0-meting Privacy & Security by Design

BVID 2.0

10.2.e

Concept

Versie 2.0

Versie datum 27 juni 2018

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
1.0	23-03-2018	Eerste conceptversie	
1.1	18-05-2018	Aanpassingen aan de hand van feedback 10.2.e)	
2.0	27-6-2018	Definitieve versie van het rapport met wederzijds akkoord 10.2.e	

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 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 BVID 2.0. Per principe wordt beschreven of BVID 2.0 voldoet aan de criteria op basis van wet of beleid. Bij het niet voldoen aan criteria wordt in een actiepunt beschreven op welke manier verbeterd moet worden. De 0-meting dient als hulpmiddel om aan te geven wat moet worden gedaan om PSbD compliant te worden.

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

0-meting BVID 2.0

Algemeen

Doel
Het doel van de PSbD 0-meting is het transparant in beeld brengen wat de actuele volwassenheid van highriskapplicaties op het gebied van PSbD. Vanuit deze 0-meting kan er op basis van de actiepunten toegewerkt worden naar een applicatie die PSbD compliant (Wpg compliant in het bijzonder) is. Om dit doel te bereiken is er gebruik gemaakt van uitvoeringskader PSbD wat in juli 2017 is vastgesteld.

Doelgroep
De landelijke portefeuillehouder kan dit document gebruiken om maatregelen te nemen om de applicatie PSbD compliant te maken. De gegevensautoriteit heeft op 22 november 2017 een brief naar de landelijke portefeuillehouder gestuurd omtrent het PSbD compliant maken van applicaties. Het portefeuilleteam voert in overleg met de portefeuillehouder de maatregelen uit. Waarbij de productowner de actiepunten prioriteert en verwerkt op de productbacklog.

Aanwezigen 0-meting

	Naam	Functie
Directe betrokkenen 0-meting BVID 2.0	10.2.e	Productowner & functioneel beheerder BVID 2.0
	10.2.e	Functioneel beheerder BVID 2.0

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

Gespreksdatum	Nummer meting	Toelichting
08-01-2018	2018010801	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

BVID 2.0

Omschrijving BVID 2.0

BVID 2.0 ondersteunt bij het vaststellen van de identiteit. Identiteitsvaststelling is er in twee processen: de intake van een verdachte (obv Strafrecht/Strafvordering, het is verplicht de identiteit van een verdachte vast te stellen) en obv de Vreemdelingenwet voor de registratie van vreemdelingen. Een aparte tak van sport is het identificeren van verdachte vreemdelingen, dan verspringt het systeem. Beide processen (strafrecht en vreemdelingen) zijn hetzelfde, maar het kader is anders. Er wordt opgeschreven wie de persoon voor de zuil is, het document wordt opgenomen, evenals de foto en vingerafdrukken. De kwaliteitseisen van de vingerafdrukken verschilden van proces, maar met de komst van BVID 2.0 zijn deze geharmoniseerd. BVID 2.0 is een doorgeefluik. Voor het proces van een verdachte wordt alles doorgegeven aan de SKDB. Alle vreemdelingengegevens gaan naar BVV. Voor een verdachte geldt dat in de eerste 9 uur dat ze vastzitten, moet worden vastgesteld wie het is. Nog voor de rechtmatigheid van de inverzekeringstelling is getoetst zijn ze al langs de zuil geweest. Voor de loggingsdoeleinden wordt alle data vastgelegd in de daarvoor bestemde database. Verder wordt een gedeelte van de data vastgehouden voor:

- Reproduceren van ID staten. Dit zijn statische PDF formulieren, die 30 dagen worden bewaard;
- Uitslagen uit Europese systemen, Eurodac en EUVIS, worden 180 dagen vastgehouden. De reden is dat ketenpartners in het vervolgtraject deze gegevens nog op kunnen en mogen vragen.

