn aan de orde stellen.

De CDO en de CISO bewaken tevens de aansluiting van het programma binnen de IV-kolom



Het platform van portefeuillehouders Wpg van de eenheden en het politiedienstencentrum (PDC) dient als adviesraad aan de stuurgroep en kan gevraagd en ongevraagd adviseren over plannen, uitvoering en resultaten van het programma.

Met de diensten IM en ICT zal nauwe afstemming zijn door deelname van vertegenwoordigers van deze diensten in het programmateam en een platform IV, waarin alle betrokken onderdelen vertegenwoordigd zullen zijn.

Voor afstemming en communicatie zal de programmamanager nauw samenwerken met de ondersteuners van de portefeuillehouders in de eenheden. Deze portefeuilleondersteuners kunnen het programma voorzien van noodzakelijke input en criteria op grond waarvan prioriteiten gesteld worden en keuzes gemaakt worden. Zij ondersteunen daarnaast hun portefeuillehouder in het borgen van de gekozen oplossingen binnen hun eenheid. De programmamanager draagt, in verbinding met de portefeuilleondersteuners, zorg voor uniformiteit in inrichting en uitvoering, zodat processen en uitkomsten uniform blijven.

Ten slotte zal gebruik worden gemaakt van bestaande overleggen en rapportagelijnen ter advisering en om samenwerking te bewerkstelligen.

3.5. Aanpak

Aangezien de politie zich nog volop aan het inrichten is en er vele initiatieven en verbeterprojecten lopen, zoekt het programma maximaal aansluiting bij deze initiatieven om privacy- en informatiebeveiligingscriteria in te brengen en zo meerwaarde te creëren, zoals het Aanvalsprogramma en het project Autoriseren. Aangezien de beoogde oplossingsrichtingen impact kunnen hebben op alle gebieden binnen de politie, is gekozen om de Centrale Ondernemingsraad nauw te betrekken bij de opzet en invulling van het programma.

Daarnaast zijn de volgende randvoorwaarden aan het programma meegegeven;

- De programmawerkwijze moet faciliterend zijn aan reeds lopende en/of geplande activiteiten.
- De programmaorganisatie is daartoe ingericht als een ondersteunende hulpstructuur vergelijkbaar met de werkwijze van het programma Administratieve lastenverlichting.
- Maatregelen met betrekking tot informatiebeveiliging vallen onder de verantwoordelijkheid van de CISO en worden aldaar begroot en uitgevoerd.

- Het programma voert geen eigen automatiseringsprojecten uit maar levert haar wensen via de geëigende kanalen aan waardoor ze onderdeel worden van de bestaande besluitvormingsprocessen voor ontwikkeling en beheer van ICT.
- De bemensing van het programmateam bestaat uit eigen (evt. nog te werven/zoeken) politiepersoneel met mogelijk een uitzondering voor specialistische functies.

3.6. Programmabeheersing en rapportages

Dit verbeterplan wordt na vaststelling uitgewerkt in deelplannen per onderwerp aan de hand waarvan de stuurgroep en de programmamanager de overeengekomen doelen kunnen realiseren. De deelplannen geven in aanvulling op dit verbeterplan een overzicht van de activiteiten die gedurende de looptijd van het programma zullen worden uitgevoerd en koppelen per jaarschijf mensen en middelen aan deze activiteiten middels een concrete tijdsplanning. Aan de hand van rapportages aan het programma door al lopende projecten wordt de voortgang op de maatregelen ten aanzien van informatiebeveiliging en autorisaties inzichtelijk gemaakt. Vervolgens zal inzichtelijk worden gemaakt wat de voortgang is en wat de kosten zijn, zodat sturing mogelijk wordt voor alle relevante gremia.

3.7. Duur van het programma en keuzes in activiteiten

Gekozen is voor een programmaduur van 2016 tot en met 2019. Na deze periode is er sprake van een duidelijke verbetering van de naleving van de Wpg en de kwaliteit van de informatiebeveiliging, maar zullen er nog projecten en activiteiten lopen. De verantwoordelijkheden zullen dan echter zodanig zijn belegd en ondersteund door een solide management control, dat sturing op deze projecten en activiteiten vanuit de lijn mogelijk is.

Voor de basisplanning van het verbeterplan is om twee redenen gekozen om op diverse onderwerpen activiteiten op te starten in 2016. Ten eerste omdat er een aantal acties zijn die direct kunnen bijdragen aan een betere naleving van de Wpg en de kwaliteit van informatiebeveiliging en ten tweede omdat er een aantal projecten en activiteiten moeten starten met een langere doorlooptijd en het van belang is om snel zicht te hebben op de effectiviteit van deze projecten, zodat tijdig bijgestuurd kan worden.

Prioriteit wordt gegeven aan de onderwerpen die door de Minister van Veiligheid en Justitie zijn aangewezen: autoriseren, informatiebeveiliging en rechten van betrokkene. Daarnaast wordt direct gestart met het ontwikkelen van risico- en control matrices en het de verbeteracties op het gebied van opleiden en trainen.

4. Inbedding P&C cyclus

4.1. Impact verbeterplan

De korpsleiding heeft met de vaststelling van dit verbeterplan een besluit genomen over de volgorde en de mate waarin uitvoering gewenst is. Het programma kent een looptijd van vier jaar waarbij zowel inhoudelijke IV ambities, wijzigingen in de politieorganisatie en werkprocessen en aanpassingen in de basisopleidingen worden voorgestaan. De beoogde maatregelen voor 2017 en verder zullen in de loop van dit jaar verwerkt worden in fase 2 van het reorganisatietraject, in de reguliere begrotings- en bedrijfsvoeringcycli en (de in ontwikkeling zijnde) portfolioprocessen zoals het IV-portfolio. Dat is tot nu toe voor het onderwerp Wpg in zijn totale samenhang nog niet eerder aan de orde geweest.

In 2016 zal gestart worden met de door de minister benoemde prioriteiten:

- Voor informatiebeveiliging is de belangrijkste verbeteractie het actueel, juist en volledig maken van tactische en operationele documentatie.
- Voor het onderwerp autorisaties betekent dit het in werking brengen van de IAM-tool (Identity Access Management) inclusief het daarbij horende beleidsmatige instrumentarium.
- Het onderwerp Rechten van betrokkene zal geborgd worden door de inrichting van een afdeling per eenheid waar de verzoeken worden afgehandeld, ondersteund door een landelijk werkend systeem dat tevens in staat zal zijn passende managementinformatie op te leveren.

Verder zal in 2016 de nadruk liggen op de voorbereiding van activiteiten die in 2017 zullen opstarten door het opstellen van impactanalyses, projectplannen en het verkrijgen van financiële middelen en menskracht door de verwerking van de plannen in de planning & controlcyclus.

4.2. Incidentele programmakosten 2016

Door de gekozen opzet kunnen de kosten voor het programma in 2016 beperkt blijven tot incidentele inhuur en het organiseren van expertsessies. De dekking hiervoor is geregeld door opname van de programmakosten ad € 500.000,00 in het IV-portfolio 2016. De kosten voor activiteiten op het gebied van autorisaties zijn gedekt in de begroting van het AVP en de kosten voor inhuur op het gebied informatiebeveiliging vallen ten laste van het reguliere budget van de directie IV.

Voor de latere jaren zal een nadere uitwerking van de kosten worden opgesteld aan de hand van de in 2016 te verrichten impactanalyses.

Nadere uitwerking

In december 2015 heeft de Korpsleiding de interne en de door de ADR uitgevoerde externe audit vastgesteld. Deze audits hadden, in afstemming met de AP, een focus op de vijf voor de politie meest risicovolle onderwerpen (autoriseren, verstrekken, protocolleren, bewaartermijnen, rechten van betrokkene). Op de overige zeven onderwerpen die met de audits onderzocht zijn is een statusupdate uitgevoerd.

In deze bijlage worden bovengenoemde onderwerpen aan de hand van de bevindingen uit de audits behandeld. Eerst worden het wettelijk kader en de context van dit onderwerp bij de politie geschetst. Vervolgens worden eindtermen benoemd. Dit zijn de doelen die uiteindelijk gerealiseerd moeten worden om op een voldoende niveau van naleving van de Wpg en kwaliteit van informatiebeveiliging te komen. Ten slotte zullen de belangrijkste verbetermaatregelen zoals die nu zijn benoemd worden weergegeven.

In de loop van dit programma kunnen eindtermen worden bijgesteld bijvoorbeeld door de inwerkingtreding van de Europese richtlijn gegevensbescherming voor opsporing en vervolging (hierna; de richtlijn), en maatregelen worden vervangen bijvoorbeeld omdat er betere alternatieven worden ontwikkeld voor de nu gekozen oplossingen.

1. Informatiebeveiliging

Artikel 4
De verantwoordelijke treft passende technische en organisatorische maatregelen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via directe geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's van de verwerking en de aard van de politiegegevens.

1.1. Algemeen

Informatiebeveiliging is een belangrijke voorwaarde voor het optimaal functioneren van de politie. De juiste maatregelen voor informatiebeveiliging kunnen voorkomen dat onbevoegden van binnen of buiten de politie toegang krijgen tot gegevens of de continuïteit van de uitvoering van de politietaak verstoren. Dit is van cruciaal belang voor zowel operationele als bedrijfsvoeringsprocessen en heeft bovendien betrekking op verschillende soorten informatie. Anders dan de overige onderdelen van het programma zien de activiteiten en maatregelen op het gebied van informatiebeveiliging dan ook niet alleen op de naleving van de Wpg.

De CISO blijft in de lijn eindverantwoordelijk voor het stellen van de kaders en uitgangspunten en het in werking brengen van het stelsel van informatiebeveiliging. Vanuit de CISO wordt gestuurd op structurele verbetering. De structurele verbetering richt zich op het in lijn brengen van het beleid en de uitvoering door onder andere het uitvoeren van beveiligingsanalyses. Deze analyses worden in eerste aanleg uitgevoerd voor de primaire politieprocessen. Verwacht wordt dat de maatregelen voor deze processen een grote overlap zullen gaan vertonen met de latere analyses voor de bedrijfsvoering. In de afgelopen periode zijn op hoofdlijnen de belangrijkste politieprocessen doorgenomen, waaruit aandachtspunten zijn ontstaan voor verdere analyse.

In de transitie van maatregel naar risicobeheersing is afgesproken dat geen enkele maatregel wordt uitgefaseerd zonder expliciet besluit. Dit om kwetsbaarheden in de uitvoering te voorkomen.

De versterking vanuit het programma richt zich op de zes constateringen uit de audits EUVIS en NSIS-II (zie paragraaf 1.2). Daarbij dient te worden opgemerkt dat deze verbeteringen generiek worden opgepakt en een nauwe samenhang hebben met de overige activiteiten aangestuurd vanuit de CISO.

1.2. Bevindingen audits

De door of in opdracht van het AP uitgevoerde audits op de systemen EUVIS en NSIS-II hebben tot een aantal bevindingen geleid die zijn samen te vatten tot:

1. Beveiligingsstelsel: de strategische lijn voor informatie beveiliging is niet geheel doorgewerkt in de tactische en operationele documentatie. Hierdoor is het moeilijk te beoordelen of maatregelen in lijn zijn met het risico gebaseerde beleid.
2. Toegangsrechten en personeelsprofielen: het autorisatiemechanisme van de politie is onvoldoende vormgegeven. Daardoor kan men niet in alle gevallen beoordelen of toegekende autorisaties terecht zijn.
3. Toekennen van autorisaties en controle op toegekende autorisaties: De politie houdt onvoldoende toezicht op de naleving van het autorisatiemodel. Met name onvoldoende zicht op autorisaties bij ketenpartners
4. Beveiligingsincidenten: de aanpak en de werkwijze van incidenten is onvoldoende geborgd in de organisatie waardoor het potentieel afhankelijk is van de persoon die deze oppakt.
5. Controle gebruik logging: De politie benut de logging onvoldoende om signalen van atypisch gedrag te onderkennen en zo mogelijk daarop preventief te reageren.
6. Opleiding personeel: in de basisopleiding en in de structurele herhaling is in de opleiding van het personeel onvoldoende aandacht voor informatiebeveiliging en specifiek voor de desbetreffende verwerking toepasselijke (Europese) wet- en regelgeving.

Hoewel deze constateringen gedaan zijn op basis van de audits naar de twee genoemde systemen zijn de aanbevelingen generiek van aard. De politie zal de verbeteringen daarom generiek aanpakken, met dien verstande dat als bij de implementatie prioriteit gegeven moet worden aan systemen de verbeteringen voor de twee genoemde systemen voorrang krijgen.

De bovengenoemde constateringen 2 en 3 ten aanzien van autoriseren en het toezicht daarop worden apart behandeld in hoofdstuk 2.

