030

0-meting PSbD

<TITEL APPLICATIE>

Versie 2.0

Versie datum 24 april 2018

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
1.0	7-12-2017	Beleid en wetgeving bij criteria aangepast	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

Review commentaar

Versie	Wanneer	Wie	Functie

Inhoudsopgave

Soorten verwerkingen van politiegegevens

Welke verschillende soorten verwerkingen van politiegegevens zijn van toepassing bij de applicatie.
Het gaat hierbij om elke handeling of elk geheel van handelingen met betrekking tot politiegegevens.

Niet-limitatieve opsomming

Soort verwerking	Soort gegevens (bijzonder, gewoon)	X	Toelichting
Verzamelen			
Vastleggen (registreren)			
Ordenen (vb. in categorieën plaatsen)			
Bewaren (opslaan)			
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)			
Wijzigen (het bestaande aanpassen)			
Opvragen (ophalen van gegevens)			
Raadplegen (bekijken van gegevens)			
Gebruiken			
Vergelijken (bv ter verificatie)			
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)			
Samenbrengen (samenvoegen)			
Met elkaar in verband brengen (vanuit de applicatie)			
Afscherming (minder zichtbaar of toegankelijk maken ter bescherming van)			
Uitwissen (weghalen/verwijderen zonder vernietigen)			
Vernietigen			

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X
Dagelijkse politietaak	Artikel 8	
Onderzoek rechtsorde bepaald geval	Artikel 9	
Informatiepositie	Artikel 10	
Informanten	Artikel 12	
Ondersteunende taken	Artikel 13	

Principe 1: eenmalige vastlegging (Z)

"Gegevens worden eenmalig vastgelegd, meervoudig gebruikt"

Criterium 1**:** maakt de voorziening gebruik van de vastgestelde referentiegegevens?	***Toelichting:*** referentiegegevens zijn een verzameling waarden van één gegevenstype waarvan de betekenis, het gebruiksdoel en de inhoud van te voren is vastgelegd. Het is een specifiek voorkomen van een referentie dat eenmalige wordt vastgelegd en meervoudig wordt gebruikt en niet door het operationele proces wordt gewijzigd. Afstemming over deze gegevens zal binnen de politie gedaan moeten worden met de GGB. Vb referentiegegevens: Lijst van nationaliteiten, maatschappelijke klassen, lijst van typen goederen	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 2*:* worden gegevens van het kernobject in het betreffende kernregister geverifieerd?	***Toelichting****:* kernobject is de verzameling gegevens van een bedrijfsobject dat een ankerpunt vormt voor transacties in de bedrijfsfuncties van de politie. Met andere woorden het is een gegevensweergave van tastbare objecten uit de wereld om ons heen. Ze hebben een eigen levenscyclus waar de politie geen bijzondere invloed op heeft. Hetzelfde object kan bij meerdere operationele processen zijn betrokken. De gegevens worden slechts een keer vastgelegd, ongeacht bij hoe veel processen het object betrokken is. Vb kernobject: personen, voertuigen, bedrijven of voorwerpen (goederen).	***Wet/beleid:*** W Art. 4. Lid 1
Evt. opmerkingen / vragen: NVT Nog niet van toepassing, omdat het in ontwikkeling is.		

Criterium 3*:* Worden gegevens van een kernobject in de betreffende Basisregistratie geverifieerd?	***Toelichting****:* Eén en hetzelfde object kan meerdere keren betrokken zijn bij verschillende operationele processen. De kerngegevens van de objecten blijven bij elk politieproces gelijk en zijn dus uitermate geschikt opnieuw gebruikt te worden. Daarom maken ze onderdeel uit van een kernregister. Deze gegevens worden eenmalige in het kernregister vastgelegd, ongeacht hoe vaak ze voorkomen.	***Wet/beleid:*** W Art. 4. Lid 1
Alleen indien er geen kernregister beschikbaar is		
Evt. opmerkingen / vragen:		

Criterium 4*:* Worden gegevens die daarvoor in aanmerking komen vastgelegd volgens het model van kernobjecten?	***Toelichting****:* Een kernobject is de verzameling gegevens van een bedrijfsobject dat een ankerpunt vormt voor vastlegging van transacties in de bedrijfsfuncties van de politie. Het is met andere woorden een gegevensweergave van tastbare objecten uit de wereld om ons heen, zoals personen, voertuigen, bedrijven of voorwerpen (goederen). Die objecten hebben in de buitenwereld hun eigen dynamiek en hun eigen levenscyclus waar de politie geen bijzondere invloed op heeft. Eén en hetzelfde object kan meerdere keren betrokken zijn bij verschillende operationele processen. De kerngegevens van die objecten blijven bij elk politieproces gelijk en deze zijn dus uitermate geschikt om opnieuw gebruikt te worden.	***Wet/beleid:*** B
Evt. opmerkingen / vragen: Deze vraag is vooral van toepassing bij nieuwe ontwikkelingen. Die zouden volgens het model van kernobjecten moeten werken.		

Criterium 5: Indien er sprake is van 'gerede twijfel' over een gegeven wordt dit aan de bronhouder teruggemeld?	***Toelichting****:* 'Gerede twijfel': Er is sprake van gerede twijfel bij een afnemer over de juistheid van een gegeven als er voldaan wordt aan de volgende criteria: • er is een sterk vermoeden dat een (authentiek) gegeven onjuist is • dat vermoeden is gebaseerd op kennis en kunde van de eigen processen en doelgroep van de afnemer (een combinatie van kennis, kunde en gezond verstand) • Men kent de definitie van dit (authentiek) gegeven. De afnemer moet weten wat de definitie van een gegeven in een basisregistratie is om te kunnen beoordelen of het niet klopt. Bij 'gerede twijfel' moet de gebruiker/afnemer dit worden gemeld via de generieke terugmeldvoorziening. De melding wordt, mogelijk na evaluatie,	***Wet/beleid:*** W Art. 4. Lid 1

	gerouteerd naar de (externe) bronhouder dan wel interne uitvoeringsverantwoordelijke.	
Evt. opmerkingen / vragen:		

Criterium 7: Wordt een kerntransactiegegeven in één kerntransactievoorziening geregistreerd.	***Toelichting****:* Een kerntransactie is de verzameling gegevens van een bedrijfsobject die een weergave zijn van een feit of een gebeurtenis, waarvoor geldt dat deze in meerdere bedrijfsfuncties gebruikt worden en veelal direct te relateren zijn aan de wettelijke politietaak: handhaven, opsporen en noodhulp. Kerntransacties bevatten de gegevens over de uitvoering van het werk. Bij de uitvoering van die activiteiten wordt informatie verzameld en vastgelegd over de bedrijfsobjecten die tot de scope van de transactie behoren. Hiermee ontstaat niet alleen informatie over die bedrijfsobjecten zelf, maar ook over de redenen waarom een object relevant is voor het uit te voeren proces. Een transactiegegeven wordt in de regel in één applicatie vastgelegd. Het komt voor dat gegevens over transacties middels functionaliteit van meerdere applicaties worden verwerkt. In dat laatste geval is expliciete inrichting van een kerntransactieregister met dataservices een vereiste. Vb kerntransactie: incidenten, aangiftes	***Wet/beleid:*** B
Alleen indien een kerntransactievoorziening beschikbaar is		
Evt. opmerkingen / vragen: NVT Nog niet van toepassing, omdat het in ontwikkeling is.		

