



0-meting Privacy & Security by Design

PSH-V

10.2.e

Definitief

Versie 1.2

Versie datum 20 december 2018

Rubricering **Politie Intern**

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
1.0	17-04-2018	Eerste conceptversie rapport	
1.1	28-09-2018	Aanpassingen adv feedback direct betrokkenen PSH-V	
1.2	20-12-2018	Definitief	

Review commentaar

Versie	Wanneer	Wie	Functie
1.0	17-04-2018	10.2.e	Gegevensautoriteit
1.1	17-04-2018	10.2.e	Gegevensautoriteit
1.2	20-12-2018	10.2.e	Gegevensautoriteit

© Politie, all rights reserved.

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

Documentinformatie	2
Inhoudsopgave	2
Inleiding	4
0-meting PSH-V	5
Algemeen	5
Doel	5
Doelgroep	5
Aanwezigen 0-meting	5
PSH-V	6
Omschrijving applicatie	6
Soorten verwerkingen van politiegegevens	6
Verwerkingsgrondslag	7
Nieuw wetsregime	7
Eindscore	8
1.1 Eenmalige vastlegging	10
1.2 PDCA-cyclus	11
1.3 Doelbinding	12
1.4 Verantwoording	13
1.5 Autorisatie	14
1.6 Metagegevens	15
1.7 Kwaliteitszorg	16
1.8 Bewaren en vernietigen	17
1.9 Informatiebeveiliging	18
1.10 Voldoen aan de wet	18
1.11 Toepassen standaarden	19
1.12 Verantwoordelijkheden belegd	19
2. Verantwoording toetsing	20
2.1 Toetsingscriteria	20
Disclaimer	22
Bijlage 1: Uitgangspunt bij compliance	23

Inleiding

Eind 2015 heeft de Auditdienst Rijk (ADR) gerapporteerd over uitgevoerde (externe) privacy audit en dat heeft aangetoond dat er op het gebied van Privacy en Security verbeteringen nodig zijn. Het verbeterprogramma Wpg en IB is daarna gestart om compliancy te realiseren (eerdere programma's hebben niet tot een bevredigend resultaat geleid). Met het meerjarig verbeterplan zijn in maart 2016 politieke toezeggingen gedaan aan de Tweede Kamer.¹

Het meten van de Privacy & Security by Design (PSbD) compliancy van highrisk applicaties is onderdeel van het verbeterprogramma Wpg en IB.² Het PSbD uitvoeringskader staat aan de basis om de highrisk applicaties van de politie te laten voldoen aan het PSbD compliancy.

Privacy & Security by Design (PSbD)

PSbD betekent dat al in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de informatievoorzieningen, mechanismen worden ingebouwd voor informatiebeveiliging en de bescherming van persoonsgegevens. 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 PSH-V. Op basis van het de 0-meting zal per principe beschreven worden of ze voldoen aan de criteria van wet en beleid en op welke manier (actiepunten) verbeterd moeten worden. De 0-meting dient als hulpmiddel om duidelijker aan te geven wat er gedaan moet worden om PSbD compliant te worden. De score uit de 0-meting is bepaald 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).

¹ Verbeterplan Wet Politiegegevens en Informatiebeveiliging

² Tranche 2018, Verbeterprogramma Wpg en IB

0-meting PSH-V

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 productowner de actiepunten prioriteert en verwerkt op de productbacklog.

Aanwezigen 0-meting

Directe betrokkenen 0-meting PSH-V	Naam	Functie
	10.2.e	Kern-lid Competence Center Privacy (CCP)
	10.2.e	IV-expert
	10.2.e	IV-expert
	10.2.e	Functioneel beheerder
	10.2.e	Privacy Functionaris
	10.2.e	Functioneel beheerder

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

Analyse datum	Nummer analyse	Toelichting
24-01-2018	2018012401	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader <u>Privacy & Security by Design versie 1.0.</u>

