0-meting Privacy & Security by Design

Summ-IT

10.2.e

Definitief

Versie 1.00

Versie datum 11 april 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	21-9-2018	Reviewen
0.9	26-9-2018	Aanpassingen verwerkt
0.92	10-04-2019	Aanpassingen overheids- en ketenstandaarden verwerkt
0.94	11-04-2019	Tekstuele aanpassing verwerkt
1.00	11-04-2019	Definitief rapport na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	21-9-2018	10.2.e	Gegevensautoriteit
0.9	26-9-2018	10.2.e	Gegevensautoriteit
0.91-0.94	26-3-2019	10.2.e	Functioneel Beheer

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 Summ-IT. 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 Summ-IT

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 Summ-IT	10.2.e	Dienstenmanager Summ-IT
	10.2.e	Business expert Summ-IT
	10.2.e	Coördinerend business expert
	10.2.e	Functioneel beheerder
	10.2.e	Requirements analist
	10.2.e	IV-expert
	10.2.e	Applicatie beheerder

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

Gespreksdatum	Nummer meting	Toelichting
28-3-2018	2018032801	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Summ-IT

Omschrijving applicatie

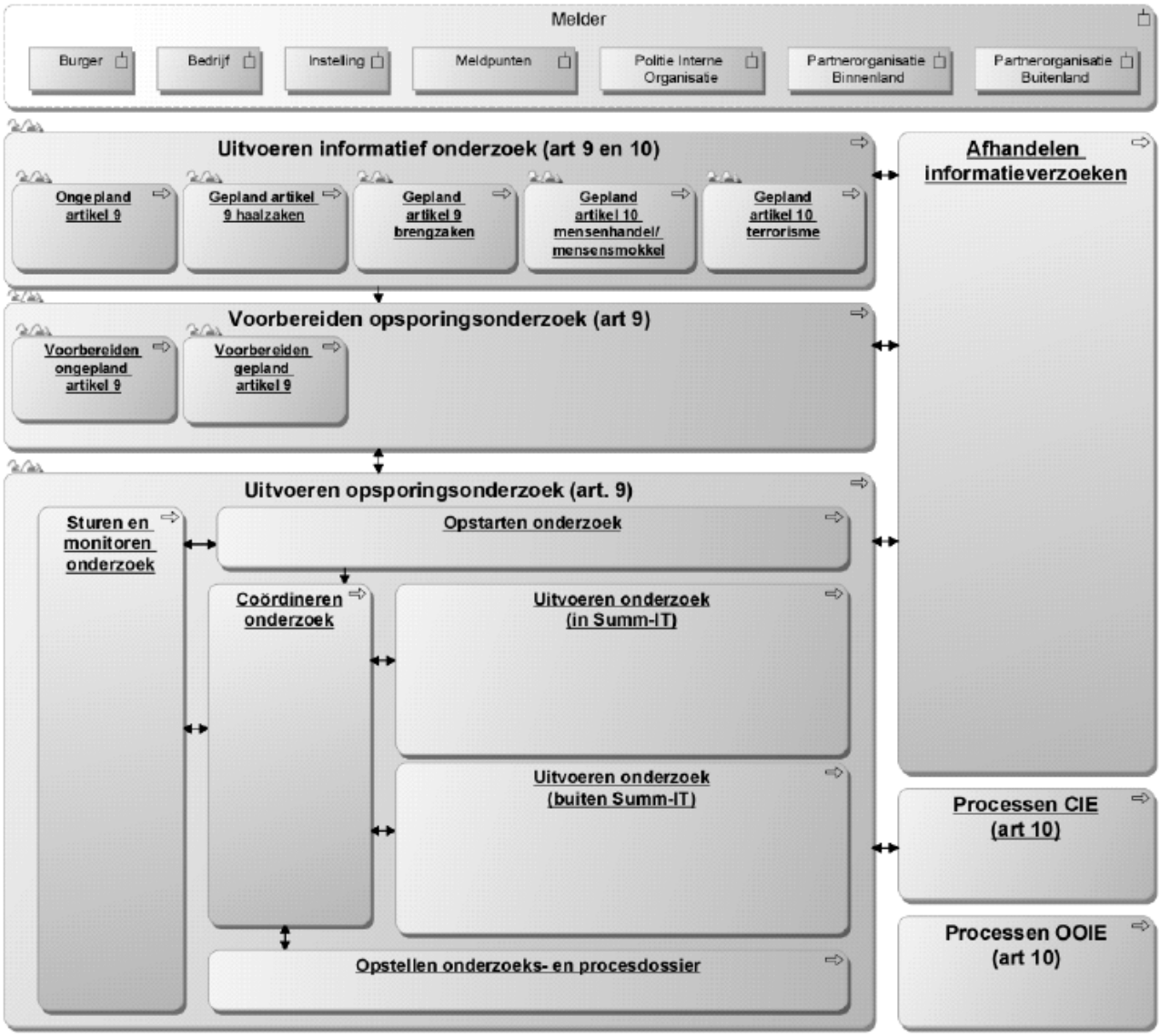
Summ-IT is hèt landelijke opsporingssysteem voor de gehele recherche en intelligence. Het ondersteunt het werkproces van een recherche-onderzoek. Alle opsporingsproducten (zoals formulieren) zijn in Summ-IT opgenomen. Het onderzoeks- en procesdossier wordt in Summ-IT gemaakt, ook in digitale vorm.
Summ-IT is gekoppeld aan BVH en daardoor ook BOSZ. Elke Summ-IT registratie is via de BVI verbonden met één of meerdere registraties in BVH. Het inzenden van de onderzoeksdossiers naar het OM loopt via BVH en BOSZ. Het samengestelde dossier (geprint danwel in HTML/PDF) wordt aangeleverd vanuit Summ-IT en gaat niet via BVH.