Criterium 8*:* Mag het wijzigen van een gegeven verkregen uit een andere bron alleen indien de (andere) bron hiervoor goedkeuring/opdracht heeft gegeven?	***Toelichting****:* Meervoudige vastlegging dient voorkomen te worden. Voor meervoudige opslag geldt dit eveneens, maar in mindere mate (bijv. voor back-ups).In geval van meervoudige opslag zijn de kaders voor zorgvuldige en rechtmatige gegevensverwerking zoals die gelden voor de bronsystemen onverkort van toepassing. Bovendien moeten extra waarborgen worden getroffen om de kwaliteit en de consistentie van de gegevensverwerking te waarborgen. Eén systeem zal leidend moeten zijn qua beheerhandelingen, en het andere volgend. Een andere consequentie is dat je vanuit de kopiegegevens (de secundaire registratie) geen nieuwe verwerkingen moet doen. Hier is geen aanpassing aan de gegevens mogelijk.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 9*:* Ondersteunt de voorziening het ter beschikking stellen van gegevens aan andere voorzieningen via een gegevensdienstenlaag?	***Toelichting****:* De politie streeft ernaar om in de informatievoorziening gegevens te scheiden van functionaliteit. Gegevens moeten voor meerdere applicaties toegankelijk worden gemaakt via een gegevensdienstenlaag (los van de gegevensverwerkingsdiensten). De moderne netwerkinfrastructuur, applicatieservers en webapplicatie-ontwikkeling moeten het mogelijk maken om webapplicaties te ontwikkelen die snelle interacties met gegevensdiensten ondersteunen.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 10*:* Wordt gecontroleerd of gegevens al bestaan, indien gegevens worden geregistreerd?	***Toelichting****:* Registreer gegevens (waar mogelijk) slechts eenmaal en wel in het daarvoor aangewezen registratieve systeem. Controleer voor invoer of gegevens niet al bestaan.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Principe 2: PDCA-Cyclus (M)

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

Criterium 1: Levert de voorziening stuurinformatie ten behoeve van de reguliere PDCA cyclus?	***Toelichting:*** We willen graag dat reguliere plan- en rapportageproducten zoals jaarplannen en jaarverslagen ook onderdelen bevatten over de omvang van de gegevensverwerking, de kwaliteit van gegevens, aantallen gebruikers, aantallen verstrekkingen, het beheer van autorisaties, beveiligingsmaatregelen en –incidenten.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 2: Worden de rapportages t.b.v. de besturing van de gegevensverwerking periodiek opgeleverd?	***Toelichting:*** Om te voorkomen dat rapportages te ver terug moeten gaan en gegevens inmiddels zijn gewijzigd, is een periodieke rapportage van belang. De besturing van de gegevensverwerking moet als onderdeel van de besturing van het politiewerk worden georganiseerd in een transparant proces met meetbare doelstellingen, rapportages, de resultaten van risicoanalyses en audits, registratie van risico's en periodieke overzichten van incidenten. De managementrapportages moeten daarom ook een paragraaf bevatten over de gegevensverwerking zodat de verantwoordelijke managers kunnen (bij)sturen.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 3: Is het beheer van gegevens, processen en software onderdeel van de PDCA cyclus?	***Toelichting:*** Een belangrijk onderscheid is dat tussen de besturingscyclus (plannen – in werking brengen) en de uitvoeringscyclus (vastleggen – vernietigen). De principes voor omgang met gegevens komen tot uitdrukking of worden vertaald in de besturingscyclus en ze worden zichtbaar in de uitvoeringscyclus; daar waar daadwerkelijk gegevens worden verwerkt. Vanuit de uitvoeringscyclus vindt terugkoppeling plaats voor verbetering en aanpassing van de inrichting van zowel de besturingscyclus als de uitvoeringscyclus. In dit referentiemodel is de PDCA-cyclus herkenbaar van cyclische terugkoppeling in de besturing van de gegevensverwerking. Een belangrijke consequentie van dit uitgangspunt is dat gegevens gedurende hun gehele levenscyclus beheerd moeten worden.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 4: Is een GEB (gegevensbeschermingseffectbeoordeling) uitgevoerd?	***Toelichting:*** Daar waar verwerkingen een risico hebben is het zelf noodzakelijk om er een GEB voor op te stellen. Er is een GEB voor zowel AVG als Wpg. Is er een controle uitgevoerd of een GEB nodig is?	***Wet/beleid:*** W art. 4c Wpg
Alleen indien er sprake is van een nieuwe verwerking met hoog risico of bij een nieuwe technologie		
Evt. opmerkingen / vragen:		

Criterium 5: Is de Autoriteit Persoonsgegevens geraadpleegd?	***Toelichting:*** indien het een verwerking met een hoog risico betreft (of er gebruik wordt gemaakt van een nieuwe technologie), moet de Autoriteit Persoonsgegevens vóóraf worden geraadpleegd.	***Wet/beleid:*** W art. 33b Wpg
Alleen indien nodig na het uitvoeren van de GEB		
Evt. opmerkingen / vragen:		

Criterium 6: Is een verwerkersovereenkomst opgesteld?	***Toelichting:*** een derde partij voert de verwerking uit voor de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke houdt de verantwoordelijkheid en bepaalt welke gegevens op welke manier moeten worden verwerkt. De derde partij (de verwerker) en de verwerkingsverantwoordelijke (de politie) zijn gelijkwaardige partijen. Vb. hierbij kan gedacht worden aan hosting, data-analyse	***Wet/beleid:*** W Art. 6c lid 2 Wpg
Evt. opmerkingen / vragen:		

Criterium 7: Voert de beleidsverantwoordelijke regie op definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens?	***Toelichting:*** Regievoering op beleid, koers en strategie - Regie op verbeteringen - Toezicht op kwaliteit en op voortgang van in werking brengen - Accorderen van definities, classificaties, richtlijnen, eisen en accorderen van regels voor beveiliging - Tijdig (laten) betrekken van de juiste belanghebbenden. Beleidsverantwoordelijke: directeuren en portefeuillehouders (politiechefs)	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Principe 3: Doelbinding (Z)

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

Criterium 1: Is in (het ontwerp van) de voorziening opgenomen wat de verwerkingsgrondslag is van de in de voorziening verwerkte gegevens?	***Toelichting:*** Bij het ontwerp van een informatievoorziening dient ervoor gezorgd te worden dat elk gegeven van zo'n verwerkingsgrondslag wordt voorzien. Zowel de AVG als de Wbp kennen limitatieve verwerkingsgrondslagen.	***Wet/beleid:*** W Art. 3 lid 1
Evt. opmerkingen / vragen:		

***Criterium 2*:** Is het mogelijk meer dan een verwerkingsgrondslag bij een politiegegeven te verwerken?	***Toelichting:*** Bij het toekennen van een nieuwe verwerkingsgrondslag aan gegevens die al een verwerkingsgrondslag hebben, blijft de oude ook bestaan. Een gegeven kan dus tegelijkertijd worden verwerkt op basis van zowel artikel 8, 9, 10, 12, 13 als 14. Zo kan een verlopen rijbewijs bijvoorbeeld in een opsporingsonderzoek gebruikt worden en dan zijn dit tegelijkertijd artikel 8 als 9-gegevens.	***Wet/beleid:*** W Art. 3 lid 1
Alleen indien de voorziening bij verwerking van gegevens meer dan een verwerkingsgrondslag ondersteunt		
Evt. opmerkingen / vragen:		

***Criterium 3*:** Kan een verwerkingsgrondslag automatisch worden herleid?	***Toelichting:*** In registratieve systemen dient een mogelijkheid te zijn om de grondslag af te leiden (indien mogelijk) en vast te leggen. Afleiding kan plaatsvinden op basis van de bedrijfsfunctie (gebaseerd op de selectielijst politie) waarvoor de applicatie bedoeld is. Verder kunnen ook de functie van de medewerker en de locatie waar hij zich bevindt gebruikt worden om de verwerkingsgrondslag af te leiden.	***Wet/beleid:*** B
Alleen bij een registratieve voorziening		
Evt. opmerkingen / vragen:		

