0-meting Privacy & Security by Design

PSH-VM

10.2.e

Definitief

Versie 1.2

Versie datum 2 mei 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
1.0	13-4-2018	Eerste versie rapport PSH-VM	
1.1	8-2-2019	Aanpassingen m.b.t. overstap van Wpg naar AVG	
1.2	2-5-2019	Aanpassingen n.a.v. review 10.2.e	

Review commentaar

Versie	Wanneer	Wie	Afdeling
1.0	17-4-2018	10.2.e	Gegevensautoriteit
1.1	8-2-2019	10.2.e i.o.m. 10.2.e	Gegevensautoriteit
1.2	2-5-2019	10.2.e	Korpscheftaken & BOA

Inhoudsopgave

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 compliance 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) compliance 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 compliance.

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 applicatie PSH-VM. 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-VM

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. Om dit doel te bereiken is er gebruik gemaakt van uitvoeringskader PSbD wat in juli 2017 is vastgesteld.

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

	Naam	Functie
Directe betrokkenen 0-meting PSH-VM	10.2.e	Waarnemend Business Expert IM portefeuille Korpscheftaken
	10.2.e	Adviseur Korpscheftaken & BOA
	10.2.e	Functioneel Beheer PSH-VM (Verona)

	Naam	Functie
Toetsing	10.2.e	Adviseur architectuur en modellering
	10.2.e	Programmamanager
Meelopen 0-meting	10.2.e	CISSP CISM CIPP/E

Gespreksdatum	Nummer meting	Toelichting
11-1-2018 & 22-1-2018	20180111/Basis Voorziening Informatie-PSH-VM Toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

PSH-VM

Soorten verwerkingen van persoonsgegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	
Vernietigen		

Verwerkingsgrondslag
Tijdens de 0-meting is PSH-VM beoordeeld alsof het onder de WPG valt. Echter tijdens het gesprek is aangegeven en aangetoond dat PSH-VM onder AVG gaat vallen vanaf januari 2019. Onderstaande verwerkingsgrondslag is dan niet van toepassing.

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8		
Onderzoek rechtsorde bepaald geval	Artikel 9		
Informatiepositie	Artikel 10		
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13		
Verlenen wapenvergunning	Art. 6 lid 1 sub c of sub e AVG	X	Ogv art. 9 lid 2 WWM en art. 5.4 lid 7 Wnb
Verlenen jachtakte	Art. 6 lid 1 sub c of sub e AVG	X	Ogv art. 9 lid 2 WWM en art. 5.4 lid 7 Wnb

Artikel 6 lid 1: de verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

Sub c: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

Sub e: de vewerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Eindscore

PSH-VM scoort een volwassenheidsniveau 1 dat betekent dat het niet voldoet aan de wettelijke criteria omtrent de Wpg. Echter PSH-VM valt officieel vanaf mei 2018 niet meer onder de Wpg en dat betekent dat de wettelijke criteria niet direct van toepassing zijn. Al kunnen de wettelijke criteria wel degelijk meegenomen worden als verbeterpunten die ook van toepassing zijn voor de AVG. We hebben bij de actiepunten ook het AVG artikel erbij gezet wat gericht is op het Wpg artikel waar de actiepunten op gebaseerd zijn (indien van toepassing). Zoals afgesproken hebben we de applicatie beoordeeld alsof het onder de Wpg zou vallen. Op het gebied van de wet (gericht op de Wpg) scoort PSH-VM 81% en op het (politie)beleid scoort het 49%. Dit houdt in dat op (politie)beleid nog stappen nodig zijn om te werken volgens het beleid van Privacy & Security by Design (PSbD). Ondanks dat PSH-VM niet meer onder de Wpg valt is het advies om initieel eerst naar punten te kijken die vallen of gaan vallen onder de Wpg aangezien veel punten ook te herleiden zijn bij de AVG.