Er wordt binnen SUMM-IT alleen gewerkt met artikel 8 (voor O&T), 9, 10 en 13 WPG. Alle opsporingsdiensten (Rijksrecherche, KMAR en BOD-en (NVWA, FIOD, ISZW, en ILT))) werken met werken met en in Summ-IT van de NP, eigen opsporingsdiensten werken ookmet een eigen versie (NVWA en FIOD worden door NP gehost). Dus de KMar (Koninklijke Marechaussee) en BOD (Bijzondere opsporingsdiensten) hebben een 'eigen' Summ-IT. Het idee is om een entiteit één enkele keer in het systeem op te slaan. Er wordt van alles samen opgeslagen waardoor alles (digitaal) naar het OM kan. Het is puur een registratief systeem (met Zoeken en Speuren functionaliteit)waarbij alle informatie op een enkele plek moet samenkomen. Er is een upload mogelijkheid van BVH naar Summ-IT, omgekeerd nog niet. Er is één database voor Summ-IT en twee opsporingsdiensten hebben hun eigen database, maar hosten die bij de politie (NVWA en FIOD). De diensten sluiten nog niet perfect op elkaar aan op het gebied van coderingen en dergelijke. Er zijn geen koppelingen tussen de databases van de diensten, maar het is wel mogelijk om gegevens over te hevelen. Ook komt het voor dat autorisatie wordt verleend aan specifieke medewerkers van andere diensten voor een specifiek onderzoek in de database van politie zodat samengewerkt kan worden tussen de diensten. Mocht er informatie nodig zijn dan is er de mogelijkheid om gegevens over te hevelen.

10.2.c

Ook bijzondere werkprocessen zoals voor vermiste personen, opsporing ontsnapte gevangenen, dienst bewaken en beveiligen en dergerlijke worden door Summ-IT ondersteunt.

Overzicht processen Summ-IT

Versie 1.02
26-4-2013



Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	
Vernietigen	X	Er blijven metagegevens over voor logging en archivering, maar vernietigd is echt vernietigd.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	(X)	Er kunnen art. 8 gegevens in worden opgenomen voor O&T.
Onderzoek rechtsorde bepaald geval	Artikel 9	X	
Informatiepositie	Artikel 10	X	Met splitsing art. 10 lid 1 onder: a: Criminele Inlichtingen b:Mensen- handel -smokkel; terrorisme c:Openbare Orde Inlichtingen
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

