0-meting
Blueview 4.0

PSbD compliancy

10.2.e

Definitief

Versie 2.1

Versie datum 11 april 2018

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-11-2017	Concept	
1.0	13-12-2017	Wet en regelgeving per criteria opnieuw beoordeeld en aangepast	
2.0	16-2-2018	• Aanpassingen n.a.v. feedback van 10.2.e en 10.2.e • Aanpassing volwassenheidsscore	
2.1	11-04-2018	• Aanpassing criteria mbt poortwachter (1.8) • Eindscore aangepast • Hoofdstuknummering aangepast	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1		10.2.e	Gegevensautoriteit
1.0	13-12-2017	10.2.e	Gegevensautoriteit
2.0	14-2-2018	10.2.e	Gegevensautoriteit
2.1	11-4-2018	10.2.e	Gegevenautoriteit

Review commentaar

Versie	Wanneer	Wie	Functie
2.0	14-2-2018	10.2.e	Rijks ICT Trainee
2.0	16-2-2018	10.2.e	Programmamanager

Inhoudsopgave

Documentinformatie 2

Inhoudsopgave 2

Inleiding 4

0-meting Blueview 4.0 5
Algemeen 5
Soorten verwerkingen van politiegegevens 6
Eindscore 7
1.1 Eenmalige vastlegging 8
1.2 PDCA-cyclus 8
1.3 Doelbinding 9
1.4 Verantwoording 9
1.5 Autorisatie 10
1.6 Metagegevens 10
1.7 Kwaliteitszorg 11
1.8 Bewaren en vernietigen 11
1.9 Informatiebeveiliging 12
1.10 Voldoen aan de wet 12
1.11 Toepassing standaarden 12
1.12 Verantwoordelijkheden belegd 13

2 Verantwoording toetsing 14
Toetsingscriteria 14
Disclaimer 16

Bijlage 1: Uitgangspunt bij compliance 17

Inleiding

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

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 Blueview 4.0. 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.

[1] Verbeterplan Wet Politiegegevens en Informatiebeveiliging
[2] Tranche 2018, Verbeterprogramma Wpg en IB

0-meting Blueview 4.0

Algemeen

Doel
Het doel van deze 0-meting is het transparant in beeld brengen van 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[3].

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 bij de 0-meting

	Naam	Functie
Direct betrokkenen 0-meting Blueview 4.0	10.2.e	Business analist, Dienst IM-Advies
	10.2.e	10.2.e , Dienst ICT-Ondersteuning

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

Analyse datum	Nummer analyse	Toelichting
11-10-2017 en 1-11-2017	20171011900/Basis Voorziening Informatie-Blueview Toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader Privacy & Security by Design versie 1.0.

[3] Commissie B&I besluit

Soorten verwerkingen van politiegegevens

Soort verwerking	X	OPM
Verzamelen		Nee gebeurt vanuit de bron
Vastleggen	X	
Ordenen	X	
Bewaren	X	
Bijwerken		
Wijzigen		
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling	X	
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	Voor zover de bron dat al niet doet door meta-gegevens te zetten, mutatieberichten te sturen of een nieuwe geschoonde set aan te leveren.
Uitwissen	X	Voor zover de bron dat al niet doet door meta-gegevens te zetten, verwijderberichten te sturen of een nieuwe geschoonde set aan te leveren.
Vernietigen	X	

Verwerkingsgrondslag Blueview 4.0

Doelbinding	Verwerkingsgrondslag	X
Dagelijkse politietaak	Artikel 8	X
Onderzoek rechtsorde bepaald geval	Artikel 9	X
Informatiepositie	Artikel 10	X
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

Blueview 4.0 scoort een volwassenheid van niveau 2 en dat betekent dat er wordt voldaan (100% score wet) op het gebied van de wet en regelgeving binnen de Wpg. Met een score van 90% bij (politie)beleid betekent dat er volop aandacht is voor Privacy & Security by Design (PSbD) en toont aan dat Blueview 4.0 een voorbeeld is op het toepassen van het uitvoeringskader PSbD.

