0-meting Privacy & Security by Design

Mappen Standaard

10.2.e

Definitief

Versie 1.00

Versie datum 30 april 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	04-10-2018	Eerste opzet rapport
0.9	16-11-2018	Aanpassingen verwerkt
0.91	05-04-2019	Reactie van betrokkenen verwerkt
0.92	18-04-2019	Actiepunten voor bewaren en vernietigen aangepast (p8c2/p8c5/p8c4)
0.93	25-04-2019	Extra alinea toegevoegd aan de eindscore ivm onenigheid over de adressering van twee actiepunten in de 0-meting.
1.00	30-4-2019	Rapport definitief akkoord na wederzijds goedkeuren (op twee actiepunten na zoals beschreven in de laatste alinea van de eindscore)

Review commentaar

Versie	Wanneer	Wie	Afdeling
0.8	4-10-2018	10.2.e	Gegevensautoriteit
0.9	9-11-2018	10.2.e	Gegevensautoriteit

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 de applicatie Mappenstandaard. 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[3]. 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.

[1] Verbeterplan Wet Politiegegevens en Informatiebeveiliging
[2] Tranche 2018, Verbeterprogramma Wpg en IB
[3] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

0-meting Mappenstandaard

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 april 2018 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 Mappenstandaard	10.2.e	Projectleider Mappenstandaard
	10.2.e	Business expert IM-advies
	10.2.e	Functioneel beheerder

	Naam	Functie
Toetsing	10.2.e	Adviseur architectuur en modellering
	10.2.e	Programmamanager
	10.2.e	Beleidsadviseur

Gespreksdatum	Nummer meting	Toelichting
04/07/2018	2018070401	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

Mappenstandaard

De Mappenstandaard definieert de manier waarop we omgaan met de mappen en schijven in de Kantoor Automatisering van de Nationale Politie.

De Mappenstandaard vindt haar bestaansrecht in het feit dat de huidige bronsystemen (BVH / SummIT) niet alle verschijningsvormen (o.a. foto's en overzichtlijstjes etc.) van politiegegevens kunnen verwerken. In de Mappenstandaard worden de verschijningsvormen die niet verwerkt kunnen worden opgeslagen.

De Mappenstandaard bestaat uit schijven, mappen en autorisaties. Er zijn schijven die bedoeld zijn voor bepaalde typen bestanden. Voor de schijven is per eenheid een mappenstructuur gedefinieerd. 10.2.c . De autorisaties voor de mappen worden beheerd met SMART(Standaard Mappen Autorisatie Registratie Tool).

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	Niet door project Mappenstandaard. Wel door eindgebruikers.
Vastleggen	X	Vinkje in aanvraagformulier Summ-IT voor aanmaken map volgens Mappenstandaard.
Ordenen	X	Migreren naar Mappenstandaard Gedurende project Mappen worden gevuld conform standaard.
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	Mits geautoriseerd
Opvragen	X	Mits geautoriseerd
Raadplegen	X	Mits geautoriseerd
Gebruiken	X	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	SMART heeft geen export Maar mappen kunnen door gebruiker verstrekt worden.
Samenbrengen	X	
Met elkaar in verband brengen		
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Artikel 14 mappen. Poortwachters moeten nog in positie komen. Toetsen op gebruik?
Vernietigen	X	Fundament is geregeld.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9	X	
Informatiepositie	Artikel 10	X	
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11		
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13	X	

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 11 (lid 1) Wpg: verwerking teneinde vast te stellen of er verbanden bestaan tussen politiegegevens die worden verwerkt op grond van artikel 8 of 9

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

De applicatie Mappenstandaard scoort een volwassenheidsniveau 1. Dit houdt in dat de Mappenstandaard onvoldoende voldoet op het gebied van Privacy & Security by Design (PSbD). Er is wel specifiek aandacht op het gebied van PSbD, maar die is vooralsnog niet toereikend om te voldoen aan de wet (Wpg) en op basis van het politiebeleid. Op de wetscriteria heeft de Mappenstandaard een score van 46% en op de criteria van het politiebeleid een score van 70%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'informatiebeveiliging', 'autorisatie' en 'bewaren en vernietigen' er negatief uitspringen.