Summ-IT scoort een volwassenheidsniveau 1. Dit houdt in dat Summ-IT onvoldoende compliant is op het gebied van Privacy & Security by Design (PSbD). Er is wel specifiek aandacht op het gebied van PSbD, maar die is vooralsnog niet toereikend om te voldoen aan de wet (Wpg) en aan het politiebeleid. Op de wetscriteria heeft Summ-IT een score van 50% en op de criteria van het politiebeleid een score van 67%. Vooral op de principes eenmalige vastlegging, metagegevens, bewaren en vernietigen en informatiebeveiliging is direct verbetering nodig. Al deze principes hebben een zware onvoldoende, maar hebben daarnaast ook zware weegfactor op het gebied van PSbD. Ons advies is eerst te kijken naar de wetscriteria en daarna pas naar mogelijke verbeteringen op het politiebeleid. Indien het niet mogelijk is te voldoen aan alle wetscriteria moet goed worden onderbouwd waarom ervoor wordt gekozen om niet aan een bepaald criterium te voldoen. Er moet dan een weloverwogen besluit worden genomen.

Advies (hieronder staan de wettelijke actiepunten opgesomd, de beleidspunten blijken uit het document):

- **(Wet artikel 4 lid 1): Zorg dat gegevens van een kernobject in de betreffende basisregistratie worden geverifieerd (zolang er nog geen kernregister is) [p1c3]**
- **(Wet artikel 4 lid 1): Zorg dat onjuistheden in de gegevens van een kernobject niet alleen handmatig aan de betreffende register worden terug gemeld, maar ook via de voorziening voor alle kernobjecten. [p1c5]**
- **(Wet artikel 4 lid 1): Zorg dat Summ-IT een terug gemeld mogelijkheid bouwt, zodat de uitvoeringsverantwoordelijke ondersteunt wordt bij het terug melden van een gegeven indien er gerede twijfel over een gegeven bestaat. [p1c6]**
- **(Wet art 32): Neem de datum einde van de verwerkingstermijn op in het gegevensmodel, of zorg er in ieder geval voor dat het voor elk gegeven duidelijk is onder welke verjaringstermijn die valt. [p3c8]**
- **(Beleid --> Wet vanaf januari 2019): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden (bijvoorbeeld naar andere data-analyseomgevingen) [p3c11]*1**
- **(Beleid --> Wet vanaf januari 2019) Zorg dat het gebruik van de functionaliteit om de herkomst en wijze van verkrijging (verplicht) vast te leggen ook voor artikel 9 afgedwongen zal worden. [p6c7]*1**
- **(Wet artikel 8, 9,10,12 en 14 wpg): Zorg dat Summ-IT voldoet aan de wettelijke bepalingen m.b.t. het bewaren, vernietigen en archiveren van gegevens [p8c2]**
- **(Wet archiefwet) Summ-IT moet gegevens voorzien ten behoeve van het bewaren en vernietigen van gegevens [p8c3]**
    - **Controleer ook het papierenarchief**
- **(Wet artikel 14 lid 4): Summ-IT moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens. [p8c9]**
- **(Wet artikel 8, 9 en 10): Zorg voor een poortwachtersfunctie voor Summ-IT. Er is een landelijk werkproces voor Summ-IT, met daarin de poortwachter, in ontwikkeling. [p8c10]**
- **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risicoanalyse. [p9c2]**
- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**

Aandachtspunten:

- Vanuit het productiehuis wil men 10.2.c volledige rechten geven (dus ook op de database). Dit vergt extra risico en dient meegenomen te worden in de overweging mbt de beveiliging van het manipuleren van de audittrail. Zorg dat er een weloverwogen besluit genomen gaat worden om de risico's uit te sluiten of in het uiterste geval te beperken. [p4]
- Zorg dat er meer aandacht gegeven gaat worden aan het proces omtrent het toekennen van autorisaties doormiddel van ATL. Hiervoor is reeds een voorstel ingediend. [p5]
- Er zijn nog diverse knelpunten waardoor het verwerken van afloopberichten belemmerd wordt. De kwaliteit van afloopberichten is bijvoorbeeld nog onvoldoende. Dit heeft ook invloed op het kunnen matchen van afloopberichten op de betreffende onderzoeken. Daarnaast is nog niet duidelijk hoe de opvolging van een vertrokken bevoegd functionaris bij een onderzoeksdossier geregeld moet worden.[p8]
- Naast de principes en criteria van Privacy & Security by Design is er ook aandacht nodig om de strafrechtketen gesloten te krijgen. Dat betekent dat alle beslissingen van het OM en de rechter over de ingezonden onderzoeksdossiers verstrekt moeten worden aan politie. [p12]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
SUMM-IT	28-3-2018	1.0	50%	67%	1

