Rapport 0-meting BVI-IB

PSbD compliance

10.2.e

Definitief

Versie 1.0

Versie datum 2 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	27-7-2018	Wet en regelgeving per criteria opnieuw beoordeeld en aangepast
0.9	02-11-2018	Aanpassingen verwerkt
0.92	02-04-2019	Opmerkingen van herijking meting op 28-03-2019 verwerkt.
1.0	02-04-2019	Rapport definitief gemaakt na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	18-10-2018	10.2.e	Gegevensautoriteit
0.9	02-11-2018	10.2.e	Gegevensautoriteit
0.91	29-3-2019	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 applicatie BVI-IB. 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 bij Amazone.
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 BVI-IB

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

	Naam	Functie
Applicatiedeskundigen	10.2.e	Applicatiemanager BVI Front-end
	10.2.e	Applicatieontwikkelaar
	10.2.e	Product Owner
	10.2.e	IV Expert Privacy & Security

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

Gesprek datum	Nummer meting	Toelichting
11-10-2017	20171011900/Basis Voorziening Informatie-BVI-IB Toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het **uitvoeringskader Privacy & Security by Design versie 1.0** Aanwezige deskundigen: 10.2.e , 10.2.e
28-03-2019	2019032801	Herijking meting. Aanwezige deskundigen: 10.2.e , 10.2.e , 10.2.e

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen		
Ordenen	X	
Bewaren		
Bijwerken		
Wijzigen		
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling		
Samenbrengen	X	
Met elkaar in verband brengen		
Afscherming	X	Er is maar één rol. Autorisatie wordt geregeld door de bron.
Uitwissen		
Vernietigen		

Verwerkingsgrondslag BVI-IB

Doelbinding	Verwerkingsgrondslag	X
Dagelijkse politietaak	Artikel 8	X
Onderzoek rechtsorde bepaald geval	Artikel 9	
Informatiepositie	Artikel 10	
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 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 BVI-IB behaald een volwassenheidsniveau 1. Dit houdt in dat BVI-IB 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 BVI-IB een score van 75% en op de criteria van het politiebeleid 79%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria van het principe 'Informatiebeveiliging' Hieronder staan de wetscriteria waarbij ons advies is hier direct wat aan te gaan doen.

UPDATE 28-3-2019: Naar aanleiding van de reacties op de eindscore van "0" uit de meting op 11-10-2017 zijn de actiepunten voor BVI-IB op 28-03-2019 opnieuw beoordeeld. Hierbij is er opnieuw gekeken naar de antwoorden die toen gegeven zijn in combinatie met de situatie zoals deze nu is. Dit heeft vooral veel invloed gehad op het principe autorisatie waarvan de actiepunten in 2018 opgepakt zijn. Gezien de tijdsspanne tussen de eerste meting en de nieuwe beoordeling is besloten om de laatste meting als maatstaf te gebruiken voor de 0-meting.

Advies

Het belangrijkste punt van advies wat gegeven kan worden is om zo snel mogelijk de punten aan te pakken die voor de wet vereist zijn.

- **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse. [p9c2]**
- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
BVI-IB	28-03-2019	v1.0	75%	79%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	NVT	100%	3
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	50%	2
Autorisatie	Z	-	100%	100%	3
Metagegevens	Z	-	NVT	83%	2
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	NVT	NVT	NVT
Informatiebeveiliging	Z	-	0%	20%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	100%	3
Principe is niet actief		-			
TOTALEN TOETSING		-	75%	79%	

In de afbeelding hierboven staan de volwassenheidsniveaus per principe beschreven. Waarbij de eerste kolom de weegfactor aangeeft van het principe op de eindscore. De tweede en derde kolom geeft het percentage aan van criteria in Wet en Beleid waarin is voldaan. Tot slot staat indien van toepassing een volwassenheidsniveau beschreven. Dit niveau is gebaseerd op de score van de toets criteria bij 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.

De gegevens in BVI-IB zijn afkomstig uit de politiesystemen. Dat betekent dat BVI-IB afhankelijk is van de kwaliteit van de gegevens in die systemen. De meeste van de criteria van dit principe zijn daardoor niet van toepassing. Hierdoor wordt voor dit principe de maximale score behaald.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	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 van informatiebeveiliging. Het is aan de betreffende verantwoordelijke managers om keuze te maken op basis van de stuurinformatie.

BVI-IB werkt op dit moment maximaal volgens de basis van cyclische terugkoppeling. Er worden (geautomatiseerd) rapportages opgeleverd t.b.v. de besturing van de gegevensverwerking. BVI-IB levert stuurinformatie op het gebied van verstrekkingen en aantallen gebruikers en rapporteert hier ook op terug.

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.

BVI-IB voldoet op zowel wet als beleid aan alles wat binnen de mogelijkheden ligt op het gebied van doelbinding. Ook hier is het afhankelijk van de bronsystemen. Staat het in het bronsysteem goed vermeld dan komt het er in BVI-IB ook correct uit.