PSH-V

Omschrijving applicatie

Politie Suite Handhaving – Vreemdelingen (PSH-V) is een landelijk informatie- en registratiesysteem ter ondersteuning van de werkprocessen die voortvloeien uit het geïntensiveerde toezicht op vreemdelingen bij de Vreemdelingenpolitie. PSH-V ondersteunt de werkprocessen van AVIM (Afdeling Vreemdelingenpolitie, identificatie en mensenhandel). Het is het primaire proces waarbij de identiteit van een vreemdeling wordt vastgesteld. Het proces begint bij BVID. De BVID-zuil neemt een foto en stuurt die naar PSH-V. Hier wordt de identiteit van een vreemdeling vastgesteld en krijgt de vreemdeling een Vreemdelingen nummer. Dit is aangesloten op BVV (Basisvoorziening Vreemdelingen) en vanuit hier wordt de vreemdeling in de systemen gezocht. Alleen de medewerkers van AVIM werken er in. De Intelligence en meldkamers raadplegen alleen.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Toelichting
Verzamelen	X	
Vastleggen (registreren)	X	
Ordenen (vb. in categorieën plaatsen)	X	
Bewaren (opslaan)	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen (ophalen van gegevens)	X	
Raadplegen (bekijken van gegevens)	X	
Gebruiken	X	
Vergelijken (bv ter verificatie)		Analyses worden door NVIK gedaan. Verdere vergelijking is een menselijke handeling.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	O.a. BVV en keten
Samenbrengen (samenvoegen)		
Met elkaar in verband brengen (vanuit de applicatie)		
Afscherming (minder zichtbaar of toegankelijk maken ter bescherming van)	X	Alleen op projecten onder embargo. Iedereen die toegang heeft tot PSH-V kan het dan nog zien.
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	NVT	
Onderzoek rechtsorde bepaald geval	Artikel 9	NVT	
Informatiepositie	Artikel 10	NVT	
Informanten	Artikel 12	NVT	
Ondersteunende taken	Artikel 13	NVT	
Overige wetten	Art. 6 lid 1 sub c AVG of art. 6 lid 1 sub e AVG jo. Art. 47 Vreemdelingenwet 2000	X	De vreemdelingentaak van de politie is met ingang van de AVG overgeheveld van het Wpg-regime, naar het AVG-regime.

Nieuw wetsregime

Vanaf mei 2018 verandert het wetsregime voor vreemdelingen. Tot deze wijziging werden vreemdelingengegevens verwerkt op grond van de Wpg en de Vreemdelingenwet 2000. Na mei 2018 zullen de vreemdelingengegevens vallen onder de Algemene verordening gegevensbescherming (AVG). Tijdens deze 0-meting is wel uitgegaan van de Wpg en het politiebeleid, maar is ook rekening gehouden met het verspringen van regime vanaf mei 2018. Het is overigens mogelijk dat een vreemdeling op grond van artikel 8 Wpg wordt aangehouden. Het kan dan gaan om een verdachte vreemdeling. Zij komen dan via BVID in PSH-V terecht.

Eindscore

PSH-V heeft een volwassenheidsniveau 1 (onvoldoende). Een voldoende volwassenheidsniveau (niveau 2) is pas te halen op het moment dat een applicatie de maximale score (100%) scoort op alle wetscriteria. Voor PSH-V is het volwassenheidsniveau 1 vooral te wijden de onvoldoende scores op de principes informatiebeveiliging en bewaren en vernietigen. Tijdens de 0-meting kwam naar voren dat een risicoanalyse voor de informatiebeveiliging stond gepland. Ook op het principe bewaren en vernietigen valt nog veel te verbeteren. Aangezien PSH-V vanaf mei 2018 niet meer onder de Wpg valt en ook nog een grondslag heeft in een andere wet wijken de bewaartermijnen af. Ook is PSH-V afhankelijk van de keten als het aankomt op bewaren en vernietigen. Aangeraden wordt hier duidelijkheid over te scheppen. Daarnaast is het van belang dat wordt gekeken naar een manier om gegevens duurzaam toegankelijk te maken en goed te archiveren. Wij adviseren om allereerst naar de wetscriteria waar nog niet aan wordt voldaan te kijken. Pas als hier aan wordt voldaan zal een voldoende volwassenheidsniveau worden behaald.