***1LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar dit is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).**

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	17%	75%	0
PDCA-cyclus	M	-	NVT	88%	2
Doelbinding	Z	-	75%	86%	1
Verantwoording	Z	-	100%	75%	2
Autorisatie	Z	-	100%	83%	2
Metagegevens	Z	-	NVT	56%	2
Kwaliteitszorg	Z	-	NVT	78%	2
Bewaren en vernietigen	Z	-	40%	13%	1
Informatiebeveiliging	Z	-	0%	40%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	86%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	50%	67%	

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.

Summ-IT scoort een onvoldoende op het principe eenmalige vastlegging. Er worden geen gegevens van een kernobject geverifieerd. Er zijn heel veel dubbelingen (initieel 1,3 miljoen wat op 28/03/2018 al is teruggebracht tot 800.000). Op dit moment moet er handmatig gekeken en gecontroleerd worden of personen dubbel zijn. Op de planning staat om in de toekomst een koppeling te initiëren met de personenserver (ter verificatie). Daarnaast zit er geen terug meld mogelijkheid in Summ-IT. Hierdoor kunnen onjuistheden alleen handmatig worden terug gemeld en is er geen mogelijkheid om melding via Summ-IT te maken van een gegeven waar gerede twijfel over bestaat.

Actiepunten:

- **(Wet artikel 4 lid 1): Zorg dat gegevens van een kernobject in de betreffende basisregistratie worden geverifieerd (zolang er nog geen kernregister is) [p1c3]**
- **(Wet artikel 4 lid 1): Zorg dat onjuistheden in de gegevens van een kernobject niet alleen handmatig aan de betreffende register worden terug gemeld, maar ook via de voorziening voor alle kernobjecten. [p1c5]**
- **(Wet artikel 4 lid 1): Zorg dat Summ-IT een terug gemeld mogelijkheid bouwt, zodat de uitvoeringsverantwoordelijke ondersteunt wordt bij het terug melden van een gegeven indien er gerede twijfel over een gegeven bestaat. [p1c6]**
- (Beleid): Zorg dat gegevens uit Summ-IT daar waar mogelijk ter beschikking kunnen worden gesteld via een gegevens diensten laag (los van gegevensverwerkingsdiensten) [p1c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	17%	75%	0

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.

Summ-IT werkt grotendeels op basis van de cyclische terugkoppeling. Als blijkt dat registraties niet volledig zijn wordt dat gemeld en wordt er een actie opgezet. Er wordt een rapportage gemaakt van incomplete registraties en op basis daarvan wordt er één keer per maand een overleg gevoerd. Daarnaast wordt er gebruik gemaakt van Cognos rapportages om te sturen op de geregistreerde gegevens. Wat nog niet goed geregeld is de evaluatie na een proces van verandering. Daarnaast is het beheer van een gegeven gedurende de gehele levenscyclus niet overal uitgerold.

Actiepunten:

- (Beleid): Zorg dat het beheer van gegevens en processen onderdeel uitmaakt van de PDCA cyclus. [p2c2]
  - Evalueer na een verandering in het proces
  - Beheer een gegeven gedurende de gehele levenscyclus

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.

Summ-IT verwerkt bij elk onderzoek de grondslag als metagegeven. Daarmee voldoet Summ-IT aan één van de belangrijkste onderdelen van doelbinding. Indien er sprake is van een artikel 13-verwerkering dan kan een teamleider Artikel 13 lid 1 of lid 2 registratie aanvragen waarbij er aangegeven moet worden (in doelomschrijving) onder welk thema dit moet vallen. Voor verwerking van artikel 13 lid is het noodzakelijk dat er een protocol wordt opgemaakt wat in afstemming is met de teamleider en de privacyfunctionaris van de betreffende eenheid.