Actiepunten:

- **(Wet): Er is nog geen verwerkersovereenkomst opgesteld voor E-screener (externe partij). Vanaf 2018 wordt er gebruik gemaakt van E-screener waarin verwerkingen van (bijzondere) persoonsgegevens wordt gedaan. Het is van belang om op basis van risico analyse beveiligingsmaatregelen te nemen waaraan externe partij aan moet voldoen d.m.v. een verwerkersovereenkomst. (Wpg art 4 lid 6 jo.14 lid 1 Wbp; Wpg nieuw art 6c lid2; AVG, Art 28 lid 2) [p2c5]**
- **(Wet): Op basis van de resultaten van de risicoanalyse moeten er informatiebeveiligingseisen bepaald worden. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f + art 25 AVG) [p9c2]**
- **(Wet): De impact van de informatiebeveiligingseisen moet beoordeeld worden ten opzichte van de realisatie binnen PSH-VM. Dat betekent dat er gekeken moet worden of en hoe de eisen gerealiseerd kunnen worden. Bij het realiseren van de eisen moet er door de ondersteunende diensten gekeken worden naar een optimale mix van maatregelen op de terreinen van ICT, Fysiek, Personeel en Organisatie. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f + art 25 AVG) [p9c3]**

Aandachtspunten:

- **Naast de punten genoemd in de 0-meting zal mbt de AVG rekening moeten worden gehouden met de rechten van betrokkenen Art 12.1 en de informatieplicht aan de betrokkene art 13.1 + 14.1.**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
PSH-VM	11-1-2018	1.0	81%	49%	1

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	70%	2
PDCA-cyclus	M	-	0%	90%	0
Doelbinding	Z	-	100%	50%	2
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	100%	40%	2
Metagegevens	Z	-	NVT	31%	0
Kwaliteitszorg	Z	-	NVT	61%	2
Bewaren en vernietigen	Z	-	100%	75%	2
Informatiebeveiliging	Z	-	0%	20%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	64%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	81%	49%	

VOLWASSENHEID
TOETSING 1
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 Wpg januari 2019
Om voorbereid te zijn op de nieuwe regelgeving mbt Wpg welke vanaf mei 2018 van kracht gaat is er ook gekeken of buiten de eerder genoemde actiepunten nog meer punten zijn die voor PSH-VM aangepast moeten worden om te voldoen aan de wet. Er zijn vier actiepunten wat nu benoemd is als beleid (en zo gescoord), maar wat in januari 2019 onderdeel zal zijn van de wet.

- **(Wet: art 5.1.D juistheid): Binnen PSH-VM blijft een metagegeven mbt verwerkingsgrondslag en verwerkingstermijn niet het gegeven begeleiden (in het naar een ander doel toe gaat). Het is van belang dat metagegevens over verwerkingsgrondslag en termijn mee reizen naar andere (data-analyse)omgevingen, zodat er op een juiste wijze gegevens getoond of al dan niet verwijderd kunnen worden. [p3c11]**
- **(Wet: Art 5.2 AVG): Het is niet mogelijk om van de audittrail een rapportage te genereren. [p4c4]**
- **(Wet Art 25 AVG): Toegang- en gebruikersrechten van gebruikers worden niet regelmatig gecontroleerd. [p5c8]**

Actiepunt bij toekomstige vernieuwingen:

- (Wet: art 35 + 36 AVG): Een GEB moet worden uitgevoerd indien er sprake is van een nieuwe verwerking en als is voldaan aan een van de volgende criteria: er wordt gebruik gemaakt van een nieuwe technologie en/of er is sprake van een hoog risico. [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 tenminste 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.

PSH-VM moet nog een aantal stappen maken om aan het principe eenmalige vastlegging te voldoen. Op het gebied van de wet ondersteunt PSH-VM de uitvoeringsverantwoordelijke niet indien er 'gerede twijfel' bestaat over het gegeven. Er moet een mogelijkheid zijn om (eventueel na evaluatie) bij de bron aan te geven dat er 'gerede twijfel' over gegeven bestaat. Daarnaast moet er een betere controle komen om meervoudige vastlegging te voorkomen.

Actiepunten:

- (Beleid): Er is geen controle om meervoudige vastlegging te voorkomen.
    - Gegevens uit een andere bron mogen gewijzigd worden zonder dat er opdracht is gegeven vanuit de bron. Oftewel er kan inconsistentie ontstaan in de gegevens na een wijziging op plek A niet hetzelfde zijn als op plek B. [p1c8]
    - Alleen het bestaan van persoonsgegevens wordt bij invoer gecontroleerd (verificatie). 10.2.c [redacted]. [p1c10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	70%	2

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

Voor PSH-VM is het vooral van belang dat er een verwerkersovereenkomst wordt opgesteld voor de externe partij E-screener aangezien dit voor de wet verplicht is. Op het gebied van beleid voldoet PSH-VM goed m.b.t. de PDCA-cyclus. Er zal alleen meer aandacht besteedt moeten worden aan het opleveren van rapportages t.b.v. besturing van gegevensverwerking.