Het advies aan Blueview 4.0 is om met aandacht te kijken naar het principe 'PDCA-cyclus'. In vergelijking met de andere principes is de score van 40% hier laag. Dit heeft vooral te maken met het gebruik van rapportages binnen Blueview 4.0. Er wordt wel volgens een cyclus overleg gevoerd, maar vanuit de applicatie wordt er niet gerapporteerd.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Blueview 4.0	11-10-2017 en 1-11-2017	20-10-2017 v1.0	100%	90%	2

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	NVT	NVT
PDCA-cyclus	M	-	NVT	40%	1
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	100%	3
Autorisatie	Z	-	100%	100%	3
Metagegevens	Z	-	100%	88%	2
Kwaliteitszorg	Z	-	NVT	88%	2
Bewaren en vernietigen	Z	-	100%	100%	3
Informatiebeveiliging	Z	-	100%	100%	3
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		-	100%	90%	

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

Nieuwe regelgeving WPG mei 2018

Om voorbereid te zijn op de nieuwe regelgeving mbt Wpg welke vanaf mei 2018 van toegepast zal worden is er ook gekeken of buiten het eerder genoemde actiepunt nog meer punten zijn die voor Blueview 4.0 aangepast moeten worden om te voldoen aan de wet. Er is één actiepunt wat nu benoemd is als beleid wat in mei 2018 verplicht zal zijn vanuit de Wpg.

- (Wet): Een GEB moet worden uitgevoerd indien er sprake is van een nieuwe verwerking en als is voldaan aan een van de volgende criteria: er wordt gebruik gemaakt van een nieuwe techniek en/of er is sprake van een hoog risico. In het geval van Blueview 4.0 zal er een gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd moeten worden.

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.

Het principe eenmalige vastlegging is voor de applicatie Blueview niet te beoordelen aangezien Blueview een raadpleeg/analyse systeem is.

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

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.

Blueview 4.0 werkt op dit moment nog onvoldoende op basis van cyclische terugkoppeling. Er wordt structureel overlegd met allerlei lagen, maar in de applicatie zelf wordt dat niet continu gerapporteerd. Incidenteel op basis van beheer en onderhoud wordt er gerapporteerd aan de beleidsverantwoordelijke. Deze manier van rapporteren gebeurt zowel handmatig als geautomatiseerd. De aandacht voor rapportage staat bij Blueview 4.0 op een lager niveau.
Om de risico's in kaart te brengen op gebied van verwerkingen is het van belang om een gegevensbeschermingseffectbeoordeling (GEB) uit te voeren. Voor Blueview 4.0 is er een bedrijfsrisicoanalyse (BRA) uitgevoerd, maar op dit moment is er nog geen GEB uitgevoerd. De GEB Wpg is op het moment van de toetsing nog niet beschikbaar, maar zodra de GEB Wpg volledig beschikbaar is dan zal dit direct uitgevoerd gaat worden. Vanaf mei 2018 is dit verplicht vanuit de Wpg.

Actiepunten:

- (Beleid): Op dit moment wordt er geen stuurinformatie geleverd via de PDCA-cyclus. Het gaat erom dat reguliere plan- en rapportageproducten zoals jaarplannen en jaarverslagen ook onderdelen bevatten over de omvang van de gegevensverwerking, de kwaliteit van gegevens, aantallen gebruikers, aantallen verstrekkingen, het beheer van autorisaties, beveiligingsmaatregelen en –incidenten.
- **(Beleid --> Wet vanaf mei '18): Een GEB moet worden uitgevoerd indien er sprake is van een nieuwe verwerking en als is voldaan aan een van de volgende criteria: er wordt gebruik gemaakt van een nieuwe techniek en/of er is sprake van een hoog risico. In het geval van Blueview 4.0 zal er een gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd moeten worden.**
- (Beleid): Rapportages op basis van besturing van gegevensverwerking moeten geautomatiseerd opgeleverd worden. Het is daarbij van belang om deze doelen meetbaar te maken zodat de uitvoering hiermee gestuurd en gecontroleerd kan worden. Op dezelfde manier moet over de uitvoering gerapporteerd worden. De managementrapportages moeten daarom ook een paragraaf bevatten over de gegevensverwerking zodat de verantwoordelijke managers kunnen (bij)sturen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	40%	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 de doelbinding te bepalen. Op basis van de doelbinding kan worden gerechtvaardigd waarom (politie)gegevens verwerkt mogen worden.

Blueview 4.0 voldoet op zowel wet als beleid aan alles wat binnen de mogelijkheden ligt op het gebied van doelbinding. De applicatie is hierin een voorbeeld voor andere applicaties. Blueview 4.0 heeft in de voorziening de verwerkingsgrondslag van een persoonsgegeven als metagegeven opgenomen. Het is mogelijk om meer dan één verwerkingsgrondslag bij een politiegegeven te verwerken. Daarnaast is er binnen Blueview 4.0 een goedgekeurd artikel 13-protocol. Binnen Blueview 4.0 blijven de metagegevens de verwerkingsgrondslag en termijn het gegeven begeleiden.

