0-meting Privacy & Security by Design

MEOS

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	03-05-2018	Eerste concept versie	
1.1	5-12-2018	Aanpassingen op basis van feedback betrokkenen	

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
1.0	3-05-2018	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 Programma Mobiel Werken en applicatie MEOS. 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 MEOS

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 MEOS	10.2.e	Beveiligingsarchitect
	10.2.e	Privacy Functionaris Midden-Nederland
	10.2.e	IV-coördinator mobiel werken
	10.2.e	Kwartiermaker / Programmamanager PH
	10.2.e	Dienstenmanager MEOS
	10.2.e	Release Train Manager Mobiel Werken (MW)
	10.2.e	Architect

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

Gespreksdatum	Nummer meting	Toelichting
18-04-2018	2018041801	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

MEOS

Omschrijving applicatie
MEOS (Mobiel Effectiever Op Straat) is een framework over andere functionaliteiten heen. Het koppelt allerlei applicaties en maakt dit toegankelijk via de telefoon. MEOS heeft zelf geen database. Op den duur is het idee dat MEOS over wordt genomen door OPP. BVIB, BVH en Tracopol zijn aangesloten.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	Tijdelijk, je bevraagt wel applicaties en je krijgt tijdelijk informatie op het toestel.
Vastleggen		Gebeurt in de back-end systemen.
Ordenen	X	
Bewaren		In principe in de back-end systemen, echter op de mobiele werkplek wordt het tijdelijk (10.2.c) opgeslagen. In geval van een technische verstoring 10.2.c
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)		
Wijzigen (het bestaande aanpassen)		
Opvragen	X	Back-end systemen, maar ook in registers
Raadplegen	X	
Gebruiken	X	
Vergelijken		In back-end systemen
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Alles gaat via de back-end naar externe partijen. Aangifte wordt digitaal opgestuurd naar de betrokkene.
Samenbrengen	X	Ja, bijvoorbeeld in één bon worden verschillende gegevens samengevoegd
Met elkaar in verband brengen	X	
Afscherming	X	Ook binnen de applicatie (transport is een aparte categorie).
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen		

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9		
Informatiepositie	Artikel 10		
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13		

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

MEOS heeft een volwassenheidsniveau 2 (voldoende) behaald op de 0-meting wat betekent dat ze Wpg-compliant zijn. Een kanttekening die bij de score moet worden gemaakt is dat bij de 0-meting MEOS als framework is getoetst en niet de applicaties die gebruik maken van MEOS. Meerdere criteria zijn daardoor niet van toepassing verklaard, omdat MEOS afhankelijk is van de back-end systemen. Aan deze criteria moet alsnog worden voldaan in de achterliggende systemen als de politie privacy compliant wil worden. Desondanks is het een goede score. De verbeterpunten van MEOS zitten vooral in het opleveren van periodieke rapportages. Het is belangrijk periodiek rapportages op te leveren. Als er regelmatig rapportages zijn kan de ontwikkeling van de applicatie goed in de gaten worden gehouden en indien dat nodig is, worden ingegrepen op bepaald niet gewenste ontwikkelingen. De invulling van de rapportages is nog in ontwikkeling, maar er wordt al wel aan gewerkt. Geadviseerd is om de verbeterpunten uit dit rapport mee te nemen in de ontwikkeling van de rapportages.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
MEOS	18-04-2018	V.1.0	100%	86%	2

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	NVT	75%	2
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	NVT	3
Autorisatie	Z	-	NVT	75%	2
Metagegevens	Z	-	NVT	100%	3
Kwaliteitszorg	Z	-	NVT	69%	2
Bewaren en vernietigen	Z	-	NVT	NVT	NVT
Informatiebeveiliging	Z	-	100%	100%	3
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	100%	3
Principe is niet actief		-			
TOTALEN TOETSING		-	100%	86%	

VOLWASSENHEID TOETSING 1 NIVEAU **2**

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.