Zoals eerder is aangegeven doet Summ-IT verwerkingen onder artikel 13 en hierin is in het werkproces de datum einde verwerkingstermijn opgenomen. Echter de datum einde verwerking is niet opgenomen in het gegevensmodel. Het is belangrijk om duidelijk te maken welke verjaringstermijn bij welk gegeven hoort. Daarnaast is het van belang om ervoor te zorgen dat de metagegevens over verwerkingsgrondslagen het gegeven blijven begeleiden, zodat ook daar deze gegevens getoond of verwijderd kunnen worden (op basis van metagegevens).

Actiepunten:

- **(Wet art 32): Neem de datum einde van de verwerkingstermijn op in het gegevensmodel, of zorg er in ieder geval voor dat het voor elk gegeven duidelijk is onder welke verjaringstermijn die valt. [p3c8]**
- **(Beleid --> Wet vanaf januari 2019): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden (bijvoorbeeld naar andere data-analyseomgevingen) [p3c11]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	75%	86%	1

1.4 Verantwoording

"De politie moet verantwoording kunnen afleggen over zijn taakuitvoering en over de gegevensverwerking die daarbij plaatsvindt."

De politie moet over zijn taakuitvoering verantwoording kunnen afleggen. Dit is vooral van belang voor gegevensverwerking in strafzaken en de inzet van opsporings- en geweldsbevoegdheden maar geldt ook voor de bedrijfsvoering in brede zin. De informatievoorziening moet het daarom mogelijk maken dat de politie verantwoording aflegt over handelingen en de totstandkoming van besluiten. De verantwoording ten aanzien van gegevensverwerking vormt het sluitstuk van de besturing van de informatievoorziening. De verantwoording zorgt tevens dat invulling gegeven kan worden aan de rechten van betrokkenen wiens persoonsgegevens verwerkt worden.

Binnen Summ-IT is de audittrail nog niet optimaal beveiligd tegen manipulatie. Binnen de applicatie kunnen de gebruikers de audittrail niet manipuleren. 10.2.g

Actiepunten:

- (Beleid): 10.2.g . Indien dit niet mogelijk is zorg dat het risico geminimaliseerd en geaccepteerd is. [p4c3]

Aandachtspunt:

- Vanuit het productiehuis willen men 10.2.c volledige rechten geven (dus ook op de database). Dit vergt extra risico en dient meegenomen te worden in de overweging mbt de beveiliging van het manipuleren van de audittrail. [p4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	75%	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.

Summ-IT maakt nog geen geautomatiseerd gebruik[3] van de generieke IAM-voorziening van de politie. Het staat wel op de planning om het in het najaar 2018 op te pakken. Echter de moeilijkheidsgraad ligt in de aanvullende opleiding die nog niet in de rollen voorkomt.

Er wordt geen goed gebruik gemaakt van de autorisatietool voor leidinggevenden (ATL). Er zijn teamchefs die tegen het autorisatiemodel in gaan. Het is heel moeilijk te controleren door functioneel beheer. De ATL kan mensen een autorisaties geven die niet passen bij het autorisatiemodel van Summ-IT. Als oplossing is het vierogen principe geopperd.

Voor de rest voldoet Summ-IT aan de autorisatie-eisen door onder meer een maandelijkse toegang en gebruikersrechten controle. Gebruikers worden geïnstrueerd m.b.t. de voor hen geldende autorisatieregels.

Actiepunten:

- (Beleid): Zorg dat BVI-IB gebruik maakt van de generieke IAM-voorziening voor het verifiëren van identiteiten.[p5c1]

Aandachtspunt:

- Zorg dat er meer aandacht gegeven gaat worden aan het proces omtrent het toekennen van autorisaties doormiddel van ATL. Hiervoor is reeds een voorstel ingediend. [p5]

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

[3] (De-)Autorisaties komen wel vanuit IAM. Via een SD-ticket.

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.

Bij het ontwerp van Summ-IT is geen gebruik gemaakt van vastgestelde definities voor bedrijfsbegrippen. Er is een verzameling van begrippen, maar nog geen thesaurus van recherchebegrippen wat er wel zou moeten zijn (op dit moment is het erg gefragmenteerd).

Op dit moment maakt BVI-IB geen gebruik van het toepassingsprofiel Metagegevens Rijk (in afwachting van het toepassingsprofiel Metagegevens politie). Bij Summ-IT worden geen metagegevens gebruikt voor audittrails en managementrapportages. Metagegevens die daarvoor in aanmerking komen worden niet geautomatiseerd afgeleid, maar ook niet op andere manieren ingevuld.

