0-meting Privacy & Security by Design

Havank

10.2.e

Definitief

Versie 1.1

Versie datum 5 december 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	06-04-2018	Eerste concept versie	
1.1	5-12-2018	Aanpassingen op basis van feedback betrokkenen	

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
1.0	6-4-2018	10.2.e	Gegevensautoriteit
1.1	5-12-2018	10.2.e	Gegevensautoriteit

Inhoudsopgave

Inleiding

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

Het meten van de Privacy & Security by Design (PSbD) compliance van highrisk applicaties is onderdeel van het verbeterprogramma Wpg en IB.[2] Het PSbD uitvoeringskader staat aan de basis om de highrisk applicaties van de politie te laten voldoen aan het PSbD compliance.

Privacy & Security by Design (PSbD)
PSbD betekent dat al in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de informatievoorzieningen, mechanismen worden ingebouwd voor informatiebeveiliging en de bescherming van persoonsgegevens. Dit vereist dat er in een zo vroeg mogelijk stadium wordt nagedacht over het gebruik van persoonsgegevens binnen de organisatie, over de noodzaak van het gebruik van gegevens en over de bescherming ervan.

Dit document beschrijft het resultaat van de 0-meting welke is uitgevoerd bij applicatie Havank. Op basis van het de 0-meting zal per principe beschreven worden of ze voldoen aan de criteria van wet en beleid en op welke manier (actiepunten) verbeterd moeten worden. De 0-meting dient als hulpmiddel om duidelijker aan te geven wat er gedaan moet worden om PSbD compliant te worden. De score uit de 0-meting is bepaald op antwoorden gegeven door de direct betrokkenen van de applicatie.
In dit document wordt bij de aanbevelingen verwezen naar de principes en de onderliggende criteria met de volgende codering [p1c3]. Dit voorbeeld staat voor principe 1 (Éénmalige vastlegging) met criterium 3 (Verificatie in basisregistratie).

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

0-meting Havank

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 Havank	10.2.e	Eindverantwoordelijke Havank
	10.2.e	Applicatiemanager Havank
	10.2.e	Functioneel beheer Havank
	10.2.e	Functioneel beheer

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

Gespreksdatum	Nummer meting	Toelichting
08-03-2018	2018030801	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Havank

Omschrijving applicatie

Havank ondersteunt twee processen: het sporenonderzoek en het afnemen van vingerafdrukken. Elke persoon die verdacht wordt van een misdrijf waarop voorlopige hechtenis staat, moet naast zijn personalia ook vingerafdrukken afgeven. Vanuit de BVID zuil gaan deze in een pakket naar Havank. Havank controleert op basis van biometrie, of deze persoon al in het systeem is opgenomen en onder welke naam. BVID is rechtstreeks gekoppeld aan Havank.

Daarnaast worden handpalmen opgenomen en vergeleken met sporen gevonden op het plaats delict. De FO stelt de sporen veilig en deze worden aan Havank beschikbaar gesteld om de donor van het spoor vast te stellen. In Havank wordt verder niet geoordeeld over de resultaten. Bij Havank wordt alleen met zaaknummers gewerkt, dus het is niet mogelijk te zien of iemand een slachtoffer, verdachte of getuige is en om wat voor zaak het gaat. Als een spoor niet wordt herkend gaat deze in een database voor onopgeloste sporen en vingerafdrukken van onbekende verdachten. De uitslag van Havank (de vingerafdruk) gaat rechtstreeks terug naar de SKDB. Het sporenonderzoek komt dan terug als rapport.

Er worden ook vreemdelingen aangeboden om te kijken of zij bekend zijn in de strafrechtketen (ogv art. 107 Vreemdelingenwet 2000). Onder strikte voorwaarden kan worden gekeken of een Vreemdeling te maken heeft met een specifieke zaak.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Toelichting
Verzamelen	X	
Vastleggen (registreren)	X	
Ordenen (vb. in categorieën plaatsen)	X	
Bewaren (opslaan)	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen (ophalen van gegevens)	X	
Raadplegen (bekijken van gegevens)	X	
Gebruiken	X	
Vergelijken (bv ter verificatie)	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen (samenvoegen)	X	
Met elkaar in verband brengen (vanuit de applicatie)	X	
Afscherming (minder zichtbaar of toegankelijk maken ter bescherming van)	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)		Er wordt niet verwijderd, alleen vernietigd. Bewaar en vernietigingstermijnen hangen af van andere wetten.
Vernietigen	X	