Na meerdere pogingen om de mappenstandaard te implementeren is er gekozen voor een technische implementatie. Dat houdt in dat er minimale aandacht is geweest om het beheer van de mappen in te richten. De verwerkingsgrondslag van de gegevens in de Mappenstandaard moet de verwerkingsgrondslag in de bronsystemen volgen. In de praktijk worden er in de Mappenstandaard nauwelijks gegevens conform de Wpg verwijderd (verplaatst naar een artikel 14 map) en vernietigd (artikel 14 map definitief vernietigd). Hierdoor worden de betreffende gegevens onrechtmatig verwerkt onder Wpg artikel 8, 9, 10 of 13.
In deze 0-meting leidt dat tot actiepunten voor de wettelijke criteria p8c2 en p8c5 en voor het beleidscriterum p8c4. De direct betrokkenen bij de 0-meting hebben aangegeven dat de portefeuillehouder van de mappenstandaard niet verantwoordelijk is voor deze actiepunten. De opdrachtgever voor de 0-meting PSbD, het verbeterprogramma Wpg & IB heeft aangegeven dat dit wel onder de verantwoordelijkheid van de portefeuillehouder van de Mappenstandaard valt.

Advies: (De wettelijke actiepunten worden hier genoemd. Beleidspunten blijken uit het document)

- **(Wet, art 6) Zorg dat, zolang nog geen gebruik gemaakt wordt van IAM, voor het verlenen van toegang gebruik gemaakt wordt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- **(Wet, art 4a) Zorg dat de toegang- en gebruiksrechten van de gebruikers regelmatig (periodiek) gecontroleerd worden. [p5c8]**
- **(Wet art 8, 9, 10, 12 en 14) Onderzoek samen met de portefeuillehouders van de bronsystemen welke maatregelen genomen kunnen worden om de bronsystemen leidend te maken voor de bewaartermijnen van de gegevens in de Mappenstandaard [p8c2] [p8c5][4]**
- **(Wet art 14 lid 4) Zorg dat de Mappenstandaard de voorziening voor duurzaam bewaren volgt zoals die in de reguliere bronsystemen worden toegepast. Als bijvoorbeeld in een bronsysteem een registratie wordt overgedragen naar het archiefsysteem dan moeten de bijbehorende politiegegevens in de Mappenstandaard ook overgedragen worden. [p8c9]**
- **(Wet art 8) Zorg dat per eenheid alleen de poortwachter toegang heeft tot verwijderde gegevens. Er is al een change ingediend om dit te realiseren. [p8c10]**
- **(Wet art 4a lid 2) Zorg dat de informatiebeveiligingseisen mede bepaald op worden basis van de resultaten van een actuele risico analyse. [p9c2]**
- **(Wet art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in de Mappenstandaard. [p9c3]**

Aandachtspunten[5]:

- Als de bronsystemen geschikt gemaakt worden voor alle verschijningsvormen van politiegegevens wordt de behoefte aan opslag buiten de bronsystemen om, en daarmee de Mappenstandaard, overbodig.
- Er is beperkte kennis bij blauw over de Wpg. Hierdoor is er ook te weinig kennis bij blauw over de toepassing van de mappenstandaard.
- 10.2.c) krijgt zonder autorisatie van de teamleider van het onderzoek toegang tot de actuele mappen van artikel 9. Dit lijkt op een opt-out regime. Zorg dat er een bewuste keuze hiervoor gemaakt wordt. We raden om hiervan een opt-in regime van te maken.
- Alle verantwoordelijkheden zijn belegd maar het is onbekend of er conform de afspraken wordt gewerkt. We bevelen aan om dit te toetsen. Zie hiervoor ook de actiepunten bij principe 2, de PDCA-cyclus.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Mappenstandaard	04/07/2018	2.0	46%	70%	1

[4] Betrokkenen z jn het niet eens met de adressering van actiepunt in deze 0-meting. Zie laatste alinea van de eindscore
[5] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	100%	3
PDCA-cyclus	M	-	NVT	38%	1
Doelbinding	Z	-	100%	NVT	3
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	33%	50%	0
Metagegevens	Z	-	NVT	100%	3
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	30%	0%	0
Informatiebeveiliging	Z	-	0%	20%	0
Privacy by default	Z	-	100%	100%	3
Toepassing standaarden	L	-	NVT	33%	0
Verantwoordelijkheden belegd	M	-	NVT	100%	3
TOTALEN TOETSING		-	46%	70%	

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.
Voor de principes “Kwaliteitszorg”, “Toepassing standaarden” en “Verantwoordelijkheden belegd” zijn er geen wettelijke criteria benoemd. Deze worden daardoor standaard met “NVT” gewaardeerd. Voor alle andere resultaten geldt dat deze alleen “NVT” krijgen als alle betreffende criteria niet van toepassing zijn.