Advies (wetscriteria):

- **(Wet): Pas PSH-V aan zodat deze het terugmelden van een gegeven in het geval van 'gerede twijfel' wordt ondersteund. (Art. 5 lid 1 sub d AVG; juistheid van gegevens) [p1c6]**
- **(Wet): Zorg dat er voor de Sigma (gegevenscomponent NP) een verwerkingsovereenkomst komt met het Ministerie van Justitie en Veiligheid. [p2c5]**
- **(Wet art 3 lid 1 Wpg): Zorg dat de verwerkingsgrondslag van de in PSH-V verwerkte gegevens in de voorziening is opgenomen (art. 5 lid 1 sub d AVG; juistheid van gegevens) [p3c1].**
- **(Beleid --> Wet vanaf Q4 2018): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden (bijvoorbeeld naar andere data-analyseomgevingen) [p3c11]**
- **(Wet): Stel vast wat de bewaartermijnen van de gegevens zijn en zorg dat dit in de voorziening wordt verwerkt. (art. 5 lid 1 sub e AVG jo. art. 107 lid 9 Vreemdelingenwet 2000). [p8c2]**
- **(Wet): Zorg voor de waardering en selectie van gegevens ten behoeve van bewaren en vernietigen. [p8c3]**
- **(Wet): Zorg dat er naar aanleiding van de risicoanalyse informatiebeveiligingseisen worden opgesteld. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f). [p9c2]**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
PSH-V	24-01-2018	V.1.0	40%	41%	1

Tabel 1: Resultaat toetsing 2 PSbD

PRINCIPE	WEEGFACTOR	PERCENTAGE		VOLWASSENHEID
		W(et)	B(eleid)	
Eenmalige vastlegging	Z	67%	50%	1
PDCA-cyclus	M	0%	30%	0
Doelbinding	Z	0%	50%	0
Verantwoording	Z	100%	0%	2
Autorisatie	Z	100%	20%	2
Metagegevens	Z	NVT	56%	2
Kwaliteitszorg	Z	NVT	44%	1
Bewaren en vernietigen	Z	0%	0%	0
Informatiebeveiliging	Z	0%	20%	0
Voldoen aan de wet	Z	NVT	NVT	NVT
Toepassing standaarden	L	NVT	83%	2
Verantwoordelijkheden belegd	M	NVT	79%	2
Principe is niet actief	-	-	-	-
TOTALEN TOETSING		40%	41%	

VOLWASSENHEID

TOETSING 2

NIVEAU

1

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: AVG mei 2018

Vanaf 25 mei 2018 is de AVG van toepassing. Dat betekent dat sommige punten die nu op beleid staan vanaf dan wet worden. Dit geldt onder andere voor het uitvoeren van een GEB. Als er plannen binnen PSH-V zijn om een nieuwe verwerking toe te passen binnen de voorziening moet er worden gekeken of er een GEB moet worden uitgevoerd.

- **(Beleid, wet vanaf mei 2018): Voer indien nodig een GEB uit als er plannen zijn voor een nieuwe verwerking binnen PSH-V. [p2c3]**

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 ten minste gelijkwaardige kwaliteit en nauwkeurigheid beschikbaar zijn. In de gevallen waarin de politie met andere partijen samenwerkt, wordt gezien of de benodigde gegevens binnen de operationele en/of bedrijfsvoering keten kunnen worden verkregen.

Op het principe eenmalige vastlegging heeft PSH-V een volwassenheidsniveau 1 (onvoldoende) gehaald. PSH-V maakt wel gebruik van verschillende referentiegegevens, maar een deel ervan is niet met zekerheid vastgesteld en een ander deel is geheel niet vastgesteld. Op het moment staat op de planning dat er een terugmeldvoorziening in PSH-V wordt opgenomen. Daarnaast is het mogelijk om gegevens die verkregen zijn uit een andere bron direct aan te passen zonder dit terug te geven aan de bron.

Actiepunten

- (Beleid): Zorg dat waar mogelijk PSH-V gebruik maakt van vastgestelde referentiegegevens. Neem hiervoor contact op met de GGB. [p1c1]
- **(Wet): Pas PSH-V aan zodat deze het terugmelden van een gegeven in het geval van 'gerede twijfel' wordt ondersteund. (Art. 5 lid 1 sub d AVG; juistheid van gegevens) [p1c6]**
- (Beleid): Zorg dat een gegeven verkregen uit een andere bron alleen kan na opdracht van de bron. [p1c8]
- (Beleid): Zorg dat in PSH-V het mogelijk is om gegevens via een gegevensdienstenlaag beschikbaar te stellen aan andere voorzieningen. [p1c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	67%	50%	1

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. Het is aan de betreffende verantwoordelijke managers om keuze te maken op basis van de stuurinformatie.