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X
Dagelijkse politietaak	Artikel 8	
Onderzoek rechtsorde bepaald geval	Artikel 9	
Informatiepositie	Artikel 10	
Informanten	Artikel 12	
Ondersteunende taken	Artikel 13	X
Overige wetten	Wet & besluit ID-vaststelling Wetboek van Strafvordering EU besluit PRUM Wet herziening bij veroordeling	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

Havank heeft op dit moment een volwassenheidsniveau van 1. Hoewel dit aangeeft dat Havank onvoldoende compliant met het uitvoeringskader Privacy & Security by Design is, moeten hier wel een kanttekening voor worden gemaakt. Bij de 0-meting kan slechts een voldoende worden gescoord als voldaan is aan alle wetscriteria. Immers, pas als aan de wet is voldaan kan worden gesteld dat een applicatie compliant is. Op de wetscriteria heeft Havank een score van 93% en dat betekent dat er op dit moment aan slechts één wetscriteria niet kan worden voldaan. Er is niet voldaan aan het principe informatiebeveiliging, omdat de laatste risicoanalyse dateert van 2009. In de tussentijd is geen nieuwe analyse op het gebied van informatiebeveiliging uitgevoerd. Vanwege de veranderende omgeving op het gebied van informatiebeveiliging is het van belang om de gehanteerde beveiligingsmaatregelen regelmatig te controleren.

Op de criteria van het politiebeleid scoort Havank 84%. Een hoge score, waarbij de verbeterpunten zitten bij de verantwoording, autorisatie en ook de informatiebeveiliging. Ons advies is om eerst te kijken hoe het punt van de wetscriteria aangepakt kan worden. Hierbij zal er gekeken moeten worden hoe snel de nieuwe applicatie beschikbaar is ten opzichte van het laten uitvoeren van een risico analyse.

Advies (alleen de wettelijke actiepunten worden hier genoemd. De beleidspunten blijken uit het document):

- **(Wet): De huidige beveiligingsrisico analyse is te lang geleden (2009) uitgevoerd. Er zullen beveiligingseisen opgesteld moeten worden op basis van een nieuwe risico analyse.**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Havank	08-03-2018	V1.0	93%	84%	1

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	NVT	88%	2
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	50%	2
Autorisatie	Z	-	100%	67%	2
Metagegevens	Z	-	NVT	86%	2
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	100%	100%	3
Informatiebeveiliging	Z	-	50%	40%	1
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		-	93%	84%	

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.

Nieuwe regelgeving Wpg mei 2018 (buiten de 0-meting)

Vanaf mei 2018 is de nieuwe Wpg van toepassing. Enkele criteria die in deze 0-meting nog als beleid zijn aangemerkt worden vanaf dat moment wet. Onder andere gaat het om de verplichting een GEB uit te voeren of de Autoriteit Persoonsgegevens (AP) te raadplegen. Havank heeft echter al aangegeven dat vanwege de bijzondere categorie persoonsgegevens (biometrische gegevens) deze trajecten al in een eerder stadium en met een hoge mate van zorgvuldigheid worden doorlopen. Aan de overige punten die van beleid naar wet veranderen voldoet Havank al.

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.

Havank heeft op het principe eenmalige vastlegging de hoogst mogelijke score behaald. Zowel op de wets- als beleidscriteria scoort Havank 100%.

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.

Op het principe PDCA-cyclus scoort Havank volwassenheidsniveau 2 (voldoende). Er zou nog kunnen worden gekeken naar de regie van de beleidsverantwoordelijke. De portefeuillehouder houdt zich vooral bezig met de interne zaken van de applicatie en reageert op aangeven van het team. De uitvoeringsverantwoordelijke is inhoudelijk bezig met de applicatie en voert de regie op definities en houdt zich met het beheer bezig. Er is alleen geen officieel mandaat.

