0-meting Privacy & Security by Design

BlueSpot Monitor (BSM)

10.2.e

Definitief

Versie 1.00

Versie datum 14 maart 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	14-11-2018	Review
0.9	16-11-2018	Aanpassingen verwerkt
0.91	13-03-2019	Reviewgesprek verwerkt
0.92	14-03-2019	Reactie 10.2.e verwerkt in actiepunten bij eindscore
1.00	14-3-2019	Rapport definitief gemaakt (wederzijds akkoord)

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	14-11-2018	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 BSM. 5

Algemeen 5

Doel 5

Doelgroep 5

Aanwezigen 0-meting 5

BSM 6

Omschrijving applicatie 6

Soorten verwerkingen van politiegegevens 6

Verwerkingsgrondslag 7

Eindscore 8

1.1 Eenmalige vastlegging 10

1.2 PDCA-cyclus 10

1.3 Doelbinding 11

1.4 Verantwoording 11

1.5 Autorisatie 12

1.6 Metagegevens 12

1.7 Kwaliteitszorg 13

1.8 Bewaren en vernietigen 13

1.9 Informatiebeveiliging 14

1.10 Privacy by default 15

1.11 Toepassen standaarden 16

1.12 Verantwoordelijkheden belegd 16

2. Verantwoording toetsing 17

Toetsingscriteria 17

Disclaimer 19

Bijlage 1: Uitgangspunt bij compliance 20

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) 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 applicatie BSM. 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 BSM.

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 v2.0 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 BSM	10.2.e	Test analist
	10.2.e	Software ontwikkelaar
	10.2.e	Productowner
	10.2.e	IV Expert Privacy & Security
	10.2.e	10.2.e

	Naam	Functie
Toetsing	10.2.e	Adviseur architectuur en modellering
	10.2.e	Programmamanager
	10.2.e	Beleidsadviseur
Onderzoek	10.2.e	Directie IV Kwaliteit en Toezicht.

Gespreksdatum	Nummer meting	Toelichting
13/03/2019	20190313	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

BSM

Omschrijving applicatie
De BSM geeft landelijk, of voor een bepaald gebied, inzicht in alle BVH-incidenten en acties. Het geeft aan wat er in een gebied is gebeurd. Welke personen er in een gebied betrokken zijn bij incidenten. Dit kan direct de toelichting zijn, maar het kan ook door de aangifte te lezen. De overzichten worden op een lijst en op de kaart getoond op basis van gebied, thema en/of maatschappelijke klassen en periode.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	Verzamelen van gegevens (Datawarehouse)
Vastleggen		
Ordenen	X	Alleen bij raadplegen. Wel voorkeurslocatie, abonnementen, e.d.
Bewaren	X	Alleen de eigen zoekvraag en eigen abonnementen.
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)		
Wijzigen (het bestaande aanpassen)		
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Excel Analyst Notebook (beperkte doelgroep)
Samenbrengen	X	Vanuit data warehouse samengevoegd.
Met elkaar in verband brengen	X	
Afscherming	X	Poortwachter/informatie medewerker/wijkagent. Functioneel beheer.
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen		

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9		BVH wordt beschouwd als art. 8.
Informatiepositie	Artikel 10		
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11	X	De analyse die plaats vindt in de BSM valt onder Wpg artikel 11.
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13	X	Gegevens uit Amazone vallen onder artikel 13.

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

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

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

Artikel 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 BSM behaald een volwassenheidsniveau 1. Dit houdt in dat BSM onvoldoende compliant is 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 haalt BSM een score van 46% en op de criteria van het politiebeleid 58%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'Doelbinding' en 'Informatiebeveiliging' en 'Toepassen standaarden' er erg negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen.