PSH-V scoort op het principe 'PDCA-cyclus' een zware onvoldoende. De Sigma is gegevenscomponent NP, een onderdeel van de PSH-V suite, bevat functionaliteit en gegevens van de politie. Deze gegevens worden verwerkt door Ministerie van Justitie en Veiligheid. Er is geen verwerkingsovereenkomst met het Ministerie J&V wat wel zou moeten.

Binnen PSH-V is er geen overzicht (stuurinformatie) van beschikbaarheid, gegevenskwaliteit, risico's en gebruikerswaardering aanwezig voor de verantwoordelijke en/of ondersteuningsteam. Enkele criteria uit dit principe zijn op het moment nog beleidscriteria, maar zullen vanaf Q4 2018 wet worden. Het gaat hierbij om het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB) en het raadplegen van de AP. Ook in de AVG zijn deze verplicht (art. 35 en 36 AVG). Op het moment dat er een nieuwe verwerking wordt toegepast in PSH-V moet worden gekeken of een GEB hiervoor nodig is. Een GEB moet *voorafgaand* een verwerking (dus bij een nieuwe verwerking) worden uitgevoerd indien er sprake is van een hoog risico of gebruik wordt gemaakt van een nieuwe technologie. Er komt een checklist waarmee kan worden vastgesteld of een GEB nodig is. Als uit de GEB blijkt dat er risico's zijn waar geen passende maatregelen voor kunnen worden genomen moet de AP worden geraadpleegd (art. 36 AVG). Mocht er sprake zijn van deze situatie is het van belang om eerst contact met de privacy functionaris op te nemen, zodat er centraal geregeld gaat worden dat er eventueel contact met de AP wordt opgenomen.

De levenscyclus van de gegevens is nog niet volledig onderworpen aan de PDCA-cyclus. Hier is nog verbetering op mogelijk. Momenteel is alleen het beheer van processen en software onderdeel van de PDCA-cyclus. Ook het beheer van gegevens moet hier onderdeel van worden. Vanaf het moment van verwerken tot het moment dat gegevens vernietigd worden zou er sprake moeten zijn van een cyclische terugkoppeling. Op de planning staat nog dat rapportages geautomatiseerd worden opgeleverd. De rapportages zijn nuttig voor de verantwoordelijke. Op basis van dergelijke rapportages kan besloten worden (bij) te sturen.

Actiepunten:

- (Beleid) Zorg dat er op basis van stuurinformatie ten behoeve van de PDCA cyclus een rapport opgeleverd wordt. [p2c1]
- (Beleid): Zorg dat de rapportages tbv de besturing van de gegevensverwerking geautomatiseerd op worden geleverd. [p2c2]
- (Beleid) Zorg dat er een GEB uitgevoerd gaat worden indien er sprake is van een nieuwe verwerking. [p2c3]
- **(Wet): Zorg dat er voor de Sigma (gegevenscomponent NP) een verwerkingsovereenkomst komt met het Ministerie van Justitie en Veiligheid. [p2c5]**
- (Beleid): Zorg dat het beheer van gegevens onderdeel wordt van de PDCA-cyclus (life-cycle management). [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	0%	30%	0

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."

Voor elke verwerking is het van belang om te bepalen voor welk doel de gegevens worden verwerkt. Op basis van de doelbinding kan worden gerechtvaardigd waarom (politie)gegevens verwerkt mogen worden.

PSH-V scoort op het principe 'Doelbinding' de laagste score (volwassenheidsniveau 0). Veel van de criteria waren niet van toepassing op PSH-V, maar de punten die van toepassing zijn is de score onvoldoende. In het oorspronkelijke ontwerp is er geen rekening gehouden met de verwerkingsgrondslag. Dat was toen op dat moment geen discussie. Ook in het huidige releasebeleid en in diverse vernieuwingstrajecten is de verwerkingsgrondslag nog geen onderwerp is. Dat neemt niet weg dat wel duidelijk moet zijn waarvoor gegevens in PSH-V worden verwerkt. Ook de AVG staat alleen verwerkingen ten behoeve van een duidelijk omschreven doel toe (art. 5 lid 1 sub b AVG). Voor een rechtmatige verwerking moet er een verwerkingsgrondslag zijn. Deze zijn in art. 6 AVG opgesomd. De grondslag voor de verwerking van persoonsgegevens van vreemdelingen vindt zijn grondslag in de Vreemdelingenwet 2000 en art. 6 lid 1 sub c of e AVG (uitvoering publieke taak van de verwerkingsverantwoordelijke). Het is van belang dat de verwerkingsgrondslag van de verwerkte gegevens in PSH-V is verwerkt.