Er zijn twee regimes in BVID: de strafrechtketen en de vreemdelingenketen.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen		
Ordenen		Niet gecategoriseerd
Bewaren	X	Wel bewaarregime (zie hierboven)
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)		In BVID wordt er niets vastgelegd, in de achterliggende systemen kan het wel worden vastgelegd
Wijzigen (het bestaande aanpassen)		Niets vastgelegd, in de achterliggende systemen kan het wel, BVID niet
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	Hits worden wel vergeleken, maar niet in BVID zelf. Vb. vingerafdrukken (resultaten vergeleken met resultaten andere applicaties)
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen		Er wordt niet samengevoegd, wel losstaande gegevens samen bekeken, maar het wordt geen nieuw gegeven.
Met elkaar in verband brengen	X	Vb. vingerafdrukken. Er wordt gekeken of vingerafdrukken gematcht kunnen worden.
Afscherming	X	Er zitten autorisatieniveaus in, er kunnen geen zaken op besloten worden gezet. Je kunt alleen de gegevens zien die voor jou van toepassing zijn.
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Als er fouten zijn wordt er wel een bericht naar SKDB gestuurd dat de gegevens er niet mogen zijn. Aangezien BVID een volgsysteem is, moet de wijziging / verwijdering / vernietiging plaatsvinden in de SKDB.
Vernietigen	X	

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	*Artikel 8*	*X*	*Alleen strafrechtketen & vreemdelingenketen kent andere verwerkingsgrondslag*
Onderzoek rechtsorde bepaald geval	*Artikel 9*	*X*	*Strafrechtketen & vreemdelingenketen kennen andere grondslagen*
Informatiepositie	Artikel 10		
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13		
Vreemdelingenwet 2000		X	*In het kader van ID-vaststellingen van vreemdelingen*

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.

Vreemdelingenwet 2000: In het kader van ID-vaststellingen van vreemdelingen

Hoewel er een grondslag is om de persoonsgegevens van de personen die voor de zuil verschijnen te verwerken (art. 8 of 9 Wpg) ligt de grondslag van de verwerking door de zuil zelf in een andere wet. Op grond van het Wetboek van Strafvordering (art. 27) en de Wet Identiteitsvaststelling verdachten, veroordeelden en getuigen moet de identiteit van verdachten worden vastgesteld.

Eindscore

BVID 2.0 scoort een volwassenheidsniveau 2 (voldoende). Dit houdt in dat BVID 2.0 voldoet aan de Wpg criteria van het uitvoeringskader PSbD. Echter zoals besproken tijdens de 0-meting valt BVID 2.0 niet (geheel) onder het Wpg-regime. De grondslagen zijn te vinden in Strafvordering en de Vreemdelingenwet. Deze regimes zijn buiten scope gelaten tijdens de 0-meting. BVID 2.0 is dus een uitzonderlijke geval bij de 0-metingen en de score kan ook een vertekend beeld laten zien. Desondanks is de behaalde score heel goed. Niet alleen de eisen uit de Wpg worden getest, ook het staande politiebeleid wordt getest. Ook daar scoort BVID 2.0 goed op (83%). Ons advies is om te kijken hoe en op welke wijze BVID meer compliant kan worden met het politiebeleid. Het is verder van belang de ontwikkelingen op het gebied van privacy en security in de gaten te houden en hier op in te spelen.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
BVID 2.0	08-01-2018	1.0	100%	85%	2

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	67%	2
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	100%	3
Autorisatie	Z	-	100%	58%	2
Metagegevens	Z	-	NVT	86%	2
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	NVT	NVT	NVT
Informatiebeveiliging	Z	-	100%	83%	2
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%	85%	

In de afbeelding hierboven staan de volwassenheidsniveaus per principe beschreven. De eerste kolom geeft de weegfactor van het principe op de eindscore weer. De tweede en derde kolom geven het behaalde percentage van de beleids- en wetscriteria weer. Tot slot staat het volwassenheidsniveau per principe weergegeven. Dit niveau is gebaseerd op de score van alle principes van deze toets. In de volgende paragrafen worden de resultaten per principe nader toegelicht.

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.

Voor het principe eenmalige vastlegging voldoet BVID 2.0 volledig aan zowel de wet als het politiebeleid 100%. Het volwassenheidsniveau is het maximaal haalbare niveau 3.