***Criterium 4*:** Kan de automatisch afgeleide verwerkingsgrondslag door de gebruiker worden aangepast?	***Toelichting:*** een gebruiker dient af te kunnen wijken van de door het registratieve systeem afgeleide verwerkingsgrondslag.	***Wet/beleid:*** B
Alleen bij een registratieve voorziening		
Evt. opmerkingen / vragen:		

Criterium 5: Kan de verwerkingsgrondslag op een andere wijze worden geregistreerd?	***Toelichting:*** We willen graag dat de verwerkingsgrondslag geautomatiseerd wordt afgeleid. Als dit niet mogelijk is moet deze op een andere manier worden bepaald. In de regel zal de gebruiker dan de verwerkingsgrondslag bepalen en dus moet deze in die gevallen de mogelijkheid hebben deze in te voeren. De verwerkingsgrondslag moet ook daadwerkelijk worden gebruikt bij het toepassen van de andere normen voor zorgvuldige en rechtmatige verwerking, met name bij het autoriseren en bij het bewaren en vernietigen.	***Wet/beleid:*** B
Alleen indien de grondslag niet automatisch kan worden herleid		
Evt. opmerkingen / vragen:		

***Criterium** 6:* Is een goedgekeurd artikel 13-protocol aanwezig?	***Toelichting**:* En als het artikel 13 is, dan ook de datum einde verwerkingstermijn. Deze dient van tevoren bepaald te zijn en vastgelegd te zijn in het artikel 13-protocol dat de betreffende verwerking rechtvaardigt.	***Wet/beleid:*** W Art. 32 lid 1 sub b Wpg
Alleen indien het een artikel 13 verwerking betreft		
Evt. opmerkingen / vragen:		

***Criterium** 7:* is de datum einde verwerkingstermijn opgenomen in het gegevensmodel?	***Toelichting**:* Deze metagegevens over de verwerkingsgrondslagen reizen mee naar de data-analyseomgeving zodat ook daar op de juiste wijze deze gegevens getoond of juist verwijderd kunnen worden.	***Wet/beleid:*** W Art. 32 Wpg
Alleen indien het een artikel 13 verwerking betreft		
Evt. opmerkingen / vragen:		

***Criterium** 8:* Kan de datum einde verwerkingstermijn worden gewijzigd?	***Toelichting**:* En als het artikel 13 is, dan ook de datum einde verwerkingstermijn. Deze dient van tevoren bepaald te zijn en vastgelegd te zijn in het artikel 13-protocol dat de betreffende verwerking rechtvaardigt. Bijvoorbeeld voor gevarenclassificatie: als een persoon als vuurwapengevaarlijk aangemerkt wordt, dan dient bij de invoer van deze gegevens in BVH ook geregistreerd te worden tot wanneer dit label blijft bestaan.	***Wet/beleid:*** B
Alleen indien het een artikel 13 verwerking betreft		
Evt. opmerkingen / vragen:		

***Criterium** 9:* Kan een datum einde verwerkingstermijn meer dan een keer worden geregistreerd?	***Toelichting**:* Binnen één artikel 13-protocol kunnen meerdere termijnen bestaan, zoals in het 'HKS-protocol' waarin beschreven is hoelang antecedentgegevens (de oude HKS-data) verwerkt mogen worden.	***Wet/beleid:*** B
Alleen indien het artikel 13 protocol dit voorschrijft		
Evt. opmerkingen / vragen:		

***Criterium** 10:* Blijft een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn blijft het gegeven begeleiden?	***Toelichting**:* Deze metagegevens over de verwerkingsgrondslagen reizen mee naar de data-analyseomgeving zodat ook daar op de juiste wijze deze gegevens getoond of juist verwijderd kunnen worden.	***Wet/beleid:*** W Art. 32a Wpg
Alleen indien dat gegeven voor een ander doel ter beschikking wordt gesteld		
Evt. opmerkingen / vragen:		

Principe 4: Verantwoording (Z)

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

Criterium 1: Wordt een audittrail geregistreerd?	***Toelichting:*** Een audittrail maakt het mogelijk voor een controlerende instantie om vast te stellen wie, wanneer welke handelingen heeft verricht en hoe besluiten tot stand zijn gekomen. In de regelgeving ten aanzien van gegevensverwerking heet deze vastlegging van handelingen en besluiten de protocolplicht.	***Wet/beleid:*** W Art. 32 Wpg
Evt. opmerkingen / vragen:		

Criterium 2: Worden gegevens van de audittrail aan een generieke voorziening beschikbaar gesteld?	***Toelichting:*** Bij het aanleggen van audittrails gaat het om de keten van handelingen en beslissingen die tot een bepaalde conclusie of besluit geleid hebben. De werkprocessen waarin deze werkzaamheden georganiseerd zijn kunnen over meerdere personen en afdelingen heen lopen. Het is ook mogelijk dat de handelingen en besluiten met behulp van verschillende instrumenten of systemen worden vastgelegd. Omwille van de controleerbaarheid en het goede beheer van de verantwoordingsinformatie heeft het de voorkeur om voor de vastlegging van handelingen en besluiten één registratie te gebruiken. Een generieke voorziening kan een loggingserver zijn, waarin alle handelingen en besluiten uit de verschillende informatievoorzieningen worden geregistreerd ten behoeve van het genereren van een audittrail.	***Wet/beleid:*** B
Alleen indien aanwezig		
Evt. opmerkingen / vragen: NVT: Nog niet van toepassing, omdat de generieke voorziening nog in ontwikkeling is		

Criterium 3: Is de audittrail beveiligd tegen manipulatie?	***Toelichting:*** De registratie van handelingen moet beveiligd worden tegen manipulatie en waarborgen bieden voor bewaring en goede toegankelijkheid om er voor te zorgen dat de bewijskracht voor het verantwoordingsdoel niet in gevaar komt. Dit is van toepassing op de gebruikers, maar ook op het beheer van de voorziening.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 4: Is het mogelijk een rapportage van de audittrail te genereren?	***Toelichting:*** De registratie is daarnaast nadrukkelijk bedoeld voor auditdoeleinden om achteraf aan controlerende instanties bewijs te kunnen leveren over de zorgvuldigheid en rechtmatigheid van de taakuitvoering.	***Wet/beleid:*** W Art. 32a Wpg
Evt. opmerkingen / vragen:		

Principe 5: Autorisatie (Z)

