0-meting Privacy & Security by Design

Digibon
&
Politie
Digibon
Backoffice

10.2.e

Definitief

Versie 1.0

Versie datum 3 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	01-10-2018	Reviewen
0.9	18-10-2018	Aanpassingen verwerkt
0.94	21-03-2019	Aanpassingen naar aanleiding van review verwerkt.
1.00	03-04-2019	Rapport definitief na wederzijds goedkeuren

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	01-10-2018	10.2.e	Gegevensautoriteit
0.9	18-10-2018	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 compliancy 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) compliancy van highrisk applicaties is onderdeel van het verbeterprogramma Wpg en IB.[2] Het PSbD uitvoeringskader staat aan de basis om de highrisk applicaties van de politie te laten voldoen aan het PSbD compliancy.

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

Dit document beschrijft het resultaat van de 0-meting welke is uitgevoerd bij applicatie Digibon en de backoffice voorziening Politie Digibon Backoffice (PDB). 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[3]. 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 applicaties.
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
[3] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

0-meting Digibon & PDB

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 v2.0 wat in april 2018 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 Digibon & PDB	10.2.e	Security Architect
	10.2.e	Functioneel beheer / Product owner
	10.2.e	Software ontwikkelaar
	10.2.e	Product 0wner

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

Gespreksdatum	Nummer meting	Toelichting
09-07-2018	2018070901	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

Digibon & Politie Digibon Backoffice (PDB)

Omschrijving applicatie
Het doel van de Politie Digibon Backoffice (PDB) is het registreren en verrijken van feit-gecodeerde zaken en deze overdragen aan het CJIB (Centraal Justitieel Incasso Bureau), dat verder zorg draagt voor de afwikkeling van de zaak. De feit-gecodeerde zaken betreffen alle misdrijven, overtredingen en Muldergedragingen zoals deze worden vastgesteld door de Commissie Feiten en Tarieven (CFT) van het Ministerie van Justitie en worden gepubliceerd in het Feitenboekje.

De feiten worden geconstateerd door de politie en door buitengewoon opsporingsambtenaren (BOA). De constatering kan gedaan worden op kenteken of door een staande houding. Er wordt dan een mini-proces verbaal opgemaakt dat ingevoerd wordt in Digibonapp (MEOS). De verdere verrijking kan plaatsvinden in de PDB, zoals bv het toevoegen van bijlagen, zodat er kwalitatief goed vervolgbare zaken ontstaan in de Keten.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	
Ordenen	X	
Bewaren	X	Browser in MEOS app bewaart nog niet verzonden registraties 9h. Verzonden na 72h.
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	Totdat verzonden is in de App. In PDB nog wel te wijzigen.
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken		Bijvoorbeeld: BSN vergelijken met behulp van MEOS onderdelen.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Wordt verstrekt vanuit Digibon aan PDB. En vanuit PDB naar CJIB. In MEOS kunnen gegevens (bijv. gba) uit registers gemaild worden. Bevat disclaimer.
Samenbrengen	X	Bijvoorbeeld entiteiten
Met elkaar in verband brengen	X	Bijvoorbeeld rollen en relaties leggen tussen entiteiten.
Afscherming	X	Bijvoorbeeld autorisatie
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Handmatig in PDB (geen vernietig functionaliteit)
Vernietigen	X	Na 9h/72h in MEOS app. In PDB wordt niets vernietigd. In Digibon 72h na verzenden naar PDB. En na succesvol verzenden nog 72h.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	Digibon & PDB
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

De applicatie Digibon en de backoffice voorziening PDB scoren samen een volwassenheidsniveau 1. Dit houdt in dat beiden onvoldoende compliant zijn 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 op basis van het politiebeleid. Op de wetscriteria scoren beiden 57% en op de criteria van het politiebeleid 55%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'bewaren en vernietigen', 'Autorisatie' en 'Éénmalige vastlegging' er negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Daarnaast zijn er een aantal aandachtspunten.