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 het 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 Blueview 4.0 worden alle handelingen, zoekvragen, klikken op resultaten en dergelijke gelogd. Kortom er wordt een audittrail geregistreerd. Ontwikkelaars en reguliere beheerders kunnen de audittrail niet wijzigen. Er is een zeer selecte groep beheerders die een audittrail kunnen wijzigen, maar het is niet mogelijk om de logging van de wijziging van de audittrail te wijzigen/verwijderen/vernietigen. Daarnaast wordt gebruik gemaakt van pro-actieve monitoring bij het wijzigen van de logfiles. Indien logfiles gewijzigd worden dan krijgt het management van DevOps direct een melding. Tot slot worden logfiles binnen een aantal seconden meervoudig gekopieerd op het bigdata platform om onder andere manipulatie lastiger te maken. Kortom Blueview 4.0 heeft het maximale gedaan wat binnen de mogelijkheden ligt om manipulatie tegen te gaan. Daarnaast is er een mogelijkheid om op verzoek doormiddel van een query een rapport samen te stellen.

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

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.

Blueview 4.0 voldoet op zowel wet als beleid aan alle voorwaarden mbt autorisatie. Er is een 10.2.c voorziening aanwezig om identiteiten te verifiëren. Daarnaast maakt Blueview 4.0 gebruik van toegangsverlening op gegevensniveau. De gebruikers zijn op de hoogte van de autorisatieregels en voor het verlenen van toegang wordt er gebruik gemaakt van een generieke autorisatietool voor leidinggevenden.

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.

Blueview 4.0 maakt gebruik van PGM en CDM voor het gebruik van vastgestelde definities en bedrijfsbegrippen. Er wordt gebruik gemaakt van de Wpg bedrijfsregels in de vorm zoals deze gepubliceerd zijn door de Gegevensautoriteit. Op dit moment maakt Blueview 4.0 geen gebruik van het toepassingsprofiel Metagegevens Rijk (in afwachting van het toepassingsprofiel Metagegevens politie). Bij Blueview 4.0 worden de metagegevens gebruikt voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. De Wpg grondslag wordt gebruikt om bewaartermijnen af te leiden en in andere gevallen worden de metagegevens van de bron overgenomen. In BVH zit ook opsporingsinformatie, terwijl dat eigenlijk artikel 9 persoonsgegevens zijn. Er is afgesproken dat alle gegevens in BVH in Blueview 4.0 worden gezien als artikel 8 gegevens, terwijl in de bron (BVH) het artikel nummer niet geautomatiseerd is ingevuld. Nu worden gegevens in Blueview 4.0 gelabeld als artikel 8, maar dat wordt niet expliciet gezegd om verkeerde aannames te voorkomen.

Actiepunten:

- (Beleid): Op dit moment is het toepassingsprofiel Metagegevens Rijk onbekend binnen Blueview 4.0. Het is van belang om te kijken of Blueview 4.0 voldoet aan de eisen/richtlijnen m.b.t. toepassingsprofiel Metagegevens Rijk. Bij een eerste controle bleek dat Blueview 4.0 al aan een hoop van de punten voldoet. Een verwijzing naar het Toepassingsprofiel Metagegevens Rijk staat beschreven in het uitvoeringskader PSbD v1 op blz 42 en op de website van het Rijk is de documentatie te vinden.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	100%	88%	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.

Blueview 4.0 voldoet aan bijna alle kwaliteitseisen. Er is nu een monitoring op datatransport (volledigheid). Er wordt gebruik gemaakt van source matrix (juistheid). Tevens wordt er getest om gegevens van Blueview 4.0 te controleren in de bron. Op basis van de grondslag worden de bewaartermijnen afgeleid, zodat gebruikers altijd rechtmatige gegevens te zien krijgen. Vanwege het feit dat Blueview 4.0 in ontwikkeling is voldoen ze nog niet aan alle kwaliteitseisen. Tijdigheid is op dit moment nog niet helemaal verwerkt in de applicatie, maar de verwachting is dat het in mei 2018 gerealiseerd is. Daarnaast wordt de gebruiker op dit moment niet geattendeerd op kwaliteitsafwijkingen. Er is een passieve raadpleging op het gebied van de metagegevens, maar niet om de gebruiker te attenderen.