1.3. Eindtermen

Onderstaande eindtermen beschrijven de normen die in het kader van het programma bereikt moeten worden ten behoeve van de verdere verbetering van de informatiebeveiliging. De verbetermaatregelen worden gedurende het programma in gang gezet (conform de tabel bij 1.4). Niet alle eindtermen worden binnen de periode van het programma bereikt.

Eind 2016 levert het programma de volgende resultaten op:

- De servicedesks HR, FM, IM (autoriseren) en ICT (servicedesk) zijn geïnstrueerd hoe om te gaan met informatiebeveiligingsincidenten en de meldplicht datalekken.
- De door de CISO gedefinieerde drempelwaarde voor escalatie bij incidenten en datalekken is geïmplementeerd.
- Servicemedewerkers (van de vier genoemde organisaties) zijn opgeleid met betrekking tot dit terrein.

Eind 2017 levert het programma de volgende resultaten op:

- Basisopleiding executief: eindtermen informatiebeveiliging en privacy zoals verder verwoordt in de overige hoofdstukken van dit plan mede in relatie tot (inter)nationale wet- en regelgeving en de operationele praktijk.
- Herhalingsopleiding executief (OBT voorheen IBT): vormgeven van herhalingsmodules informatiebeveiliging en privacy zoals verder verwoordt in de overige hoofdstukken van dit plan en bewerkstelligen dat ieder jaar ten minste vier uur van de opleiding hiervoor wordt gereserveerd.

Eind 2018 levert het programma de volgende resultaten op:

- Tactische en operationele documentatie betrekking hebbend op informatiebeveiliging is, actueel, juist en volledig. Aan de hand van indexatie en versiebeheer is te beoordelen of maatregelen overeenkomstig het vigerend beleid zijn. Van de tien prioritaire onderwerpen zijn de uitvoeringsregelingen opgesteld en vastgesteld, doordat relevante uitvoeringsregelingen en de hiaten in kaart zijn gebracht.

1.4. Verbetermaatregelen

1 Beveiligingsstelsel
Ten aanzien van het beveiligingsstelsel en het in lijn brengen van de tactische en operationele documentatie loopt op dit moment – onder regie van de CISO – het traject om te komen tot een informatiebeveiligingsarchitectuur. Deze architectuur zal enerzijds een deel van de documentatie in lijn brengen, anderzijds de kaders scheppen voor het in lijn brengen van de overige documentatie.

De onderstaande twee punten worden hier geadresseerd;

a) indexeren van operationele documentatie. Het voorzien van een ontsluitingsindex op alle nog relevante operationele documentatie op het gebied van beveiliging welke deze documentatie in lijn brengt met de architectuur zonder de documentatie te herschrijven.
b) uitvoeringsregelingen opstellen. Daar waar hiaten geconstateerd worden in het operationaliseren van het beleid richting medewerkers of de uitvoeringsorganisaties wordt zo nodig een uitvoeringsregeling opgesteld in lijn met het bovenliggende beleid.

Eind 2018 levert het verbeterprogramma de volgende resultaten op;

- Operationele documentatie is geïnventariseerd en aan de lijn is voorgelegd welke nog relevant zijn of welke afgeschaft kunnen worden. Relevante operationele documenten zijn:
  - voorzien van een index
  - tenminste in een 1.0 versie vastgesteld
- Relevante uitvoeringsregelingen en de hiaten zijn in kaart gebracht en van de tien prioritaire onderwerpen zijn de regelingen opgesteld en vastgesteld.

2 Toegangsrechten en personeelsprofielen
Zie hoofdstuk 2

3 Toekennen van autorisaties en controle op toegekende autorisaties
Zie hoofdstuk 2

4 Beveiligingsincidenten
Implementatie van het in 2015 opgestelde proces omtrent informatiebeveiligingsincidenten door de dienst ICT, dienst IM en directie IV. Randvoorwaardelijk daarvoor is dat de lijn van de CISO zorg draagt voor vaststelling voor dit proces uiterlijk mei 2016. In 2016 zal de CISO met ketenpartners afspraken maken over incidentafhandeling en melding.

Eind 2016 levert het verbeterprogramma de volgende resultaten op:

- gerichte instructies voor de servicedesks HR, FM, IM (autoriseren) en ICT (servicedesk) hoe om te gaan met informatiebeveiligingsincidenten en de wet op datalekken.
- het implementeren van de drempelwaarde voor escalatie bij incidenten en datalekken.
- het opleiden van de servicedeskmedewerkers (van de vier genoemde onderdelen) op dit terrein.

5 Controle gebruik logging
De CISO/ Informatiebeveiligingsautoriteit zal het voortouw nemen om in samenspraak met VIK korpsstaf te komen tot een voorstel voor het proactief toezicht. Onderdeel daarvan zal zijn of en hoe in te regelen is om atypisch gedrag te signaleren. Gelet op de mogelijke consequenties voor medewerkers wordt de Centrale Ondernemingsraad (COR) hierbij betrokken.

Het voorstel zal ingaan op verschillende categorieën personeel, waarbij het uitgangspunt is hoe hoger de toegangsrechten hoe meer proactief toezicht. De mogelijkheden voor proactief toezicht in de systemen zal functioneel behelzen dat er afgesproken wordt wat normaal en wat afwijkend gedrag is. De norm kan verschillen per categorie medewerkers, een generalist recherche zal wellicht een ander aantal abonnementen hebben dan een medewerker TCI. Leidinggevenden zullen in een dergelijk traject een belangrijke rol hebben bij het prudent toekennen van autorisaties en het waakzaam monitoren van het gebruik.

Of het voorstel uiteindelijk gerealiseerd zal gaan worden is afhankelijk van meerdere factoren. Zodra besluitvorming heeft plaatsgevonden moet bezien worden of en in hoeverre de implementatie in het verbeterprogramma ingebed kan worden.

6 Opleiding personeel
Het verbeterprogramma zorgt in afstemming met de PA voor een opleidingsplan voor diverse doelgroepen.

Eind 2017 levert het verbeterprogramma de volgende resultaten op:
- het ontwerpen van eindtermen en een opleidingssystematiek
- het regelen van besluitvorming over de opleidingsplannen. Voorlopig wordt uitgegaan van:
    - Basisopleiding executief: eindtermen informatiebeveiliging en privacy mede in relatie tot internationale wet- en regelgeving (inclusief het inregelen).
    - Herhalingsopleiding executief (OBT voorheen IBT): vormgeven van herhalingsmodules informatiebeveiliging en privacy en het inregelen dat ieder jaar ten minste vier uur van de opleiding hiervoor wordt ingeregeld.
    - Het inregelen van een herhalingsprogramma voor administratief/ technisch personeel voor informatie beveiliging en privacy van ten minste 8 uur per jaar en het vormgeven van de inhoud van de modules.
    - Het inregelen van alle decentrale introductieprogramma's in het korps informatiebeveiliging en privacy opnemen.

Eind 2018 levert het verbeterprogramma de volgende resultaten op:
- het inregelen van de opleidingen/cursussen voor informatiebeveiliging

	Noodzakelijke maatregel	**2016**	**2017**	**2018**	**2019**	**Betrokkenen**	**Budgettaire impact**
1	Indexeren van operationele documentatie					Diensten IM en ICT	Inhuur 2 FTE
2	Uitvoeringsregelingen opstellen in lijn met bovenliggende beleid					Diensten IM en ICT	
3	Implementatie proces voor opvolging informatiebeveiligingsincidenten					Diensten IM en ICT, Directie IV	
4	Ontwerpen van eindtermen en een opleidingssystematiek					Directies HRM, Operatiën, Dienst HRM en PA	Neutraal
5	Regelen van besluitvorming over de opleidingsplannen.					Directies HRM, Operatiën, Dienst HRM en PA	Neutraal
6	Organiseren herhalingsprogramma voor administratief/ technisch personeel voor informatiebeveiliging en privacy					Directies HRM, Operatiën, Dienst HRM en PA	Neutraal

7	Opname privacy en security aspecten in introductieprogramma's					Directies HRM, Operatiën, Dienst HRM	Neutraal
8	Implementatie opleidingen/cursussen IB					Directies HRM, Operatiën, Dienst HRM	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

1.5. Risico's

- Een aantal werkzaamheden zal plaatsvinden door tijdelijke inhuur wegens gebrek aan capaciteit. Als hiervoor geen middelen beschikbaar zijn komen de beoogde resultaten in gevaar.
- Werven en screenen van deze tijdelijke inhuur kan vertraging voor het programma opleveren.
- Vele factoren beïnvloeden de vernieuwing van het opleidings- en trainingsprogramma waardoor de prioriteit voor privacy en security in het geding kan komen.
- Voor implementatie van het proces van opvolging van beveiligingsincidenten is wellicht aanvullende structurele capaciteit nodig. Hiervoor kunnen budgettaire restricties gelden. Daarnaast kan krapte op de arbeidsmarkt voor dergelijke functionarissen resulteren in vertraging bij het in werking brengen.

2. Autorisaties

Artikel 6
De verantwoordelijke onderhoudt een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

2.1. Algemeen

Eén van de belangrijkste pijlers onder de informatiebeveiliging is een goed werkend systeem van autorisaties. Voor veel organisaties geldt tegenwoordig dat informatie een van de meest belangrijke middelen is en dat autorisaties een van de belangrijkste middelen is om vertrouwelijkheid, integriteit en beschikbaarheid daarvan te waarborgen. Voor de politie geldt dit in het bijzonder, inbreuken op het systeem door onterecht of bovenmatig autoriseren kunnen verstrekkende gevolgen hebben. Een goed systeem van autorisaties verleent alle medewerkers van de politie precies toegang tot die informatie die zij nodig hebben voor het succesvol uitoefenen van hun functie. En niet meer dan dat. De veiligheid van de medewerkers, burgers en de maatschappij vereisen dat de politie uiterst waakzaam met haar informatie omgaat. Er dient een gerechtvaardigd vertrouwen te bestaan op het stelsel van maatregelen, waaronder autorisaties, waardoor medewerkers informatie met elkaar kunnen delen en zo de efficiëntie van de uitvoering van de politietaak kunnen verhogen. Het is om die reden dat ook autoriseren, als onderdeel van informatiebeveiliging en naast rechten van betrokkene, één van de drie prioriteiten van het programma is.

Op het moment van vaststellen van dit verbeterplan lopen diverse activiteiten om het geheel van autoriseren te verbeteren. Een van deze activiteiten is het definitief maken en vaststellen van het autorisatiebeleid. Met dit beleid is gekozen voor role based access, een systeem waarbij medewerkers bij het aanloggen op basis van hun functie en rollen toegang krijgen tot applicaties en gegevens. Door een koppeling met het personeelssysteem kan gezorgd worden dat de autorisaties op basis van profielen (rollen) ieder moment worden toebedeeld op basis van de meest actuele informatie. Deze autorisaties worden daarmee toegekend op basis van iemands functie en afdeling en kunnen vervolgens worden aangevuld voor de verschillende, vaak tijdelijke, rollen die een medewerker kan hebben als lid van tijdelijke taken en/of teams.

Al enige tijd geleden is de politie gestart met de implementatie van de geautomatiseerde tooling die dit principe ondersteunt. De omvang van de politie en de diversiteit is activiteiten stelt bijzondere eisen aan deze tooling. De tooling dient dan ook snel en vlekkeloos te functioneren. Ook de personele reorganisatie die leidt tot grote verschuivingen van medewerkers en functies leidt tot een verhoging van de complexiteit van een goede invoering van role based access.

2.2. Bevindingen audits

De bevindingen uit de Wpg audit geven aan dat er nog geen landelijke procedure voor autorisaties is opgesteld. De meeste eenheden hebben autorisatieloketten opgezet, echter de medewerkers zijn hier nog vaak onbekend mee. Het autorisatieproces is daarmee onvoldoende op orde. Het aanvragen van autorisaties wordt heel divers ingevuld door de eenheden met behulp van eigen vaste procedures. Slechts bij één van de eenheden is een procedure aangetroffen voor het intrekken van autorisaties. Ook ontbreken

regelmatig de autorisatiematrixen en/of zijn deze niet actueel. Ten slotte worden er geen gestructureerde controles uitgevoerd op autorisaties.

De door of in opdracht van de AP uitgevoerde audit op de systemen EUVIS en NSIS-II hebben tot een aantal bevindingen geleid die voor het onderwerp autorisaties zijn samen te vatten tot:

- Toegangsrechten en personeelsprofielen: het autorisatiemechanisme van de politie is onvoldoende vormgegeven. Daardoor kan niet in alle gevallen beoordeeld worden of toegekende autorisaties terecht zijn.
- Toekennen van autorisaties en controle op toegekende autorisaties: de politie houdt onvoldoende toezicht op de naleving van het autorisatiemodel. Er is met name onvoldoende zicht op autorisaties toegekend aan ketenpartners

2.3. Eindtermen

Onderstaande eindtermen beschrijven de normen die in het kader van het programma bereikt moeten worden ten behoeve van de verdere verbetering van autorisatiebeheer. Deze verbetermaatregelen worden weliswaar gedurende het programma gerealiseerd (conform de tabel bij 2.4), maar daarmee verlopen nog niet alle autorisaties via de ingevoerde tooling en het ingerichte en werkende proces.