Daarnaast kwam tijdens de 0-meting naar voren dat procedures zoals het raadplegen van de Autoriteit Persoonsgegevens (AP) vaak al aan het begin van een ontwikkelingstraject worden doorlopen. Vanwege de gevoeligheid van biometrische gegevens worden dergelijke trajecten zeer zorgvuldig doorlopen. Vanaf mei 2018 is het uitvoeren van een Gegevensbeschermingseffectbeoordeling (GEB) verplicht. Dit geldt voor nieuwe verwerkingen waarbij sprake is van een hoog risico of gebruik wordt gemaakt van een nieuwe technologie. Aangezien Havank biometrische gegevens verwerkt zal snel sprake zijn van een hoog risico. Afgaand op hoe nu wordt omgegaan met dergelijke procedures hoeft hier geen actiepunt van worden gemaakt.

Actiepunt:

- (Beleid): de rol van uitvoeringsverantwoordelijk zou officiëler ingevuld kunnen worden. Op basis van de huidige situaties zijn er beperkte mogelijkheden om beslissingen te nemen zonder een officieel mandaat. [p2c6]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	88%	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.

Havank scoort op het principe doelbinding een volwassenheidsniveau van 3, dat is de maximaal haalbare score.

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.

Op het principe verantwoording heeft Havank een volwassenheid van niveau 2 (voldoende). Naast dat er een audittrail wordt geregistreerd is het ook mogelijk op basis hiervan een rapportage te genereren. Waar nog naar kan worden gekeken is naar de mogelijkheid tot manipulatie van de audittrail. Er is een speciale audit functionaliteit die (tegen licentiekosten) aan kan worden gezet (Oracle) waarbij de acties van o.a. de database administrator kunnen worden geregistreerd. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten Het is van belang dat Havank bekend is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's).

Actiepunten

- (Beleid): afweging maken of de beveiliging tegen manipulatie van de audittrail aangezet moet worden. [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.

Op het principe autorisatie scoort Havank een voldoende met volwassenheidsniveau 2 (voldoende). Er zijn nog verbeteringen mogelijk op de toegangsverlening. Op het moment is Havank niet aangesloten op IAM en maakt het geen gebruik van de generieke autorisatietool voor leidinggevenden. De reden hiervoor is dat Havank een apart systeem binnen de politie is en niet mocht worden gekoppeld aan politiesystemen. Tijdens de 0-meting werd al aangegeven dat het eventueel wel wordt meegenomen bij de nieuwe versie. Gebruikers van het systeem worden goed up-to-date gehouden over de autorisatieregels. Dagelijks is er een briefing en per mail stelt FB iedereen op de hoogte in het geval van een wijziging. Ook worden de toegang- en gebruiksrechten regelmatig gecontroleerd. Iedere maand wordt gekeken wie wel en niet hebben ingelogd.

Actiepunten

- (Beleid): Havank is op dit moment niet aangesloten op IAM, er zal onderzocht moeten worden of IAM toegepast kan worden in de nieuwe versie van Havank. [p5c1]
- (Beleid): Stel vast of en op welke wijze gebruik kan worden gemaakt van de generieke autorisatietool voor leidinggevenden in de nieuwe versie. [p5c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	67%	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.

Ook bij het principe metagegevens scoort Havank een voldoende (niveau 2). Hierbij zijn geen wetscriteria 'actief', maar de score op de beleidscriteria is hoog (86%). Aangezien Havank is ontwikkeld voordat het Toepassingsprofiel Metagegevens Rijk (TMR) is opgesteld, is deze niet toegepast. Voor de nieuwe versie kan dit wel worden gedaan.

Actiepunten

- (Beleid): onderzoek of het mogelijk is TMR op te nemen in de nieuwe versie van Havank. [p6c4]

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.

De maximale score van 100% (volwassenheidsniveau 3) is voor het principe kwaliteitszorg behaald. Havank heeft kwaliteitseisen gesteld en voldoet aan de ISO-normen. Daarnaast zijn er kwaliteitsnormen opgesteld die in BVID worden gehandhaafd. Als een registratie niet voldoet aan de normen, kan die niet in het systeem worden opgenomen. Ook vindt een tweewekelijks overleg plaats waarin de (eventuele) incidenten worden besproken.

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.