Actiepunten:

- **(Wet): Er is nog geen verwerkersovereenkomst opgesteld voor E-screener (externe partij). Vanaf 2018 wordt er gebruik gemaakt van E-screener waarin verwerkingen van (bijzondere) persoonsgegevens wordt gedaan. In de verwerkersovereenkomst worden afspraken tussen de verwerker en de verwerkingsverantwoordelijke worden gemaakt. Hierin staan onder andere de maatregelen om ongeoorloofd gebruik van gegevens tegen te gaan, de procedure van het melden van datalekken en het verder verwerken van persoonsgegevens. Het is van belang om op basis van risico analyse beveiligingsmaatregelen te nemen waaraan externe partij aan moet voldoen d.m.v. een verwerkersovereenkomst. (Wpg art 4 lid 6 jo.14 lid 1 Wbp; Wpg nieuw art 6c lid2; AVG, Art 28 lid 2) [p2c5]**
- (Beleid): Er worden nog onvoldoende rapportages opgeleverd t.b.v. besturing van gegevensverwerking. Er is op dit moment geen periodiek managementrapportage met een paragraaf over de gegevensverwerking zodat erop (bij)gestuurd kan worden. Er worden wel rapportages opgeleverd op gebied van kluiscontroles (toezicht in het kader van de politietaak) en een lijst van werkvoorraden voor de afdelingen. [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	0%	90%	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-VM voldoet op het gebied van doelbinding aan de Wpg. Echter vanaf mei 2018 is het wettelijk vereist dat een metagegeven mbt verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden. Dit is van toepassing bij het versturen naar data-analyseomgeving, zodat de juiste gegevens getoond of verwijderd/niet beschikbaar gesteld kunnen worden. Daarnaast is het van belang dat binnen PSH-VM een verwerkingsgrondslag van een persoonsgegeven als metagegeven wordt opgenomen in het gegevensmodel.

Actiepunten:

- (Beleid): Er is geen verwerkingsgrondslag van een persoonsgegeven als metagegeven opgenomen in het gegevensmodel. [p3c2]
- **(Wet: art 5.1.D juistheid): Binnen PSH-VM blijft een metagegeven mbt verwerkingsgrondslag en verwerkingstermijn niet het gegeven begeleiden (indien het naar een ander doelvoorziening toe gaat). Het is van belang dat metagegevens over de verwerkingsgrondslag en termijn mee reizen naar andere (data-analyse)omgevingen, zodat er op een juiste wijze gegevens getoond of al dan niet verwijderd kunnen worden. [p3c11]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	100%	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 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.

De audittrail is een belangrijk onderdeel om verantwoording af te kunnen leggen wie, wanneer welke handelingen heeft verricht. Het is dan ook van belang dat de audittrail beveiligd is tegen manipulatie. Dat is niet alleen voor de gebruikers, maar ook voor de databasebeheerders. Vanaf januari 2019 moet er een er eenvoudig een rapportage gemaakt kunnen worden van de audittrail.

Actiepunten:

- (Beleid): De audittrial is niet beveiligd tegen manipulatie van een databasebeheerder. Voor gebruikers is de audittrail voldoende beveiligd. Het is de vraag of het voor een databasebeheerder voldoende beveiligd is (ondanks a-screening). Initieel staat de auditfunctie op de databaseserver uit. Er zijn licentiekosten eraan verbonden om dit aan te zetten. Het zal een bewuste keuze moeten zijn hoe er omgegaan gaat worden met beveiliging omtrent manipulatie van de audittrail m.b.t. databasebeheer. [p4c3]
- **(Wet: Art 5.2 AVG): Het is niet mogelijk om van de audittrail een rapportage 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-VM voldoet vooralsnog aan de wettelijke criteria van de Wpg, maar zal meer aandacht gevestigd moeten worden op de controle van toegang- en gebruikersrechten. Het is hierbij van belang dat dit periodiek gedaan wordt. Daarbij is het kunnen gebruiken van rapportages van autorisaties van belang. Op dit moment wordt ook geen gebruik gemaakt van de generieke autorisatietool voor leidinggevende (ATL).