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

Binnen BVI-IB is de audittrail nog niet optimaal beveiligt tegen manipulatie. Binnen de applicatie kunnen de gebruikers de audittrail niet manipuleren. Echter het is nu nog wel mogelijk dat een ontwikkelaar en/of beheerder de audittrail kan wijzigen zonder dat dit opgemerkt wordt. Een beheerder en/of ontwikkelaar moet een audittrail niet kunnen wijzigen zonder dat hiervan iets geregistreerd wordt. De registratie van handelingen moet beveiligd worden tegen manipulatie en moet waarborg bieden voor bewaring en goede toegankelijkheid. Het uiteindelijke doel is ervoor te zorgen dat de bewijskracht voor het verantwoordingsdoel niet in gevaar komt. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten. Het is van belang dat BVI-IB bekend is met het risico en dat het risico geminimaliseerd en/of geaccepteerd is(restrisico's).

Actiepunten:

- (Beleid): Zorg dat de audittrail beveiligd is tegen manipulatie en indien dat niet mogelijk is zorg er dan voor dat het risico geminimaliseerd en geaccepteerd is. [p4c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	50%	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.

BVI-IB voldoet aan alle criteria voor het principe autorisatie. IAM is de basis voor autorisaties in BVI-IB. Hierdoor wordt voor dit principe de hoogst mogelijke score gehaald.

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

1.6 Metagegevens

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

Om de juistheid en de rechtmatigheid van het gebruik te kunnen waarborgen worden metagegevens vastgelegd over bijvoorbeeld de context, inhoud, structuur, vorm en gedrag evenals het beheer en gebruik. Deze metagegevens bepalen de wijze waarop deze gegevens (mogen) worden verwerkt.

De gegevens in BVI-IB zijn afkomstig uit de politiesystemen. Dat betekent dat BVI-IB afhankelijk is van de kwaliteit van de gegevens in die systemen. Er is slechts één actiepunt. Dat betreft onderzoek naar het Toepassingsprofiel Metagegevens Politie (TMP). In eerste instantie het profiel van het rijk, en zodra het beschikbaar is, het profiel van politie.

Actiepunten:

- (Beleid): Kijk naar de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is [p6c4].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT[3]	83%	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.

De gegevens in BVI-IB zijn afkomstig uit de politiesystemen. Dat betekent dat BVI-IB afhankelijk is van de kwaliteit van de gegevens in die systemen. De meeste criteria van dit principe zijn daardoor niet van toepassing. Het enige kwaliteitscriterium dat wel van toepassing is betreft het beschikbaar zijn van de brondata. De gebruiker wordt geïnformeerd als daar niet aan voldaan wordt.

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

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

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.

BVI-IB voldoet aan dit principe omdat de verwerkingstermijnen worden beheerd in de bronsystemen.

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

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.

BVI-IB heeft recent geen risico analyse uitgevoerd. Het is belangrijk om 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 al kan zijn achterhaald. Het advies hier luidt om een risico analyse uit te laten voeren. Naar aanleiding van de resultaten uit de analyse moet worden gekeken welke informatiebeveiligingseisen moeten worden genomen en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Daar waar mogelijk moet er gebruik worden gemaakt van de standaard informatiebeveiligingsdiensten. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's in beeld zijn en in beheer zijn.

Actiepunten:

- (Beleid): Zorg dat er een nieuwe risicoanalyse voor de verwerkingen uitgevoerd gaat worden. [p9c1]
    - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse. [p9c2]**
    - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**
    - (Beleid): Controleer of alle informatiebeveiligingseisen gerealiseerd worden door de standaard informatiebeveiligingsdiensten. [p9c5]
        - Beleid): Neem maatregelen indien niet alle informatiebeveiligingsdiensten zijn gerealiseerd door de standaard informatiebeveiligingsdiensten. [p9c6]
    - (Beleid): Beheer de restrisico's op een periodieke basis. [p9c7]

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

1.10 Voldoen aan de wet

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

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

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

1.11 Toepassing 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.

BVI-IB maakt daar waar mogelijk is gebruik van bestaande overheids- en ketenstandaarden. De standaard referentiearchitectuur wordt gevolgd zoals deze door team Technische Architectuur van de Dienst ICT voorgelegd wordt. Er zijn bij dit principe geen wetscriteria actief dus BVI-IB heeft de maximale volwassenheidsscore van 100%.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassing standaarden	Zwaar (Z)	NVT[4]	100%	3

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

BVI-IB voldoet aan alle gestelde criteria op het gebied van 'verantwoordelijkheden belegd'. Het is van te voren vastgesteld dat de beleidsverantwoordelijke voor de gegevens die verwerkt worden bij BVI-IB de portefeuillehouder van BI is. De definities, beleid, koers en strategie zijn vastgesteld voor het verwerken van gegevens. BVI-IB ondersteunt de uitvoeringsverantwoordelijke met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[5]	100%	3

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

2 Verantwoording toetsing

2.1 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 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[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	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.

2.2 Disclaimer

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

3 Bijlage 1: Uitgangspunt bij compliance

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

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