Op het principe bewaren en vernietigen heeft Havank het volwassenheidsniveau 3 behaald. In principe kan Havank zelf niet besluiten tot verwijderen of vernietigen, aangezien het JustID volgt. De wetgever heeft deze keuze gemaakt. Een bestand is óf actief of wordt vernietigd en JustID gaat hier over. Indien iets moet worden vernietigd (er bestaat geen optie tot verwijderen) wordt vanuit JustID een vernietigingsbericht verstuurd. Bij sporen van onbekende verdachten is er een verloopdatum en wordt het gegeven automatisch vernietigd. De gegevens worden ook niet ten behoeve van duurzame toegankelijkheid opgeslagen of gearchiveerd. Dat is namelijk op grond van de wet niet mogelijk. Tijdens de 0-meting kwam naar voren dat dit wel iets is om over na te denken. Sommige zaken zijn zo belangrijk of hebben veel impact gehad dat het vernietigen van de gegevens zonde zou zijn. Dit is echter iets voor de wetgever en de strafrechtketen en niet alleen voor Havank.

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 principe informatiebeveiliging scoort Havank een volwassenheidsniveau 1 (onvoldoende). Dit heeft te maken met het feit dat de risicoanalyse gedateerd is. De laatste keer dat een dergelijke analyses is uitgevoerd is in 2009. Het is van belang regelmatige de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. Vandaar dat is besloten om de criteria betreffende de risicoanalyse op deels te zetten. Verder is vanuit de keten opgelegd welke beveiligingseisen moesten worden gerealiseerd. Het niet realiseren van alle beveiligingseisen is dan ook een bewuste keuze. Ook worden de restrisico's niet beheerd.

Van belang is dat nu een nieuwe risicoanalyse op het gebied van informatiebeveiliging wordt uitgevoerd. Naar aanleiding van deze analyse moeten de beveiligingseisen worden bepaald.

Actiepunten:

- (Beleid): voer een nieuwe risicoanalyse voor de verwerking uit. [p9c1]
- **(Wet): bepaal de informatiebeveiligingseisen obv de resultaten uit de risicoanalyse.** [p9c2]
- (Beleid): beoordeel de impact van de informatiebeveiligingseisen op de realisatie van de voorziening. [p9c3]
- (Beleid): stel een lijst van restrisico's op en kijk hoe deze moeten worden beheerd. [p9c7]

Aandachtspunten:

- (Beleid): indien het mogelijk is bij de nieuwe versie, maak gebruik van de generieke voorzieningen voor informatiebeveiliging. [p9c4]
- (Beleid): bekijk of het mogelijk is alle informatiebeveiligingseisen te realiseren met de standaard informatiebeveiligingseisen. [p9c5]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	50%	40%	1

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.

Het volwassenheidsniveau van het principe Toepassen standaarden is maximaal (niveau 3).

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 dat de verantwoordelijkheden voor gegevensverwerking belegd zijn om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen

Ook op het principe Verantwoordelijkheden belegd wordt maximaal gescoord met een volwassenheidsniveau van 3.

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'. Vervolgens zijn er criteria toegevoegd of aangescherpt op basis van documenten waar in het uitvoeringskader naar wordt verwezen. Het resultaat is met de auteurs van het uitvoeringskader besproken. Hun commentaar is verwerkt en nogmaals besproken.

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van compliancy van de informatievoorziening.

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

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

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

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[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
Als de criteria zijn beoordeeld als “niet van toepassing” dan zijn er geen criteria benoemd of de criteria zijn niet van toepassing gebleken voor de applicatie.

Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan minder dan 35% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan minder dan 35% van de beleidscriteria wordt voldaan.

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan ten minste 35% maar minder dan 100% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria, en aan niet alle van de beleidscriteria wordt voldaan.
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria en aan alle beleidscriteria wordt voldaan
b: aan alle wettelijke criteria wordt voldaan en de beleidscriteria zijn niet van toepassing
c: de wettelijke criteria zijn niet van toepassing, en aan alle beleidscriteria wordt voldaan

NVT : Een volwassenheidsniveau NVT moet worden toegekend, indien de volgende voorwaarde van toepassing is:

a: de wettelijke criteria en de beleidscriteria zijn niet van toepassing

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

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

Weegfactor	Licht (L)	Middel (M)	Zwaar (Z)
Aantal	1	3	5

Aandachtspunten
1: Volwassenheidsniveau 1:

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

2: Beleidscriteria:

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

3: Privacy functionaris:

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

Disclaimer

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

Bijlage 1: Uitgangspunt bij compliance

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

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