Actiepunten:

- (Beleid): PSH-VM maakt geen gebruik van de generieke autorisatietool voor leidinggevende (ATL) [p5c4]
- (Beleid): PSH-VM kan geen rapportages genereren op het gebruik van autorisaties [p5c7]
- **(Wet: art 25 AVG): Toegang- en gebruikersrechten van gebruikers worden niet regelmatig gecontroleerd. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	40%	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.

PSH-VM is in een eerder stadium ontwikkeld toen er nog geen aandacht was op metagegevens zoals er hedendaags naar gekeken wordt. Dat betekent dat PSH-VM aandacht moet besteden om te voldoen aan de onderstaande actiepunten.

Actiepunten:

- (Beleid): Zorg dat er gebruik wordt gemaakt van vastgestelde definities en een begrippenlijst. [p6c1]
- (Beleid): Kijk in hoeverre het Toepassingsprofiel Metagegevens Rijk (TMR) voldoet binnen PSH-VM (in afwachting van het Toepassingsprofiel Metagegevens Politie (TMP). [p6c4]
- (Beleid): Metagegevens die niet geautomatiseerd worden vastgelegd worden niet op andere manieren ingevuld. Dit zou wel moeten. [p6c9]
- (Beleid): Metagegevens worden niet gebruikt voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. [p6c10]
- (Beleid): Het is onbekend of metagegevens worden meegeleverd bij koppelingen in andere voorzieningen. [p6c11]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	31%	0

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.

Binnen PSH-VM moet de kwaliteit van de gegevensverwerking verhoogd worden. Om dit te bereiken is het van belang dat er bedrijfsregels geformuleerd zijn om de kwaliteit van de gegevens te kunnen meten. Daarnaast moet over de kwaliteit gerapporteerd worden en de resultaten opgeslagen worden.

Actiepunten (deze actiepunten vallen onder art 5.1.D juistheid AVG):

- (Beleid): Er zijn geen bedrijfsregels geformuleerd om de kwaliteit van de gegevens te meten. Dit zou kunnen door [p7c5]:
    - Het signaleren op basis van kennisregels: geautomatiseerd en handmatig
    - Bewaken van geconstateerde fouten
    - Monitoren doormiddel van dashboards en rapportages
- (Beleid): Er is geen rapport over de kwaliteit van gegevens wat gemonitord wordt door een beleidsverantwoordelijke [p7c7]
    - De resultaten van uitgevoerde kwaliteitscontroles worden niet bewaard. [p7c8]
- (Beleid): Gebruikers worden niet geattendeerd op kwaliteitsafwijkingen (op basis van de geformuleerde kwaliteitseisen). [p7c9]

TIP:
Maak gebruik van het raamwerk om kwaliteitseisen op te stellen (zie uitvoeringskader PSbD v1.0 blz 45).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	61%	2

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.

PSH-VM voldoet nog niet aan alle kwaliteitseisen omtrent de DUTO (duurzame toegankelijkheid van overheidsinformatie). Het is aan te raden om hiervoor contact op te nemen met DIV (Documentaire informatievoorziening).

Actiepunten:

- (Beleid): De voorziening voldoet niet aan de kwaliteitseisen van de DUTO. Tijdens de meting is genoteerd dat aan de volgende kwaliteitseisen niet wordt voldaan [p8c8]:
    - 1: Er is een informatiemodel waarin alle informatieobjecten zijn beschreven die de organisatie ontvangt en creëert.
    - 2: Informatieobjecten zijn ingedeeld in risicoklassen. Per risicoklasse is het toegankelijkheidsniveau bepaald waaraan de betreffende informatieobjecten moeten voldoen.
    - 9: Informatieobjecten zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen. Conform de geldende standaarden voor informatiebeveiliging.
    - 12: Informatieobjecten worden niet eerder en niet later vernietigd dan is aangeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar.
    - 13: Een blijvend te bewaren informatieobject wordt binnen twintig jaar overgebracht naar een archiefbewaarplaats.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	100%	75%	2

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.