In de volgende paragrafen worden de resultaten per principe nader toegelicht.

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.

De Mappenstandaard haalt hier het hoogst mogelijke volwassenheidsniveau.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	NVT	100%	3

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.

Voor dit principe haalt de Mappenstandaard volwassenheidsniveau 1. Op dit moment wordt er binnen de Mappenstandaard nog onvoldoende gewerkt volgens de PDCA cyclus. Tijdens de sessie is bijvoorbeeld aangegeven dat er behoefte is aan meer rapportages.

Actiepunten:

- (Beleid) Zorg dat er meer rapportages ontwikkeld worden ten behoeve van de PDCA cyclus. Bijvoorbeeld over de omvang van de gegevensverwerking, de kwaliteit van de gegevens of aantallen gebruikers. Deze kunnen gebruikt worden in de reguliere plan- en rapportageproducten zoals jaarplannen en jaarverslagen. [p2c1]
- (Beleid) Zorg dat de rapportages periodiek worden opgeleverd. [p2c2]
- (Beleid) Zorg dat er business rules opgesteld worden voor het beheer van gegevens zodat deze onderdeel uit kunnen maken van de PDCA cyclus. [p2c3]
- (Beleid) Zorg dat het beheer van processen onderdeel uit gaat maken van de PDCA cyclus. [p2c3]
- (Beleid) Zorg dat de applicatie formeel in beheer wordt genomen. [p2c3]
- (Beleid) Zorg dat het beheer van de software onderdeel uit gaat maken van de PDCA cyclus. [p2c3]

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.*"

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.

De Mappenstandaard haalt voor de principe het hoogst mogelijke volwassenheidsniveau. Er is alleen een aandachtspunt over het gebruik van de mappen. Maar dit valt buiten de scope van de Mappenstandaard.

Aandachtspunten:

- Er is beperkte kennis bij blauw over de Wpg. Hierdoor is er ook te weinig kennis bij blauw over de toepassing van de mappenstandaard.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	100%	NVT	3

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 Mappenstandaard haalt hier een volwassenheidsniveau 2. Om te komen tot het hoogste niveau moet de audittrail beter beveiligd worden tegen manipulatie.

Actiepunten:

- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. De logging in de audittrail kan nu uitgezet worden, of in zijn geheel verwijderd worden, door technisch applicatiebeheer.[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 levert een reductie in beheerslast op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

De Mappenstandaard haalt voor dit principe een dikke onvoldoende. Dat wordt veroorzaakt omdat er gebruik gemaakt wordt van SMART in plaats van IAM en doordat de huidige autorisaties onvoldoende gecontroleerd worden.

Actiepunten:

- (Beleid) Zorg dat voor het verlenen van toegang gebruik gemaakt wordt van de generieke IAM voorzieningen. [p5c1]
- **(Wet, art 6) Zorg dat, zolang nog geen gebruik gemaakt wordt van IAM, voor het verlenen van toegang gebruik gemaakt wordt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- (Beleid) Zorg dat voor het verlenen van toegang gebruik gemaakt wordt van de generieke autorisatietool voor leidinggevenden. Daar wordt nu deels gebruik van gemaakt. [p5c4]
- (Beleid) Zorg dat de huidige rudimentaire rapportage op het gebruik van autorisaties wordt uitgebreid tot een rapportage die het beheer beter ondersteunt. [p5c7]
- **(Wet, art 4a) Zorg dat de toegang- en gebruiksrechten van de gebruikers regelmatig gecontroleerd worden. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	33%	50%	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.

Dit principe is voor de Mappenstandaard nauwelijks van toepassing omdat deze applicatie alleen gaat over de mappen en niet over de inhoud van de mappen. En er wordt voldaan aan één criterium wat wel van toepassing is. Hierdoor behaald de Mappenstandaard voor dit principe het hoogste volwassenheidsniveau.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	100%	3

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.

De Mappenstandaard haalt voor dit principe het hoogste volwassenheidsniveau.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[6]	100%	3

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 Mappenstandaard haalt voor dit principe volwassenheidsniveau 0. Dat is een dikke onvoldoende. De applicatie Mappenstandaard is zelf niet verantwoordelijk voor de bewaking van de termijnen. De reguliere bronsystemen zijn dat wel. Maar de politiegegevens in de Mappenstandaard zouden mee moeten lopen met de termijnen in de reguliere basis applicaties.