De in dit plan genoemde eindtermen en verbetermaatregelen hebben betrekking op de activiteiten binnen het programma.
Eind 2016 levert het verbeterprogramma de volgende resultaten op;

- 80% van de autorisatiemutaties (toekennen en intrekken) voor operationele systemen wordt geautomatiseerd uitgevoerd[1].
- 100% van autorisaties bij het verlaten van het korps wordt geautomatiseerd geblokkeerd.
- de procedure voor het handmatig toekennen van autorisaties is voorzien van de door de lijn verzochte borgingsmaatregelen.
- handmatig toegekende rechten worden voor alle operationele medewerkers geautomatiseerd ingetrokken bij functiewisseling.
- Het ontwerp van de AO-IC (interne controle) voor autoriseren, inclusief toezicht bij ketenpartners.
- Het inregelen van de toetsing op de autorisatiesystematiek bij ketenpartners die gebruik maken van EU-VIS en NSIS II.

Eind 2017 levert het verbeterprogramma de volgende resultaten op:

- het inregelen van onderhoud op het personeelsprofielenmatrix.
- het inregelen van AO-IC voor autoriseren intern de politie en bij ketenpartners.
- 80% van de autorisatiemutaties (toekennen en intrekken) voor bedrijfsvoeringssystemen wordt geautomatiseerd uitgevoerd[2].
- handmatig toegekende rechten worden voor alle bedrijfsvoeringsmedewerkers geautomatiseerd ingetrokken bij functiewisseling.

Eind 2018 levert het verbeterprogramma de volgende resultaten op:

- het inregelen van AO-IC voor autoriseren bij samenwerkingspartners.

[1] Voor die systemen die aangesloten kunnen worden op IAM-tooling.
[2] Voor die systemen die aangesloten kunnen worden op IAM-tooling.

2.4. Verbetermaatregelen

- Het implementeren van de geautomatiseerde tooling voor het toekennen en het intrekken van autorisaties.
- Het implementeren van de AO-IC (interne controle) voor autoriseren, inclusief het toezicht op aan ketenpartners toegekende autorisaties.
- Het implementeren van de toetsing op de autorisatiesystematiek bij ketenpartners die gebruik maken van EU-VIS en NSIS II.
- De personeelsprofielenmatrix wordt geactualiseerd.
- Het inregelen van AO-IC voor autoriseren bij samenwerkingspartners

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Implementatie geautomatiseerde tooling					Diensten IM en ICT, Eenheden Directie IV,	Budget AVP
2	Ontwerp en inregelen van een AO / IC inclusief toezicht bij ketenpartners					Directie IV, Dienst IM	Neutraal
3	Het inregelen van de toetsing op de autorisatiesystematiek bij ketenpartners EUVIS en NSIS II					Diensten IM en ICT, Directie IV,	Neutraal
4	Actualiseren van personeelsprofielenmatrix					Dienst ICT, Directie IV,	Neutraal
5	Het inregelen van AO / IC bij samenwerkingspartners					Diensten IM en ICT, Directie IV,	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

2.5. Risico's

- De mogelijkheid bestaat dat technische problemen verhinderen dat de tooling eind 2016 voldoende adequaat functioneert.
- Management en medewerkers kunnen weerstand hebben tegen de nieuwe wijze van werken doordat ze op basis van de nieuwe vastgestelde profielen niet langer toegang zullen hebben tot applicaties waar ze in het verleden wel toegang tot hadden.
- De mogelijkheid bestaat dat de informatie in het personeelsinformatiesysteem niet juist, actueel en volledig is waardoor de tooling niet voorzien wordt van adequate informatie.

3. Rechten van de betrokkene

Artikel 25
De verantwoordelijke deelt een ieder op diens schriftelijke verzoek binnen zes weken mede of, en zo ja welke, deze persoon betreffende politiegegevens verwerking ondergaan. Hij verstrekt daarbij tevens desgevraagd inlichtingen over de vraag of de deze persoon betreffende politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt. (…)

Artikel 28
Een ieder over wiens persoon politiegegevens worden verwerkt kan de verantwoordelijke schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

3.1. Bevindingen audit

Er is een landelijke procedure voor rechten van betrokkenen vastgesteld, echter is deze nog niet binnen alle eenheden geïmplementeerd. De processtappen zoals kennisneming en verzoek om verbetering, aanvulling, verwijdering of afscherming zijn op dit moment nog onvoldoende op orde en voldoen daarmee niet aan de Wpg-eisen. De politie brengt geen kosten in rekening.

3.2. Algemeen

Rechten van betrokkene is een belangrijke pijler binnen de Wpg voor het waarborgen van de privacy van de burger en past binnen het streven van de politie om daar waar mogelijk transparant te zijn richting burger en maatschappij. Dit recht biedt de burger namelijk de mogelijkheid informatie te verkrijgen over de gegevens die de politie over hem heeft opgeslagen en te verzoeken deze te corrigeren of te verwijderen indien de politiegegevens onjuist zijn.

In 2014 is onderzoek gedaan naar de toegevoegde waarde van een zogeheten ‘Wpg-loket’ voor het afhandelen van verzoeken om kennisneming en het doen van complexe verstrekkingen. Een dergelijk loket heeft belangrijke voordelen voor de burger doordat verzoeken meer eenduidig, sneller en meer betrouwbaar worden beantwoord.

De politie meent dat in het geheel van de maatregelen die genomen moeten worden om te kunnen voldoen aan de Wpg, het onderwerp rechten van betrokkenen topprioriteit moet krijgen. Het Wpg-loket, dat gaat zorgdragen voor een accurate en adequate afhandeling van verzoeken van betrokkenen, zal daarom in 2016 per eenheid worden gerealiseerd op basis van uniforme werkwijzen, gestandaardiseerde processen, één ondersteunend IT-systeem en deugdelijke managementinformatie.
Verder wordt de haalbaarheid onderzocht van een digitale postbus waardoor burgers gemakkelijker dan tot dusver verzoeken kunnen indienen.

Het huidige stadium in het proces van de rationalisering van het IT-landschap impliceert dat op dit moment nog op vele plaatsen politiegegevens zijn opgeslagen en het (over-)zicht daarop tekort schiet. Vanuit de toelichting op de wet dat de inspanning om te voldoen aan een verzoek niet onevenredig hoeft te zijn moet de verzoeker er echter mee rekening houden dat er een zekere onzekerheidsmarge is ten aanzien van de volledigheid van beantwoording.
De doorlooptijd van de behandeling van verzoeken om kennisneming van personen die in meerdere onderzoeken bij verschillende eenheden voorkomen kan worden beïnvloed doordat per onderzoek in afstemming met een bevoegd functionaris een afweging moet worden gemaakt tussen het belang van het onderzoek en de het recht van de betrokkene.

3.3. Eindtermen

Onderstaande eindtermen beschrijven hoe het proces ter waarborging van de rechten van betrokkenen uiteindelijk dient te verlopen. Het gaat om kwalitatieve en processuele normen die bereikt moeten worden met de maatregelen die het programma neemt. De verbetermaatregelen worden weliswaar gedurende het programma in gang gezet (conform de tabel bij 7.4.), maar niet alle eindtermen worden binnen de periode van het programma bereikt.

- Alleen schriftelijke verzoeken worden in behandeling genomen. De identiteit van de verzoeker wordt deugdelijk vastgesteld en ook aan de overige formaliteiten wordt voldaan.
- Van de vaststelling van de identiteit van de verzoeker en van overige formaliteiten wordt een aantekening gemaakt in het dossier.
- Alle relevante systemen worden geraadpleegd om de vraag van de verzoeker op een juiste en voldoende manier te beantwoorden, mits dit geen onevenredige tijdsinspanning vergt. Deze werkwijze dient onderbouwd en vastgelegd te zijn.
- De wijze van kennisneming wordt in het dossier vastgelegd. Er worden landelijke afspraken gemaakt over de te bevragen relevante systemen, zodat kennisnemingsverzoeken zo volledig mogelijk en uniform worden afgedaan.
- Een afwijzing vindt schriftelijk en met redenen omkleed plaats en wordt gedaan door een daartoe bevoegde ambtenaar.
- Een besluit tot aanpassing, verwijdering of vernietiging van gegevens wordt uitgevoerd door de ambtenaar die het gegeven heeft vastgelegd, dan wel door degene die verantwoordelijk is voor de gegevens.
- Indien is beslist tot aanpassing, verwijdering of vernietiging van gegevens wordt gemonitord of aan de beslissing uitvoering is gegeven
- Personen en instanties aan wie de gegevens het voorgaande jaar zijn verstrekt worden over de correctie geïnformeerd, tenzij dit een onevenredige inspanning vergt.
- Bij de beslissing op het verzoek worden belanghebbenden gewezen op de mogelijkheid van beroep bij de rechtbank dan wel bemiddeling door de AP.
- Mandaatbesluiten worden zo nodig geactualiseerd opdat besluiten getekend worden door een bevoegde medewerker.

3.4. Verbetermaatregelen

- Per eenheid wordt een zogeheten Wpg-loket ingericht. Dit loket behandelt onder andere de verzoeken om kennisneming en verwijdering of correctie.
- De landelijke procedure voor de behandeling van kennisnemings- en correctieverzoeken wordt, voor zover dat nog niet is gebeurd, bij de eenheden in gebruik genomen, waaronder het gebruik van modelbrieven.

- Kennisnemings- en correctieverzoeken worden centraal in één landelijk systeem geregistreerd en inzichtelijk gemaakt ter voorkoming van dubbel werk bij meerdere verzoeken bij verschillende eenheden en ten behoeve van managementinformatie en beleidsontwikkeling om de uitvoering verder te verbeteren. Termijnbewaking en procesverloop worden daarbij maximaal ondersteund.
- Bezien hoe een digitaal aanvraagformulier met behulp van DigID ontwikkeld kan worden.

	Noodzakelijke maatregel	**2016**	**2017**	**2018**	**2019**	**Betrokkenen**	**Budgettaire impact**
1	Inrichten Wpg-loket per eenheid					Eenheden	Ombuiging
2	Standaardisering processen					Eenheden	Neutraal
3	IT-systeem optimaliseren					Eenheden, Diensten IM en ICT	Neutraal
4	Procedures beoordelen en zo nodig aanpassen					Directie IV	Neutraal
5	Voorwaarden digitaal aanvraagformulier vaststellen					Directie IV	PM
6	Digitaal aanvragen realiseren i.c.m. DigID					Eenheden, Diensten IM en ICT	PM

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)
Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

3.5. Risico's

- De inrichting van een Wpg-loket per eenheid betekent een verschuiving van capaciteit, die niet in het inrichtingsplan is opgenomen. Hiervoor dient een aanpassing plaats te vinden in de inrichtingsplannen en de herijking.
- Het systeem voor procesondersteuning, termijnbewaking en registratie is al wel aanwezig, maar nog niet ingericht voor de ondersteuning van rechten van betrokkenen. Aanpassingen kunnen vertraging oplopen door gebrek aan IV-capaciteit of de al eerder gekozen inrichting van het systeem.
- Het digitaal aanvraagformulier strijdt in de prioritering van IV-capaciteit met andere initiatieven en is afhankelijk van de prioriteiten die de politie geeft aan het onderwerp Digitale Overheid.

4. Verstrekkingen

Artikel 16 t/m 24
De verantwoordelijke kan politiegegevens verstrekken aan:
- opsporingsambtenaren en gezagsdragers (art. 16);
- inlichtingendiensten en buitenlandse opsporingsinstanties (art 17);
- politie en gezagsdragers Bonaire, Sint Eustatius en Saba (art 17a);
- derden structureel (art 18);
- derden incidenteel (art 19);
- derden structureel voor samenwerkingsverbanden (art 20);
- wetenschappelijk onderzoek en statistiek (art 22);
- rechtstreeks aan leden van het Openbaar Ministerie (art 23);
- rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten (art 24).

4.1. Bevindingen audit

Er is een landelijke procedure voor verstrekkingen opgesteld. Deze is echter nog niet (volledig) binnen alle eenheden geïmplementeerd. Niet elk type verstrekking voldoet aan de Wpg. Dit geldt bijvoorbeeld voor die aan de burgemeesters en buitengewone opsporingsambtenaren (boa's), waarbij nog onvoldoende invulling wordt gegeven aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsbeginsel. Bij steeds meer eenheden zijn convenantenloketten opgezet.