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

Criterium 1: Maakt de voorziening voor het verlenen van toegang gebruik van de generieke IAM- voorziening voor het verifiëren van identiteiten?	***Toelichting:*** Het autorisatiebeheer moet eenvoudig en efficiënt worden ingericht en zo veel mogelijk gebruik maken van geautomatiseerde procedures. We moeten dus zoveel mogelijk voorkomen dat autorisaties op ad hoc basis aan individuen worden toegekend. Noodzakelijke ad hoc autorisaties worden centraal vastgelegd en zijn van tijdelijke aard. Voor nieuwe applicaties geldt daarom de richtlijn om gebruik te maken van een generieke voorziening die autorisaties toekent op basis van de rollen van gebruikers en de kenmerken van de verwerkte gegevens. We noemen dit rol gebaseerde- en attribuut gebaseerde toegang. Momenteel is het beheer van autorisaties versnipperd, regionaal verschillend, chaotisch, het vindt veelal handmatig plaats en er is geen landelijke sturing op. Om deze problemen op te lossen en een systeem van autorisaties te krijgen dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid en de mogelijkheid daar een actueel overzicht van te genereren is het noodzakelijk dat: - de registratie van medewerkers en dienstverbanden uniform, eenduidig en actueel is. Autorisaties komen bij voorkeur geautomatiseerd via het personeelssysteem tot stand. Zodra daar een functie, rol of taak wordt toegekend, gewijzigd of ingetrokken zal dit automatisch tot een autorisatiewijziging leiden. - er een landelijk autorisatiebeheersysteem komt waarin autorisaties centraal worden vastgelegd en decentraal kunnen worden beheerd. Dit autorisatiebeheersysteem moet geautomatiseerd signalen van het HRM-systeem kunnen verwerken (zoals uitdiensttreding en schorsing).	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 2: Maakt de voorziening voor het verlenen van toegang gebruik van de vastgestelde autorisatierollen van de politie?	***Toelichting:*** De visie op autoriseren is verwoord in het document Autorisatiebeleid politie 2016-2020 en vertaalt in de voorziening Identity en Access Management (IAM). Indien geen gebruik wordt gemaakt van de IAM dient de voorziening alsnog te voldoen aan de wettelijke bepalingen van de Wpg en Bpg en de regels uit die visie.	***Wet/beleid:*** **W Art. 6 Wpg**
Alleen indien (nog) niet aangesloten op het autorisatiebeheersysteem IAM		
Evt. opmerkingen / vragen:		

Criterium 3: Maakt de voorziening gebruik van toegangsverlening op gegevensniveau (in plaats van uitsluitend op applicatieniveau)?	***Toelichting:*** Op dit moment worden autorisaties aan gebruikers toegekend per applicatie. Met de ontwikkeling van kernregisters en gegevensdiensten komt het echter steeds vaker voor dat dezelfde gegevens via meerdere applicaties geraadpleegd en verwerkt kunnen worden. Het is daarbij van belang dat gebruikers die niet geautoriseerd zijn voor het raadplegen en verwerken van gegevens via de ene applicatie ook niet onbedoeld via een andere applicatie bij dezelfde gegevens kunnen. Op dit moment wordt dit gewaarborgd door de autorisaties voor verschillende applicaties te baseren op dezelfde autorisatieregels.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 4: Maakt de voorziening voor het verlenen van toegang gebruik van de generieke autorisatietool voor leidinggevenden?	***Toelichting: -***	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 5: Ondersteunt de voorziening Audit Based Access Control toegang?	***Toelichting:*** met de ruimere toegang tot gegevens kan oneigenlijk gebruik van deze gegevens niet worden uitgesloten. Zodanig moet er ter ondersteuning van ABA een goed controle (audit) proces en sanctiebeleid zijn, de kans op controle en een eventuele sanctie achteraf moet misbruik voldoende gesanctioneerd kunnen worden. Herleidbaarheid van de gebruiker en de acties van deze gebruiker moeten dan ook altijd te achterhalen zijn wil ABA succesvol zijn. De focus van ABA concentreert zich volledig op de vraag of de medewerker de verwerking heeft verricht binnen de hem daarvoor opgelegde taakstelling. **Beschrijving hiervan staat in het autorisatiebeleid 2016-2020**	***Wet/beleid:*** **B**
Alleen indien (nog) niet aangesloten op het autorisatiebeheersysteem IAM		
Evt. opmerkingen / vragen:		

Criterium 6: Zijn de gebruikers geïnstrueerd m.b.t. de voor hen geldende autorisatieregels?	***Toelichting:*** Omdat er in de visie op autoriseren autorisaties breed worden toebedeeld is het van belang dat de gebruiker correct wordt geïnstrueerd en opgeleid in de wijziging van het autorisatiebeleid. Meerdere rechten die binnen de (politie)taakstelling vallen hoeven niet altijd daadwerkelijk voor de gebruiker van toepassing te zijn. Ruimere autorisaties versnelt het delen van informatie binnen de organisatie.	***Wet/beleid:*** **W** Art.4a Wpg
Evt. opmerkingen / vragen:		

Criterium 7: Genereert de voorziening rapportages op het gebruik van autorisaties?	***Toelichting:*** Lever rapportages of het gebruik van autorisaties. Vb laatste inlog moment gebruiker.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 8: Worden de toegang- en gebruiksrechten van gebruikers regelmatig gecontroleerd?	***Toelichting:*** Controleren: Voer regelmatig controles uit op toegangs- en gebruiksrechten van medewerkers	***Wet/beleid:*** W Art. 4a Wpg
Evt. opmerkingen / vragen:		

Principe 6: Metagegevens (Z)

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

Criterium 1: Wordt in het ontwerp gebruik gemaakt van de vastgestelde definities voor bedrijfsbegrippen?	***Toelichting:*** Bedrijfsbegrippen worden gedefinieerd zodat de betekenis van de woorden die gebruikt worden bij de uitvoering van het werk, eenduidig beschreven is. Stel definities op voor te verwerken gegevens en gebruik hierbij de leidraad. Dit moet in overleg gedaan worden met het GGB.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

~~***Criterium 2:*** Zijn de van toepassing zijnde vastgestelde Wpg bedrijfsregels geïmplementeerd?~~	~~***Toelichting:*** De bedrijfsbegrippen worden gebruikt in bedrijfsregels. Dit zijn ondubbelzinnige afspraken over de wijze waarop het werk uitgevoerd moet worden. Voor zowel bedrijfsbegrippen als bedrijfsregels is een leidraad opgesteld. Bedrijfsobjecten zijn de bedrijfsbegrippen waar de politie gegevens over verwerkt of wil verwerken. Het Bedrijfsobjectenmodel (BOM) geeft een opsomming van deze bedrijfsobjecten per business-domein. Tevens geeft het aan wat de belangrijkste relaties tussen de objecten zijn. Ten slotte zijn er bedrijfsregels van kracht op de objecten. Voor artikel 1 tot en met 10 van de Wpg zijn er bedrijfsregels beschikbaar die vastgesteld zijn door de Gegevensautoriteit. Het registreren van de herkomst en wijze van verkrijgen van een art. 9-gegeven en art. 10-gegeven is als bedrijfsregel in de set Wpg bedrijfsregels opgenomen.~~	~~***Wet/beleid:*** **B**~~
Evt. opmerkingen / vragen:		

Criterium 3: Wordt het Toepassingsprofiel Metagegevens Politie (TMP) gebruikt?	***Toelichting:*** Het Ontwerpkader Toepassingsprofiel Metagegevens Politie beschrijft hoe het gegevensmodel TMP opgezet moet worden. De afdeling GGB stelt dit gegevensmodel TMP op. Het TMP zal gebaseerd worden op het Toepassingsprofiel Metagegevens Rijk (TMR). Het geformuleerde ontwerpkader is in lijn met de Informatiearchitectuur en het Bestemmingsplan IV. Zo lang het gegevensmodel nog niet beschikbaar is, is het ontwerpkader het document dat de contouren bepaalt.	***Wet/beleid:*** **B**
Alleen indien dit is vastgesteld		
Evt. opmerkingen / vragen: NVT: Nog niet van toepassing, omdat dit nog in ontwikkeling is.		