Actiepunten

- **(Wet art 8, 9, 10, 12 en 14) Onderzoek samen met de portefeuillehouders van de bronsystemen welke maatregelen genomen kunnen worden om de bronsystemen leidend te maken voor de bewaartermijnen van de gegevens in de Mappenstandaard. [p8c2] [p8c5]**[7]
- (Beleid) Onderzoek samen met de portefeuillehouders van de bronsystemen welke maatregelen genomen kunnen worden om de bronsystemen **geautomatiseerd** leidend te maken voor de bewaartermijnen van de gegevens in de Mappenstandaard. [p8c4][7]
- **(Wet art 14 lid 4) Zorg dat de Mappenstandaard de voorziening voor duurzaam bewaren volgt zoals die in de reguliere basisapplicaties worden toegepast. Als bijvoorbeeld in een basisapplicatie een registratie wordt overgedragen naar het archiefsysteem dan moeten de bijbehorende politiegegevens in de Mappenstandaard ook overgedragen worden. [p8c9]**
- **(Wet art 8) Zorg dat per eenheid alleen de poortwachter toegang heeft tot verwijderde gegevens. Er is al een change ingediend om dit te realiseren. [p8c10]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	30%	0%	0

[6] Er zijn voor dit principe geen wettelijke criteria benoemd.

[7] Betrokkenen z jn het niet eens met de adressering van actiepunt in deze 0-meting. Zie laatste alinea van de Eindscore

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 regelmatige 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.

Aangezien er geen risicoanalyse voor de Mappenstandaard is gevonden kan deze niet meegenomen worden in de beoordeling van de criteria voor dit principe. Hierdoor haalt de mappenstandaard voor dit principe volwassenheidsniveau 0.

Actiepunten:

- (Beleid) Zorg dat er een risicoanalyse voor de Mappenstandaard wordt uitgevoerd. [p9c1]
- **(Wet art 4a lid 2) Zorg dat de informatiebeveiligingseisen mede bepaald op worden basis van de resultaten van een actuele risico analyse. [p9c2]**
- **(Wet art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in de Mappenstandaard. [p9c3]**
- (Beleid) Toets of alle informatiebeveiligingseisen gerealiseerd zijn door de standaard informatiebeveiligingsdiensten? [p9c5]
- (Beleid) Toets of er maatregelen genomen zijn voor alle informatiebeveiligingseisen die niet gerealiseerd zijn door de standaard informatiebeveiligingsdiensten. [p9c6]
- (Beleid) Zorg dat de eventuele restrisico's in de beveiliging van de Mappenstandaard beheerd worden. [p9c7]

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

1.10 Privacy by default

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

Voor dit principe is het hoogst mogelijke volwassenheidsniveau gehaald. Er is slechts één aandachtspunt.

Aandachtpunten:

- 10.2.c) krijgt zonder autorisatie van de teamleider van het onderzoek toegang tot de actuele mappen van artikel 9. Dit lijkt op een opt-out regime. Zorg dat er een bewuste keuze hiervoor gemaakt wordt. We raden om hiervan een opt-in regime van te maken.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	100%	3

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.

De Mappenstandaard haalt voor dit principe een dikke onvoldoende. Dat wordt veroorzaakt doordat de Mappenstandaard geen gebruik maakt van standaarden vanuit de overheid of de keten.

Actiepunten:

- (Beleid) Onderzoek of de Mappenstandaard gebruik kan gaan maken van bestaande overheids- en ketenstandaarden. [p11c1]
- (Beleid) Zorg dat er een toets is uitgevoerd op de standaarden voor gegevens verwerking die van toepassing zijn. [p11c2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[8]	33%	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

De Mappenstandaard haalt voor dit principe het hoogst mogelijke volwassenheidsniveau. Desondanks is er een aandachtspunt met betrekking tot de uitvoering van de afspraken.

Aandachtspunten:
Alle verantwoordelijkheden zijn belegd maar het is onbekend of er conform de afspraken wordt gewerkt. We bevelen aan om dit te toetsen. Zie hiervoor ook de actiepunten bij principe 2, de PDCA-cyclus.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[9]	100%	3

[8] Er zijn voor dit principe geen wettelijke criteria benoemd.
[9] Er zijn voor dit principe geen wettelijke criteria benoemd.

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-24_Uitvoeringskader_Privacy en Security by Design_v2.0'. 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
- 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[10].

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.

[10] 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	5

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