Advies: (De wettelijke actiepunten hier genoemd. Beleidspunten blijken uit het document)

- **(Wet, art 4 lid 1) Zorg dat bij gerede twijfel over een gegeven in Digibon of de PDB dit geautomatiseerd kan worden teruggemeld aan de bronhouder. Bijvoorbeeld de kleur van een voertuig. [p1c5]**
- **(Wet, art 4a) Zorg als er wijzigingen zijn in het autorisatiebeleid deze via Digibon aan de gebruiker getoond worden. [p5c6]**
- **(Wet, art 4a) Zorg dat de toegang- en gebruiksrechten van Digibon en PDB regelmatig worden gecontroleerd. [p5c8]**
- **(Wet, art 4a) Zorg dat in Digibon en PDB alle kenmerken van de te verwerken gegevens worden vastgelegd. De wettelijke grondslag wordt nu bijvoorbeeld niet vastgelegd. [p6c6]**
- **(Wet, art 14) Zorg dat de gegevens in de PDB maximaal 5 jaar na verwijderen vernietigd worden. [p8c1]**
- **(Wet, art 8) Zorg dat in de PDB voldaan wordt aan de wettelijke bepalingen met betrekking tot het bewaren, vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- **(Wet, archiefwet) Zorg dat in de PDB de verwerkte gegevens voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen. [p8c3]**
- **(Wet, art. 8) Zorg dat zodra er (handmatig) verwijderd is in de PDB de poortwachter nog toegang heeft tot de verwijderde gegevens. [p8c10]**

Aandachtspunten[4]:

- Digibon en PDB krijgen gegevens van RDW en de BRP via de BVI en de personenserver. Er is geen mogelijkheid om bij gerede twijfel over een gegeven dat afkomstig is van RDW of de BRP dit (geautomatiseerd) terug te melden via de BVI of de personenserver naar de bronhouders. Bijvoorbeeld de kleur van een voertuig. [p1c5]
- **(Wet, art 4c, art 33b) Zorg dat nieuwe ontwikkelingen getoetst worden doormiddel van een gegevensbeschermingseffectbeoordeling (GEB). De volgende ontwikkelingen worden nu al genoemd: progressief boetestelsel, recidive register, automatische detectie handheld bellen en bulk afhandeling foutparkeerders. [p2c4][p2c5]**
- De applicaties Digibon en PDB zijn onlosmakelijk met elkaar verbonden. Ze staan echter als aparte applicaties in LIPS en ieder heeft ook een eigen portefeuillehouder. Zorg ervoor dat de applicaties in LIPS zijn samengevoegd en te koppelen aan slechts één portefeuillehouder.
- Het serviceniveau van Digibon zorgt alleen voor ondersteuning gedurende kantooruren. Dat is ontoereikend voor een applicatie die 24/7 gebruikt wordt. Zorg ervoor dat het serviceniveau aangepast is aan de vereiste ondersteuning.
- De gegevens van Digibon van een niet verzonden registratie worden maximaal 9 uur op het device bewaard. Hierdoor kan een verbalisant een registratie later afronden en versturen. Daarnaast worden verzonden registraties maximaal 72 uur bewaard omdat het MEOS device niet altijd netwerkbereik heeft. Het is niet duidelijk waar deze termijnen op gebaseerd zijn. Het komt in de praktijk nog wel eens voor dat registraties verdwijnen. Zorg ervoor dat onderzocht is wat de optimale bewaartermijnen zijn en zorg dat deze gedocumenteerd worden. [p10]
- Vanuit de betrokkenen komt de behoefte naar voren om te onderzoeken of MQTT gebruikt kan worden voor een betrouwbaardere interface tussen Digibon en PDB. Daarnaast zijn er wellicht nog andere standaarden die de betrouwbaarheid kunnen verbeteren. [p11]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Digibon & PDB	09-07-2018	2.0	57%	55%	1

[4] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	83%	2
PDCA-cyclus	M	-	NVT	63%	2
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	25%	75%	0
Metagegevens	Z	-	0%	25%	0
Kwaliteitszorg	Z	-	NVT	56%	2
Bewaren en vernietigen	Z	-	20%	0%	0
Informatiebeveiliging	Z	-	100%	70%	2
Privacy by default	Z	-	100%	50%	2
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	100%	3
TOTALEN TOETSING		-	57%	55%	

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.
Voor de principes “Kwaliteitszorg”, “Toepassing standaarden” en “Verantwoordelijkheden belegd” zijn er geen wettelijke criteria benoemd. Deze worden daardoor standaard met “NVT” gewaardeerd. Voor alle andere resultaten geldt dat deze alleen “NVT” krijgen als alle betreffende criteria niet van toepassing zijn.