PSH-V stelt gegevens beschikbaar aan het strafrecht middels NVIK en BVI extracties, daarbij worden geen metagegevens bijgevoegd rondom verwerkingsgrondslag en verwerkingstermijn.

Op dit moment is het in PSH-V niet mogelijk dat een metagegeven een gegeven blijft begeleiden. Dit is van belang om de juistheid en rechtvaardigheid van een gegeven te waarborgen.

Actiepunten:

- **(Wet art 3 lid 1 Wpg): Zorg dat de verwerkingsgrondslag van de in PSH-V verwerkte gegevens in de voorziening is opgenomen (art. 5 lid 1 sub d AVG; juistheid van gegevens) [p3c1].**
- **(Beleid): Zorg dat de verwerkingsgrondslag is opgenomen in het gegevensmodel van PSH-V [p3c2].**
- **(Beleid --> Wet vanaf Q4 2018): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden (bijvoorbeeld naar andere data-analyseomgevingen) [p3c11]**

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

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 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.

PSH-V voldoet aan de wetscriteria uit het principe verantwoording. Echter wordt niet voldaan aan het politiebeleid (0%). Aangezien wel aan de wet wordt voldaan is het volwassenheidsniveau 2 (voldoende). Uit de 0-meting kwam naar voren dat PSH-V wil aansluiten op de loggingserver. De audittrail die wordt geregistreerd is echter niet volledig beveiligd tegen manipulatie. De gebruikers kunnen niets wijzigen, maar de databasebeheerder wel. Er zijn mogelijkheden om een auditfunctie aan te zetten in de voorziening (als PSH-V onder Oracle valt). Dit brengt licentiekosten met zich mee. Er moet een bewuste keuze worden gemaakt om dit wel of niet te doen. Daarnaast zou PSH-V de mogelijkheid een rapportage van de audittrail te genereren moeten ondersteunen. Op deze manier kan beter bewijs worden geleverd aan de toezichthoudende instanties over de zorgvuldigheid en rechtmatigheid van de taakuitvoering.

Actiepunten:

- (Beleid): De audittrail is alleen beveiligd voor gebruikers, maar niet voor databasebeheerders. Het is mogelijk de audittrail te beveiligen tegen manipulatie door databasebeheerders. Zorg dat er een overwogen keuze worden gemaakt om de auditfunctie, waarmee ook de handelingen van databasebeheerders kunnen worden gelogd, aan te zetten of niet. Daarbij zal er gekeken moeten worden na de risico's, kosten en baten [p4c3]
- (Beleid): Zorg dat het mogelijk is om een rapportage van de audittrail te genereren. [p4c4]

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 levert een reductie in beheerslast op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

PSH-V heeft op het principe autorisatie een volwassenheidsniveau van niveau 2. Dat betekent dat het voldoet aan de wet, maar dat er wel verbeterpunten zijn op het gebied van politiebeleid. Uit de 0-meting kwam naar voren dat het niet mogelijk is voor PSH-V om aan te sluiten op IAM. De IAM profielen passen namelijk niet op de AVIM profielen. De ATL staat nog op de planning om in te voeren, maar is nu nog niet actief. Verder maakt PSH-V geen gebruik van toegangsverlening op gegevensniveau, maar uitsluitend op applicatieniveau. Het nadeel daarvan is dat gebruikers die niet geautoriseerd zijn voor het verwerken van gegevens, via een andere applicatie onbedoeld toch toegang kunnen krijgen tot die gegevens.

Het is op dit moment niet mogelijk om periodiek rapportages over de autorisaties te genereren. Op deze manier kan er zicht worden verkregen over het aantal personen die geautoriseerd zijn en of daar nog op gestuurd moet worden door de verantwoordelijke.