Actiepunten:

- **(Wet art 3 lid 1) Zorg dat de verwerkingsgrondslag van de politiegegevens zichtbaar is. Deze is afkomstig uit het bronsysteem. [p3c1]**
    - **(Wet art 3 lid 1) Zorg dat als een politiegegeven meerdere verwerkingsgrondslagen heeft dat dit ook in de BSM getoond wordt. Let op met conformeren van persoonsgegevens. [p3c2]**
- **(Wet art 32a) Onderzoek of het exporteren van gegevens naar Excel altijd een doel heeft en borg zo nodig de maatregelen. Als de analyse ook binnen de BSM uitgevoerd kan worden dan is een export van persoonsgegevens een onnodig risico op privacy schendingen. [p3c10]**
- **(Wet art 32a) Zorg dat bij een export de metagegevens zoals de verwerkingsgrondslag en de verwerkingstermijn het gegeven blijven begeleiden. Een disclaimer is daarbij niet voldoende. [p3c10]**
- **(Wet art 32) Zorg dat abonnementen volledig worden opgenomen in de audittrail. Nu wordt er 2 maanden een beperkte logging bijgehouden. [p4c1]**
- **(Wet art 4a) Zorg dat zolang de oude autorisaties nog bestaan de betreffende toegang- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. Denk hierbij aan pre-pensioen, langdurig ziek, langdurig niet ingelogd. [p5c8]**
- **(Wet art 4a) Zorg dat de autorisatieregels voor de gebruikers centraal worden opgeslagen. [p5c6]**
- **(Wet art 4a lid 2) Zorg dat de informatiebeveiligingseisen mede bepaald worden op basis van de resultaten van de risicoanalyse. [p9c2]**
- **(Wet art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in BSM. [p9c3]**
- **(Wet) Onderzoek of het noodzakelijk is om alle gegevens te tonen die nu getoond worden en neem zo nodig maatregelen. De verwerking van persoonsgegevens moet zo beperkt mogelijk gehouden worden. [p10c1]**
- **(Wet) Onderzoek of het noodzakelijk is om alle gegevens te verstrekken die nu verstrekt worden via Excel of naar Analyst Notebook en neem zo nodig maatregelen. De verstrekking van persoonsgegevens moet zo beperkt mogelijk gehouden worden. [p10c2]**

Aandachtspunten:

- **(Wet art 4c) Bij toekomstige ontwikkelingen (zoals zoeken en vinden) moet beoordeeld worden of er een GEB (gegevensbeschermingseffectbeoordeling) noodzakelijk is. Bijvoorbeeld voor diepgaande analyse van relaties en netwerken. [p2c4]**
- Vanuit de dienst ICT wordt aangegeven dat er vanuit de opdrachtgever te weinig kaders en richtlijnen worden meegegeven. Deze zijn noodzakelijk voor de realisatie van wijzigingen. [p12]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
BSM	13/03/2019	2.0	46%	58%	1

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	100%	3
Doelbinding	Z	-	33%	NVT	0
Verantwoording	Z	-	50%	0%	1
Autorisatie	Z	-	50%	63%	1
Metagegevens	Z	-	NVT	60%	2
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	100%	NVT	3
Informatiebeveiliging	Z	-	0%	20%	0
Privacy by default	Z	-	50%	33%	1
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	90%	2
TOTALEN TOETSING		-	46%	58%	

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 ten minste 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.

BSM haalt voor dit principe het hoogste volwassenheidsniveau. De gegevens worden conform het principe van "eenmalige vastlegging" verwerkt.

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.

BSM levert stuurinformatie ten behoeve van de PDCA cyclus. Het beheer van gegevens, processen en software is onderdeel van de PDCA cyclus. De beleidsverantwoordelijke voert regie op definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens. Er is alleen een aandachtspunt voor een GEB (gegevensbeschermingseffectbeoordeling).

Aandachtspunten:

- **(Wet art 4c) Bij toekomstige ontwikkelingen (zoals zoeken en vinden) moet beoordeeld worden of er een GEB (gegevensbeschermingseffectbeoordeling) noodzakelijk is. Bijvoorbeeld voor diepgaande analyse van relaties en netwerken. [p2c4]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	100%	3

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 verwerkingsgrondslag van een politiegegeven wordt vastgelegd in een bronsysteem. Deze verwerkingsgrondslag moet ook zichtbaar zijn in de BSM en in de gegevens die daar uit geëxporteerd worden. Aangezien de BSM niet voldoet aan deze wettelijke criteria is het volwassenheidsniveau voor het principe doelbinding een zware onvoldoende. De analyse die plaats vindt in de BSM valt altijd onder Wpg artikel 11 (geautomatiseerd vergelijken en in combinatie zoeken). Een Wpg artikel 13 protocol is dan ook niet van toepassing.