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.

De applicaties Digibon en PDB bereiken hier een volwassenheidsniveau 2. Dat houdt in dat er voldaan wordt aan alle criteria vanuit de wet. Er is slechts één actiepunt en één aandachtspunt:

Actiepunten:

- (Beleid) Zorg dat gegevens via een gegevensdienstenlaag vanuit de PDB beschikbaar worden gesteld aan de BVI. [p1c8]

Aandachtspunten:

- Digibon en PDB krijgen gegevens van RDW en de BRP via de BVI en de personenserver. Er is nu geen mogelijkheid om bij gerede twijfel over een gegeven dat afkomstig is van RDW of de BRP dit (geautomatiseerd) terug te melden via de BVI of de personenserver naar de bronhouders. Bijvoorbeeld de kleur van een voertuig. [p1c5]

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

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.

Voor dit principe is een volwassenheidsniveau 2 gemeten. Dat houdt in dat er nog niet volledig voldaan wordt aan (politie)beleid. Het betreft hier het nog niet goed besturen van de applicaties Digibon en PDB volgens het PDCA principe. Daarnaast is er een aandachtspunt met betrekking tot een GEB bij nieuwe ontwikkelingen.

Actiepunten:

- (Beleid) Onderzoek welke extra stuurinformatie ten behoeve van de PDCA cyclus van Digibon gewenst is en borg de realisatie daarvan. Daarnaast dienen er nog rapportages ontwikkeld te worden voor de PDB. [p2c1]
- (Beleid) Zorg dat de betreffende rapportages periodiek opgeleverd worden. [p2c2]
- (Beleid) Zorg dat het beheer van gegevens uit de PDB onderdeel wordt van de PDCA cyclus. [p2c3]
- (Beleid) Zorg dat het beheer van de processen gekanaliseerd wordt. Zowel intern als vanuit de keten. [p2c3]

Aandachtspunten:

- **(Wet, art 4c, art 33b) Zorg dat nieuwe ontwikkelingen getoetst worden doormiddel van een gegevensbeschermingseffectbeoordeling (GEB). De volgende ontwikkelingen worden nu al genoemd: progressief boetestelsel, recidive register, automatische detectie handheld bellen en bulk afhandeling foutparkeerders. [p2c4][p2c5]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	63%	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.

Er wordt hier voldaan aan alles eisen aangezien alle informatie automatisch onder Wpg artikel 8 valt.

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.

Er wordt hier een volwassenheidsniveau 2 behaald. Om te komen tot volwassenheidsniveau 3 moet alleen voorkomen worden dat een database administrator de audittrail kan wijzigen.

Actiepunten

- (Beleid) Zorg dat de audittrail van PDB door niemand gewijzigd kan worden. Ook niet door de database administrator. [p4c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	0%	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.

Voor Digibon en PDB is hier het laagst mogelijke volwassenheidsniveau gemeten. De knelpunten waardoor niet voldaan wordt aan de wet betreffen het informeren van gebruikers over wijzigingen in het autorisatiebeleid en regelmatige controle van de toegangs- en gebruiksrechten.

Actiepunten:

- **(Wet, art 4a) Zorg dat in Digibon wijzigingen in het autorisatiebeleid als berichten naar de gebruiker gestuurd kunnen worden. [p5c6]**
- (Beleid) Digibon en PDB moeten rapportages kunnen genereren op het gebruik van autorisaties. [p5c7]
- **(Wet art 4a) Zorg dat de toegang- en gebruiksrechten van Digibon en PDB regelmatig worden gecontroleerd. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	25%	75%	0

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.