Actiepunten:

- (Beleid): Zorg dat er gebruik gemaakt gaat worden van de IAM-voorziening (incl. IAM profielen). [p5c1]
- (Beleid): Onderzoek de mogelijkheden om de toegangsverlening uitsluitend op gegevensniveau te laten plaatsvinden en niet op applicatieniveau. Op deze manier voorkom je dat gebruikers via een omweg alsnog bij bepaalde gegevens kunnen komen, terwijl ze daar niet voor geautoriseerd zijn. [p5c3]
- (Beleid): Zorg dat PSH-V gebruik maakt van ATL. [p5c4]
- (Beleid): Zorg dat de voorziening periodiek rapportages over de autorisaties kan genereren. [p5c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	20%	2

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.

De score op het principe metagegevens is voldoende met een volwassenheidsniveau 2. Tijdens de 0-meting kwam naar voren dat het Politie Gegevensmodel (PGM) niet is toegepast omdat deze dateert van na de ontwikkeling van PSH-V. Iets toepassen dat nog niet bestaat is niet mogelijk, maar het is belangrijk om te kijken of de architectuur nog aansluit op de hedendaagse ontwikkelingen. Daarnaast moeten de kenmerken van de verwerkte gegevens bepaalde onderdelen bevatten. Zoals een identificatiekenmerk, de wettelijke grondslag, noodzakelijk kenmerken voor het verwerken van gegevens binnen het politieproces en de loggingsgegevens. Voor een uitgebreider beschrijving van deze gegevens verwijzen wij naar het uitvoeringskader Privacy & Security by Design V1.0 pagina 43.

Metagegevens zouden ook moeten worden gebruikt voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. Daar is op het moment nog geen sprake van.

Actiepunten

- (Beleid): Zorg dat er gebruik wordt gemaakt van vastgestelde definities voor bedrijfsbegrippen. Neem zo nodig contact met de GGB. [p6c1]
- (Beleid): Zorg dat PSH-V op architectuurniveau bekeken gaat worden met de hedendaagse ontwikkelingen. [p6c5]
- (Beleid): Stel de kenmerken vast waar verwerkte gegevens aan moeten voldoen. Zie ook het uitvoeringskader v.1.0 p. 43. [p6c7]
- (Beleid): Zorg dat metagegevens gebruikt worden voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. [p6c10]

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

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.

Op het principe kwaliteitszorg wordt onvoldoende gescoord door PSH-V. Het heeft een volwassenheidsniveau 1 en een score van 44% op de beleidscriteria (er zijn geen wetscriteria bij de principe). Er is op een aantal punten verbetering mogelijk. Allereerst de bedrijfsregels die zijn geformuleerd om de kwaliteit van gegevens te meten. Uit de 0-meting kwam naar voren dat hier niet aan is voldaan. Identiteitsonderzoeken moeten aan bepaalde eisen voldoen om te worden meegenomen, maar er is wel aandacht voor verbetering nodig. Daarnaast kan er geen rapport worden samengesteld over de kwaliteit van gegevens. Dit is wel handig om te gebruiken voor eventuele sturing op (het gebrek aan) kwaliteit. Er kwam naar voren dat rapporten die worden gemaakt niet worden bewaard. Het is een eenrichtingsverkeer waarbij het rapport naar de desbetreffende eenheid gaat en zij zelf moeten besluiten of er iets mee wordt gedaan. Er is vanuit PSH-V geen sturing op basis van de rapportages. Om de kwaliteit over de gehele linie te waarborgen zou dat een verbeterpunt kunnen zijn. Het moet ook duidelijk zijn voor de gebruikers wanneer er sprake is van een kwaliteitsafwijking (attenderen).

Actiepunten

- (Beleid): Kijk kritisch naar de bedrijfsregels voor de gegevenskwaliteit en pas ze zo nodig aan. [p7c5]
- (Beleid): Zorg dat er op basis van bedrijfsregels ook geautomatiseerde controles ingebouwd worden om de gegevenskwaliteit te meten. [p7c6]
- (Beleid): Zorg dat er rapportages worden opgesteld over de kwaliteit van gegevens. [p7c7]
- (Beleid): Bewaar de rapportages over gegevenskwaliteit en kijk of er naar aanleiding daarvan zaken moeten worden gewijzigd of acties moeten worden ondernomen. [p7c8]
- (Beleid): Zorg dat gebruikers geattendeerd worden op kwaliteitsafwijkingen [p7c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	44%	1

1.8 Bewaren en vernietigen

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

De politie mag alleen gegevens verwerken indien en voor zolang daar een wettelijke grondslag voor bestaat. Als die grondslag komt te vervallen moeten de gegevens worden verwijderd of vernietigd. Ook voor gegevens waarvan blijkt dat ze onjuist zijn geldt dat ze moeten worden vernietigd of gecorrigeerd. De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden.