De herkomst en wijze van verkrijging zijn kenmerken waaraan binnen Summ-IT nog onvoldoende aan wordt voldaan. Dit komt omdat er veel gebruik wordt gemaakt van open tekstvelden, waardoor het dus niet altijd volledig is. Het is wel mogelijk, maar op dit moment wordt het niet afgedwongen voor artikel 9. Bij artikel 10 is dit niet van toepassing.

Actiepunten:

- (Beleid): Zorg dat er binnen Summ-IT gebruik gemaakt gaat worden van één vastgestelde lijst van definities voor bedrijfsbegrippen. Dit zou afgestemd moeten worden met het GGB [p6c1]
- (Beleid): Kijk naar de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is [p6c4].
- **(Beleid --> Wet vanaf januari 2019) Zorg dat het gebruik van de functionaliteit om de herkomst en wijze van verkrijging (verplicht) vast te leggen ook voor artikel 9 afgedwongen zal worden. [p6c7]**
- (Beleid): Zorg dat metagegevens die daarvoor in aanmerking komen geautomatiseerd afgeleid en vastgelegd worden.[p6c8]
- (Beleid): Zorg dat Summ-IT gebruik maakt van metagegevens voor het gebruik van audittrails en managementrapportages [p6c10].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	56%	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.

Summ-IT voldoet bijna volledig aan het principe kwaliteitszorg. Er is alleen op dit moment geen budget/capaciteit om alle kwaliteitseisen te realiseren. Daarnaast is het op dit moment alleen mogelijk om een rapport over de kwaliteit van gegevens op aanvraag (ad-hoc) op te vragen. Dit zou periodiek geregeld moeten worden, waarbij het van belang is om de resultaten van de uitgevoerde kwaliteitscontroles te bewaren.

Actiepunten:

- (Beleid): Zorg dat de kwaliteitseisen gerealiseerd worden. [p7c3]
- (Beleid): Zorg dat uitgevoerde kwaliteitscontroles periodiek gebeuren en dat het resultaat daarvan bewaard blijft. [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	78%	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.

Op dit moment voldoet Summ-IT niet op het gebied van bewaren en vernietigen. Er is een papierenarchief waar niet gecontroleerd wordt op bewaren en vernietigen. De onherroepelijke beslissingen van het OM en de rechter worden in de vorm van afloopberichten naar een centrale mailbox van elke eenheid verstuurd. De bewaartermijnen van de politiegegevens met verwerkingsgrondslag 9 zijn daar van afhankelijk. De kwaliteit van de afloopberichten is nog onvoldoende. Daarnaast is er nog geen automatische verwerking. Hieronder een overzicht van de actiepunten die verbeterd moeten worden om te voldoen aan het principe 'Bewaren en vernietigen'.

Actiepunten:

- **(Wet artikel 8, 9,10,12 en 14 wpg): Zorg dat Summ-IT voldoet aan de wettelijke bepalingen m.b.t. het bewaren, vernietigen en archiveren van gegevens [p8c2]**
- **(Wet archiefwet) Summ-IT moet gegevens voorzien van een waardering en selectie ten behoeve van het bewaren en vernietigen van gegevens [p8c3]**
    - **Controleer ook het papierenarchief**
- (Beleid) Zorg dat de artikel 9 gegevens op basis van de geldende termijnen geautomatiseerd worden verwijderd en vernietigd. Dit betekent dat als persoon niet langer als verdachte mag worden gezien de rol verdachte automatisch verwijderd moet worden. Tevens moet de gehele verwerking automatisch verwijderd worden na ontvangst van een afloopbericht met een onherroepelijke beslissing. [p8c4]
- (Beleid): Zorg dat de beslissingen uit de afloopberichten geautomatiseerd worden overgenomen [p8c6]
- (Beleid): Zorg dat de beslissing van het afloopbericht automatisch wordt verwerkt. [p8c7]
    - Bij een sepot of een veroordeling
- (Beleid): Zorg dat Summ-IT moet voldoet aan de kwaliteitseisen van DUTO. Hiervoor kan contact worden op genomen met het DIV [p8c8]
- **(Wet artikel 14 lid 4): Summ-IT moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens. [p8c9]**
- **(Wet artikel 8, 9 en 10): Zorg voor een poortwachtersfunctie voor Summ-IT. Er is een landelijk werkproces voor Summ-IT, met daarin de poortwachter, in ontwikkeling. [p8c10]**