Criterium 4: Wordt het Toepassingsprofiel Metagegevens Rijk toegepast?	***Toelichting:*** Neem toepassingsprofiel metagegevens mee in requirements. Zolang het TMP nog niet beschikbaar is kan teruggevallen worden op het TMR.	***Wet/beleid:*** **B**
Alleen indien geen TMP is vastgesteld		
Evt. opmerkingen / vragen:		

Criterium 5: Wordt het Politie Gegevensmodel (PGM) toegepast?	***Toelichting:*** Het Politiegegevensmodel (PGM) kan worden gezien als een gegevensgerichte invulling van het BOM, waarbij bedrijfsobjecten uit het BOM geïmplementeerd worden in de logische onderdelen van het PGM. De conceptuele modellen PGM en het dossiermodel zijn geïmplementeerd in fysieke databasemodellen en specificaties voor berichtuitwisseling.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 6: Worden kenmerken van de te verwerken gegevens vastgelegd?	***Toelichting:*** De kenmerken die van de verwerkte gegevens worden vastgelegd moeten onder andere de volgende onderdelen kunnen bevatten: • identificatiekenmerken, • wettelijke verwerkingsgrondslag • kenmerken die noodzakelijk zijn voor het verwerken van gegevens binnen het politieproces en/of binnen de keten, voorbeelden zijn transactie/event, datum, status, vorm, • kenmerken die noodzakelijk zijn voor het verwerken van gegevens in de keten, • de herkomst van de gegevens (verplicht voor art. 9 en 10-gegevens) • de wijze van verkrijging (verplicht voor art. 9 en 10-gegevens is dit verplicht), • logginggegevens, zoals tijd en datum en wie met welke taak is ingelogd.	***Wet/beleid:***: W Art. 4a Wpg
Evt. opmerkingen / vragen:		

Criterium 7: Worden metagegevens die daarvoor in aanmerking komen geautomatiseerd afgeleid en vastgelegd?	***Toelichting:*** Het is van belang dat deze metagegevens op het juiste niveau worden vastgelegd. -De systemen die gebruikt worden voor de gegevensverwerking (de toepassingsdiensten) moeten voorzieningen bieden om de vereiste gegevenskenmerken zo veel mogelijk geautomatiseerd af te leiden uit het object of de transactie. - Bij aanpassingen in informatiesystemen Ontwerpen - Pas de relevante gegevensmodellen aan, waarbij ook de relaties tussen de modellen wordt beheerd. - Zorg dat IV-toepassingen de vereiste metagegevens zoveel mogelijk geautomatiseerd vastleggen.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 8: Worden de metagegevens die niet geautomatiseerd worden vastgelegd op andere manieren ingevuld?	***Toelichting:*** Zie criterium 7	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 9: Worden de metagegevens ook daadwerkelijk gebruikt voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages?	***Toelichting: -***	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		
Criterium 10: Worden de metagegevens meegeleverd bij koppelingen voor verwerking in andere voorzieningen?	***Toelichting:*** Dit is van toepassing bij zowel interne als externe koppelingen	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Principe 7: Kwaliteitszorg (Z)

"De informatievoorziening waarborgt de kwaliteit van de gegevensverwerking"

Criterium 1: Bevat (het ontwerp van) de voorziening requirements met betrekking tot de kwaliteit van gegevens?	***Toelichting:*** Door in de testfase al te meten op de geformuleerde eisen is de kwaliteit van gegevens in een vroegtijdig stadium inzichtelijk. Dit monitoringproces kan ook gestart worden n.a.v. geconstateerde problemen of n.a.v. een GEB. Zie kwaliteitsraamwerk (Kwaliteitszorg).	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 2: Zijn de kwaliteitseisen uit het ontwerp afgestemd met de beleidsverantwoordelijke?	***Toelichting:*** Voorafgaand aan de gegevensverwerking worden de kwaliteitseisen vastgesteld door de beleidsverantwoordelijke voor de gegevens. Voor het formuleren van de kwaliteitseisen kan de politie gebruik maken van onderstaand raamwerk van kwaliteitskenmerken. Gegevenskwaliteit wordt in dit raamwerk ingedeeld in de groepen juistheid, doeltreffendheid en controleerbaarheid.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 3: Zijn de kwaliteitseisen (van het ontwerp) gerealiseerd?	***Toelichting:*** Gegevenskwaliteitseisen van gebruikers (processen of ketenpartners) worden opgesteld en beheerd. De eisen worden gebruikt in IV-voortbrengingsprocessen om First time right (FTR) mogelijk te maken.	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 4: Kunnen afwijkingen van de gegevenskwaliteit handmatig worden aangepast?	***Toelichting:*** Bij herstel van gegevens kan onderscheid gemaakt worden naar dweilen (gegevensherstel/correctie) en het dichtdraaien van de kraan (structureel). Denk bij structureel herstel aan het doorvoeren van verbeteringen in applicaties en procedures. Verbetering van de omgang met gegevens kan ook bereikt worden door opleiding. **Vb. Als er vaak incidenten zijn, wordt het probleem per keer opgelost of wordt gekeken naar de software en waar het probleem vandaan komt?**	***Wet/beleid:*** B
Evt. opmerkingen / vragen:		

Criterium 5: Zijn er bedrijfsregels geformuleerd om de kwaliteit van gegevens te meten?	***Toelichting:*** zijn er definities / regels opgesteld omtrent de gewenste kwaliteit van gegevens. Bijvoorbeeld een volledig adres, ipv alleen de straatnaam of een afgeronde vingerafdruk in plaats van een platte.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 6: Zijn er op basis van deze bedrijfsregels ook geautomatiseerde controles ingebouwd om de gegevenskwaliteit te meten?	***Toelichting:*** het moet duidelijk zijn voor de gebruiker indien hij niet voldoet aan de vereiste kwaliteit. Bijvoorbeeld een rood randje om het invulvakje als het niet voldoet (vb. een postcode moet voldoen aan CCCCLL en iemand vult het als CCCC LL (incl spatie) in.)	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 7: Kan een rapport over de kwaliteit van de gegevens worden samengesteld?	***Toelichting:*** het is belangrijk om een rapportage over de kwaliteit te kunnen opstellen, op deze manier kan in de gaten worden gehouden hoe de kwaliteit van de invoer is en of hier eventueel op gestuurd moet worden.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 8: Worden uitgevoerde kwaliteitscontroles en het resultaat daarvan bewaard?	***Toelichting:***	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 9: Wordt een gebruiker geattendeerd op kwaliteitsafwijkingen? (op basis van de geformuleerde kwaliteitseisen)	*Toelichting:* wordt een melding gegeven als de gebruiker niet voldoet aan de kwaliteitseisen? Vb. een gebruiker kan niet verder / opslaan als niet alle (verplichte) velden zijn ingevuld.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Principe 8: Bewaren en vernietigen (Z)

"Gegevens worden niet langer verwerkt dan is toegestaan en worden vernietigd zodra ze niet langer nodig zijn"

Criterium 1: Zijn de gegevensverwerkende processen geanalyseerd op basis van de Generieke Selectielijst?	***Toelichting:*** In de nieuwe Generieke Selectielijst voor de Nationale Politie (concept, v 0.12, voortaan 'selectielijst') worden de kaders voor het bewaren en vernietigen van politiegegevens en bedrijfsvoeringsgegevens in één instrument gecombineerd. Hierin vind je dus zowel de wettelijke termijnen voor het bewaren en vernietigen van persoonsgegevens volgens de Wpg als de termijnen voor het bewaren en vernietigen van andere (persoons)gegevens op basis van hun waarde voor het bedrijfsvoerings-, verantwoordings- en cultuur-historisch belang. Gaat het hierbij om alle informatie, ongeacht de vorm, die door de politie bij de taakuitvoering wordt opgemaakt of ontvangen. Dit omvat naast documenten ook gestructureerde gegevens en naast tekstinformatie ook multimedia-informatie.	***Wet/beleid:*** **W Art. 14 Wpg**
Indien de GS niet gebruikt wordt, dan is het belangrijk dat art 14 toegepast wordt		
Evt. opmerkingen / vragen:		