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

BVID 2.0 heeft een volwassenheid van 2 op de PDCA-cyclus. Tijdens de 0-meting kwam al naar voren dat het idee van PDCA wel is verwerkt in de processen, maar vanwege de andere werking werkt het net anders. Gegevens over wie wanneer is ingelogd worden 30 dagen bewaard, voor de rest worden er geen gegevens vast gehouden. De maandelijks gegenereerde gegevens worden niet door BVID 2.0 zelf gegeneerd, maar door de systemen er omheen. De controles zijn niet automatisch, maar komen voort uit query’s.

De rapportages die worden opgeleverd ten behoeve van de besturing worden nog niet geautomatiseerd opgeleverd. Hoewel dit wel op de backlog staat is BVID 2.0 hiervoor afhankelijk van BVI. BVID heeft namelijk zelf geen gegevens.

Actiepunt:

- (beleid): het opleveren van rapportages tbv besturing moet worden opgeleverd. Dit is echter afhankelijk van BVI. Het is aangekaart bij BVI en staat daar op de backlog.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	67%	2

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.

Op het principe doelbinding scoort BVID 2.0 100% voor zowel de wet als het politiebeleid. De grondslag voor gegevensverwerking in BVID 2.0 ligt in het Wetboek van strafrecht (art. 27a) en in de Vreemdelingenwet. Tijdens de 0-meting bestond nog enige onduidelijkheid over de protocolplicht, maar aangezien BVID 2.0 geen gegevens verder verwerkt op grond van de Wpg is een art. 13 Wpg-protocol niet nodig.

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.

BVID 2.0 heeft een volwassenheidsniveau van 3 bij het principe verantwoording. Zowel op de wets- als beleidscriteria scoort BVID 2.0 de maximale score van 100%.

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.

Voor het principe autorisatie heeft BVID 2.0 op de wet 100%, maar op beleid slechts 58%. Hier zit, ondanks de voldoende score op volwassenheid, nog verbetering in. Voor het verlenen van toegang tot de applicatie maakt BVID 2.0 geen gebruik van IAM, omdat er een opleiding is vereist. De rollen die nodig zijn zitten niet in IAM. Er moet wel worden gekeken of er mogelijkheden zijn om aan te sluiten op IAM. En zo ja, op welke manier. BVID 2.0. maakt verder geen gebruik van toegangsverlening op gegevensniveau, waardoor het mogelijk zou zijn dat gebruikers (onbedoeld) toegang kunnen verkrijgen via een andere applicatie. Toegangs- en gebruiksrechten worden niet regelmatig gecontroleerd. De functioneel beheerder doet dit handmatig. Er moet nog beleid worden gemaakt omtrent de periode waarin iemand niet in kan loggen. Als een gebruiker van functie verandert wordt dat niet automatisch aangepast, maar moet dat via ATL. Bij een functieverandering wordt de autorisatie niet automatisch gewijzigd. Er moet een signaal af worden gegeven en naar aanleiding daarvan handmatig de autorisatie aan worden gepast. Het nadeel hier aan is dat als er geen signaal wordt afgegeven er niet wordt geacteerd op de functieverandering. Op het moment krijgen alle gebruikers eerst een opleiding voordat ze van BVID 2.0 gebruik mogen maken. Indien zaken wijzigen kan dat bij de informatieknop bij het in te vullen veld worden opgevraagd. Het zou nog wel een idee zijn om actief de wijzigingen te communiceren met de gebruiker. Bijvoorbeeld door middel van een alarmbelletje (zoals op de intranet pagina) waarmee de gebruiker gewaarschuwd wordt.

Actiepunten:

- (Beleid): BVID 2.0 moet kijken of en op welke manier IAM kan worden gebruikt voor de autorisatie.
- (Beleid): er moeten periodieke rapportages worden gemaakt van het gebruik van autorisaties. Op deze manier kan goed in de gaten worden gehouden wie er nog wel gebruik maakt van de voorziening en of ze daar ook nog recht op hebben.
- (Beleid): momenteel worden de toegang- en gebruiksrechten nog niet regelmatig gecontroleerd. Ook moet worden gekeken naar hoe de autorisatie naar aanleiding van functieverandering wordt ingevuld. Er moet worden voorkomen dat gebruikers die een andere functie hebben gekregen, of lange tijd inactief zijn, nog wel toegang tot de applicatie kunnen hebben.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	58%	2

1.6 Metagegevens

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

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

De wettelijke criteria voor het principe metagegevens zijn niet van toepassing op BVID 2.0. Op de beleidscriteria scoort BVID 86%, waarmee het een voldoende volwassenheid behaalt. Het Toepassingsprofiel Metagegevens Rijk wordt niet toegepast, omdat moet worden voldaan aan het elektronische berichtenverkeer zoals is vastgesteld door Justitie. De politie is niet de eigenaar van de voorziening, maar slechts beheerder.