De score op het principe bewaren en vernietigen is 0% en een volwassenheidsniveau van 0 (onvoldoende). De bewaartermijnen voor de gegevens in PSH-V worden bepaald door de AVG en de Vreemdelingenwet 2000. In PSH-V moet verder worden gekeken naar de Archiefwet. Volgens de AVG mogen gegevens net zo lang worden bewaard als noodzakelijk is voor het doel van de verwerking. Het kan zijn dat er in een aanvullende wet, zoals hier het geval is met de Vreemdelingenwet 2000, specifieke termijnen zijn vastgesteld. In art. 107 lid 9 Vreemdelingenwet 2000 is opgenomen dat *bij of krachtens* een AMvB regels kunnen worden opgesteld omtrent de vernietiging van gegevens. Gezichtsopnames en vingerafdrukken mogen daarbij nooit langer dan 10 jaar na de afwijzing of beëindiging van een rechtmatig verblijf worden bewaard. Er moet worden nagegaan welke termijnen zijn gesteld voor de gegevens uit de Vreemdelingenwet en hoe dat in de keten is afgesproken.

Er moet een waardering en selectie ten behoeve van bewaren en vernietigen worden gemaakt. Er is ook nog verbetering mogelijk op de automatische verwijdering en vernietiging van gegevens.

Op het moment wordt nog gewacht op een archiefservice en multimediadataservice. Zo lang dit er nog niet is, wordt er in PSH-V niet gekeken naar de kwaliteitseisen van DUTO. Daarnaast worden de gegevens niet beschikbaar gesteld ten behoeve van het duurzaam bewaren en archiveren van gegevens. Slechts een klein deel gaat naar CDD+ maar niet met het doel om te archiveren.

Actiepunten:

- **(Wet): Stel vast wat de bewaartermijnen van de gegevens zijn en zorg dat dit in de voorziening wordt verwerkt. (art. 5 lid 1 sub e AVG jo. art. 107 lid 9 Vreemdelingenwet 2000). [p8c2]**
- **(Wet): Zorg voor de waardering en selectie van gegevens ten behoeve van bewaren en vernietigen. [p8c3]**
- (Beleid): Zorg dat de gegevens geautomatiseerd worden verwijderd en vernietigd. Waarbij de in de wet gestelde termijnen worden aangehouden. [p8c4]
- (Beleid): Kijk hoe de PSH-V kan voldoen aan de kwaliteitseisen van DUTO. [p8c8]
- (Beleid): Zorg dat PSH-V waar nodig gegevens beschikbaar stelt ten behoeve van het duurzaam bewaren van gegevens. [p8c9]

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.

Er is geen recente risicoanalyse voor de informatiebeveiliging uitgevoerd. Dit stond op het moment van de 0-meting echter wel op de planning. Nu staan de criteria die gebaseerd zijn op de analyse op nee. Op het moment dat er een risicoanalyse is uitgevoerd moet worden bepaald welke informatiebeveiligingseisen nodig zijn. De volgende actiepunten moeten worden gezien in het licht van de nog uit te voeren risicoanalyse.

Actiepunten

- (Beleid): Zorg dat er een risicoanalyse wordt uitgevoerd op het gebied van informatiebeveiliging. [p9c1]
- **(Wet): Zorg dat er naar aanleiding van de risicoanalyse informatiebeveiligingseisen worden opgesteld. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f). [p9c2]**
- (Beleid): Zorg dat de impact van de informatiebeveiligingseisen wordt beoordeeld ten behoeve van de realisatie in de voorziening. [p9c3]
- (Beleid): Zorg dat waar mogelijk de informatiebeveiligingseisen moeten worden gerealiseerd door de standaard informatiebeveiligingsdiensten. [p9c5]
- (Beleid): Zorg dat er passende maatregelen worden genomen als er informatiebeveiligingseisen zijn die niet door de standaard informatiebeveiligingsdiensten kunnen worden gerealiseerd. [p9c6]
- (Beleid): Zorg dat als niet aan alle beveiligingseisen kan worden voldaan dat er periodiek restrisico's worden beheerd. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	20%	0

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 van 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.