Actiepunten:

- **(Wet art 3 lid 1) Zorg dat de verwerkingsgrondslag van de politiegegevens zichtbaar is. Deze is afkomstig uit het bronsysteem. [p3c1]**
    - **(Wet art 3 lid 1) Zorg dat als een politiegegeven meerdere verwerkingsgrondslagen heeft dat dit ook in de BSM getoond wordt. Let op met conformeren van persoonsgegevens. [p3c2]**
- **(Wet art 32a) Onderzoek of het exporteren van gegevens naar Excel altijd een doel heeft en borg zo nodig de maatregelen. Als de analyse ook binnen de BSM uitgevoerd kan worden dan is een export van persoonsgegevens een onnodig risico op privacy schendingen. [p3c10]**
- **(Wet art 32a) Zorg dat bij een export de metagegevens zoals de verwerkingsgrondslag en de verwerkingstermijn het gegeven blijven begeleiden. Een disclaimer (zie afb.) is daarbij niet voldoende. [p3c10]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	33%	NVT	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.

BSM haalt voor dit principe volwassenheidsniveau 1. De audittrail is nog niet volledig en kan bovendien gewijzigd worden. Om te komen tot het volgende niveau moet in ieder geval de audittrail volledig zijn. Voor het hoogste volwassenheidsniveau is het van belang dat de audittrail door niemand gewijzigd kan worden.

Actiepunten:

- **(Wet art 32) Zorg dat abonnementen volledig worden opgenomen in de audittrail. Nu wordt er 2 maanden een beperkte logging bijgehouden. [p4c1]**
- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. Op dit moment kan deze nog gewijzigd worden door de database administrators. [p4c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	50%	0%	1

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.

BSM is op de goede weg door voor alle nieuwe autorisaties gebruik te maken van IAM. De oude autorisaties moeten nog overgezet worden. Daarnaast is het van belang dat gebruikers op de hoogte zijn van de voor hen geldende autorisatieregels.

Actiepunten:

- (Beleid) Zorg dat de oude autorisaties, die nog niet via IAM verlopen, zo snel mogelijk overgezet worden naar IAM. [p5c1]
    - **(Wet art 4a) Zorg dat zolang de oude autorisaties nog bestaan de betreffende toegang- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. Denk hierbij aan pre-pensioen, langdurig ziek, langdurig niet ingelogd. [p5c8]**
- **(Wet art 4a) Zorg dat de autorisatieregels voor de gebruikers centraal worden opgeslagen. [p5c6]**
- (Beleid) Zorg dat er periodiek rapportages worden gemaakt op het gebruik van autorisaties (niet alleen ad-hoc). [p5c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	50%	63%	1

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.

In de BSM wordt al gebruik gemaakt van vastgestelde definities voor bedrijfsbegrippen en van het Politie Gegevensmodel (PGM). Desondanks zijn er voor het principe metagegevens een aantal actiepunten. Om te komen tot volwassenheidsniveau 2 moeten de kenmerken van de bevraging vastgelegd worden. Voor het hoogste volwassenheidsniveau moeten ook de actiepunten vanuit beleid opgepakt worden.

Actiepunten:

- (Beleid) Bestudeer de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is [p6c4].
- (Beleid) Zorg dat de metagegevens meegeleverd worden bij koppelingen voor verwerking in andere voorzieningen zoals Analyst Notebook en Excel. [p6c10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	60%	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.

BSM voldoet voor dit principe aan alle criteria. In BSM zijn geautomatiseerde controles ingebouwd om op basis van de bedrijfsregels de gegevenskwaliteit te meten. De gebruiker wordt geattendeerd als er niet voldaan wordt aan een bedrijfsregel. De bronsystemen zijn zelf verantwoordelijk voor de kwaliteit van de gegevens. Daardoor is het grootste deel van de criteria voor BSM niet van toepassing.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[3]	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.