4.2. Algemeen

De Wpg beoogt ruimte te bieden voor door de praktijk gewenste verstrekkingen in het kader van de samenwerking van de politie met derden. Deze samenwerking met derden is wenselijk en noodzakelijk voor een goede uitvoering van de politietaak. Ook de goede taakuitvoering van andere overheidsdiensten kan een reden zijn voor het verstrekken van politiegegevens. Zo is de politie verplicht gegevens te verstrekken aan gezagsdragers en boa's, en zijn in het Besluit politiegegevens ontvangstgerechtigde personen en instanties aangewezen. Daarnaast is er ruimte om in geval van een zwaarwegend algemeen belang, in overeenstemming met het bevoegd gezag, in bijzondere gevallen incidenteel gegevens te verstrekken, dan wel in het kader van een structureel samenwerkingsverband.

Als het verstrekken van politiegegevens niet goed verloopt, is er kans op ernstige schending van de privacy van burgers. Aangezien de regels omtrent incidentele verstrekkingen, verstrekkingen aan opsporingsambtenaren en gezagsdragers, maar ook overige complexere verstrekkingen, veel onduidelijkheid opleveren voor de uitvoerenden, wordt per eenheid een Wpg-loket ingericht dat hierbij ondersteunt. Dit loket zal tevens een ondersteunende en coördinerende rol hebben bij de totstandkoming en het beheer van convenanten en bijbehorende art. 20-beslissingen, en adviseren over de verstrekkingen die al dan niet aan samenwerkingsverbanden kunnen worden gedaan.

Landelijk wordt gestuurd op centrale registratie, uniforme afspraken en werkwijzen met betrekking tot convenanten, met ruimte voor lokaal maatwerk. Dit geldt zeker voor samenwerkingsverbanden bij meerdere eenheden die zien op vergelijkbare problematiek, zoals de RIEC's, Veiligheidshuizen, hennepaanpak en

omgevingsdiensten. Een goed middel om naleving van de Wpg te bevorderen is het gebruik van modelformuleringen in convenanten. Daarnaast worden de convenanten landelijk geregistreerd en toegankelijk gemaakt.

De audit was met name kritisch over bovenmatige verstrekkingen aan burgemeesters en boa's. Eén van de activiteiten die al in gang is gezet, is het inventariseren van de informatiebehoefte van burgemeesters teneinde ook op dit gebied de verstrekkingen uniform in te richten, met ruimte voor lokaal maatwerk. De informatiebehoefte van burgemeesters zal immers verschillen vanwege gemeentespecifieke problematiek. Daarbij worden het noodzakelijkheidscriterium en de beginselen van proportionaliteit en subsidiariteit vanzelfsprekend betrokken.

Het verstrekken van politiegegevens is steeds weer maatwerk. Waar mogelijk worden verstrekkingen gestandaardiseerd en geautomatiseerd gedaan, maar op onderwerpen waarbij dat niet mogelijk is en het afhankelijk is van de beoordeling van de individuele politieambtenaar zal het risico op bovenmatige dan wel onrechtmatige verstrekkingen altijd bestaan. Om dit risico zoveel mogelijk te ondervangen zal doorlopend aandacht besteed moeten worden aan opleiding, awareness en sturing door leidinggevenden.

4.3. Eindtermen

Onderstaande eindtermen beschrijven hoe de verschillende verstrekkingen uiteindelijk dienen te verlopen. De verbetermaatregelen worden weliswaar gedurende het programma in gang gezet (conform de tabel bij 7.4.), maar niet alle eindtermen worden binnen de periode van het programma bereikt.

- Verstrekkingen, waaronder geautomatiseerde, zijn niet bovenmatig en voldoen aan vereisten als doelbinding, rechtmatigheid, juistheid en aan beveiligingseisen.
- Ontvangers van politiegegevens treffen passende en organisatorische maatregelen om politiegegevens tegen een passend niveau te beveiligen.
- De verstrekkingenwijzer is actueel, wordt beheerd en is goed toegankelijk.
- Verstrekkingen worden getoetst aan principes als doelbinding, noodzakelijkheid, proportionaliteit en subsidiariteit.
- Verstrekkingen op grond van artikel 16 van de Wpg vinden slechts aan gezagsdragers zelf of hun gemandateerden plaats.
- De politie neemt alleen deel aan een samenwerkingsverband indien uit een convenant of overeenkomst blijkt wat het doel en de aard van de samenwerking is, op welke wijze dit bijdraagt aan de uitvoering van de politietaak en welke partijen aan het samenwerkingsverband deelnemen.
- Politiegegevens worden alleen aan een samenwerkingsverband verstrekt indien, in overeenstemming met het bevoegd gezag, een beslissing op grond van artikel 20 van de Wpg is genomen.
- Convenanten met betrekking tot vergelijkbare problematiek (Veiligheidshuis, RIEC, hennepaanpak) zijn uniform, met ruimte voor lokaal maatwerk. Deze convenanten worden getoetst door de Gegevensautoriteit.
- Bij dergelijke convenanten worden naast een convenant ook privacyprotocollen of informatieprotocollen en werkprocessen opgesteld.
- Bij landelijke samenwerkingsverbanden wordt bij voorkeur gewerkt aan de opstelling van een machtigingsbesluit van de Minister van Veiligheid en Justitie op grond van artikel 18 lid 2 Wpg.

4.4. Verbetermaatregelen

- Per eenheid wordt een Wpg-loket ingericht. Dit loket ondersteunt bij de uitvoering van complexe verstrekkingen, maar ook bij de totstandkoming en het beheer van convenanten.

- De processen binnen het Wpg-loket worden zoveel mogelijk gestandaardiseerd, zoals:
  - Identiteit verzoeker controleren.
  - Ontvangers van politiegegevens wijzen op geheimhouding.
  - Afspraken met het 'bevoegd gezag' over wijze te verstrekken politiegegevens, waaronder mandaatafspraken.
  - Afspraken met ontvangers van politiegegevens over het treffen van passende en organisatorische maatregelen om politiegegevens tegen een passend niveau te beveiligen, waaronder afspraken over controle op de uitvoering (met name bij structurele verstrekkingen).
- De verstrekkingenwijzer wordt geactualiseerd en landelijk beschikbaar gesteld.
- Er wordt een centrale registratie van convenanten ingericht en deze worden landelijk toegankelijk gemaakt.
- Inventarisatie informatiebehoefte van burgemeesters en ontwikkeling uniforme wijze van verstrekken.
- Met behulp van een quickscan worden de huidige geautomatiseerde verstrekkingen getoetst op noodzakelijkheid, proportionaliteit en subsidiariteit. Aan de hand van genoemde quickscan worden eventuele bovenmatige verstrekkingen stopgezet.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Inrichten Wpg-loket per eenheid					Eenheden	Neutraal
2	Standaardisering processen en werkwijzen					Eenheden	Neutraal
3	Beschikbaar stellen modelformuleringen voor convenanten					Eenheden, Diensten IM en ICT	Neutraal
4	IT-systeem optimaliseren					Directie IV	Neutraal
5	Actualiseren en beschikbaar stellen verstrekkingenwijzer					Directie IV	Neutraal
6	Harmoniseren burgemeestersverstrekkingen					Directie IV	Neutraal
7	Quickscan geautomatiseerde verstrekkingen					Directie IV, Dienst IM, Eenheden	Neutraal
8	Opleiding en awareness					Eenheden, Diensten IM en ICT	PM

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)
Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

4.5. Risico's

- De inrichting van een Wpg-loket per eenheid betekent een verschuiving van capaciteit, die niet in het inrichtingsplan is opgenomen. Hiervoor dient een aanpassing plaats te vinden in de inrichtingsplannen en de herijking.
- Het risico bestaat dat de veranderende opstelling van de politie om te kunnen voldoen aan de Wpg leidt tot weerstand bij ontvangende partijen.

5. Protocolplicht

Artikel 32
De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
a. de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid;
b. de gegevens die op grond van het bepaalde bij of krachtens artikel 13, vierde lid, worden vastgelegd;
c. de toekenning van de autorisaties, bedoeld in artikel 6;
d. de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8, derde lid, en 11, eerste, tweede en vierde lid;
e. de hernieuwde verwerking van politiegegevens op grond van artikel 9 of 10, bedoeld in artikel 14, derde lid;
f. de verstrekking van politiegegevens op grond van paragraaf 3 met uitzondering van de verstrekking, bedoeld in artikel 17, eerste lid, en artikel 24, eerste en tweede lid, indien dit zich niet verdraagt met het belang van de veiligheid van de staat;
g. verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht;
h. een geautomatiseerde vergelijking van gegevens als bedoeld in artikel 11, vijfde lid.

5.1. Bevindingen audit

Er is een landelijke procedure protocolplicht opgesteld. Deze is echter nog niet (volledig) binnen alle eenheden geïmplementeerd. Voor alle categorieën waarvoor geprotocolleerd dient te worden gebeurt dit nog niet conform de Wpg.

5.2. Algemeen

De Wpg verplicht tot het vastleggen van bepaalde gegevensverwerkingen, de zogeheten protocolplicht. Gelet op het streven naar administratieve lastenverlichting wordt het protocolleren idealiter zoveel mogelijk geautomatiseerd uitgevoerd. In dit verband is het van belang te beseffen dat het huidige applicatielandschap het onmogelijk maakt dit op korte termijn te realiseren.
Tegelijkertijd schrijft de richtlijn, die waarschijnlijk in april 2016 in werking treedt en vanaf medio 2018 geïmplementeerd moet zijn in nationale wetgeving, voor dat de volgende geautomatiseerde handelingen worden gelogd:

- verzamelen;
- wijzigen;
- raadplegen;
- verstrekken waaronder doorgifte;
- combineren, en
- verwijderen.

Aan de protocolplicht wordt in beginsel invulling gegeven conform de huidige praktijk, zoals het gebruik van formulieren bij ‘in combinatie verwerken’ en ‘hernieuwd verwerken’, het vastleggen van de doelen van artikel 9-onderzoeken in Summ-IT en het vastleggen van verstrekkingen met behulp van BVH-codes I90 en E62. Op langere termijn is het de bedoeling om zoveel mogelijk middels logging tegemoet te komen aan de protocolplicht. Een dergelijke invulling van de protocolplicht biedt mogelijkheden de toezicht- en

controlfunctie uit te oefenen maar het maakt vooral het werk eenvoudiger voor de individuele politieambtenaar. Om dit gestructureerd te realiseren wordt met behulp van een quickscan onderzocht in hoeverre de bestaande logging de huidige protocolplicht ondersteunt, zodat waar mogelijk delen van de protocolplicht geautomatiseerd kunnen worden opgevolgd. Vervolgens wordt een mijlpalenplanning opgesteld om binnen de periode die hiervoor wettelijk staat aangegeven de logging aan te passen voor de relevante systemen. Deze mijlpalenplanning zal in 2017 opgesteld kunnen worden, maar de daadwerkelijke aanpassing en inrichting van de logging neemt meer tijd in beslag en valt voor een belangrijk deel buiten de duur van het programma.

5.3. Eindtermen

- De protocolplicht is geautomatiseerd ingericht.
- Voor zover geautomatiseerde protocollering (nog) niet mogelijk is wordt volgens een landelijke uniforme werkwijze handmatig geprotocolleerd conform de huidige praktijk.
- Periodiek vindt monitoring op deze bestaande manier van werken plaats.
- De protocolgegevens worden minimaal voor de auditperiode bewaard.
- Instellingsprotocollen met betrekking tot artikel 13-verwerkingen worden landelijk vastgesteld, centraal geregistreerd en toegankelijk gemaakt.
- Nieuwe artikel 13-instellingsprotocollen worden conform een modelprotocol opgesteld en volgens een procedure vastgesteld.

5.4. Verbetermaatregelen

- Er wordt een impactanalyse gedaan op de loggingseisen die de richtlijn stelt.
- Met behulp van een quickscan wordt onderzocht in hoeverre de bestaande logging de protocolplicht ondersteunt zodat de complexiteit rond protocolleren voor de individuele politieambtenaar verminderd kan worden
- Er wordt een stelsel van monitoring en toezicht ingericht.
- Achterstallig onderhoud van instellingsprotocollen met betrekking tot artikel 13-verwerkingen wordt uitgevoerd (vaststelling, centrale registratie, toegankelijkheid).
- Aan de hand van een kosten-/ batenanalyse is de invulling van de loggingseisen, binnen de gestelde termijnen van de richtlijn, geprioriteerd en is een mijlpalenplanning opgesteld.
- De mijlpalenplanning is verwerkt in de activiteiten van de Dienst IM en Dienst ICT.