PSH-V voldoet bijna volledig aan de gestelde eisen voor het principe toepassen standaarden. Afwijkingen van geldende standaarden zouden moeten worden voorzien van een motivatie die geaccepteerd is door de verwerkingsverantwoordelijke. Dit is bij PSH-V geregeld in de bijeenkomst van de vreemdelingenketen, maar dit zou geregeld moeten worden in de PDCA-cyclus

Actiepunt:

- (Beleid): Zorg dat afwijkingen mbt geldende standaarden worden geregeld als onderdeel van de PDCA-cyclus. [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	83%	2

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

PSH-V scoort een volwassenheidsniveau van 2 (voldoende) op verantwoordelijkheden belegd. Er zijn twee punten waar niet aan werd voldaan. Het eerste punt is dat alleen de definitie is vastgelegd, maar er is vooralsnog geen koers, beleid en strategie vastgesteld voor de verwerking van gegevens. Het tweede punt gaat over de mogelijkheid van de voorziening de verantwoordelijke te ondersteunen met het verwerken van de juiste classificatie en metagegevens.

Actiepunt

- (Beleid): Zorg dat naast de definitie ook de koers, beleid en strategie is vastgesteld voor de verwerking van gegevens. [p12c2]
- (Beleid): PSH-V moet de uitvoeringsverantwoordelijke ondersteunen met het verwerken van de juiste classificatie en metagegevens. Onder andere voor de informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. [p12c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	79%	2

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 compliance 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 op basis van het (politie)beleid.
- 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' staan³.

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

Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien de voorziening of het principe aan geen enkel wettelijk criterium voldoet

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

- a: aan ten minste 35% van de wettelijke criteria, maar niet alle wordt geheel of ten dele voldaan.
- b: Geen wettelijke criteria zijn benoemd en aan tenminste 35% maar minder dan 50% van de wettelijke criteria wordt voldaan.
- c: Geen beleidscriteria zijn benoemd en aan tenminste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

- a: de voorziening of het principe voldoet aan alle wettelijke criteria, maar niet aan alle beleidscriteria
- b: Geen wettelijke criteria zijn benoemd en aan tenminste 50% maar minder dan 100% van de wettelijke criteria wordt voldaan.
- c: Geen beleidscriteria zijn benoemd en aan tenminste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

- a: de voorziening voldoet aan alle wettelijke en aan alle beleidscriteria.
- b: de voorziening voldoet aan alle beleidscriteria en er geen wettelijke criteria zijn benoemd
- c: de voorziening voldoet aan alle wettelijke criteria en er geen beleidscriteria zijn benoemd

NVT : Een principe of toetsing moet de indicatie NVT krijgen, indien wordt voldaan aan een van de volgende voorwaarden:

- a: Alle criteria van een principe of een toetsing zijn met NVT gewaardeerd
- b: Alle criteria van een principe of een toetsing zijn met een NVT en/of een BS gewaardeerd

BS : Een principe of toetsing moet de indicatie BS krijgen, indien alle criteria van een principe of een toetsing met BS zijn gewaardeerd.

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.

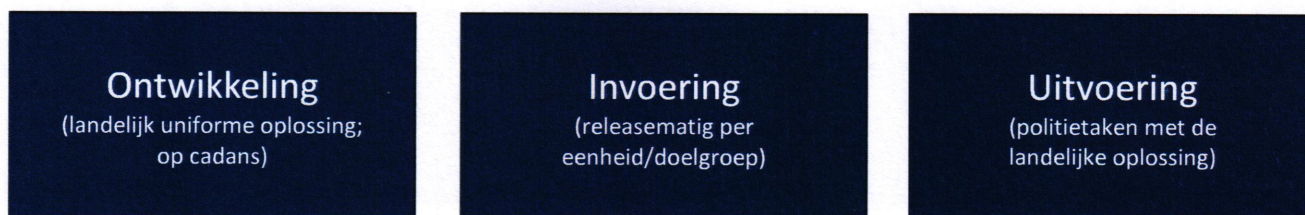
3: Privacy functionaris:

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.

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