MEOS heeft een maximale score op het principe eenmalige vastlegging gehaald. Een deel van de criteria was echter niet van toepassing, omdat MEOS hiervoor afhankelijk is van de back-end systemen waar MEOS aan is gekoppeld. De criteria die wel van toepassing waren is aan voldaan. Er wordt namelijk gebruik gemaakt van de tabellen van GGB en de kernobjecten worden in de betreffende basisregistratie geverifieerd. Ook is het mogelijk om onjuistheden aan de bronhouder terug te melden.

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

1.2 PDCA-cyclus

"*De werking van de informatievoorziening wordt bestuurd op basis van cyclische terugkoppeling*"

Om in de managementverantwoordelijkheid te kunnen voorzien is het belangrijk dat de informatievoorziening stuurinformatie levert zodat er zicht is op de gegevenskwaliteit van informatiebeveiliging. Het is aan de betreffende verantwoordelijke managers om keuze te maken op basis van de stuurinformatie.

MEOS behaalt een volwassenheidsniveau 2 (voldoende) voor het principe PDCA-cyclus. Het beheer van de gegevens, software en processen verloopt volgens de PDCA-cyclus. Op het moment zijn er wel rapporten voor stuurinformatie, maar de precieze invulling hiervan is nog in ontwerp. Dit is ook een actiepunt, want het is belangrijk dat er periodiek rapportages worden opgeleverd. De rapportages hoeven niet perse geautomatiseerd worden opgeleverd, maar periodiek is wel sterk aan te raden. Het voordeel hiervan is dat de ontwikkeling van een applicatie kan worden bijgehouden en dat op eventuele afwijkingen kan worden gestuurd. Op het moment zijn er wel dienstverlening rapportages, de rest is nog in ontwikkeling.

Tijdens de 0-meting kwam naar voren dat vanaf mei 2018 het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB) verplicht wordt. Dit geldt niet voor MEOS, aangezien de verwerkingen allemaal worden uitgevoerd door de achterliggende applicaties. Hierdoor moeten deze applicaties bij een nieuwe verwerking vaststellen of een GEB moet worden uitgevoerd en dit ook doen. Dit verandert op het moment dat MEOS zelf apart verwerkingen uit gaat voeren die niet vanuit een back-end systeem komen.

Actiepunt:

- (Beleid): ontwikkel de invulling van rapportages waardoor het mogelijk wordt regelmatig rapportages op te leveren. Door periodiek rapportages op te stellen kan de ontwikkeling van MEOS worden bijgehouden en eventueel worden gestuurd op niet-wenselijke ontwikkelingen. [p2c1]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	75%	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.

MEOS heeft de maximale score (100%) en volwassenheidsniveau 3 behaald op het principe doelbinding. De verwerkingsgrondslag is altijd artikel 8 Wpg, maar als het nodig is, kan de diender zelf de grondslag aanpassen. Hoewel het gewenst is de verwerkingsgrondslag automatisch te herleiden, moeten er ook mogelijkheden blijven om van deze automatische grondslagen af te wijken. Verder is MEOS voor veel zaken afhankelijk van de achterliggende applicaties.

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.

In zowel de back-end systemen als in MEOS zelf wordt een audittrail geregistreerd. In MEOS wordt gebruik gemaakt van Proco (proactief controleren). Hierin wordt elke controle geturfd. Doordat ook hier MEOS zeer afhankelijk is van de back-end systemen en verder geen invloed kan uitoefenen op de audittrails van die systemen, zijn veel criteria niet van toepassing. Daar waar het mogelijk was, voldoet MEOS aan de criteria. Hierdoor is een maximale score van 100% gehaald.