Aandachtspunten:

- Er zijn nog diverse knelpunten waardoor het verwerken van afloopberichten belemmerd wordt. De kwaliteit van afloopberichten is nog onvoldoende. Dit heeft ook invloed op het kunnen matchen van afloopberichten op de betreffende onderzoeken. Daarnaast is nog niet duidelijk hoe de opvolging van een vertrokken bevoegd functionaris bij een onderzoek geregeld moet worden.[p8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	40%	13%	1

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.

Summ-IT heeft recent geen risico analyse uitgevoerd. De laatste risicoanalyse was in 2012 op technisch vlak (infrastructuur). Het is belangrijk om regelmatig de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen al kan zijn achterhaald. Het advies hier luidt om een risico analyse uit te laten voeren. Naar aanleiding van de resultaten uit de analyse moet worden gekeken welke informatiebeveiligingseisen moeten worden genomen en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Daar waar mogelijk moet er gebruik worden gemaakt van de standaard informatiebeveiligingsdiensten. Als er risico's overblijven die niet kunnen worden weggenomen dan moeten deze restrisico's in beeld zijn en in beheer zijn.

Actiepunten:

- (Beleid): Zorg dat er een nieuwe risicoanalyse voor de verwerkingen uitgevoerd worden. [p9c1]
    - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse. [p9c2]**
    - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**
    - (Beleid): Gebruik waar mogelijk de standaard informatiebeveiligingsdiensten. Als dat niet mogelijk is neem dan passende maatregelen. [p9c6]
    - (Beleid): Zorg dat de restrisco's periodiek beheert worden. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	40%	0

1.10 Voldoen aan de wet

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

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

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

1.11 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.

Summ-IT is extern ontwikkeld en later door de politie in gebruik genomen. Het is op dit moment onduidelijk in hoeverre Summ-IT gebruik maakt van bestaande overheids- en ketenstandaarden. Dat is ook meteen de reden dat Summ-IT hier heel laag op scoort.

Actiepunten:

- (Beleid): Onderzoek welke overheids- en ketenstandaarden van toepassing zijn op Summ-IT. [p11c1]
  - (Beleid): Voer toetsen uit op de toepasselijke standaarden. [p11c2]
  - (Beleid): In het geval van afwijkingen van standaarden moet er een motivatie zijn die is geaccepteerd door de verwerkingsverantwoordelijke (pas toe of leg uit) [p11c13]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	0%	0

1.12 Verantwoordelijkheden belegd

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

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

De verantwoordelijkheden zijn binnen Summ-IT voldoende belegd. Echter er zijn wel verbeteringen te maken met het verschil in kennis tussen de recherchechefs. Hier moet actief op gemonitord worden tijdens het SUO (Senior UsersOverleg). Daarnaast ondersteunt Summ-IT de uitvoeringsverantwoordelijke met het verwerken van de juiste classificaties en metagegevens voor informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. Echter de vraag is hoe de uitvoering is in de praktijk.

Actiepunten:

- (Beleid): Zorg dat de uitvoeringsverantwoordelijke voldoende bewust is wat zijn verantwoordelijkheden zijn
  - Rechherchechefs moeten actief gemonitord doormiddel van het SUO. [p12c3]
- (Beleid): Zorg dat niet alleen Summ-IT de uitvoeringsverantwoordelijke met het verwerken van de juiste classificaties en metagegevens voor informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid ondersteunt, maar ook dat het in de praktijk uitgevoerd wordt. [p12c4]

Aandachtspunten:

- Naast de principes en criteria van Privacy & Security by Design is er ook aandacht nodig om de strafrechtketen gesloten te krijgen. Dat betekent dat alle beslissingen van het OM en de rechter over de ingezonden onderzoeksdossiers verstrekt moeten worden aan politie. [p12]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	86%	2

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 compliance van de informatievoorziening.

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

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

- Niveau 0: Er is geen specifieke aandacht voor PSbD 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	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