	Noodzakelijke maatregel	**2016**	**2017**	**2018**	**2019**	**Betrokkenen**	**Budgettaire impact**
1	Impactanalyse richtlijn					Directie IV, JZ	Neutraal
2	Quickscan bestaande logging					Directie IV, Dienst ICT	Neutraal
3	Stelsel monitoring en toezicht					Directie IV, Eenheden	Neutraal
4	Procedure artikel 13-verwerkingen					Directie IV	Neutraal
5	Onderhoud artikel 13-instellingsprotocollen					Directie IV, Diensten Operatiën en ICT, Eenheden	Neutraal
6	Kosten-/batenanalyse, prioritering en mijlpalenplanning					Directie IV, Diensten IM en ICT	Neutraal
7	Mijlpalenplanning verwerken IM/ICT					Directie IV, Diensten IM en ICT	PM

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

5.5. Risico's

- De daadwerkelijk aanpassing is afhankelijk van het budget dat hiervoor vrijgemaakt zal kunnen worden.
- Aanpassing van de logging ten behoeve van de Wpg dient aan te sluiten bij de wijzigingen die vanuit informatiebeveiliging worden gewenst. De verschillende wijzigingen hebben mogelijk een ander tijdspad.

6. Bewaartermijnen

Artikel 14
1. De op grond van de artikelen 8, zesde lid, 9, vierde lid, en artikel 10, zesde lid, verwijderde politiegegevens worden gedurende een termijn van vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd.
(…)
3. In bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10, kunnen politiegegevens die overeenkomstig het eerste lid worden bewaard, in opdracht van het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, ter beschikking worden gesteld voor hernieuwde verwerking op grond van artikel 9 of 10.

6.1. Bevindingen audit

De bewaartermijnen zijn onvoldoende op orde. Dit komt mede omdat deze niet zijn geborgd in de IT. De medewerkers dienen zelf schoningstermijnen in de gaten te houden en handmatig te schonen. Dit gebeurt meestal niet.

6.2. Algemeen

Bij het formuleren van eindtermen ten aanzien van verwerkings- en bewaartermijnen is het van belang te realiseren dat de voormalige 26 korpsen over 1900 verschillende applicaties beschikten. Het uitfaseren en harmoniseren hiervan heeft ertoe geleid dat in februari 2016 nog driehonderd (landelijk beheerde) applicaties in gebruik zijn. Dit is een vooruitgang wat betreft technisch beheer, functioneel beheer en kosten, maar zeker ook wat betreft gegevensbescherming. Er zijn immers minder gegevensbronnen beschikbaar en dus ook minder risico's dat wetgeving rondom bijvoorbeeld autoriseren, verwijderen en vernietigen niet goed wordt nageleefd. De vereenvoudiging van het applicatielandschap én de gegevenshuishouding maken het mogelijk een aantal realistische eindtermen voor de belangrijkste basissystemen, zoals de Basisvoorziening Handhaving (BVH) en Summ-IT, te formuleren.
In 2015 is de ontwikkeling van een verwijderingsalgoritme voor BVH reeds in gang gezet. In de loop van 2016 wordt dit bij de verschillende eenheden doorgevoerd.

Daarnaast vindt de ontwikkeling van nieuwe systemen (of functionaliteit) plaats volgens de principes van 'privacy & security by design'. Privacy en informatiebeveiliging worden vroegtijdig in het ontwerp van nieuwe systemen (of functionaliteit) meegenomen.

Tegelijkertijd worden de privacyrisico's in de 'legacy' geïnventariseerd. Het gaat daarbij om bestaande systemen die zo veel als mogelijk op termijn uitgefaseerd worden. Ten aanzien van de grootste risico's worden mitigerende maatregelen genomen waarbij rekening wordt gehouden met de snelheid van de vernieuwing (van systemen).

Het verwijderen en vernietigen van gegevens die zijn verzameld in het kader van de politaak wordt bemoeilijkt door het diverse applicatielandschap, het oneigenlijk gebruik van kantoorautomatisering en het

gebruik van publieke applicaties. Voor het voldoen aan de eisen uit de wet ten aanzien van bewaren en vernietigen speelt een complicerende rol dat de politie in een keten opereert waarin verschillende wetgeving wordt gehanteerd. Hierdoor blijft er een spanningsveld bestaan op deze eisen welke alleen kan worden opgeheven door een vereenvoudiging van het wettelijk regime.

6.3. Eindtermen

Onderstaande eindtermen beschrijven hoe wordt gerealiseerd dat de naleving van de verwerkings- en bewaartermijnen uiteindelijk wordt ondersteund door de belangrijkste basissystemen en de nieuw te ontwikkelen systemen, en welke maatregelen worden getroffen ten aanzien van de legacy. De verbetermaatregelen worden weliswaar gedurende het programma in gang gezet (conform de tabel bij 6.4.), maar niet alle eindtermen worden binnen de periode van het programma bereikt.

- Politiegegevens die op basis van artikel 8 in BVH, het basissysteem voor het uitvoeren van de dagelijkse politietaak, worden verwerkt, worden na een termijn van vijf jaar geautomatiseerd verwijderd en na een vervolgperiode van vijf jaar (dus in totaal tien jaar) indien mogelijk geautomatiseerd vernietigd.
- Politiegegevens die in Summ-IT, het huidige systeem ter ondersteuning van de opsporing, worden verwerkt, worden aan de hand van afloopberichten zoveel mogelijk geautomatiseerd verwijderd. Aanvullend is er een procedure voor het handmatig verwijderen van artikel 9-gegevens.
- De afhandeling van afloopberichten is geborgd in de organisatie.
- Een beperkte groep medewerkers is opgeleid als ‘poortwachter’ en is uitgerust voor hun taak. Alleen de poortwachter heeft toegang tot verwijderde gegevens voor de in de wet genoemde doeleinden.
- Verwijderde gegevens worden slechts voor de in de wet bepaalde doeleinden (hernieuwd) verwerkt.
- Er wordt vernietigd conform de termijnen zoals vastgelegd in een artikel 13-instellingsprotocol.
- Nieuwe informatievoorzieningen worden vormgegeven conform privacy & security by design; het verwijderen en vernietigen van politiegegevens wordt zo mogelijk geautomatiseerd ondersteund.

6.4. Verbetermaatregelen

- Er wordt een algoritme geïmplementeerd dat geautomatiseerd alle gegevens na vijf jaar uit BVH verwijdert die conform de wet verwijderd moeten worden.
- Er wordt een algoritme geïmplementeerd dat geautomatiseerd reeds uit BVH verwijderde gegevens na vijf jaar vernietigt die conform de wet vernietigd moeten worden.
- Er wordt een algoritme geïmplementeerd dat geautomatiseerd gegevens uit Summ-IT verwijdert aan de hand van afloopberichten.
- Er wordt een algoritme geïmplementeerd dat geautomatiseerd, daar waar mogelijk, alle gegevens na de wettelijke bewaartermijnen uit de in dit kader meest relevante basissystemen verwijdert.
- De inrichting van de poortwachtersorganisatie wordt geëvalueerd en zo nodig bijgesteld.
- Het proces van afhandeling van afloopberichten afkomstig van JustID wordt geoptimaliseerd.
- Er wordt een procedure voor het handmatig verwijderen van artikel 9-gegevens ingericht. De procedure wordt in ieder geval afgestemd met het OM en met functioneel beheer.
- Er wordt een landelijk uniform proces ingericht voor ‘hernieuwd verwerken’, afgestemd met het OM, functioneel beheer en de DRIO als verantwoordelijke voor de poortwachtersorganisatie.
- Er wordt een project “herbruikbare informatie” opgestart welke regelt dat informatie uit stilliggende dan wel afgesloten opsporingsonderzoeken welke voor hergebruik in aanmerking komen, worden gedeeld met andere lopende onderzoeken.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Implementatie algoritme dat geautomatiseerd alle gegevens na vijf jaar uit BVH verwijdert die conform de wet verwijderd moeten worden.					Diensten IM en ICT, Directie IV, Eenheden	Neutraal
2	Implementatie algoritme dat geautomatiseerd reeds uit BVH verwijderde gegevens na vijf jaar vernietigt die conform de wet vernietigd moeten worden.					Diensten IM en ICT, Directie IV, Eenheden	Neutraal
3	Implementatie algoritme dat geautomatiseerd gegevens uit Summit verwijdert aan de hand van afloopberichten.					Diensten IM en ICT, Directie IV	Neutraal
4	Implementatie algoritme dat geautomatiseerd gegevens na vijf jaar uit overige basissystemen verwijdert.					Diensten IM en ICT, Directie IV, Eenheden	Neutraal
5	De inrichting van de poortwachtersorganisatie wordt geëvalueerd en zo nodig bijgesteld.					Directie IV	Neutraal
6	Het proces van afhandeling van afloopberichten afkomstig van JustID wordt geoptimaliseerd.					Directie IV, Eenheden	Neutraal
7	Procedure handmatig verwijderen van artikel 9-gegevens opgesteld.					Directie IV, Eenheden	Neutraal
8	Landelijk uniform proces voor 'hernieuwd verwerken'.					Dienst ICT, Directie IV, Eenheden	Neutraal
9	Opstarten project "herbruikbare informatie".					Dienst ICT, Directie IV, Eenheden	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

6.5. Risico's

- De impact van de voorgestelde maatregelen in een divers applicatielandschap is zodanig dat er mogelijk grote aanvullende investeringen nodig zijn als voor bepaalde systemen de formulering van een algoritme geen oplossing biedt. .
- De invoer van een aantal maatregelen vraagt om grote betrokkenheid van de operatie, die ook andere prioriteiten kent en haar eigen afwegingen maakt in het belang van het bewaren van gegevens.

7. De kwaliteit van gegevens

Artikel 3 (noodzakelijkheid, rechtmatigheid en doelbinding)
1. Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden.
2. Politiegegevens worden slechts verwerkt voor zover zij rechtmatig zijn verkregen en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.
3. Politiegegevens worden uitsluitend voor een ander doel verwerkt dan waarvoor zij zijn verkregen voor zover deze wet daar uitdrukkelijk in voorziet, deze verwerking niet onverenigbaar is met het doel waarvoor deze gegevens zijn verkregen en de verwerking voor dat andere doel overigens noodzakelijk is en in verhouding staat tot dat doel. De verdere verwerking is alleen mogelijk door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang zijn aangewezen.
4. Bij de verwerking van politiegegevens op grond van de artikelen 9, 10 en 12 worden de herkomst van de gegevens en de wijze van verkrijging vermeld.

Artikel 4 (juistheid, volledigheid en beveiliging politiegegevens)
1. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij verbetert of vernietigt politiegegevens of vult deze aan indien hem blijkt dat deze onjuist of onvolledig zijn.
2. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.
(…)

7.1. Bevindingen audit

In alle eenheden wordt TrueBlue gebruikt als tool voor kwaliteitsverbetering. De kennisregels zijn echter te beperkt en de naleving van waarschuwingen is niet optimaal, waardoor dit onderwerp nog niet op orde is.

7.2. Algemeen

Kwaliteit van gegevens is een essentieel thema bij het realiseren van de twee hoofddoelen van de wet, te weten een effectieve en efficiënte informatiehuishouding en de bescherming van de privacy van de burger. Bij de uitvoering van de politietaak moeten politieambtenaren er vanuit kunnen gaan dat de informatie die zij voor handen hebben zoveel mogelijk juist, volledig, actueel is. Pas dan kunnen de juiste beslissingen genomen worden. Tegelijkertijd moet de burger er vanuit kunnen gaan dat onjuiste gegevens worden verbeterd of vernietigd ter voorkoming van ingrijpende gebeurtenissen als onheuse bejegening, onterechte aanhoudingen of identiteitsfraude.
De kwaliteit van gegevens is overigens niet alleen belangrijk vanwege het functioneren van de eigen organisatie, maar ook van andere partijen in de strafrechtketen. De politie fungeert als belangrijke bron van informatie in die keten en haar legitimiteit en vertrouwen staat of valt bij de juistheid van de gegevens die ze verwerkt en deelt.

Kwaliteit van gegevens is een veelzijdig onderwerp dat vraagt om een integrale aanpak met aandacht voor zowel het gedrag van de individuele politiemedewerker, als voor de politieprocessen en -systemen. Een geïsoleerde oplossing, zoals een aparte afdeling of specifiek controlesysteem, zal niet effectief zijn. De eerste resultaten van de nulmeting naar de kwaliteit van gegevens en de mate waarin datamanagement wordt uitgevoerd maakt duidelijk dat de politie nog een flink aantal stappen te nemen heeft. De voorgestelde maatregelen hebben dan ook betrekking op de invoer van gegevens ('ín één keer goed' vastleggen), het bewaren van de gegevens (gegevens worden eenmalig vastgelegd in kernregisters) en het verwerken van gegevens. Belangrijk hierbij is dat leidinggevenden en medewerkers zijn doordrongen van het belang van een goede kwaliteit van gegevens en het belang van hun eigen rol en verantwoordelijkheid hierbij. De kaders voor gegevensverantwoordelijkheid worden in 2016 opgesteld en tevens wordt dan gestart met de identificatie van verantwoordelijken voor de verschillende gegevens.