BSM voldoet voor dit principe aan alle criteria. Voor verwijdering en de vernietiging wordt het registratieve bronsysteem gevolgd. De poortwachter heeft zo nodig toegang tot de verwijderde gegevens. De bronsystemen zijn zelf verantwoordelijk voor de bewaartermijnen van de gegevens. Daardoor is het grootste deel van de criteria niet van toepassing voor BSM.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	100%	NVT	3

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

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.

BSM haalt voor dit principe het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt doordat er geen risicoanalyse is uitgevoerd. BSM maakt wel gebruik van de generieke voorzieningen voor informatiebeveiliging.

Actiepunten:

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

Zowel de AVG als de Wpg bevatten Privacy by Default en Privacy by Design als verplichte principes. Deze dienen ertoe om gegevensbescherming vanaf het moment van ontwikkeling van informatiediensten tot aan het laatste gebruik zoveel mogelijk in de gegevensverwerking te integreren. Daar waar Privacy by Design vooral toeziet op ontwerpkeuzes bij de *ontwikkeling* van informatiediensten is Privacy by Default van belang bij keuzemomenten tijdens *gebruik* van de informatiediensten. Dit principe verplicht organisaties om de privacy van betrokkenen zo veel mogelijk te beschermen door de verwerking van persoonsgegevens standaard (by default) op de meest privacyvriendelijke stand te zetten.

BSM maakt correct gebruik van een opt-in regime door middel van abonnementen. Het is echter de vraag of alle gegevens die getoond en verstrekt worden noodzakelijk zijn voor de verwerking. Daarnaast zijn er voor de ontwikkel test en acceptatie omgevingen vragen over het gebruik van productie data en over Privacy Enhancement Technology (PET) hulpmiddelen.

Actiepunten:

- **(Wet) Onderzoek of het noodzakelijk is om alle gegevens te tonen die nu getoond worden en neem zo nodig maatregelen. De verwerking van persoonsgegevens moet zo beperkt mogelijk gehouden worden. [p10c1]**
- **(Wet) Onderzoek of het noodzakelijk is om alle gegevens te verstrekken die nu verstrekt worden via Excel of naar Analyst Notebook en neem zo nodig maatregelen. De verstrekking van persoonsgegevens moet zo beperkt mogelijk gehouden worden. [p10c2]**
- (Beleid) Onderzoek of het gebruik van productie data in de test en acceptatie omgevingen is toegestaan en borg zo nodig de maatregelen. [p10c4]
- (Beleid) Onderzoek of er voor de ontwikkel, test en acceptatie omgevingen nog meer gebruik gemaakt kan worden van Privacy Enhancement Technology (PET) hulpmiddelen zoals pseudonimisering, anonimisering en versleuteling. [p10c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	50%	33%	1

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.

Aangezien nog niet onderzocht is of er standaarden van toepassing zijn alle criteria negatief beantwoord.

Actiepunten:

- (Beleid) Onderzoek of er gebruik wordt gemaakt van de van toepassing zijnde bestaande overheids- en ketenstandaarden. [p11c1]
- (Beleid) Toets of de standaarden goed worden toegepast. [p11c2]
- (Beleid) Borg dat als er afwijkingen zijn van geldende standaarden dat deze voorzien zijn van een motivatie die is geaccepteerd door de verwerkingsverantwoordelijke. [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[4]	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

Voor dit principe zijn er alleen criteria vanuit beleid. Aangezien nog niet onderzocht is of er standaarden van toepassing zijn alle criteria negatief beantwoord.

Actiepunten:

- (Beleid) Zorg dat BSM de uitvoeringsverantwoordelijke ondersteund met het verwerken van de juiste classificatie en metagegevens voor de vastlegging van de grondslag en de rechtmatigheid. Er zijn verbeteringen mogelijk voor de verwerkingsgrondslag en de rechtmatigheid van de verwerking.[p12c4]

Aandachtspunten:

- Vanuit de dienst ICT wordt aangegeven dat er vanuit de opdrachtgever te weinig kaders en richtlijnen worden meegegeven. Deze zijn noodzakelijk voor de realisatie van wijzigingen. [p12]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[5]	90%	2

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

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-26_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 compliancy van de informatievoorziening.

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

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

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

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[6].

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.

[6] 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