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

MEOS maakt gebruik van de IAM-voorziening voor het verifiëren van identiteiten. Daardoor worden de toegangs- en gebruiksrechten automatisch gecontroleerd. Ook bij dit principe spelen de back-end systemen een belangrijke rol. Voor een goede beveiliging moeten er zowel technische als organisatorische maatregelen worden genomen. Bij MEOS worden de organisatorische maatregelen genomen in de zin van een uitgebreide opleiding voor het gebruik. Er worden implementatiedagen en extra opleiding georganiseerd voor gebruikers. Het enige punt bij het principe autorisatie waar MEOS nog op kan verbeteren is het genereren van rapportages op het gebruik van autorisaties. Er is wel zicht op de aantallen, maar er worden geen rapportages gemaakt. Bij eerdere principes is het belang van periodieke rapportages al aangestipt en bij autorisaties geldt dit ook.

Actiepunt:

- (Beleid): Zorg dat er rapportages over het gebruik van autorisaties worden opgeleverd. [p5c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	NVT	75%	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.

Afhankelijk van de back-end systemen worden metagegevens geleverd. De back-end systemen zijn leidend en MEOS levert de gevraagde metagegevens mee. Daarnaast worden de handelingen in MEOS ook gelogd. Het gaat dan niet om een inhoudelijke logging, maar alleen om het feit dat een handeling is uitgevoerd.

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

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.

Het is belangrijk dat gebruikte gegevens van goede kwaliteit zijn. MEOS heeft enkele verbeterpunten op het principe kwaliteitszorg. Allereerst kan een afwijking van de gegevenskwaliteit niet handmatig worden aangepast. Via de functioneel beheerder kan er wel een tijdige oplossing worden geregeld. Ook hier is MEOS weer afhankelijk van de onderliggende systemen en de door hun gebruikte tabellen. Het kan immers voorkomen dat deze achterlopen op de werkelijkheid. Via de functioneel beheerder zou dit per situatie opgelost kunnen worden, maar nog niet structureel. Ook hier is nog verbetering mogelijk op het gebied van rapportages. Enkele zaken worden op het moment wel bekeken, maar echte rapportages die de ontwikkeling van de kwaliteit van MEOS in de gaten houden zijn er nog niet.

Actiepunten:

- (Beleid): het moet mogelijk worden de afwijkingen van gegevenskwaliteit handmatig aan te passen. [p7c4]
- (Beleid): ontwikkel de voorziening zo dat een rapport over de kwaliteit van gegevens kan worden samengesteld. [p7c7]
- (Beleid): voer kwaliteitscontroles uit en bewaar de resultaten. Op deze manier is het mogelijk bij te houden waar er kwaliteitsverbeteringen nodig zijn. [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	69%	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.

MEOS is een framework dat over andere applicaties heen ligt. Er worden geen gegevens bewaard. Het bewaren en vernietigen van de gegevens moet dan ook gebeuren in de achterliggende applicaties. MEOS maakt wel gebruik van een tijdelijke opslag. Op deze manier kan de gebruiker later verder gaan met de verwerking. 10.2.c

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.

MEOS heeft de maximale score op het principe informatiebeveiliging behaald. Het is belangrijk om regelmatig de informatiebeveiliging te laten controleren. In de snel veranderende wereld kan het betekenen dat de gebruikte informatiebeveiliging vandaag nog voldoende is, maar morgen achterhaald.

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

1.10 Voldoen aan de wet

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

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

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

1.11 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 van 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.

MEOS maakt gebruik van meerdere overheids- en ketenstandaarden, zoals NORA en ISO. Indien af moet worden geweken van de standaard, bijvoorbeeld omdat een oudere versie wordt gebruikt, wordt die afwijking voorzien van een motivatie. Het volwassenheidsniveau voor het principe toepassen standaarden is dan ook maximaal.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	100%	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

Bij MEOS zijn de verantwoordelijkheden duidelijk belegd, vandaar dat MEOS een volwassenheidsniveau van 3 behaald op dit principe. Voor het vaststellen van de definities, beleid, koers en strategie is MEOS afhankelijk van de back-end systemen.

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