Voor het principe metagegevens wordt is voor Digibon en PDB het laagst mogelijke volwassenheidsniveau gemeten. Er wordt niet aan de wet voldaan omdat nog niet alle kenmerken van de te verwerken gegevens vastgelegd worden. Daarnaast zijn er diverse actiepunten met betrekking tot beleid.

Actiepunten:

- (Beleid) Beoordeel of het Toepassingsprofiel Metagegevens Rijk (TMR) kan helpen bij het ontwikkelen van metagegevens.) Pas het Toepassingsprofiel Metagegevens Politie (TMP) toe zodra dit gereed is. [p6c4]
- (Beleid) Toets aan de hand van het Politie Gegevens Model (PGM) of de berichten nog aangepast moeten worden. [p6c5]
- **(Wet, art 4a) Zorg dat in Digibon en PDB alle kenmerken van de te verwerken gegevens worden vastgelegd. De wettelijke grondslag wordt nu bijvoorbeeld niet vastgelegd. [p6c6]**
- (Beleid) Zorg dat metagegevens die daarvoor in aanmerking komen geautomatiseerd worden afgeleid en vastgelegd. Bijvoorbeeld verwerkingsgrondslag, bewaartermijn en metagegevens op basis van TMR of TMP. [p6c7]
- (Beleid) Zorg dat metagegevens ook daadwerkelijk gebruikt worden voor het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. Bijvoorbeeld verwerkingsgrondslag, bewaartermijn en metagegevens op basis van TMR of TMP. [p6c9]
- (Beleid) Onderzoek of het meerwaarde biedt om naast afstemming van berichtenboeken metagegevens mee te leveren. Zowel intern als extern naar ketenpartners (CJIB). [p6c10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	0%	25%	0

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.

Voor dit principe is volwassenheidsniveau 2 gemeten omdat nog niet (volledig) voldaan wordt aan alle beleidscriteria. Het feit dat 40% van alle ingezonden zaken door Digibon/PDB naar het CJIB wordt afgewezen of geseponeerd geeft de urgentie aan voor kwaliteitszorg. Dat wordt in onderstaande actiepunten uitgedrukt.

Actiepunten:

(Beleid) Dring de uitval van zaken bij het CJIB terug. Op dit moment is er een uitval van 40% (inclusief sepots). Dit kan onder andere gedaan worden door samen met het CJIB de kwaliteitseisen aan de feitcodes te verbeteren. Deze worden vastgelegd in opties en variabelen per feitcode. [p7c3]

- (Beleid) Zorg dat de bedrijfsregels om de kwaliteit van de gegevens te meten, naast de opties en variabelen van de feitcodes, worden uitgebreid. [p7c5]
- (Beleid) Zorg dat alle bedrijfsregels om de kwaliteit van de gegevens te meten worden ingebouwd in Digibon en de PDB. [p7c6]
- (Beleid) Zorg dat er een rapport over de kwaliteit van de gegevens kan worden samengesteld en zorg dat deze bewaard wordt. [p7c7][p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[5]	56%	2

[5] Er zijn voor dit principe geen wettelijke criteria benoemd.

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.

Voor bewaren en vernietigen is het laagst mogelijke volwassenheidsniveau gemeten. Er wordt deels voldaan aan duurzame toegankelijkheid omdat de data uit de gesaneerde applicatie PSH-TM raadpleegbaar zijn gemaakt via een light variant. Voor de rest wordt aan geen enkel criterium voldaan omdat er nog geen aandacht is voor bewaartermijnen.

Actiepunten:

- **(Wet, art 14) Zorg dat de gegevens in de PDB maximaal 5 jaar na verwijderen vernietigd worden. [p8c1]**
- **(Wet, art 8) Zorg dat in de PDB voldaan wordt aan de wettelijke bepalingen met betrekking tot het bewaren, vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- **(Wet, archiefwet) Zorg dat in de PDB de verwerkte gegevens voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen. [p8c3]**
- (Beleid) Zorg dat in de PDB gegevens op basis van de geldende termijnen automatisch worden verwijderd en vernietigd. [p8c4]
- (Beleid) Onderzoek hoe afloopberichten in de PDB automatisch verwerkt kunnen worden en borg de maatregelen. Onderzoek daarbij ook of de verstrekking van afloopberichten conform de BJSG (Besluit Justitiële en Strafvorderlijke Gegevens) is. [p8c6] [p8c7]
- (Beleid) Toets of de nieuwe applicatie PSH-TM light voor het raadplegen van de oude verwerkingen voldoet aan de DUTO (Duurzame Toegankelijkheid) standaard. [p8c8]
- **(Wet, art. 8) Zorg dat zodra er (handmatig) verwijderd is in de PDB de poortwachter nog toegang heeft tot de verwijderde gegevens. [p8c10]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	20%	0%	0

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.