De verbetering van de kwaliteit van gegevens wordt nauwelijks ondersteund door de huidige, verouderde politiesystemen. Naast het doorzetten van de vernieuwingsstrategie (onder andere het gebruik van kernregisters) is het doorvoeren van verbeteringen in bestaande processen en systemen essentieel voor het verhogen van de kwaliteit van gegevens. Hiervoor wordt een verbeterproces in werking gebracht gedurende 2016. De verbeteringen worden aangedragen en geprioriteerd vanuit de operatie met inachtneming van de vernieuwingsstrategie en lopen na de periode van het programma door.

7.3. Eindtermen

- Politiemedewerkers hebben inzicht in de eigen bijdrage in de keten en het belang van kwaliteit van politiegegevens daarbij.
- Politiemedewerkers voelen zich verantwoordelijk voor de kwaliteit van politiegegevens gedurende de gehele levenscyclus.
- Verantwoordelijkheid voor eisen aan, richtlijnen voor, en correct gebruik van politiegegevens is belegd in de lijn.
- Inzicht in de betekenis van en samenhang tussen politiegegevens is beschikbaar en wordt door de lijn gebruikt bij vastlegging en controle van gegevens en daarnaast bij veredeling, ontsluiting en interpretatie van informatieproducten.
- Processen en systemen zijn zo ingericht dat gegevens 'in één keer goed' vastgelegd worden, waarbij controle op kwaliteit in het proces ondersteund wordt. Daar waar dit nog niet mogelijk is zijn controles achteraf ingericht conform de huidige werkwijze.
- Processen en systemen zijn zo ingericht dat bij vastlegging van gegevens gebruik gemaakt wordt van kernregisters. Daar waar dit nog niet door systemen ondersteund wordt, zal dit procedureel worden opgelost.
- Fouten in gegevens worden terug gemeld aan de bron, zowel intern als extern (aan basisregistraties en ketenpartners).
- Gegevenskwaliteitsissues, zowel intern als in ketenverband, worden opgelost met betrokkenheid van de operatie, de teams Kwaliteit van Informatie, de dienst IM en betrokkenen in de keten. In een continu verbeterproces worden issues geanalyseerd en worden herstelstappen gedefinieerd en geprioriteerd. Hierbij is er naast correctieve actie aandacht voor systeemaanpassingen, vernieuwing van procedures en training van medewerkers.

7.4. Verbetermaatregelen

- Bewustzijn van het belang van kwaliteit van politiegegevens en inzicht in de eigen bijdrage in de keten wordt gestimuleerd door periodieke communicatie naar relevante doelgroepen.

- Kaders en richtlijnen voor omgang met politiegegevens worden helder en volledig beschreven en voor politiemedewerkers eenvoudig toegankelijk gemaakt.
- Strategisch (lijn)verantwoordelijken voor politiegegevens worden geïdentificeerd en vastgelegd in een gegevensregistratie.
- De verantwoordelijkheden in de omgang met politiegegevens worden gedefinieerd in een RACI en in werking gebracht.
- In vernieuwingsprocessen wordt in requirements en ontwerp rekening gehouden met kaders en richtlijnen voor omgang met gegevens, borging door opname in de Projectstartarchitectuur.
- Processen en middelen voor beschrijven- en verbeteren van gegevens worden gedefinieerd en in werking gebracht met expliciete betrokkenheid van de lijn i.s.m. de afdeling Gegevensgebruik enBeheer en de teams Kwaliteit van Informatie.
- Concrete verbeteringen in kwaliteit van gegevens worden opgepakt, uitgewerkt en doorgevoerd: onder meer kwaliteit van strafrechtsketennummer en kwaliteit van het proces verbaal.
- Gegevenskwaliteit monitoring voor de relevante aspecten vanuit de Wpg wordt ingericht (bijv. in TrueBlue), met specifiek ook een inhaalslag voor SummIT.
- IV-toepassingen worden zoveel als mogelijk voorzien van een functionaliteit voor het terugmelden van fouten aan de bronhouder, inclusief een proces om de voortgang te monitoren.
- In IV-dashboards worden begrijpelijke, relevante en meetbare output- en outcome-indicatoren opgenomen voor ‘gegevens zijn de kern’; meting en rapportage per kwartaal door de teams KvI & GGB aan MT-CIO en Korpsleiding.
- Voor lijn-, programma- en projectorganisatie worden trainingen in omgang met gegevens ontwikkeld.
- De afdelingen Gegevensautoriteit, Gegevensgebruik en Beheer (GGB) en Kwaliteit van Informatie (KvI) worden volledig in werking gebracht volgens het inrichtingsplan, aangevuld met inzichten vanuit onder andere de nulmeting datamanagement.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	**Bewustzijn van het belang van kwaliteit van politiegegevens en inzicht in de eigen bijdrage in de keten wordt gestimuleerd door periodieke communicatie naar relevante doelgroepen.**					Directie IV, Diensten IM en ICT, Eenheden	PM
2	**Kaders en richtlijnen voor omgang met politiegegevens worden helder en volledig beschreven en voor politiemedewerkers eenvoudig toegankelijk gemaakt.**					**Directie IV**	**Neutraal**
3	**Strategisch (lijn)verantwoordelijken voor politiegegevens worden geïdentificeerd en vastgelegd in een gegevensregistratie.**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**
4	**De verantwoordelijkheden in de omgang met politiegegevens worden gedefinieerd in een RACI en in werking gebracht.**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**
5	**In vernieuwingsprocessen wordt in requirements en ontwerp rekening gehouden met kaders en richtlijnen voor omgang met gegevens, borging door opname in de Project Start Architectuur.**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**
6	**Processen en middelen voor beschrijven- en verbeteren van**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**

	gegevens worden gedefinieerd en in werking gebracht met expliciete betrokkenheid van de lijn i.s.m. GGB en Kvl.						
7	**Concrete verbeteringen in kwaliteit van gegevens worden opgepakt, uitgewerkt en doorgevoerd: onder meer kwaliteit van strafrechtsketennummer en kwaliteit van PV.**					Directie IV, Diensten IM en ICT, Eenheden	**PM**
8	**Toepassing van kernregisters.**					Directie IV, Diensten IM en ICT, Eenheden	**PM**
9	**Gegevenskwaliteit monitoring voor de relevante aspecten vanuit de Wpg wordt ingericht in TrueBlue of andere oplossing, specifiek ook een inhaalslag voor SummIT.**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**
10	**IV toepassingen worden zoveel als mogelijk voorzien van een functionaliteit voor het terugmelden van fouten aan de bronhouder, inclusief een proces om de voortgang te monitoren.**					Directie IV, Diensten IM en ICT, Eenheden	**PM**
11	**In IV Dashboards worden begrijpelijke, relevante en meetbare output en outcome indicatoren opgenomen voor 'gegevens zijn de kern'.**					Directie IV, Diensten IM en ICT, Eenheden	**PM**
12	**Voor lijn- en programma/project organisatie worden trainingen in omgang met gegevens ontwikkeld.**					Directie IV, Diensten IM en ICT, Eenheden	**PM**
13	**De afdelingen Gegevensautoriteit, GGB en Kvl worden volledig in werking gebracht volgens het inrichtingsplan, aangevuld met inzichten vanuit onder andere de nulmeting datamanagement.**					Directie IV, Diensten IM en ICT, Eenheden	**Neutraal**

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

7.5. Risico's

- De impact van de voorgestelde maatregelen in een divers applicatielandschap is zodanig dat er mogelijk grote aanvullende investeringen nodig zijn.
- Verbeteringen van gegevenskwaliteit komen alleen tot stand als er een breed scala van maatregelen wordt genomen op het gebied van mensen, processen en systemen, hiervoor is in het verleden niet altijd het belang gezien. De mogelijkheid bestaat dat de aandacht voor dit onderwerp gedurende het programma afneemt.

8. Gevoelige gegevens

Artikel 5
De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

8.1. Bevindingen audit

De landelijke richtlijnen zoals verwoord in het Praktijkhandboek Wpg en de instructies voor de bevoegd functionaris worden gevolgd. Er worden in de eenheden wel gevoelige gegevens vastgelegd, maar dit is vrijwel altijd in relatie tot bijvoorbeeld de aanpak van criminele groepen. Er worden ten aanzien van gevoelige gegevens ook opleidingen gevolgd. In de grote steden wordt aangegeven dat omgaan met andere etniciteiten als normaal wordt beschouwd. Desondanks is uit de audit naar voren gekomen dat op dit punt nog verdere verbetering nodig is.

8.2. Algemeen

Gevoelige gegevens mogen slechts worden verwerkt in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is. Dit staat soms op gespannen voet met de behoefte aan managementinformatie over bijvoorbeeld homogerelateerd geweld of de recente discussie over incidenten waarbij asielzoekers betrokken zijn. Het is typisch een onderwerp dat via communicatie en awareness onder de aandacht moet worden gebracht. Periodiek toezicht op dergelijke gegevensverwerkingen zal daaraan bijdragen.

8.3. Eindtermen

- Landelijk is er een eenduidige interpretatie van het begrip ‘gevoelig gegeven’ en dit maakt onderdeel uit van het begrippenkader dat in beheer is bij de Afdeling Gegevensgebruik en Beheer (GGB).
- Zo mogelijk wordt de verwerking van gevoelige gegevens opgenomen in TrueBlue-regels.
- Het begrip ‘gevoelig gegeven’ en de regels omtrent het gebruik daarvan zijn bekend bij politieambtenaren.

8.4. Verbetermaatregelen

- Definities worden vastgesteld en landelijk raadpleegbaar gemaakt.
- Het onderwerp ‘gevoelige gegevens’ is verwerkt in de opleidingen en trainingen en maakt onderdeel uit van de awareness-activiteiten.
- Onderzocht wordt op welke wijze TrueBlue onrechtmatig gebruik van gevoelige gegevens kan detecteren zodat rechtmatig gebruik bevorderd kan worden.
- Het toezicht op gegevensverwerking met als doel het voorkomen van onnodige vastlegging van gevoelige gegevens wordt verscherpt.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Vaststellen definitie					Directie IV, Dienst IM	Neutraal
2	Onderzoek mogelijkheid TrueBlue					Directie IV, Dienst IM	PM
3	Communicatie & awareness					Eenheden, PA	Neutraal
4	Periodiek toezicht					Privacyfunctionarissen	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)
Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

8.5. Risico's

- Actualiteiten kunnen leiden tot verminderd begrip voor de naleving van dit artikel waardoor de naleving in het geding komt.

9. Geautomatiseerd vergelijken en in combinatie verwerken

Artikel 11
1. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen, na instemming van een daartoe bevoegde functionaris, voor dat onderzoek verder worden verwerkt.
2. Voor zover dat noodzakelijk is voor een verwerking als bedoeld in artikel 10, eerste lid, kunnen politiegegevens die voor dat doel zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van de artikelen 8, 9 of 10 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen, na instemming van een daartoe bevoegde functionaris, voor die verwerking verder worden verwerkt.
(…)
4. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, of een verwerking als omschreven in artikel 10, eerste lid, kunnen in bijzondere gevallen in opdracht van het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 in combinatie met elkaar worden verwerkt teneinde vast te stellen of verbanden bestaan tussen de gegevens. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens, na instemming van een daartoe bevoegde functionaris, voor dat onderzoek of die verwerking verder worden verwerkt.
5. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, of een verwerking als omschreven in artikel 10, eerste lid, kunnen politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 geautomatiseerd worden vergeleken met andere dan politiegegevens.

9.1. Bevindingen audit

Binnen de politie is een aantal medewerkers belast met werkzaamheden van geautomatiseerd vergelijken en in combinatie met elkaar verwerken binnen artikel 9 en 10 verwerkingen. Vaak zijn deze informatiecoördinatoren niet aangewezen in deze tijd van reorganiseren. Zo is niet geborgd dat in combinatie met elkaar verwerken van artikel 8 politiegegevens ouder dan 1 jaar door de informatiecoördinator moet gebeuren.

9.2. Algemeen

De behoefte aan de mogelijkheid om geautomatiseerd te kunnen vergelijken en in combinatie te verwerken zal, mede gelet op technologische ontwikkelingen, de komende jaren sterk toenemen. Het is van belang inzichtelijk te hebben op welke plekken in de organisatie deze zoekslagen worden uitgevoerd en of de medewerkers die deze werkzaamheden uitvoeren daartoe zijn aangesteld en opgeleid. Zij moeten immers

bekend zijn met het onderscheid tussen beide termen en de respectievelijke voorwaarden waaronder de zoekslagen mogen worden uitgevoerd.