Actiepunten:

- (Beleid): Niet aan alle kwaliteitseisen is op dit moment voldaan. Tijdigheid is (nog) niet helemaal verwerkt. Het gaat hierbij om de mate waarin gegevens binnen een afgesproken tijdsbestek beschikbaar zijn. (De verwachting is dat dit klaar is in mei 2018)
- (Beleid): De gebruiker wordt op dit moment niet geattendeerd op kwaliteitsafwijkingen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	88%	2

1.8 Bewaren en vernietigen

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

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

Blueview neemt hierin de bron over en in afwijkende gevallen kiest Blueview 4.0 voor een eigen veilige oplossing. Aan de wettelijke bepalingen m.b.t. bewaren, vernietigen en archiveren van (persoons)gegevens wordt voldaan. Blueview 4.0 geeft daarbij wel aan dat het bronsysteem hierin leidend is. Verwijdering en vernietiging kan in het bronsysteem worden gevolgd in Blueview 4.0. Op dit moment gebruikt Blueview 4.0 de rol en de bijbehorende functionaliteiten van de poortwachter niet.

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

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.

Op het gebied van informatiebeveiliging voldoet Blueview 4.0 aan alle criteria. Er is een risicoanalyse uitgevoerd en op basis daarvan zijn er beveiligingseisen opgesteld. Blueview ondersteunt het gebruik van 10.2.c . Als er een informatiebeveiligingsstandaard is dan zal Blueview 4.0 die gebruiken. Kortom Blueview 4.0 voldoet aan alle informatiebeveiligingseisen.

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

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.

Blueview 4.0 maakt gebruik van referentiearchitecturen die zijn goedgekeurd door het ABI (Architectuur Board ICT) welke zijn gebaseerd op overheidskaders. Op architectuur niveau worden keuzes gemaakt en afwijkingen worden in de stuurgroep van Blueview 4.0 besproken en gemotiveerd. Indien van toepassing maakt Blueview 4.0 gebruik van standaarden.

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

1.12 Verantwoordelijkheden belegd

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

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

Blueview 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 Blueview 4.0 de portefeuillehouder van BI is. De definities, beleid, koers en strategie zijn vastgesteld voor het verwerken van gegevens. Blueview 4.0 ondersteunt de uitvoeringsverantwoordelijke met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. Door gebruik te maken 10.2.c wordt de rechtmatigheid van gegevensverwerking gewaarborgd.

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

2 Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2017-07-20_Uitvoeringskader_Privacy en Security by Design_v1.0'. In deze versie is geen rekening gehouden met de bepalingen uit de AVG en de Europese richtlijn m.b.t. de Wpg. 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 op basis van het (politie)beleid.
- Niveau 1: Er is wel specifieke aandacht op het gebied van PSbD, maar die is niet toereikend om te voldoen aan de wet (Wpg) op basis van het (politie)beleid.
- Niveau 2: Er is wel specifieke aandacht op het gebied van PSbD en is afdoende om te voldoen aan de wet (Wpg), maar niet toereikend voor het (politie)beleid.
    - Wpg compliant
- Niveau 3: Het aandacht op het gebied van PSbD voldoet aan de wet en het vastgestelde (politie)beleid.
    - PSbD compliant

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[4].

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.

[4] Bijlage 1: Uitgangspunt bij compliance

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

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

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

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

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

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

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

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

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

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

Weegfactor
Van ieder principe is een weegfactor bepaald. Dit zijn L(icht) - M(iddel) en Z(waar). In combinatie met de procentuele score op zowel de wettelijke als beleidscriteria biedt dit de mogelijkheid te prioriteren welke werkzaamheden als eerste moeten worden uitgevoerd om een principe compliant te krijgen aan het uitvoeringskader.

De verdeling van de principes over de weegfactoren is als volgt:

Weegfactor	Licht (L)	Middel (M)	Zwaar (Z)
Aantal	1	3	9

Aandachtspunten
1: Volwassenheidsniveau 1:

Voor het vaststellen van dit niveau maakt het geen verschil of de voorziening of het principe geheel of deels aan een of alle min 1 wettelijke criteria voldoet.

2: Beleidscriteria:

Met uitzondering van niveau 3 geldt dat de mate waarin de voorziening voldoet aan de beleidscriteria, uitgedrukt in een percentage, niet van invloed is op de vaststelling van het volwassenheidsniveau. Het percentage beleidscriteria bij een principe is wel een indicatie of meer of minder inspanning moet worden geleverd om het principe compliant te krijgen aan het uitvoeringskader. Met name in combinatie met de percentages van de wettelijke criteria bij het volwassenheidsniveau 1 en in combinatie met de weegfactor geeft het inzicht bij het prioriteren van werkzaamheden om de voorziening compliant te maken.

3: Privacy functionaris:

De applicatie specifieke requirements mbt PSbD worden tijdens de ontwikkeling bepaald in samenwerking met de Privacy Functionaris en de business expert. Daarnaast is de privacy functionaris eerste aanspreekpunt mbt vragen over privacy.

Disclaimer

Aan de resultaten op basis van het gebruik van de 0-meting wordt geen enkele garantie met betrekking tot de mate van compliancy 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