Actiepunten:

- (beleid): Kijk of het Toepassingsprofiel Metagegevens Rijk kan worden geïmplementeerd.
- (beleid): Kijk naar de mogelijkheden om metagegevens geautomatiseerd vast te leggen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	86%	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.

Ook bij het principe Kwaliteitszorg zijn er geen wettelijke criteria van toepassing. Op beleidscriteria scoort BVID 2.0 100%. De controles op de kwaliteit van foto's zijn volgens ISO en ICAO normeringen. De controles op de kwaliteit van de vingerafdrukken worden getoetst volgens de NFIQ normering. Daarnaast vindt de identificatie en verificatie van subjecten geprotocolleerd plaats, waarbij voor zowel vingerafdrukken als voor gelaatsfoto's geautomatiseerde kwaliteitscontroles zijn ingebouwd inclusief feedback naar de gebruiker.

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

BVID 2.0 functioneert als doorgeefluik, dus slaat zelf geen gegevens op. Alle gegevens zijn afkomstig uit de achterliggende systemen. Hierdoor is het principe bewaren en vernietigen niet van toepassing.

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.

De week voor de 0-meting was de risico-analyse opgeleverd. Hierin stond dat BVID compliant was en ze voldoen aan de informatiebeveiligingseisen. Eventuele opmerkingen of verbeterpunten waren op moment van de 0-meting nog niet meegenomen. Op basis van PSbD voldoet BVID 2.0 volledige aan de wettelijke criteria en voor 83% aan de beleidscriteria. Het is van belang dat eventuele verbeterpunten uit de risicoanalyse worden meegenomen en geïmplementeerd.

Actiepunt:

- (beleid): BVID 2.0 maakt nog niet maximaal (deels) gebruik van de specifieke ontwerprichtlijnen die in de informatievoorziening van politie moeten worden toegepast.
    - Gelaagde beveiliging
    - Segmentering
    - Koppelvlakken
    - Identificatie en authenticatie
    - Registratie en controle
    - Beschikbaarheidsfuncties

  Er moet worden gekeken waar dit nog verbeterd en toegepast zou kunnen worden. Toelichting staat op blz 55 van het uitvoeringskader PSbD v1.0.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	100%	83%	2

1.10 Voldoen aan de wet

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

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

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

1.11 Toepassen standaarden

"*Bij de gegevensverwerking wordt gebruik gemaakt van bestaande overheids- en ketenstandaarden*"

Door het gebruik van bestaande overheids- en ketenstandaarden bevordert de samenwerking tussen de organisaties en de interoperabiliteit van systemen. In de basis is het ban belang om waar mogelijk gebruik te maken van standaardisatie en uniformiteit binnen een informatievoorziening. Indien een organisatie hierin een eigen keuze maakt en afwijkt van standaarden zullen er afspraken gemaakt moeten worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

BVID 2.0 heeft de maximale score op het principe toepassen standaarden. De voorziening maakt gebruik van EBV en voldoet waar mogelijk aan het toepassen van de standaarden.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen 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

Op het laatste geteste principe, verantwoordelijkheden belegd, heeft BVID een volwassenheid van niveau 3.

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

2. Verantwoording toetsing

2.1 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[3].

De betekenis van de volwassenheidsniveau ’s is meetbaar gemaakt door het formuleren van de volgende bedrijfsregels. Het uitgangspunt hierbij is dat wettelijke criteria zwaarder wegen dan beleidscriteria.

[3] Bijlage 1: Uitgangspunt bij compliance

Bedrijfsregels volwassenheidsniveau
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