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.

Het principe informatiebeveiliging is voor Digibon en PDB vastgesteld op volwassenheidsniveau 2. Voor beide beleidsmatige actiepunten geldt dat onderzocht moet worden hoe nog beter voldaan kan worden aan de standaard.

Actiepunten:

- (Beleid) Onderzoek welke standaard beveiligingsdiensten gebruikt kunnen worden bij de PDB. Bijvoorbeeld Single Sign On, inloggen ketenpartners en encryptie. [p9c5]
- (Beleid) Onderzoek welke toegepaste maatregelen voor informatiebeveiliging die buiten de standaard vallen generiek gemaakt kunnen worden. [p9c6]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	100%	70%	2

1.10 Privacy by default

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

Voor dit principe is een volwassenheidsniveau 2 gemeten. Om te komen tot het hoogste volwassenheidsniveau dient onderzocht te worden of er Privacy Enhancement Technology (PET) hulpmiddelen toegepast kunnen worden. Daarnaast is er een aandachtspunt betreffende tijdelijke opslag van gegevens op het MEOS device.

Actiepunten:

- (Beleid) Onderzoek welke Privacy Enhancement Technology (PET) hulpmiddelen kunnen worden toegepast. Denk daarbij bijvoorbeeld aan versleuteling van de data in Digibon en anonimisering van de data in de testomgeving. [p10c4]

Aandachtspunten:

- (Beleid) De gegevens van Digibon van een niet verzonden registratie worden maximaal 9 uur op het device bewaard. Hierdoor kan een verbalisant een registratie later afronden en versturen. Daarnaast worden verzonden registraties maximaal 72 uur bewaard omdat het MEOS device niet altijd netwerkbereik heeft. Het is niet duidelijk waar deze termijnen op gebaseerd zijn. Het komt in de praktijk nog wel eens voor dat registraties verdwijnen. Zorg ervoor dat onderzocht is wat de optimale bewaartermijnen zijn en zorg dat deze gedocumenteerd worden. [p10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	50%	2

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.

Voor dit principe wordt voldaan aan de wet en aan (politie)beleid. Er is alleen een aandachtspunt voor de betrouwbaarheid van de interface.

Aandachtpunten:

- Vanuit de betrokkenen komt de behoefte naar voren om te onderzoeken of MQTT gebruikt kan worden voor een betrouwbaardere interface tussen Digibon en PDB. Daarnaast zijn er wellicht nog andere standaarden die de betrouwbaarheid kunnen verbeteren. [p11]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[6]	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

Digibon en PDB voldoen aan alle beleidscriteria. Er zijn voor dit principe geen criteria van uit de wet.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[7]	100%	3

[6] Er zijn voor dit principe geen wettelijke criteria benoemd.
[7] Er zijn voor dit principe geen wettelijke criteria benoemd.

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-26_Uitvoeringskader_Privacy en Security by Design_v2.0'. In deze versie is geen rekening gehouden met de bepalingen uit de AVG en de Europese richtlijn m.b.t. de Wpg. Vervolgens zijn er criteria toegevoegd of aangescherpt op basis van documenten waar in het uitvoeringskader naar wordt verwezen. Het resultaat is met de auteurs van het uitvoeringskader besproken. Hun commentaar is verwerkt en nogmaals besproken.

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van 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[8].

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.

[8] 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 één of alle wettelijke criteria voldoet.

2: Beleidscriteria:

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

3: Privacy functionaris:

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

Disclaimer

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

Bijlage 1: Uitgangspunt bij compliance

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

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