9.3. Eindtermen

- De vastgestelde begrippen ‘geautomatiseerd vergelijken’ en ‘in combinatie verwerken’ worden actief geïnstrueerd en maken onderdeel uit van het begrippenkader dat in beheer is bij GGB.
- Deze verwerkingen worden slechts gedaan door daartoe geautoriseerde en opgeleide medewerkers.
- Zo nodig wordt de opdracht van het bevoegd gezag in het dossier vastgelegd.
- Protocollering van deze verwerkingen wordt geautomatiseerd ondersteund. Voor zover geautomatiseerde protocollering (nog) niet mogelijk is wordt volgens een landelijke uniforme werkwijze handmatig geprotocolleerd conform de huidige praktijk.
- De bevoegd functionaris is aangewezen, opgeleid, kent zijn bevoegdheden en verantwoordelijkheden en kan deze ook nakomen.

9.4. Verbetermaatregelen

- Definities worden vastgesteld en landelijk raadpleegbaar gemaakt.
- Inventarisatie van de informatiemedewerkers die deze zoekslagen uitvoeren en nagaan of zij voldoende opgeleid zijn. Indien dat niet het geval is dan gebeurt dit alsnog.
- Mede gelet op de naderende Europese Richtlijn wordt de invulling van de loggingseisen, binnen de gestelde termijnen van de richtlijn, geprioriteerd en wordt een mijlpalenplanning opgesteld. De protocollering van ‘geautomatiseerd vergelijken’ en ‘in combinatie verwerken’ maakt daar in ieder geval onderdeel van uit.
- De opleiding voor informatiemedewerkers zal periodiek worden aangeboden en is van voldoende kwaliteit.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Vaststelling definities					Directie IV	Neutraal
2	Inventarisatie en training van informatiemedewerkers					Eenheden	Neutraal
3	Impactanalyse Europese Richtlijn logging en mijlpalenplanning en uitvoeren roadmap					Directie IV, Diensten IM en ICT	Neutraal
4	Optimaliseren opleiding informatiemedewerker					Directies IV en HRM, PA, Eenheden	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

9.5. Risico’s

- De opleiding voor informatiemedewerkers zal moeten concurreren met andere opleidingswensen en is sterk afhankelijk van prioritering van de politie en de Politieacademie.

10. Ter beschikking stellen

Artikel 15
De verantwoordelijke stelt politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verantwoordelijke overeenkomstig artikel 6, tweede lid, zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak.

14.1. Bevindingen audit

De meeste executieve medewerkers hebben de tool BVI-IB ter beschikking gesteld gekregen. Hiermee kunnen online op straat de meest voorkomende systemen met artikel 8- en 13.1-gegevens worden geraadpleegd voor de uitvoering van de dagelijkse politietaak. Voor wat betreft de overige gegevens blijkt dat bevoegd functionarissen vaak te weinig informatie over hun onderzoek willen delen met collega's buiten hun team. Op basis van de interviews stellen wij vast dat er binnen de eenheden nog geen uniform beleid is met betrekking tot het aanstellen en opleiden van bevoegd functionarissen. Bevoegd functionarissen weten niet welke verantwoordelijkheden en bevoegdheden zij hebben en handelen dus niet daarnaar.

14.2. Algemeen

Het centrale principe binnen de Wpg is 'delen, tenzij'. Dit betekent dat politiegegevens ter beschikking gesteld moeten worden ten behoeve van verdere verwerking door andere geautoriseerde personen, zowel binnen de eigen eenheid als binnen andere eenheden, maar ook door ambtenaren van de Kmar en de bijzondere opsporingsdiensten. Voor het politiewerk is het cruciaal om over zoveel mogelijk volledige en juiste gegevens te beschikken.

Om aan dit principe tegemoet te kunnen komen is het noodzakelijk dat het systeem van autorisaties goed is ingericht en daar ook invulling aan wordt gegeven, dat zoveel mogelijk gebruik wordt gemaakt van de basissystemen die het ter beschikking stellen ondersteunen en dat de bevoegd functionaris voldoende is opgeleid en zich bewust is van zijn verantwoordelijkheden op dit vlak.

Ontwikkelingen om politiegegevens eenvoudig te kunnen ontsluiten zijn reeds in gang gezet doordat verschillende applicaties tegelijk bevraagd kunnen worden via BVI-IB en MEOS. Bovendien wordt met het fors terugbrengen van het aantal applicaties en het stimuleren van gebruik van de basissystemen bijgedragen aan een verbeterde terbeschikkingstelling van gegevens.

14.3. Eindtermen

- Nieuwe informatievoorzieningen worden vormgegeven conform privacy en security by design; het ter beschikking stellen van politiegegevens wordt zo mogelijk geautomatiseerd ondersteund.
- Gegevens worden verwerkt in daartoe bestemde (basis)systemen.
- De bevoegd functionaris is aangewezen, opgeleid, kent zijn bevoegdheden en verantwoordelijkheden en kan deze ook nakomen.
- De bevoegd functionaris bepaalt of artikel 9 en 10-gegevens voor een ander doel verder verwerkt kunnen worden.

14.4. Verbetermaatregelen

- De aanwijzing van bevoegd functionarissen wordt geactualiseerd en van de aangewezen personen wordt een registratie bijgehouden.
- Er wordt een procedure ontwikkeld waarin wordt beschreven welke stappen moeten worden ondernomen indien de bevoegd functionaris van functie wisselt.
- De opleiding voor bevoegd functionarissen zal periodiek worden aangeboden en gevolgd
- Door een communicatie- en awarenesscampagne zijn medewerkers zich ervan bewust dat gegevens verwerkt moeten worden in daartoe bestemde systemen.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Actualiseren aanwijzing BF					Directie IV, Eenheden	Neutraal
2	Inrichten registratie BF					Directie IV, Eenheden	Neutraal
3	Procedure functiewisseling BF					Directie IV, Eenheden	Neutraal
4	Opleiding BF verzorgen					Directies IV en HRM, PA, Eenheden	PM
5	Communicatie & awareness					Directie IV, Eenheden	PM

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

14.5. Risico's

- Optimale terbeschikkingstelling is sterk afhankelijk van de IV-vernieuwing, niet alleen binnen de politie maar ook bij de overige partners binnen het Wpg-domein.
- Daarnaast is er een sterke afhankelijkheid van het autorisatieproject. Vertragingen binnen dit project leiden direct tot een verminderde kwaliteit van de terbeschikkingstelling.

11. Audit

Artikel 33
1. De verantwoordelijke doet de uitvoering van de bij of krachtens deze wet gegeven regels controleren door middel van het periodiek doen verrichten van privacy audits.
2. De verantwoordelijke zendt een afschrift van de controleresultaten van de privacy audits aan het College bescherming persoonsgegevens.
3. Indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde, laat de verantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. Het tweede lid is van overeenkomstige toepassing.
(…)

11.1. Bevindingen audit

De Afdeling Korpsaudit is verantwoordelijk voor de interne audits ten behoeve van de Wpg. Daarnaast zijn binnen de eenheden interne auditors aangewezen die de werkzaamheden uitvoeren voor de interne audit. Wij hebben vastgesteld dat de kwaliteit van de eenheidsauditors divers is. Hoewel de kennis op het gebied van politieprocessen en Wpg voldoende aanwezig is, ontbreekt de specifieke auditervaring en opleiding en is de onafhankelijkheid onvoldoende geborgd.

11.2. Algemeen

Een auditfunctie is een belangrijk onderdeel voor een goed functionerende governance en ondersteunt de interne beheersing van de organisatie. De werkzaamheden van de interne auditafdeling kunnen een grote bijdrage leveren aan verbeterde naleving van de Wpg doordat deze door gestructureerd onderzoek een objectief oordeel kunnen verschaffen over de mate waarin op de verschillende deelgebieden wordt voldaan aan de bepalingen van de wet. Vanzelfsprekend zullen wij in nauw overleg met de afdeling Korpsaudit staan om hen in staat te stellen hun toegevoegde waarde te leveren.

De politie heeft besloten de werkzaamheden voor de interne Wpg- audit uit te laten voeren door de auditors van Korpsaudit en de auditors van de eenheden op andere taken in te zetten. Het team Korpsaudit valt beheersmatig onder de directeur Korpsstaf en heeft een rechtstreeks lijn met de Korpschef als opdrachtgever. Vanwege wisseling van de Korpschef en een tijdelijk andere portefeuille verdeling, wordt team Korpsaudit tijdelijk (2015/2016) aangestuurd door het sectorhoofd Nationale Briefing/Korpsstaf. De huidige capaciteit van Korpsaudit is beperkt en kan onder gelijkblijvende omstandigheden niet op een met 2015 vergelijkbare wijze de volgende externe privacy audit ondersteunen. Dit kan deels worden opgevangen door intensiever en gecoördineerd toezicht door privacyfunctionarissen. In het kader van de herijking heeft de directeur Korpsstaf de opdracht om de verdere doorontwikkeling van Korpsaudit naar een brede interne audit functie te realiseren.

11.3. Eindtermen

Onderstaande eindtermen beschrijven hoe interne audits worden uitgevoerd.

- Jaarlijks worden interne audits uitgevoerd conform de eisen uit de regeling door de interne auditor welke voldoet aan de eisen uit de regeling.
- Interne audits worden uitgevoerd op een zodanige wijze dat de externe auditor maximaal kan steunen op het verrichte werk.
- Interne audits worden uitgevoerd door auditors van de afdeling Korpsaudit die voldoende waarborgen heeft ter bescherming van haar onafhankelijkheid.

11.4. Verbetermaatregelen

- De afdeling Korpsaudit stelt een vierjarenplan voor de Wpg audit welke aansluit op de ontwikkelingen in de organisatie en de eisen vanuit de externe audit.
- De activiteiten van de privacyfunctionarissen worden afgestemd met die van de interne auditors, zodat beide functies elkaar versterken en de auditors kunnen steunen op de toezichtactiviteiten.
- Het contact en de kennisuitwisseling tussen Korpsaudit, de portefeuilleondersteuners Wpg, de Wpg-trainers en de privacyfunctionarissen wordt geïntensiveerd door gemeenschappelijke scholing
- De afdeling Korpsaudit zorgt voor voldoende capaciteit (kwalitatief en kwantitatief) voor de uitvoering van de Wpg-audit.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	De afdeling Korpsaudit stelt een vierjarenplan voor de Wpg audit					Korpsaudit, Korpsleiding	Neutraal
2	De activiteiten van de privacyfunctionarissen worden afgestemd met die van de interne auditors					Privacyplatform en Korpsaudit	Neutraal
3	Gemeenschappelijke scholing voor auditors ondersteuners, trainers en privacyfunctionarissen.					Privacyplatform en Korpsaudit, Eenheden, Directie IV	Neutraal
4	De afdeling Korpsaudit zorgt voor voldoende capaciteit (kwalitatief en kwantitatief) voor de uitvoering van de Wpg-audit					Korpsaudit, Korpsleiding	PM

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

11.5. Risico's

- Doordat slechts een beperkt aantal van de auditors voldoet aan de eisen van de Wpg bestaat een continuïteitsrisico voor de uitvoering van interne audits op de Wpg.
- Het waarborgen van de onafhankelijkheid van de afdeling Korpsaudit kan de afstemming van de werkzaamheden van de interne audit met de privacyfunctionarissen bemoeilijken.

12. Privacyfunctionaris

Artikel 34
De verantwoordelijke benoemt een privacyfunctionaris. De privacyfunctionaris ziet namens de verantwoordelijke toe op de verwerking van politiegegevens overeenkomstig het bij of krachtens de wet bepaalde en dient de verantwoordelijke van advies.

12.1. Bevindingen audit

Alle eenheden hebben de beschikking over één of meerdere privacyfunctionarissen. Echter de capaciteit is in een aantal eenheden onvoldoende. Slechts een aantal privacyfunctionarissen houdt op eigen initiatief, veelal beperkt, toezicht. In het verleden is er bij een aantal oud korpsen wel toezicht uitgeoefend en controles gehouden.

12.2. Algemeen

De privacyfunctionaris heeft een belangrijke rol binnen de eenheid in het houden van toezicht en adviseren over de naleving van de Wpg. Hij heeft een eigenstandige taak binnen de eenheid en ondersteunt op nationaal niveau door samenwerking binnen het privacy platform. Dit heeft tot doel een evenredige verdeling van werkzaamheden, afstemming, een effectievere inzet van kennis en capaciteit en het komen tot een zoveel mogelijk eenduidige omgang met en advisering over privacyvraagstukken. De privacyfunctionaris ondersteunt de politiechef op het gebied van privacy en doet dit dus ook op de landelijke portefeuilles van zijn politiechef. Hij is op deze portefeuilles voor zijn collega's het eerste aanspreekpunt

Dat de politie in de audit geen voldoende scoort op dit onderwerp komt doordat onvoldoende capaciteit beschikbaar is voor de functie, maar vooral ook doordat advisering in de praktijk een te zware focus krijgt, ten nadele van toezicht. Oorzaken hiervan kunnen zijn dat sommige eenheden geen meerwaarde erkennen in toezicht of bij de privacyfunctionarissen zelf, die door onvoldoende kennis van de Wpg binnen de organisatie veelvuldig om advies worden gevraagd en in mogelijk niet de vereiste competenties hebben voor toezicht.