Criterium 2: Wordt voldaan aan de wettelijke bepalingen m.b.t. het bewaren, vernietigen en archiveren van (persoons)gegevens?	***Toelichting:*** De Generieke selectielijst voor de documentaire informatie van de politie is te vinden op Agora. Bijlage 1 en 2 bevatten termijn van bewaren en vernietigen. Indien de selectielijst volledig wordt toegepast is de aanname dat daarmee volledig wordt voldaan aan de bewaar- en vernietigplicht van de Wpg. Waar het gaat over verwijderen, bewaren en vernietigen van politiegegevens hebben we te maken met o.a. de volgende wetten: 1: Wet politiegegevens, specifieke regels m.b.t. de verwerkingsgrondslagen 2: Wetboek van Strafrecht, geeft een grondslag voor de periode van bewaring van processen-verbaal met een onbekende dader (PV OD) middels de verjaartermijnen van strafbare feiten. 3: Wetboek van Strafvordering, a: regelt de bewaartermijnen van de 'niet-gevoegde stukken' en de (kopieën) van de processen-verbaal met een bekende dader (PV BD). b: regelt de vernietigingstermijnen, opdracht OM, van artikel 9-gegevens verkregen op grond van artikel 125n en 126cc WvSv (aftappen telecommunicatie) 4: Wet bescherming persoonsgegevens (Wbp). De vernietigingstermijnen worden vastgesteld op basis van het noodzaakscriterium door de verwerkingsverantwoordelijke.	***Wet/beleid:*** **W artikel 8, 9, 10, 12 en 14 Wpg**
Evt. opmerkingen / vragen:		

Criterium 3: Worden de verwerkte gegevens voorzien van een waardering en selectie ten behoeve van bewaren en vernietigen?	***Toelichting:*** In dit uitvoeringskader worden de voorschriften en termijnen voor bewaren en vernietigen niet gespecificeerd, daarvoor verwijzen we naar de selectielijst. We geven hier alleen een toelichting op de systematiek en het gebruik van de selectielijst. De selectielijst is opgesteld aan de hand van de taak- en bedrijfsprocessen van de politie. De processen zijn daarin ingedeeld naar een drietal hoofdcategorieën: Besturen, Uitvoeren en Ondersteunen. In de selectielijst wordt per proces een waardering toegekend aan de informatie die uit dat proces voortvloeit in de zin van bewaren (B) of vernietigen (V).	***Wet/beleid:*** **W Archiefwet**
Evt. opmerkingen / vragen:		

Criterium 4: Worden de gegevens op basis van de geldende termijnen geautomatiseerd verwijderd en vernietigd?	***Toelichting:*** De basissystemen van de politie moeten voorzieningen bevatten voor beheersprocessen en het bewaken van termijnen voor bewaren en vernietigen. Deze beheerhandelingen moeten op één plaats in de informatievoorziening worden uitgevoerd. Als dezelfde gegevens ook in andere systemen gebruikt worden, dan volgen die andere systemen het gegevensbeheer van het bronsysteem. Op deze manier zorgen we er voor dat er maar één versie van de waarheid bestaat zoals het principe Eenmalige vastlegging vereist. Er zijn ook specifieke kaders die richting geven aan het verwijderen en vernietigen van gegevens in de registratieve politiesystemen.	***Wet/beleid:*** **B**
Alleen indien het een registratieve voorziening betreft		
Evt. opmerkingen / vragen:		

Criterium 5: Wordt de verwijdering en de vernietiging van het registratieve bronsysteem gevolgd?	***Toelichting:*** De basissystemen van de politie moeten voorzieningen bevatten voor beheersprocessen en het bewaken van termijnen voor bewaren en vernietigen. Deze beheerhandelingen moeten op één plaats in de informatievoorziening worden uitgevoerd. Als dezelfde gegevens ook in andere systemen gebruikt worden, dan volgen die andere systemen het gegevensbeheer van het bronsysteem. Op deze manier zorgen we er voor dat er maar één versie van de waarheid bestaat zoals het principe Eenmalige vastlegging vereist. Er zijn ook specifieke kaders die richting geven aan het verwijderen en vernietigen van gegevens in de registratieve politiesystemen.	***Wet/beleid:*** **W** Art. 8, 9, 10,12 en 14 OPM: vloeit voort uit de bewaartermijn/verw.grondslagen want als je niet langer mag verwerken moet verwijderd en vervolgens vernietigd worden.
Alleen indien het een raadpleeg- of analysevoorziening betreft		
Evt. opmerkingen / vragen:		

Criterium 6: Worden afloopberichten langs geautomatiseerde weg overgenomen?	***Toelichting:*** Op het juiste moment verwijderen en vernietigen betekent onder andere dat er afloopberichten verwerkt moeten worden. Het gaat bij afloopberichten om twee dingen: juistheid en bewaartermijnen. Als een persoon niet langer als verdachte mag worden gezien, moet deze worden verwijderd.	***Wet/beleid:*** **B**
Alleen indien deze worden verwerkt		
Evt. opmerkingen / vragen:		

Criterium 7: Wordt de beslissing in het afloopbericht automatisch verwerkt?	***Toelichting:*** Dit criterium gaat over het automatisch verwerken van de gevolgen van de beslissing die in het afloopbericht staat. Dus welke gegevens moeten worden verwijderd/vernietigd in geval van een sepot of een veroordeling. Hiervoor moeten bedrijfsregels worden geformuleerd.	***Wet/beleid:*** **B**
Alleen indien deze worden verwerkt		
Evt. opmerkingen / vragen:		

Criterium 8: De voorziening voldoet aan de kwaliteitseisen van de DUTO standaard	***Toelichting:*** Uitvoeringskader: Voor de termijnen waarop gegevens duurzaam bewaard moeten worden, moet de informatievoorziening waarborgen bieden voor duurzame beschikbaarheid en toegankelijkheid. De daarbij geldende kwaliteitseisen zijn te vinden in de DUTO standaard. Eis 1 Er is een informatiemodel waarin alle informatieobjecten zijn beschreven die de organisatie ontvangt en creëert. Eis 2 Informatieobjecten zijn ingedeeld in risicoklassen. Per risicoklasse is het toegankelijkheidsniveau bepaald waaraan de betreffende informatieobjecten moeten voldoen. Eis 3 Er is een vastgestelde Selectielijst waarin is beschreven hoe lang informatieobjecten bewaard worden. Eis 4 Er is een zoekfunctie waarmee alle informatieobjecten vindbaar, binnen redelijk tijd en inspanning. Eis 5 Van elk informatieobject is een weergave beschikbaar, binnen redelijke tijd en inspanning. Eis 6 Van elk informatieobject is een export beschikbaar, binnen redelijke tijd en inspanning. Eis 7 Een informatieobject is toegankelijk voor iedereen die op basis van regelgeving en beleid inzagerecht heeft. Eis 8 Als een informatieobject slechts gedeeltelijk openbaar is, dan zijn er een gedeeltelijke weergave en export beschikbaar waarin alleen de openbare delen zijn opgenomen. Eis 9 Informatieobjecten zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen. Conform de geldende standaarden voor informatiebeveiliging. Eis 10 De export van een informatieobject voldoet aan een open standaard formaat. Eis 11 De weergave en export van elk informatieobject bevat minimaal volledige en actuele metagegevens zoals voorgeschreven in de Richtlijn Metagegevens Overheidsinformatie. Eis 12 Informatieobjecten worden niet eerder en niet later vernietigd dan is aangeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar. Eis 13 Een blijvend te bewaren informatieobject wordt binnen twintig jaar overgebracht naar een archiefbewaarplaats. DUTO is een standaard programma van eisen voor de duurzame toegankelijkheid van overheidsinformatie. De eisen gaan over de inhoud van de overheidsinformatie en de functionaliteit om toegang te krijgen tot overheidsinformatie. Het totale programma van eisen is bedoeld als een specificatie van het hoogste kwaliteitsniveau dat een overheidsorgaan hanteert voor de toegankelijkheid van zijn informatie. Voor informatie waarvoor een minder streng beheerregime toereikend is, kan worden volstaan met een deel van de eisen (zie: 'Implementatie van DUTO'). Dit is ter beoordeling van de overheidsorganisatie zelf, op basis van "pas toe of leg uit". DUTO definieert (nog) geen lagere toegankelijkheidsniveaus, maar een overheidsorgaan kan deze al voor zichzelf vaststellen.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 9: De voorziening ondersteunt het beschikbaar stellen van gegevens aan de voorziening ten behoeve van het duurzaam bewaren van die gegevens	De basissystemen van de politie zijn geen archiefsystemen en bevatten doorgaans ook geen voorzieningen voor duurzaam bewaren. De gegevens die voor langere tijd bewaard moeten worden, moeten dus worden overgebracht naar een archiefsysteem dat daarvoor is toegerust.	***Wet/beleid:*** **W Art. 14 lid 4 Wpg**
Evt. opmerkingen / vragen:		

Criterium 10: Heeft de Poortwachter toegang tot de verwijderde gegevens?	***Toelichting:*** Gegevens die verwijderd zijn maar nog niet vernietigd, kunnen ontsloten worden door een poortwachter. Deze persoon kan zowel gegevens beschikbaar stellen voor hernieuwde verwerkingen als voor audits, toezicht, inzageverzoeken en klachtafhandeling.	***Wet/beleid:*** **W art. 8 Wpg**
Evt. opmerkingen / vragen:		

Principe 9: Informatiebeveiliging (Z)

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

Criterium 1: Is een risicoanalyse voor de verwerking uitgevoerd?	***Toelichting:*** De risico gebaseerde benadering houdt in dat informatiebeveiliging integraal onderdeel is van de verantwoordelijkheid van het lijnmanagement. De verantwoordelijke voor een werkproces of voor een systeem moet de risico's voor informatiebeveiliging in kaart brengen en op basis daarvan eisen stellen aan de ondersteunende diensten. De informatiebeveiligingsarchitectuur biedt hiervoor een methode voor risicoanalyses op basis van beveiligingskenmerken. Naast de bekende beveiligingskenmerken als beschikbaarheid, integriteit en vertrouwelijkheid zijn dit ook andere kenmerken zoals de waarde van informatie, de oorsprong van informatie en het belang van informatie voor het proces. Hieronder valt tevens de wettelijke verplichting tot bescherming van persoonsgegevens.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 2: Zijn de informatiebeveiligingseisen mede bepaald op basis van de resultaten van de risicoanalyse?	***Toelichting:*** Het resultaat is een pakket van informatiebeveiligingseisen. De ondersteunende diensten beoordelen deze eisen op de impact, dat wil zeggen of en hoe deze eisen gerealiseerd kunnen worden en of dit de beveiliging van andere dienstverlening beïnvloed. Bij het realiseren van de eisen wordt door de ondersteunende diensten samengewerkt om te komen tot een optimale mix van maatregelen op de terreinen ICT, Fysiek, Personeel en Organisatie.	***Wet/beleid:*** **W Art. 4a lid 2**
Evt. opmerkingen / vragen:		

Criterium 3: Is de impact van de informatiebeveiligingseisen beoordeeld ten behoeve van de realisatie in de voorziening?	***Toelichting:*** Het resultaat is een pakket van informatiebeveiligingseisen. De ondersteunende diensten beoordelen deze eisen op de impact, dat wil zeggen of en hoe deze eisen gerealiseerd kunnen worden en of dit de beveiliging van andere dienstverlening beïnvloed. Bij het realiseren van de eisen wordt door de ondersteunende diensten samengewerkt om te komen tot een optimale mix van maatregelen op de terreinen ICT, Fysiek, Personeel en Organisatie. Voorbeeld: Is er gekeken naar de impact die een beveiligingseis kan hebben op het gebruik. Je moet een tweefactor authenticatie doen en opeens wil daardoor niemand meer gebruik van de voorziening maken. Dat is een impact die bewust al dan niet geaccepteerd moeten worden.	***Wet/beleid:*** **W Art. 4a lid 2**
Evt. opmerkingen / vragen:		

Criterium 4: Maakt de voorziening gebruik van de aanwezige generieke voorzieningen voor informatiebeveiliging?	***Toelichting:*** De meeste van deze ontwerprichtlijnen gelden niet voor individuele systemen maar moeten generiek in de infrastructuur en de werkprocessen van de organisatie worden georganiseerd. Het is wel van belang om te zorgen dat deze systemen ook daadwerkelijk gebruik maken van deze generieke voorzieningen voor informatiebeveiliging. Voor nadere toelichting op de toepassing van de informatiebeveiligingsprincipes verwijzen we naar de Informatiebeveiligingsarchitectuur en de Uitvoeringsregelingen Informatiebeveiliging van de Dienst ICT	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 5: Zijn alle informatiebeveiligings eisen gerealiseerd door de standaard informatiebeveiligings diensten?	***Toelichting:*** Bij een beveiligingsanalyse wordt er een match gemaakt tussen de beveiligingseisen van de business en de beveiligingsdienstverlening van de uitvoerende diensten. Wanneer beveiligingseisen niet door de standaard informatiebeveiligingsdiensten worden gerealiseerd moet een afweging worden gemaakt om tegen extra kosten aanvullende maatregelen te nemen of om restrisico's te accepteren. Deze restrisico's moeten vervolgens wel worden beheerst door de verantwoordelijke lijnmanager. Hij moet de risico's periodiek monitoren en evalueren. In de reguliere planning- en rapportagecyclus moet daartoe een informatiebeveiligingsparagraaf worden opgenomen.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 6: Zijn maatregelen genomen om informatiebeveiligingseis en te realiseren die niet door de standaard informatiebeveiligingsdie nsten zijn gerealiseerd?	***Toelichting:*** Bij een beveiligingsanalyse wordt er een match gemaakt tussen de beveiligingseisen van de business en de beveiligingsdienstverlening van de uitvoerende diensten. Wanneer beveiligingseisen niet door de standaard informatiebeveiligingsdiensten worden gerealiseerd moet een afweging worden gemaakt om tegen extra kosten aanvullende maatregelen te nemen of om restrisico's te accepteren. Deze restrisico's moeten vervolgens wel worden beheerst door de verantwoordelijke lijnmanager. Hij moet de risico's periodiek monitoren en evalueren. In de reguliere planning- en rapportagecyclus moet daartoe een informatiebeveiligingsparagraaf worden opgenomen.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 7: Worden restrisico's in de beveiliging van de informatievoorziening beheerd?	***Toelichting:*** Bij een beveiligingsanalyse wordt er een match gemaakt tussen de beveiligingseisen van de business en de beveiligingsdienstverlening van de uitvoerende diensten. Wanneer beveiligingseisen niet door de standaard informatiebeveiligingsdiensten worden gerealiseerd moet een afweging worden gemaakt om tegen extra kosten aanvullende maatregelen te nemen of om restrisico's te accepteren. Deze restrisico's moeten vervolgens wel worden beheerst door de verantwoordelijke lijnmanager. Hij moet de risico's periodiek monitoren en evalueren. In de reguliere planning- en rapportagecyclus moet daartoe een informatiebeveiligingsparagraaf worden opgenomen.	***Wet/beleid:*** **B**
Alleen als niet alle informatiebeveiligingseisen zijn gerealiseerd		
Evt. opmerkingen / vragen:		