Het is van belang regelmatig de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. PSH-VM heeft hier op dit moment onvoldoende aandacht voor. In de basis betekent dat PSV-VM allereerst een risicoanalyse laat uitvoeren en controle gaat houden op informatiebeveiligingsrisico's.

Actiepunten:

- (Beleid): Er moet een risicoanalyse uitgevoerd worden. Dit zal uitgevoerd moeten worden door team informatiebeveiliging (dienst IM) en team veiligheid en continuïteit (dienst ICT) [p9c1]
- **(Wet): Op basis van de resultaten van de risicoanalyse moeten er informatiebeveiligingseisen bepaald worden. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f + art 25 AVG) [p9c2]**
    - (Beleid): Binnen PSH-VM wordt er gebruik gemaakt van de generieke voorzieningen voor informatiebeveiliging, maar er moet gekeken worden of die voldoen aan alle informatiebeveiligingseisen. [p9c5]
    - (Beleid): Er moeten maatregelen genomen worden om informatiebeveiligingseisen te realiseren die niet door de standaard beveiligingsdiensten zijn gerealiseerd. [p9c6]
    - (Beleid): Restrisico's in de beveiliging van PSH-VM moeten worden beheerd. Dit zijn risico's die wel in beeld zijn, maar niet zijn opgelost (bijvoorbeeld vanwege de extra kosten of gebrek aan capaciteit). Indien er sprake is van restrisico('s) moeten die periodiek gemonitord en geëvalueerd worden. Hiervoor moet een specifieke informatiebeveiligingsparagraaf opgenomen worden in de reguliere rapportagecyclus. [p9c7]
- **(Wet): De impact van de informatiebeveiligingseisen moet beoordeeld worden ten opzichte van de realisatie binnen PSH-VM. Dat betekent dat er gekeken moet worden of en hoe de eisen gerealiseerd kunnen worden. Bij het realiseren van de eisen moet er door de ondersteunende diensten gekeken worden naar een optimale mix van maatregelen op de terreinen van ICT, Fysiek, Personeel en Organisatie. (Wpg art 4 lid 3; Wpg nieuw art 4a lid 2; AVG, art 5 lid 1 sub-f + art 25 AVG) [p9c3]**

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 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.

Het is onduidelijk in hoeverre PSH-VM gebruik maakt van overheids- en ketenstandaarden. Dit zal verder onderzocht moeten worden om te bekijken hoe de samenwerking tussen de overheids- en ketenpartners verloopt tussen de verschillende systemen die PSH-VM gebruikt.

Actiepunten:

- (Beleid): Het is onduidelijk in hoeverre PSH-VM gebruik maakt van de van toepassing zijnde bestaande overheids- en ketenstandaarden. [p11c1]
    - (Beleid): Indien er gebruik wordt gemaakt van de standaarden voor gegevensverwerking dan is het van belang daarop getoetst wordt [p11c2]
    - (Beleid): Indien er afgeweken wordt van geldende standaarden, dan moet dat worden voorzien van een motivatie (pas toe of leg uit) door de verwerkingsverantwoordelijke. [p11c3]

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

1.12 Verantwoordelijkheden belegd

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

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

Binnen PSH-VM zijn veel verantwoordelijkheden juist belegd. Echter er zal vooral gekeken moeten worden naar de kwaliteitsverbetering van gegevensverwerking. Dit valt binnen de AVG onder Art .6.1.F en 6.4.B.

Actiepunten:

- (Beleid): Op dit moment zijn de definities, beleid, koers en strategie maar voor een deel vastgesteld. Autorisatiematrix, notitie kwaliteitsbeheer en handboekkorpscheftaken zijn vastgelegd. Echter de strategie voor kwaliteitsverbetering voor gegevensverwerking is niet vastgesteld. [p12c2]
- (Beleid): PSH-VM ondersteunt de uitvoeringsverantwoordelijke onvoldoende met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. [p12c4]
- (Beleid): Taken van de gegevensverwerkers om gegevens zorgvuldig en rechtmatig te verwerken worden niet ondersteunt door PSH-VM [p12c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	64%	2

Verantwoording toetsing

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).
- 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.

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