12.3. Eindtermen

Onderstaande eindtermen beschrijven hoe de privacyfunctie conform de wet kan worden ingevuld:

- Er is een landelijke functiebeschrijving van de rol, taken en bevoegdheden van de privacyfunctionaris, met inachtneming van bepalingen in de naderende Europese Richtlijn.
- De privacyfunctionaris is benoemd en aangemeld bij de AP.
- De privacyfunctionaris adviseert gevraagd en ongevraagd aan de (leiding van de eenheid en) operatie en de informatie-organisatie.
- De privacyfunctionaris ziet toe op de verwerking van politiegegevens. De resultaten van het toezicht worden vastgelegd in rapportages en in het jaarverslag.
- De activiteiten van de privacyfunctionaris maken onderdeel uit van een stelsel van toezichthoudende maatregelen.

12.4. Verbetermaatregelen

- Aan de hand van een impactanalyse op de naderende Europese Richtlijn wordt bezien in hoeverre de rol, taken en bevoegdheden van de privacyfunctionaris zullen wijzigen.
- Met inachtneming van die wijzigingen wordt een landelijke functiebeschrijving van de rol, taken en bevoegdheden van de privacyfunctionaris opgesteld en deze wordt ondergebracht in het landelijke functiehuis.
- Er wordt capaciteit vrijgemaakt om daadwerkelijk invulling te kunnen geven aan de wettelijke taken.
- Met het instellen van het Privacyplatform wordt de positie van de privacyfunctionaris versterkt door kennisdeling en werkverdeling.
- Het toezicht van de privacyfunctionarissen vindt gecoördineerd plaats conform een jaarlijkse toezichtkalender.
- Activiteiten van de privacyfunctionarissen worden afgestemd met de interne auditor zodat beide functies elkaar versterken.

	Noodzakelijke maatregel	**2016**	**2017**	**2018**	**2019**	**Betrokkenen**	**Budgettaire impact**
1	Aan de hand van een impactanalyse op de naderende Europese Richtlijn wordt bezien in hoeverre de rol, taken en bevoegdheden van de privacyfunctionaris zullen wijzigen.					Directie IV, Privacyplatform	Neutraal
2	Een landelijke functiebeschrijving van de rol, taken en bevoegdheden van de privacyfunctionaris wordt opgesteld en deze wordt ondergebracht in het landelijke functiehuis.					Directie IV, Privacyplatform	Neutraal
3	Er wordt capaciteit vrijgemaakt om invulling te kunnen geven aan de wettelijke taken.					Eenheden, Privacyplatform	PM
4	Met het instellen van het Privacyplatform wordt de positie van de privacyfunctionaris versterkt door kennisdeling en werkverdeling					Privacyplatform	Neutraal
3	Het toezicht van de privacyfunctionarissen vindt gecoördineerd plaats conform een jaarlijkse toezichtkalender.					Privacyplatform	Neutraal
4	Activiteiten van de privacyfunctionarissen worden afgestemd met de interne auditor zodat beide functies elkaar versterken.					Korpsaudit, Privacyplatform	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

12.5. Risico's

- De competenties van de privacyfunctionarissen kunnen onvoldoende aansluiten bij de eisen die gesteld worden aan toezicht waardoor de interne auditfunctie onvoldoende kan steunen op het verrichtte toezicht.
- Door budgetbeperkingen en andere prioritieten blijft er onvoldoende capaciteit beschikbaar voor een goede invulling van de toezichtstaken.

13. Verantwoordelijkheid en in control

Memorie van Toelichting bij art. 33
Met behulp van een systeem van monitoring (evaluaties en privacy audits) dient de verantwoordelijk na te gaan in hoeverre de getroffen verwerkingsmaatregelen en -procedures de doelstelling van de wettelijke normen en het geformuleerde privacybeleid realiseren. De resultaten van de uitgevoerde monitoring vormen de basis voor eventuele correctieve acties, aanpassing van getroffen maatregelen en procedures, dan wel bijstelling van het geformuleerde beleid.

13.1. Bevindingen audit

Er vindt weinig actieve sturing plaats op het onderwerp Wpg. De Wpg krijgt in het totaal van prioriteiten niet altijd voldoende aandacht. In een aantal eenheden staat de Wpg wel met enige regelmaat op de agenda van het eenheidsleidingoverleg (ELO). Bij opsporing en bij informatie-onderdelen is over het algemeen meer sturing, kennis en interesse voor de Wpg aanwezig. Het merendeel van de geïnterviewden geeft aan dat er een vorm van controle van het werk van de medewerker is. Soms in de vorm van collegiale toetsing, soms wordt de controle door de leidinggevende uitgevoerd en dan vaak steekproefsgewijs. Een aantal geïnterviewden geeft aan dat controle op hun werk gemist wordt. Er is nog niet voldoende managementinformatie beschikbaar om te kunnen bijsturen. Er vindt kortom onvoldoende monitoring en (bij)sturing plaats.

13.2. Algemeen

Naleving van wetgeving dient geborgd te zijn in de processen en systemen. IT-systemen kunnen deze borging ondersteunen, maar zijn bij de politie tot dusver in beperkte mate aangepast aan de eisen van de Wpg. In de procesbeheersing strijdt het onderwerp met andere prioriteiten en heeft naleving van de Wpg hinder van de reorganisatie. Managementinformatie is slechts zeer beperkt voor handen. Enerzijds doordat de systemen deze informatie nog niet genereren, anderzijds doordat er onvoldoende vastleggingen zijn van operationele activiteiten (protocollering).

De politie heeft de wens uitgesproken dat de lijn in staat wordt gesteld te sturen op de naleving van de Wpg. Dat betekent dat de politiechefs de verantwoordelijkheid moeten kunnen nemen voor deze naleving. Informatie over de mate waarin activiteiten worden uitgevoerd en hoe controles op die uitvoering verlopen is dan noodzakelijk. Het project Wpg dat liep van 2012 tot 2015 heeft een eerste stap gedaan door het ontwikkelen van indicatoren die de naleving van de Wpg kunnen ondersteunen. Met de invoering van deze indicatoren en de periodieke bespreking van de uitkomsten op die indicatoren in managementgesprekken tussen politiechefs en korpsleiding wordt een belangrijke stap gezet in de sturing op naleving van de Wpg.

Door het opstellen van risico- en control matrices wordt een vervolgstap gemaakt die leidt tot een instrumentarium dat het management in staat gaat stellen gestructureerd de naleving van de Wpg te monitoren en te sturen. Hiervoor wordt een aanpak gehanteerd vergelijkbaar met die van organisaties die zich laten certificeren op basis van normen als ISAE 3402 of ISO 27000. Door de identificatie van de materiële risico's en de belangrijkste beheersmaatregelen op die risico's ontstaat een gestructureerd overzicht van de hiaten in het control-raamwerk dat leidt tot aanvullende acties. Voor de belangrijkste

werkende beheersmaatregelen wordt een rapportage ingeregeld die in de reguliere planning & control cyclus wordt meegenomen.

13.3. Eindtermen

- De voorgestelde aanpak van risico- en control matrices sluit niet aan bij het bestaande management control instrumentarium.
- Er bestaat inzicht in risico's en controls die relevant zijn voor de beheersing van die risico's.
- Indien risico's niet voldoende beheerst worden, worden aanvullende maatregelen getroffen.
- Er is monitoring op de naleving van de Wpg.
- Op korpsniveau zijn periodieke rapportages op de risico's en beheersmaatregelen beschikbaar. Deze worden in managementgesprekken besproken en aan de hand van de uitkomsten wordt indien nodig bijgestuurd.
- Op eenheidsniveau zijn periodieke rapportages op de maatregelen beschikbaar. Deze worden besproken in de managementteams en aan de hand van de uitkomsten wordt indien nodig bijgestuurd.

13.4. Verbetermaatregelen

- Aan de hand van een procesmodel worden de belangrijkste risico's en bijbehorende controls geïdentificeerd. De effectiviteit van de controls wordt beoordeeld
- Daar waar nodig worden aanvullende maatregelen ingevoerd middels actieplannen.
- Er wordt een stelsel van toetsingen en rapportages ingericht
- Door de Directie Financiën (Team Korpscontrol) worden de in 2015 ontwikkelde Wpg-indicatoren verwerkt in de planning & control cyclus.
- De Wpg wordt, net als eerdere jaren, in de korpsprioriteiten meegenomen in de managementgesprekken tussen korpsleiding en eenheidsleiding.

	Noodzakelijke maatregel	2016	2017	2018	2019	Betrokkenen	Budgettaire impact
1	Aan de hand van een procesmodel worden de belangrijkste risico's en bijbehorende controls geïdentificeerd. De effectiviteit van de controls wordt beoordeeld					Directie Operatiën, Privacyfunctionarissen	PM
2	Daar waar nodig worden aanvullende maatregelen ingevoerd middels actieplannen.					Privacyfunctionarissen Eenheidscontrol, Eenheidsleiding	PM
3	Er wordt een stelsel van toetsingen en rapportages ingericht					Eenheidscontrol, Eenheidsleiding, Korpscontrol, Korpsleiding	PM
4	Door de Directie Financiën (Team Korpscontrol) worden de in 2015 ontwikkelde Wpg-indicatoren verwerkt in de planning & control cyclus.					Korpscontrol	Neutraal
5	De Wpg wordt, net als eerdere jaren, in de korpsprioriteiten meegenomen in de managementgesprekken tussen korpsleiding en eenheidsleiding.					Korpscontrol	Neutraal

PM = Pro Memorie (de impact van de activiteiten is nog niet bekend en wordt voorafgaand aan de uitvoering bepaald en verwerkt in de P&C-cyclus)

Budget neutraal = dient binnen bestaande kaders te worden ingevuld na herprioritering

13.5. Risico's

- De aanpak sluit niet aan bij de meer actiegerichte cultuur van de politie waardoor weerstand kan ontstaan tegen de verbetermaatregelen.
- De organisatie en het procesmanagement zijn als gevolg van de reorganisatie mogelijk nog onvoldoende uitgekristalliseerd om risicomanagement op de naleving van de Wpg mogelijk te maken
- De ICT systemen kunnen mogelijk onvoldoende worden aangepast om nieuwe beheersmaatregelen in te voeren en managementinformatie te genereren.

Bijlage A – Afkortingen

afkorting	omschrijving
ADR	Auditdienst Rijk
AP	Autoriteit persoonsgegevens
AVG	Algemene Verordening Persoonsgegevens
AVP	Aanvalsprogramma politie
BF	Bevoegd Functionaris
boa	buitengewoon opsporingsambtenaar
BBVO	Breed Bedrijfsvoeringsoverleg
BOO	Breed Operationeel Overleg
BVH	Basisvoorziening Handhaving
BVI	Basisvoorziening Informatie
BVI-IB	Basisvoorziening Informatie-Integrale Bevraging
Cbp	College bescherming persoonsgegevens
CDO	Chief Data Officer
CIE	Criminele inlichtingen eenheid (thans: TCI)
CISO	Concern Information & Security Officer
DICT	Dienst Informatie- en Communicatietechnologie
DIM	Dienst Informatiemanagement
DRIO	Dienst Regionale Informatie Organisatie
ELO	Eenheidsleiding overleg
EU-VIS	Europees Visuminformatiesysteem
Fb	Functioneel beheer
HRM	Human Resource Management
IAM	Identity & Access Management
IT	Informatietechnologie
ITGC	IT general controls
IV	Informatievoorziening
KMO	Korps management overleg
MEOS	Mobiel Effectiever op Straat
OBT	Operationele Begeleiding en Training
NSIS II	Nationaal Schengen Informatiesysteem II
OM	Openbaar Ministerie
OvJ	Officier van Justitie
PA	Politieacademie
PDC	Politiedienstencentrum
PDCA	Plan, Do, Check, Act kwaliteit cyclus
PF	Privacyfunctionaris
PIA	Privacy Impactassessment
PM	Pro Memorie
RIEC	Regionale Inlichtingen en Expertise Centrum
RTIC	Real Time Intelligence Centre
RvB	Rechten van betrokkene
TCI	Team Criminele Inlichtingen
TOOI	Team Openbare Orde Inlichtingen
VIK	Veiligheid Integriteit en Klachten
VtsPN	(toenmalige) Voorziening tot samenwerking Politie Nederland (thans PDC)
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens