0-meting Privacy & Security by Design

AVR

10.2.e & 10.2.e

Definitief

Versie 1.21

Versie datum 1 mei 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

1 Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.9	13-7-2018	Eerste review
1.0	17-7-2018	Conceptversie
1.1	23-11-2018	Aanpassingen na feedback verwerkt
1.2	19-12-2018	Definitief
1.21	01-05-2019	Typefout percentage aangepast

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.9	13-7-2018	10.2.e	Gegevensautoriteit
1.0	17-7-2018	10.2.e	Gegevensautoriteit
1.1	23-11-2018	10.2.e	Gegevensautoriteit
1.2	19-12-2018	10.2.e	Gegevensautoriteit

Inhoudsopgave

Inleiding

In 2015 heeft een externe audit aangetoond dat verbeteringen op het gebied van Privacy en Security nodig zijn. Nadat eerdere programma's niet tot een bevredigend resultaat hebben geleid, is het verbeterprogramma Wpg en IB gestart om compliancy te realiseren. Met het verbeterprogramma van 2015 zijn politieke toezeggingen in de Tweede Kamer gedaan.

Het meten van de Privacy & Security by Design (PSbD) compliancy van highrisk applicaties is onderdeel van het verbeterprogramma Wpg en IB. Het PSbD uitvoeringskader staat aan de basis om de (highrisk) applicaties van de politie Privacy en Security compliant te laten zijn.

Privacy & Security by Design (PSbD)
PSbD betekent dat tijdens het ontwerpen van informatievoorzieningen rekening moet worden gehouden met informatiebeveiliging en de bescherming van persoonsgegevens. In de ontwerpfase moeten keuzes worden gemaakt die de informatiebeveiliging en bescherming van persoonsgegevens waarborgen. Het betreft zowel technische als organisatorische maatregelen. Dit vereist dat er in een zo vroeg mogelijk stadium wordt nagedacht over het gebruik van persoonsgegevens binnen de organisatie, over de noodzaak van het gebruik van gegevens en over de bescherming ervan.

Dit document beschrijft het resultaat van de 0-meting welke is uitgevoerd bij applicatie AVR. Per principe wordt beschreven of AVR voldoet aan de criteria op basis van wet of beleid. Bij het niet voldoen aan criteria wordt in een actiepunt beschreven op welke manier verbeterd moet worden. De 0-meting dient als hulpmiddel om aan te geven wat moet worden gedaan om PSbD compliant te worden. De score uit de 0-meting is gebaseerd op antwoorden gegeven door de direct betrokkenen van de applicatie.
In dit document wordt bij de aanbevelingen verwezen naar de principes en de onderliggende criteria met de volgende codering [p1c3]. Dit voorbeeld staat voor principe 1 (Éénmalige vastlegging) met criterium 3 (Verificatie in basisregistratie).

0-meting AVR

Algemeen

Doel
Het doel van de PSbD 0-meting is het transparant in beeld brengen wat de actuele volwassenheid van highriskapplicaties op het gebied van PSbD. Vanuit deze 0-meting kan er op basis van de actiepunten toegewerkt worden naar een applicatie die PSbD compliant (Wpg compliant in het bijzonder) is.

Doelgroep
De landelijke portefeuillehouder kan dit document gebruiken om maatregelen te nemen om de applicatie PSbD compliant te maken. De gegevensautoriteit heeft op 22 november 2017 een brief naar de landelijke portefeuillehouder gestuurd omtrent het PSbD compliant maken van applicaties. Het portefeuilleteam voert in overleg met de portefeuillehouder de maatregelen uit. Waarbij de product owner de actiepunten prioriteert en verwerkt op de productbacklog.

Aanwezigen 0-meting

	Naam	Functie
Directe betrokkenen 0-meting AVR	10.2.e	IM Relatiemanager
	10.2.e	Senior Tactische Opsporing
	10.2.e	Dienstenmanager verhoorregistratie
	10.2.e	Landelijke Functioneel beheerder AVR / projectondersteuner
	10.2.e	Functioneel beheerder
	10.2.e	IV-coördinator Functioneel beheer
	10.2.e	Senior Tactische Opsporing
	10.2.e	Senior coördinerend business expert

	Naam	Functie
Toetsing	10.2.e	Adviseur architectuur en modellering
	10.2.e	Programmamanager
	10.2.e	Rijks ICT Trainee

Gesprek datum	Nummer meting	Toelichting
20-12-2017	20171220/AVR toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader Privacy & Security by Design versie 1.0.

AVR

Omschrijving applicatie
AVR is een landelijke applicatie waarmee bepaalde verhoren kunnen worden opgenomen. Door middel van een beslisboom kan een medewerker zien wanneer een verhoor moet worden opgenomen. Het opnemen en het opslaan van de opnames gebeurt in AVR. In principe kunnen alle medewerkers in het systeem. Ook de ketenpartners, zoals het OM en de Rechtbank hebben toegang. Het type delict bepaalt in welke verhoorruimte men gaat zitten. De verhoorruimtes zijn unaniem ingericht (dus elke ruimte is op dezelfde manier met dezelfde apparatuur ingericht). De door AVR opgeslagen gegevens zijn zowel gestructureerd als ongestructureerd. Het gaat om multimediagegevens en om ingevulde invoervelden die vrij zijn. Er is geen toegang op afstand mogelijk. Er is wel een mobiele variant waarmee de gegevens achteraf in AVR kunnen worden opgenomen. Het gaat dan alleen om audio bestanden.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Opm.
Verzamelen		
Vastleggen	X	
Ordenen		
Bewaren	X	
Bijwerken		Metagegevens kunnen worden bijgewerkt, maar dat zijn puur zaakgegevens. Opnamen kunnen niet worden bijgewerkt.
Wijzigen	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken		Binnen de applicatie kan het niet.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling	X	
Samenbrengen	X	Verhoor aan een zaak koppelen, wordt niet gebruikt maar is wel mogelijk. Twee verhoren samenvoegen kan niet.
Met elkaar in verband brengen	X	BVH is leading, dus daar hangt alles aan (BVH-nummer). Maar op het met elkaar wordt samen gebracht in AVR? Nee, want het gaat om een vrij veld (wel verplicht in te vullen, maar je mag er van alles in zetten). AVR moet worden gebruikt voor verhoor, niet voor administratie (zou ook erg foutgevoelig zijn). Het s niet de afspraak (zou niet moeten), maar het wordt wel gedaan.
Afscherming	X	Als X een verhoor opneemt, kan Y er niet zo maar bij. De operationeel beheerder kan er wel bij. Dus afscherming dmv autorisatie.
Uitwissen		
Vernietigen	X	Uitwissen is vernietigen. Weg = weg. Er zijn geen back-ups. NAS-schijf. Toekomstverwachting is het op meerdere fysieke plekken op te slaan.

Verwerkingsgrondslag

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

Artikel 8 (lid 1) Wpg: verwerking met het oog op de uitvoering van de dagelijkse politietaak

Artikel 9 (lid 1) Wpg: gerichte verwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval

Artikel 10 (lid 1) Wpg: gerichte verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde

Artikel 12 (lid 1) Wpg: verwerking met het oog op de controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens.

Artikel 13 Wpg: de politiegegevens van artikel 8, 9 en 10 Wpg mogen verder worden verwerkt ten behoeve van de ondersteuning van de politietaak

Eindscore

AVR scoort een volwassenheidsniveau 0 (onvoldoende). Dit houdt in dat er geen specifieke aandacht voor Privacy & Security by Design (PSbD) is. Zowel op grond van de wet als het politiebeleid voldoet de applicatie niet. Van belang is om nu dat AVR een plan van aanpak maakt hoe zij denkt de applicatie compliant te krijgen. Wij raden aan eerst de wetscriteria te behandelen. Voor een voldoende volwassenheidsniveau is het vereist dat een applicatie voldoende scoort op de wetscriteria. Daarnaast raden wij aan ook goed te kijken naar de 'zware' principes. Het is denkbaar dat, om wat voor reden dan ook, AVR niet kan voldoen aan alle criteria. In ieder geval moet AVR een bewuste en weloverwogen afweging maken waarom niet wordt voldaan aan een bepaald principe.

Advies (de wettelijke actiepunten worden genoemd, de beleidspunten blijken verder uit het document):

- **(Wet artikel 4 lid 1): Zorg dat gegevens van een kernobject worden geverifieerd in de betreffende basisregistratie. [p1c3]**
- **(Wet artikel 4 lid 1): Zorg dat onjuistheden aan de bronhouder kunnen worden teruggemeld. Tijdens de 0-meting kwam al naar voren dat dit technisch wel mogelijk is, maar niet wordt toegepast. [p1c4]**
- **(Wet artikel 14): Zorg dat gegevens niet langer worden bewaard dan noodzakelijk voor het onderzoek. Dit is afhankelijk per onderzoek, het is nog niet duidelijk in hoeverre AVR deze termijnen in de gaten houdt. Indien AVR toch de termijnen van art. 9 Wpg in acht neemt, heeft dit een positieve invloed op de score. [[p8c1]**
- **(Wet artikel 8, 9,10,12 en 14 Wpg): Zorg dat er onderscheid wordt gemaakt tussen bewaren en vernietigen. Als weg daadwerkelijk weg is, kan nooit meer na de afloop van een onderzoek worden gecontroleerd of alles juist is verlopen. Nadat een onderzoek is afgelopen en de gegevens niet langer noodzakelijk zijn, moeten deze 5 jaar 'achter het schot' worden geplaatst (ze zijn dan verwijderd). Op deze manier kan men er niet meer bij, maar kunnen de gegevens door de Poortwachter worden ontsloten in het geval deze nodig zijn voor de afhandeling van klachten en de verantwoording van verrichtingen. Na deze termijn kunnen ze worden vernietigd (art. 14 lid 1 Wpg). De vraag is ook of er überhaupt gegevens weggegooid worden of dat dit alleen op verzoek gebeurt. [p8c2]**
- **(Wet archiefwet): de verwerkte gegevens moeten worden voorzien van een waardering en selectie tbv bewaren en vernietigen. [p8c3]**
- **(Wet artikel 14): de voorziening moet gegevens beschikbaar stellen ten behoeve van het duurzaam bewaren van die gegevens. Op het moment is er nog geen duidelijk lijn waar de politiegegevens duurzaam kunnen worden opgeslagen. Het lijkt er op dat gegevens tbv een strafdossier in CDD+ (het systeem van JustID) worden opgeslagen. Meer informatie hierover is te krijgen bij DIV [p8c9].**
- **(Wet artikel 8): er moet een Poortwachter komen die toegang heeft tot de verwijderde gegevens en deze, indien nodig, kan ontsluiten. Op deze manier kunnen de gegevens weer beschikbaar worden voor audits, klachtenafhandeling etc. [p8c10]**

Aandachtspunt:

- **Tijdens de 0-meting is aangegeven dat veel verhoren op USB-stick of DVD gezet zijn. Door het plaatsen van gegevens buiten het systeem is het niet mogelijk om de zorgvuldigheid en rechtmatigheid te waarborgen. Zorg dat er een manier komt zodat een verhoor niet meer buiten het systeem beschikbaar hoeft te zijn.**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
AVR	20-12-2017	20-12-2017 v1.0	27%	43%	0

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	0%	50%	0
PDCA-cyclus	M	-	NVT	38%	1
Doelbinding	Z	-	NVT	50%	2
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	0%	40%	0
Metagegevens	Z	-	NVT	43%	1
Kwaliteitszorg	Z	-	NVT	56%	2
Bewaren en vernietigen	Z	-	0%	0%	0
Informatiebeveiliging	Z	-	100%	50%	2
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	43%	1
Principe is niet actief		-			
TOTALEN TOETSING		-	27%	43%	

In de afbeelding hierboven staan de volwassenheidsniveaus per principe beschreven. De eerste kolom geeft de weegfactor van het principe op de eindscore weer. De tweede en derde kolom geven het behaalde percentage van de beleids- en wetscriteria weer. Tot slot staat het volwassenheidsniveau per principe weergegeven. Dit niveau is gebaseerd op de score van alle principes van deze toets. In de volgende paragrafen worden de resultaten per principe nader toegelicht.

Nieuwe regelgeving Wpg mei 2018 (buiten de 0-meting)

Vanaf mei 2018 zal nieuwe wetgeving van toepassing zijn. In de huidige score zijn sommige criteria nog als B(eleid) gedefinieerd, terwijl deze van mei 2018 W(et) zullen zijn. De volgende actiepunten zijn nu dus nog beleid, maar AVR moet deze vanaf mei 2018 toepassen om aan de wet te voldoen.

- (Beleid vanaf Q1 2019 wet): Een GEB hoeft alleen uitgevoerd te worden indien er sprake is van een nieuwe verwerking. Dat houdt in dat zodra er aanpassingen aan de functionaliteit worden uitgevoerd, er moet worden gecontroleerd of een GEB moet worden uitgevoerd. Aangezien er aanpassingen voor AVR worden verwacht met betrekking tot mobiel werken moet dit criterium in de gaten worden gehouden. [p2c3]
- (Beleid vanaf Q1 2019 wet): de metagegevens met betrekking tot de verwerkingsgrondslag (en de specifieke doelomschrijving) en verwerkingstermijn moeten het gegeven blijven begeleiden. Het enkel afleiden is niet voldoende. Tijdens de 0-meting werd aangegeven dat gegevens niet worden verstuurd en er dus geen metagegevens moeten worden toegevoegd. Op het moment staat dit punt nog als actiepunt, want er werd ook aangegeven dat de gegevens worden verstrekt. [p3c11]
- (Beleid en vanaf Q1 2019 wet): Zorg dat het mogelijk is om een rapportage van de audittrail te genereren. [p4c4]
- (Beleid en vanaf Q1 2019 wet (artikel 4a)): Zorg dat de instructie voor de gebruikers mbt de autorisatieregels verbeterd wordt. Het moet voor een gebruiker te allen tijde duidelijk zijn wat de geldende autorisatieregels zijn. Niet alleen bij opleiding, maar ook bij een aanpassing van bijvoorbeeld de wet. Hierbij is het van belang dat de gebruiker eventuele aanpassingen op het gebied van autorisatieregels niet gemist kan hebben. Dit moet op meerdere manieren geborgd zijn (bv mail, nieuwspagina, in de voorziening). Dit is een organisatorische maatregel om te voorkomen dat er ongeoorloofde toegang wordt verschaft tot de gegevens. Op dit moment moet ervoor gezorgd worden dat er een nieuwe e-learning komt. [p5c6]
- (Beleid en vanaf Q1 2019 wet): Zorg dat er een periodieke controle op toegang- en gebruiksrechten is. [p5c8]

1.1 Eenmalige vastlegging

"Gegevens worden eenmalig vastgelegd en meervoudig gebruikt"

Naast dat het efficiënter en goedkoper is om gegevens te hergebruiken dan om gegevens opnieuw aan te maken of te verkrijgen zal ook de kwaliteit van gegevens verbeterd worden. Meerdere administratieve registraties van hetzelfde gegeven kunnen zorgen voor onduidelijkheid of inconsistentie van informatie. Bij de inzet van gegevens zal eerst gekeken moeten worden of er een authentieke bron is of dat al gegevens van eenzelfde of aantoonbaar minimaal gelijkwaardige kwaliteit en nauwkeurigheid beschikbaar zijn. In de gevallen waarin de politie met andere partijen samenwerkt, wordt bezien of de benodigde gegevens binnen de operationele en/of bedrijfsvoering keten kunnen worden verkregen.

Het vastleggen van gegevens in AVR gebeurt op dit moment nog niet volgens de criteria van het principe eenmalige vastlegging. De gegevens worden niet geverifieerd in de basisregistratie, terwijl dit op grond van artikel 4 lid 1 Wpg verplicht is. Van de mogelijkheid om onjuistheden terug te melden wordt in AVR geen gebruik gemaakt. Tijdens de 0-meting is aangegeven dat AVR geen terugmeldvoorziening ondersteunt waarmee een 'gerede twijfel' kan worden doorgegeven. Na intern over leg vragen wij ons af of het mogelijk is dat er sprake is van 'gerede twijfel'. Bij 'gerede twijfel' heeft de desbetreffende gebruiker goede gronden om aan te nemen dat het gegeven dat hij gebruikt niet correct is. Een voorbeeld kan zijn als bij een huisbezoek blijkt dat persoon X helemaal niet woonachtig is op dat adres of dat er omschrijvingen zijn van gezichtskenmerken die er later niet blijken te zijn (vb. tattoeages). Het gaat hier niet om een onjuistheid (criterium 5). Bij onjuistheden gaat het meer om kleine foutjes zoals een foutief gespelde achternaam (bijvoorbeeld Jansen ipv Janssen).

Actiepunten:

- **(Wet artikel 4 lid 1): Zorg dat gegevens van een kernobject worden geverifieerd in de betreffende basisregistratie. [p1c3]**
- **(Wet artikel 4 lid 1): Zorg dat onjuistheden aan de bronhouder kunnen worden teruggemeld. Tijdens de 0-meting kwam al naar voren dat dit technisch wel mogelijk is, maar niet wordt toegepast. [p1c4]**
- (Beleid): De gegevens zouden voor de registratie moeten worden gecontroleerd of deze al bestaan. [p1c10].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	0%	50%	0

1.2 PDCA-cyclus

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

Om in de managementverantwoordelijkheid te kunnen voorzien is het belangrijk dat de informatievoorziening stuurinformatie levert zodat er zicht is op de gegevenskwaliteit en de informatiebeveiliging

De volwassenheid van AVR op de cyclische terugkoppeling is niveau 1. Veel van de criteria worden deels toegepast. Er worden bijvoorbeeld wel rapportages opgesteld, maar niet in de applicatie zelf. Bovendien gaan de rapportages niet over de kwaliteit of inhoud van AVR, maar over waar en wanneer AVR is gebruikt. Daarnaast is er te weinig toezicht op kwaliteit. Er worden wel signalen afgegeven, maar er wordt geen volledige regie gevoerd op definities, beleid, de koers en strategie. Tijdens de 0-meting kwam naar voren dat al wel duidelijk is op welke manier de cyclische terugkoppeling zou moeten worden geïmplementeerd, maar dat nog niet alles ook volgens dit systeem werkt.

Voor de AVR is geen gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd. Dit is vanaf mei 2018 alleen verplicht indien er sprake is van een nieuwe verwerking, waarbij er een hoog risico of nieuwe technologie wordt gebruikt. Op het moment dat functionaliteiten worden aangepast in AVR (zoals het mobiel werken) zal wel een GEB moeten worden uitgevoerd. Indien uit de GEB voortvloeit dat het om een verwerking met een hoog risico gaat moet ook de AP worden geraadpleegd. In 2010 is dit al gedaan bij de totstandkoming van de AVR, maar vanaf mei 2018 is dit verplicht in het geval van een nieuwe verwerking met een hoog risico of bij het gebruik van een nieuwe technologie. Aangezien audio een biometrische gegeven is, valt dit in de bijzondere categorie persoonsgegevens. Dit houdt in dat er verzwaarde voorwaarden voor de bescherming van deze gegevens gelden.

Actiepunten:

- (Beleid): De rapportages van AVR zouden niet alleen informatie moeten bevatten over waar en wanneer AVR is gebruikt, maar ook over de kwaliteit en omvang van de gegevens. Ook zou AVR een voorziening moeten bevatten waarmee de rapportage kan worden gemaakt. [p2c1]
- (Beleid): Zorg dat de gehele levenscyclus (vastleggen-vernietigen) van een gegeven beheert wordt volgens de PDCA cyclus. [p2c2]
- **(Beleid --> Wet vanaf Q1 2019): Een GEB hoeft alleen uitgevoerd te worden indien er sprake is van een nieuwe verwerking. Dat houdt in dat zodra er aanpassingen aan de functionaliteit worden uitgevoerd, er moet worden gecontroleerd of een GEB moet worden uitgevoerd. Aangezien er aanpassingen voor AVR worden verwacht met betrekking tot mobiel werken moet dit criterium in de gaten worden gehouden. [p2c3]**
- (Beleid): De beleidsverantwoordelijke (portefeuillehouder, directeur of politiechef) moet meer regie houden op definities, beleid, koers en strategie. Nu is het vooral reactief, maar er moet op voorhand al maatregelen worden genomen. [p2c6]
- (Beleid): AVR zou een voorziening moeten bevatten die de rapportages tbv de besturing geautomatiseerd oplevert. [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	38%	1

1.3 Doelbinding

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

De verwerking van persoonsgegevens kan een inbreuk vormen op de persoonlijke levenssfeer van betrokken. Voor een rechtvaardige gegevensverwerking en om de inbreuk op de levenssfeer van betrokken te beperken mogen gegevens alleen worden verwerkt ten behoeve van voorafgaand opgesteld doel. Verdere verwerking van gegevens kan alleen indien het nieuwe doel niet onverenigbaar is met het doel waarvoor de gegevens oorspronkelijk werden verwerkt. In alle gevallen dat AVR wordt gebruikt gaat het om artikel 9 Wpg-gegevens. Door middel van een beslisboom wordt bepaald of van AVR gebruik moet worden gemaakt. Het is echter niet te controleren of iedereen die gebruik maakt van AVR dit volgens het juiste proces en op de juiste grondslag doet.

Actiepunten:

- (Beleid): op een bepaalde manier zal moeten worden gecontroleerd of iedereen die gebruik maakt van AVR dit op grond van artikel 9 Wpg doet. [p3c6]
- **(Beleid --> Q1 2019 wet): de metagegevens met betrekking tot de verwerkingsgrondslag (en de specifieke doelomschrijving) en verwerkingstermijn moeten het gegeven blijven begeleiden. Het enkel afleiden is niet voldoende. Tijdens de 0-meting werd aangegeven dat gegevens niet worden verstuurd en er dus geen metagegevens moeten worden toegevoegd. Op het moment staat dit punt nog als actiepunt, want er werd ook aangegeven dat de gegevens worden verstrekt. [p3c11]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	NVT	50%	2

1.4 Verantwoording

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

De politie moet over zijn taakuitvoering verantwoording kunnen afleggen. Dit is vooral van belang voor gegevensverwerking in strafzaken en de inzet van opsporings- en geweldsbevoegdheden maar het geldt ook voor de bedrijfsvoering in brede zin. De informatievoorziening moet het daarom mogelijk maken dat de politie verantwoording aflegt over handelingen en de totstandkoming van besluiten. De verantwoording ten aanzien van gegevensverwerking vormt het sluitstuk van de besturing van de informatievoorziening. De verantwoording zorgt tevens dat invulling gegeven kan worden aan de rechten van betrokkenen wiens persoonsgegevens verwerkt worden.

Op het moment scoort AVR een volwassenheidsniveau van 2 (voldoende) op het principe Verantwoording. Een audittrail maakt het voor de controlerende instantie mogelijk om te zien wie wanneer welke handeling heeft uitgevoerd. Hoewel in AVR wel een audittrail wordt geregistreerd, is het niet mogelijk hier een rapportage van te generen. In de huidige Wpg is dit niet verplicht, maar vanaf mei 2018 is dit wel een wettelijke verplichting (artikel 32a Wpg nieuw). Daarnaast is de audittrail niet volledig beveiligd tegen manipulatie. De database-administrator kan er bij. Indien het een Oracle database is moet gecontroleerd worden of de auditfunctie aan staat. In principe staat deze uit en aan het aanzetten zijn licentiekosten verbonden. Er moet een weloverwogen besluit worden genomen om deze wel of niet aan te zetten. Daarnaast worden de gegevens geleverd in een Excel-sheet, dus eventuele manipulatie na ontvangst is niet uitgesloten.

Actiepunt:

- **(Beleid en vanaf Q1 2019 wet): Zorg dat het mogelijk is om een rapportage van de audittrail te genereren. [p4c4]**
- (Beleid): Zorg dat de audittrail optimaal beveiligd is tegen manipulatie. De gegevens worden nu in Excel aangeleverd, waardoor er de mogelijkheid bestaat deze te wijzigen. Door een optimalere beveiliging wordt het verantwoordingsdoel gewaarborgd. Daarnaast is het mogelijk dat een DBA-er een audittrail kan manipuleren indien de auditfunctie in de database uit staat (dit is initieel het geval). Er moet gecontroleerd worden of de auditfunctie uitstaat en of dit een bewuste keuze is. [p4c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	0%	2

1.5 Autorisatie

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

Door de toegang en het gebruik van informatie en systemen te koppelen aan de werkzaamheden waarvoor deze nodig zijn, hoeven autorisaties niet meer op de persoon of het systeem te worden toegekend en wordt het mogelijk om de rechten vanuit de registratie van functies en werkzaamheden te organiseren en te beheren. Dit reduceert de beheerslast, geeft een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

AVR scoort op het principe autorisatie een volwassenheidsniveau van 0 (onvoldoende). De applicatie maakt voor de toegang tot de applicatie wel gebruik van een IAM-voorziening, maar binnen de applicatie niet. Het is mogelijk dat standaardgebruikers bij het aanmaken van een nieuwe zaak, zichzelf de status 'leidinggevende' geven. Op deze manier hebben zij toegang tot alle verhoren, ook van zaken waar ze verder niets mee te maken hebben. Dit is niet toegestaan, maar het is wel mogelijk en dus misbruikgevoelig. De instructie met betrekking tot de bestaande autorisatieregels van AVR is niet voldoende. Nieuwe medewerkers gaan met een ervaren collega zitten, maar het ontbreekt in de applicatie aan waarschuwingen / instructies omtrent (nieuwe) autorisatieregels. Op het moment genereert AVR nog geen rapportages op het gebruik van autorisaties, maar dit is in de nieuwe versie wel opgenomen. De toegang- en gebruiksrechten van gebruikers worden wel middels de techniek gecontroleerd, maar is nog niet operationeel. Dit is vanaf mei 2018 een wettelijke verplichting. Het is verder nog niet duidelijk of AVR gebruik maakt van de generieke autorisatietool voor leidinggevenden.

Actiepunt:

- (Beleid): het zou niet mogelijk moeten zijn dat standaardgebruikers zichzelf de status van leidinggevende geven met de daarbij horende rechten. Binnen de applicatie moet ook gebruik worden gemaakt van een IAM-voorziening. [p5c1]
- (Beleid): Zoek uit of er gebruik wordt gemaakt van de generieke autorisatietool voor leidinggevende [p5c4]
- **(Beleid en vanaf Q1 2019 wet (artikel 4a)): Zorg dat de instructie voor de gebruikers mbt de autorisatieregels verbeterd wordt. Het moet voor een gebruiker te allen tijde duidelijk zijn wat de geldende autorisatieregels zijn. Niet alleen bij opleiding, maar ook bij een aanpassing van bijvoorbeeld de wet. Hierbij is het van belang dat de gebruiker eventuele aanpassingen op het gebied van autorisatieregels niet gemist kan hebben. Dit moet op meerdere manieren geborgd zijn (bv mail, nieuwspagina, in de voorziening). Dit is een organisatorische maatregel om te voorkomen dat er ongeoorloofde toegang wordt verschaft tot de gegevens. Op dit moment moet ervoor gezorgd worden dat er een nieuwe e-learning komt. [p5c6]**
- (Beleid): Zorg dat AVR rapportages geneert op basis van het gebruik van autorisaties. [p5c7]
- **(Beleid en vanaf Q1 2019 wet): Zorg dat er een periodieke controle op toegang- en gebruiksrechten is. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	0%	40%	0

1.6 Metagegevens

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

Om de juistheid en de rechtmatigheid van het gebruik te kunnen waarborgen worden metagegevens vastgelegd over bijvoorbeeld de context, inhoud, structuur, vorm en gedrag evenals het beheer en gebruik. Deze metagegevens bepalen de wijze waarop deze gegevens (mogen) worden verwerkt. Het voordeel van goede metadatering is dat gegevens beter kunnen worden beheerd en teruggevonden.

Op het principe van metagegevens heeft AVR een volwassenheidsniveau van 0 (onvoldoende). Zo lang het Toepassingsprofiel Metagegevens Politie (TMP) nog niet is vastgesteld moet worden teruggevallen op het Toepassingsprofiel Metagegevens Rijk (TMR). Zie voor het volledige overzicht het PSbD uitvoeringskader p. 52 (v. 2.0). De metagegevens worden niet geautomatiseerd afgeleid en vastgelegd. Voor de manieren van het niet-geautomatiseerd invullen van metagegevens bestond ooit een lijst met informatie hoe dit moest. Deze is alleen al heel lang niet meer geactualiseerd.

Actiepunten:

- (Beleid): Zorg dat waar mogelijk bij vernieuwing het TMR moet wordt toegepast. Het toepassingsprofiel moet worden meegenomen in de requirements. Daarnaast is het van belang om de ontwikkeling van het TMP in de gaten te houden. De kenmerken staan op p. 52 van het uitvoeringskader (v.2.0). [p6c4]
- (Beleid): Zorg dat de metagegevens die er voor in aanmerking komen geautomatiseerd worden vastgelegd en afgeleid. [p6c8]
- (Beleid): Zorg dat de lijst waarmee niet-geautomatiseerde metagegevens worden ingevuld wordt geactualiseerd. [p6c9]
- (Beleid): Zorg dat de metagegevens waar mogelijk gebruikt worden voor het verlenen van toegang, de bewaartermijnen, audittrails en managementrapportages. [p6c10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	43%	1

1.7 Kwaliteitszorg

"*De informatievoorziening waarborgt de kwaliteit van de gegevensverwerking*"

Van de politie wordt verwacht dat de kwaliteitseisen (juistheid, doeltreffendheid, controleerbaarheid) van de te verwerken gegevens van te voren bekend zijn. Waarborgen voor gegevenskwaliteit zijn onmisbaar om de juiste werking van systemen en de integriteit van de informatievoorziening als geheel te waarborgen.

AVR heeft een volwassenheidsniveau van 2 (voldoende) op het principe Kwaliteitszorg. Bij het principe Kwaliteitszorg gaat het om de kwaliteit van gegevens. De voorziening moet de gebruiker zo veel mogelijk ondersteunen om er voor te zorgen dat de gegevens correct in worden gevoerd. Hier wordt het First Time Right (FTR) principe gehanteerd. Het moet duidelijk zijn wat de kwaliteitseisen voor een voorziening zijn. Dit kan door middel van het vaststellen van bedrijfsregels.[1]

Actiepunten:

- (Beleid): Zorg dat er bedrijfsregels worden geformuleerd om de kwaliteit van gegevens mee te meten. Bedrijfsregels geven de lat voor de kwaliteit van de benodigde regels aan. In het uitvoeringskader staan in paragraaf 5.7.1 de uitgangspunten en activiteiten omtrent gegevenskwaliteit opgenomen (p. 55, v.2.0). Voor kwaliteitseisen kan worden gekeken naar het raamwerk van kwaliteitskenmerken (p. 56, v.2.0). [p7c5]
- (Beleid): Zorg dat er op basis van de bedrijfsregels regelmatige controles worden ingebouwd zodat de gegevenskwaliteit gemeten kan worden. Met een controle wordt bedoeld dat de voorziening automatisch aangeeft als er door een foutieve invoer de kwaliteit van de gegevens aantast (bijvoorbeeld een postcode die niet uit CCCCLL bestaat). Het gaat hier om het First Time Right (FTR) principe. [p7c6]
- (Beleid): Zorg dat het mogelijk is om een rapport op te stellen over de gegevenskwaliteit. [p7c7]
- (Beleid): Zorg dat indien kwaliteitscontroles worden uitgevoerd dat de resultaten hiervan worden bewaard. [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	56%	2

[1] Uitvoeringskader PSbD v. 1 0, p. 44-45.

1.8 Bewaren en vernietigen

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

Het verwerken van gegevens mag alleen indien er een wettelijke grondslag voor bestaat. Op het moment dat de grondslag komt te vervallen moeten de gegevens worden verwijderd of vernietigd. De bewaartermijn is afhankelijk van het doel waarvoor de gegevens worden verzameld. De gegevens moeten ook duurzaam toegankelijk zijn.

AVR voldoet niet aan het principe van bewaren en vernietigen. Op zowel wettelijke als beleidscriteria scoort de applicatie 0%. Gegevens mogen niet langer worden bewaard dan noodzakelijk. Wat betreft artikel 9-gegevens is de bewaartermijn afhankelijk van de looptijd van het onderzoek. Indien het onderzoek is afgerond moeten de gegevens nog 5 jaar worden bewaard ten behoeve van klachtenafhandeling en verantwoording (artikel 14 lid 1 Wpg). Hierna moeten ze worden vernietigd. Het verschil tussen verwijderen en vernietigen is dat bij verwijderen de gegevens niet meer toegankelijk zijn voor operationele doeleinden. Ze worden 'achter schot' geplaatst. Bij vernietigen bestaat het gegeven daadwerkelijk niet meer, ook niet op een back-up.
In de Generieke Selectielijst zijn de kaders voor het bewaren en vernietigen van politiegegevens opgenomen. Alle gegevensverwerkende processen moeten op basis van deze lijst worden geanalyseerd. Gegevens moeten worden voorzien van een waardering en selectie die voor bewaren en vernietigen wordt gebruikt. Deze processen kunnen worden onderverdeeld in bewaren of (op termijn) vernietigen. Op het moment is de Generieke Selectielijst nog niet van toepassing, dus hoeft alleen te worden voldaan aan de wet (art. 9 jo. Art. 14 Wpg).
Er zijn ook aanvullend kwaliteitseisen voor de DUTO-standaarden. Oftewel de duurzame toegankelijkheid. Er zijn verschillende redenen waarom overheidsinformatie duurzaam toegankelijk moet zijn, maar verantwoording is er een van. Tijdens de 0-meting kwam nog naar voren dat veel verhoren op USB sticks worden opgenomen en daardoor niet in AVR zitten. Hoewel dit buiten de scope van de 0-meting lijkt te vallen is het niet aan te raden dergelijke politiegegevens op te slaan op een USB stick. Het is moeilijk toezicht te houden op dergelijke bestanden, maar alle wetgeving is nog wel van toepassing. Zoals bijvoorbeeld de bewaartermijn. Indien een gegeven moet worden vernietigd geldt dat ook voor versies op andere dragers dan in de applicatie. Daarnaast kan het verlies van een USB stick een datalek opleveren.
Actiepunten:

- **(Wet artikel 14): Zorg dat gegevens niet langer worden bewaard dan noodzakelijk voor het onderzoek. Dit is afhankelijk per onderzoek, het is nog niet duidelijk in hoeverre AVR deze termijnen in de gaten houdt. Indien AVR toch de termijnen van art. 9 Wpg in acht neemt, heeft dit een positieve invloed op de score. [p8c1]**
- **(Wet artikel 8, 9,10,12 en 14 Wpg): Zorg dat er onderscheid wordt gemaakt tussen bewaren en vernietigen. Als weg daadwerkelijk weg is, kan nooit meer na de afloop van een onderzoek worden gecontroleerd of alles juist is verlopen. Nadat een onderzoek is afgelopen en de gegevens niet langer noodzakelijk zijn, moeten deze 5 jaar 'achter het schot' worden geplaatst (ze zijn dan verwijderd). Op deze manier kan men er niet meer bij, maar kunnen de gegevens door de Poortwachter worden ontsloten in het geval deze nodig zijn voor de afhandeling van klachten en de verantwoording van verrichtingen. Na deze termijn kunnen ze worden vernietigd (art. 14 lid 1 Wpg). De vraag is ook of er überhaupt gegevens weggegooid worden of dat dit alleen op verzoek gebeurt. [p8c2]**
- **(Wet archiefwet): de verwerkte gegevens moeten worden voorzien van een waardering en selectie tbv bewaren en vernietigen. [p8c3]**
- (Beleid): de AVR moet waarborgen bieden voor de duurzame beschikbaarheid adhv de DUTO standaarden. [p8c8]
- **(Wet artikel 14): De voorziening moet gegevens beschikbaar stellen ten behoeve van het duurzaam bewaren van die gegevens. Op het moment is er nog geen duidelijk lijn waar de politiegegevens duurzaam kunnen worden opgeslagen. Het lijkt er op dat gegevens tbv een strafdossier in CDD+ (het systeem van JustID) worden opgeslagen. Meer informatie hierover is te krijgen bij DIV [p8c9].**
- **(Wet artikel 8): Er moet een Poortwachter komen die toegang heeft tot de verwijderde gegevens en deze, indien nodig, kan ontsluiten. Op deze manier kunnen de gegevens weer beschikbaar worden voor audits, klachtenafhandeling etc. [p8c10]**

Aandachtspunt:

- Tijdens de 0-meting is aangegeven dat veel verhoren op USB-stick of DVD gezet zijn. Door het plaatsen van gegevens buiten het systeem is het niet mogelijk om de zorgvuldigheid en rechtmatigheid te waarborgen. Zorg dat er een manier komt zodat een verhoor niet meer buiten het systeem beschikbaar hoeft te zijn.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	0%	0%	0

1.9 Informatiebeveiliging

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

Het belang van informatiebeveiliging is op basis van risicobeheersing al mogelijke schadelijke gevolgen door bedreigingen van de informatievoorziening op een bewuste manier afweegt tegen kosten en belemmeringen van beveiligingsmaatregelen. Met daarbij in acht nemen dat de politie een verantwoordelijkheid en verplichting heeft om de gegevens van de burgers te beschermen.

AVR heeft voor het principe informatiebeveiliging een volwassenheidsniveau 2 (voldoende). Er is al een risicoanalyse uitgevoerd, maar nog niet alle eisen zijn al gerealiseerd.

Actiepunten:

- (Beleid): Zorg dat IAM niet alleen voor de toegang van de applicatie worden gebruikt, maar ook in de applicatie. [p9c4]
- (Beleid:) Zorg dat de informatiebeveiligingseisen die uit de risicoanalyse na voren zijn gekomen worden gerealiseerd. [p9c5]
- (Beleid): Zorg dat de restrisico's periodiek worden beheerd. Indien het niet mogelijk is aan de beveiligingseisen te voldoen met behulp van een standaard informatiebeveiligingsdienst, moet de afweging worden gemaakt of extra kosten moeten worden gemaakt. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	100%	50%	2

1.10 Voldoen aan de wet

"*Gegevensverwerking door de politie voldoet aan de daarvoor geldende wettelijke kaders*"

Dit principe is niet besproken aangezien dit in de volgende versie verwijderd gaat worden en de vragen omtrent wetgeving verweven zitten in de andere principes.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Voldoen aan de wet	Zwaar (Z)	NVT	NVT	NVT

1.11 Toepassen standaarden

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

Door het gebruik van bestaande overheids- en ketenstandaarden bevordert de samenwerking tussen de organisaties en de interoperabiliteit van systemen. In de basis is het ban belang om waar mogelijk gebruik te maken van standaardisatie en uniformiteit binnen een informatievoorziening. Indien een organisatie hierin een eigen keuze maakt en afwijkt van standaarden zullen er afspraken gemaakt moeten worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

AVR maakt geen gebruik van overheids- en ketenstandaarden. Vandaar dat de applicatie een volwassenheid van 0 (onvoldoende) heeft. Er moet worden gekeken welke overheids- en / of ketenstandaarden van toepassing zijn op AVR. Hierbij kan worden gedacht aan NORA of ISO en NEN.

Actiepunten:

- (Beleid:) Zoek uit welke overheids- en /of ketenstandaarden van toepassing op AVR zijn en pas deze toe. Zie het uitvoeringskader PSbD v.1.0 op p. 59 en de website van het Rijk voor de verschillende soorten standaarden.[2] [p11c1]
- (Beleid): Zorg dat indien er standaarden van toepassing zijn dat er een toets uitgevoerd wordt op deze standaarden. [p11c2]
- (Beleid): Zorg dat als blijkt dat er afwijkingen van de geldende standaarden zijn, dat deze worden voorzien van een motivatie die is geaccepteerd door de verwerkingsverantwoordelijke. Dit heet ook wel de "comply or explain" procedure. [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	0%	0

[2] Uitvoeringskader PSbD v.1.0, p. 59.

1.12 Verantwoordelijkheden belegd

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

Het is van belang om de verantwoordelijkheden voor gegevensverwerking belegd zijn om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen.

AVR is op bepaalde onderdelen in dit principe afhankelijk van ketenpartners. Op sommige onderdelen moet AVR zelf nog stappen zetten. Het volwassenheidsniveau is 1 (onvoldoende), maar zit dicht tegen een voldoende aan. Dit komt ook omdat enkele criteria met deels zijn beantwoord.

Actiepunten:

- (Beleid): Op het gebied van strategie, beleid, koers en definities moeten waar mogelijk nog enkele zaken worden vastgesteld. De richtlijnen, aanwijzing en brancherichtlijn zijn al wel vastgesteld. Zorg dat er op het gebied van zwerfbestanden afspraken worden gemaakt. Op welke gebieden afspraken moeten worden gemaakt moet worden geïnventariseerd en zo nodig naar gehandeld. Dit geldt ook voor de zaken waar de ketenpartners voor in actie moeten komen. [p12c2]
- (Beleid): Nog niet iedereen die van AVR gebruik maakt is zich bewust van de rechten die zij binnen de voorziening hebben. Een zaakverantwoordelijk is degene met de meeste rechten, maar niet iedereen weet welke rechten hier precies bij horen. De uitvoeringsverantwoordelijk is niet in alle gevallen bekend met de gegevens. Zorg dat de rollen en rechten bekend zijn. [p12c3]
- (Beleid): Zorg dat het proces zo wordt aangepast dat AVR niet alleen de mogelijkheden biedt, maar dat hier ook gebruik van wordt gemaakt. Nu zit het formulier wel in het systeem, maar is het zo slecht dus veel medewerkers willen het niet ondertekenen. Sommige medewerkers gebruiken ook eigen formulieren omdat het formulier in AVR niet (altijd) klopt. In de nieuwe versie zou het formulier zijn aangepast. Deze aanpassing moet dusdanig zijn dat medewerkers geen eigen formulieren meer gaan gebruiken.
- (Beleid): Zorg dat de voorziening de uitvoeringsverantwoordelijke ondersteunen met het verwerken van de juiste classificatie en metagegevens. [p12c4]
- (Beleid): Op het moment kan alleen de beheerder verwijderen en vernietigen, maar het is beter voor de zorgvuldigheid om ook er voor te zorgen dat de uitvoeringsverantwoordelijke correcties uit kan voeren. [p12c5]
- (Beleid): De vrijheid die men heeft om open velden in te vullen is groot en dat ondermijnt de zorgvuldigheid van de ingevoerde gegevens. Zorg dat de voorziening de uitvoeringsverantwoordelijke ondersteunt bij het uitvoeren van correcties. [p12c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	42%	1

2 Verantwoording toetsing

2.1 Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2017-07-20_Uitvoeringskader_Privacy en Security by Design_v1.0'. Vervolgens zijn er criteria toegevoegd of aangescherpt op basis van documenten waar in het uitvoeringskader naar wordt verwezen. Het resultaat is met de auteurs van het uitvoeringskader besproken. Hun commentaar is verwerkt en nogmaals besproken.

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van compliancy van de informatievoorziening.

Herkomst
De herkomst van de criteria is met een W (wetgeving) en een B (beleid politie) gemarkeerd. Het toevoegen van de herkomst is gebaseerd op de gebruikte brondocumenten. Een W werd toegekend als de herkomst rechtstreeks herleidbaar was naar een wet, anders werd het een B. Tevens kan een criteria een W hebben, terwijl daarvan afgeleide criteria een B hebben gekregen. Ter verduidelijking het voorbeeld van het gebruik van basisregistraties. Voorzieningen moeten van de gegevens in die registraties gebruik maken. De politie heeft besloten om niet iedere voorziening afzonderlijk met een basisregistratie te koppelen, maar hiervoor kernregisters te gaan gebruiken. Het gebruik van de basisregistratie is dan een W, terwijl het gebruik maken van het kernregister een B is.

Volwassenheid:
Het resultaat van de toetsing is uitgedrukt in een volwassenheidsniveau voor de volledige toets en per principe. Het volwassenheidsniveau wordt uitgedrukt in een getal, 0 tot en met 3. De niveaus hebben de volgende betekenis (bron: Vooronderzoek_PSbD_Highrisk_applicaties v1.doc):

- Niveau 0: Er is geen specifieke aandacht voor PSbD.
- Niveau 1: Er is wel specifieke aandacht op het gebied van PSbD, maar die is niet toereikend om te voldoen aan de wet (Wpg) op basis van het (politie)beleid.
- Niveau 2: Er is wel specifieke aandacht op het gebied van PSbD en is afdoende om te voldoen aan de wet (Wpg), maar niet toereikend voor het (politie)beleid.
    - Wpg compliant
- Niveau 3: Het aandacht op het gebied van PSbD voldoet aan de wet en het vastgestelde (politie)beleid.
    - PSbD compliant

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[3].

De betekenis van de volwassenheidsniveau ’s is meetbaar gemaakt door het formuleren van de volgende bedrijfsregels. Het uitgangspunt hierbij is dat wettelijke criteria zwaarder wegen dan beleidscriteria.

[3] Bijlage 1: Uitgangspunt bij compliance

Bedrijfsregels volwassenheidsniveau
Als de criteria zijn beoordeeld als “niet van toepassing” dan zijn er geen criteria benoemd of de criteria zijn niet van toepassing gebleken voor de applicatie.

Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan minder dan 35% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan minder dan 35% van de beleidscriteria wordt voldaan.

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan ten minste 35% maar minder dan 100% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria, en aan niet alle van de beleidscriteria wordt voldaan.
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria en aan alle beleidscriteria wordt voldaan
b: aan alle wettelijke criteria wordt voldaan en de beleidscriteria zijn niet van toepassing
c: de wettelijke criteria zijn niet van toepassing, en aan alle beleidscriteria wordt voldaan

NVT : Een volwassenheidsniveau NVT moet worden toegekend, indien de volgende voorwaarde van toepassing is:

a: de wettelijke criteria en de beleidscriteria zijn niet van toepassing

Weegfactor
Van ieder principe is een weegfactor bepaald. Dit zijn L(icht) - M(iddel) en Z(waar). In combinatie met de procentuele score op zowel de wettelijke als beleidscriteria biedt dit de mogelijkheid te prioriteren welke werkzaamheden als eerste moeten worden uitgevoerd om een principe compliant te krijgen aan het uitvoeringskader.

De verdeling van de principes over de weegfactoren is als volgt:

Weegfactor	Licht (L)	Middel (M)	Zwaar (Z)
Aantal	1	3	9

Aandachtspunten
1: Volwassenheidsniveau 1:

Voor het vaststellen van dit niveau maakt het geen verschil of de voorziening of het principe geheel of deels aan een of alle min 1 wettelijke criteria voldoet.

2: Beleidscriteria:

Met uitzondering van niveau 3 geldt dat de mate waarin de voorziening voldoet aan de beleidscriteria, uitgedrukt in een percentage, niet van invloed is op de vaststelling van het volwassenheidsniveau. Het percentage beleidscriteria bij een principe is wel een indicatie of meer of minder inspanning moet worden geleverd om het principe compliant te krijgen aan het uitvoeringskader. Met name in combinatie met de percentages van de wettelijke criteria bij het volwassenheidsniveau 1 en in combinatie met de weegfactor geeft het inzicht bij het prioriteren van werkzaamheden om de voorziening compliant te maken.

3: Privacy functionaris:

De applicatie specifieke requirements mbt PSbD worden tijdens de ontwikkeling bepaald in samenwerking met de Privacy Functionaris en de business expert. Daarnaast is de privacy functionaris eerste aanspreekpunt mbt vragen over privacy.

Disclaimer

Aan de resultaten op basis van het gebruik van de 0-meting wordt geen enkele garantie met betrekking tot de mate van compliance van de getoetste voorziening gegeven. Tevens wordt geen enkele garantie gegeven inzake de juistheid of volledigheid van de checklist als gevolg van veranderende wet- of regelgeving.

3 Bijlage 1: Uitgangspunt bij compliance

De Portefeuillehouder is verantwoordelijk voor ontwikkeling en invoering van de landelijke uniforme oplossing
De Eenheidschef is verantwoordelijk voor het uitvoering van de politietaken met gebruik van de landelijke uniforme oplossing. Na invoering is de landelijke oplossing én de gebruikers in staat om politietaken uit te voeren met de landelijke oplossing

Ergo voor compliance betekent
Compliance in de uitvoering is een verantwoordelijkheid van de Politiechef (eenheidschef)
Compliance in de landelijk uniforme oplossing is een verantwoordelijkheid van de Portefeuillehouder.
Bij compliance van de landelijke uniforme oplossing gaat het óók om de invoering