Principe 10: Privacy by default

"De verwerking van persoonsgegevens is standaard zo beperkt mogelijk ingericht"

Criterium 1: De informatievoorziening is ingericht om de verwerking van persoonsgegevens zo beperkt mogelijk te houden.	***Toelichting:*** Dat geldt voor: • de hoeveelheid verzamelde persoonsgegevens • de mate waarin zij worden verwerkt • de termijn waarvoor zij worden opgeslagen en • de toegankelijkheid daarvan Hierbij is 'pas toe of leg uit'-principe van toepassing. Afwijkingen kunnen mits daar een dwingende reden voor is.	***Wet/beleid:*** **W**
Evt. opmerkingen / vragen:		

Criterium 2: Worden er binnen de informatievoorziening alleen (persoons)gegevens verzameld die voor het doel betreffend zijn.	***Toelichting:*** Als een (persoons)gegeven niet nodig is vraag dit dan niet. Dit is ook van toepassing bij het versturen van gegevens. Indien (persoons)gegeven niet nodig zijn voor een (externe) partij geef deze dan ook niet.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 3: Is er binnen de voorziening sprake van een opt-in regime.	***Toelichting:*** Opt-in: Pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie Opt-out: Automatisch ontvangen totdat het wordt stopgezet	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 4: De informatievoorziening maakt gebruik van Privacy Enhancement Technology (PET) hulpmiddelen.	***Toelichting:*** PET hulpmiddelen zijn: Pseudonimsering: De verwerking van gegevens op zodanige wijze dat het niet meer aan een specifieke betrokkene gekoppeld kunnen worden zonder dat er aanvullende gegevens worden gebruikt. Anonimiseren: De verwerking van gegevens op zodanige wijze dat het niet meer aan een specifieke betrokkene gekoppeld kan worden. Dit proces is onomkeerbaar. Daar moet wel in ogenschouw worden genomen dat alle middelen die hiervoor redelijkerwijs gebruikt kunnen worden door zowel de verantwoordelijke als een derde partij. Versleutelen: De gegevens (in elke vorm) digitaal overgebracht zodanig bewerken dat deze alleen begrijpelijk is als men de beschikking heeft over de toegepaste code.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Principe 11: Toepassen standaarden (L)

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

Criterium 1: Wordt gebruik gemaakt van de van toepassing zijnde bestaande overheids- en ketenstandaarden?	***Toelichting:*** Een standaard is een document dat een set van regels bevat die beschrijven hoe materialen, producten, diensten, technologieën, taken, processen en systemen dienen te worden ontwikkeld en beheerd. (NORA) Standaarden worden vastgelegd binnen een organisatie, een samenwerkingsverband of via een erkende standaardisatie-organisatie (zoals ISO of NEN). Verder kennen standaarden doorgaans een proces waarmee ze ontwikkeld, erkend en beheerd worden. Standaarden kunnen door wet- en regelgeving verplicht worden gesteld. Daarbij wordt doorgaans het ‘pas toe of leg uit’-principe gehanteerd waardoor afwijkingen kunnen worden toegestaan als daar een dwingende reden voor is. De politie moet ook actief deelnemen aan interdepartementale en internationale fora waarin standaarden voor gegevensverwerking worden ontwikkeld en vastgesteld.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 2: Is er een toets uitgevoerd op de standaarden voor gegevensverwerking die van toepassingen zijn?	***Toelichting:*** maak bij ontwerpen en ontwikkelen zo veel mogelijk gebruik van beschikbare standaarden	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 3: Zijn de afwijkingen van geldende standaarden voorzien van een motivatie die is geaccepteerd door de verwerkingsverantwoordelijke?	***Toelichting:*** Pas toe of leg uit	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Principe 12: Verantwoordelijkheden belegd (M)

"De verantwoordelijkheden voor de zorgvuldige en rechtmatige verwerkingen van gegevens zijn eenduidig belegd"

Criterium 1: Is de beleidsverantwoordelijke voor de gegevens die verwerkt worden met de informatievoorziening bekend?	***Toelichting:*** De rol van beleidsverantwoordelijke is belegd bij directeuren en portefeuillehouders (politiechefs). De beleidsverantwoordelijke zal zich voor de uitoefening van de verantwoordelijkheden in de regel laten ondersteunen. Het gaat hierbij om ondersteuning op grond van proces- en beleidskennis en informatiemanagement.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 2: Zijn definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens?	***Toelichting:*** De beleidsverantwoordelijkheid omvat het vaststellen van definities, richtlijnen en kwaliteitseisen. Deze worden, in afstemming met eventuele afnemers, opgesteld door adviseurs. De beleidsverantwoordelijke gaat ook over de beleid, koers en strategie voor de verwerking van gegevens. Denk bij strategie aan kwaliteitsverbetering of verwerven van extra gegevens.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 3: Is de uitvoeringsverantwoordelijke voor de gegevens die verwerkt worden met de informatievoorziening bekend?	***Toelichting:*** De rol van uitvoeringsverantwoordelijke is belegd bij leidinggevenden in de operatie en PDC, bijvoorbeeld een teamchef van een basisteam. Voor politiechefs betekent dit een dubbele rol: zij hebben de uitvoeringsverantwoordelijkheid als lijnchef, maar zij hebben ook een beleidsverantwoordelijkheid in hun rol als landelijk portefeuillehouder. Binnen de operatie worden specifieke taken en bevoegdheden die behoren bij de uitvoeringsverantwoordelijke belegd bij rollen zoals de poortwachter, de privacyfunctionaris (adviseur), de taakaccenthouder (onder andere kwaliteit en gevoelige gegevens) en de bevoegd functionaris (hieronder nog kort toegelicht). Iedere individuele politiemedewerker heeft in zijn rol als gegevensverwerker de taak om gegevens juist te verwerken volgens kaders en richtlijnen. Denk hierbij onder andere aan terugmelden, vastlegging van de verwerkingsgrondslag, verwijderen, archiveren en vernietigen. Verder valt hier ook onder de ontsluiting, interpretatie, het gebruik en mogelijk verstrekken van gegevens met afweging van noodzaak, grondslag en toepassing van beschikbare metagegevens. Specifiek voor artikel 9- en 10-verwerkingen vereist de Wpg dat een bevoegd functionaris aangewezen wordt door de uitvoeringsverantwoordelijke (in naam van 'de verantwoordelijke'). Kern van deze rol is dat zorgvuldig wordt omgegaan met doelafwijkend gebruik van politiegegevens. De bevoegd functionaris besluit onder andere welke gegevens uit een art. 9- of 10-verwerking mogen worden gebruikt binnen een andere verwerking en wie geautoriseerd mag zijn voor gegevens uit 'zijn' onderzoek.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 4: Ondersteunt de voorziening de uitvoeringsverantwoordelijke met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid?	***Toelichting:*** Verkrijgen en vastleggen van gegevens in de werkprocessen, met de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 5: Ondersteunt de voorziening de uitvoeringsverantwoordelijke bij het uitvoeren van correcties?	***Toelichting:*** Herstel: Voor gegevens onder eigen (uitvoerings)verantwoordelijkheid worden waar nodig correcties uitgevoerd.	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 6: Ondersteunt de voorziening de uitvoeringsverantwoordelijke bij het verstrekken van politiegegevens?	***Toelichting:*** Verstrekken: extern delen van politiegegevens conform wet- en regelgeving	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		

Criterium 7: Worden de taken van de gegevensverwerkers om gegevens zorgvuldig en rechtmatig te verwerken door de voorziening ondersteund?	***Toelichting: -***	***Wet/beleid:*** **B**
Evt. opmerkingen / vragen:		