0-meting Privacy & Security by Design

Servicemodule

10.2.e

Definitief

Versie 1.0

Versie datum 11 april 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.8	11-9-2018	Opzet concept rapport	
0.9	19-9-2018	Aanpassingen n.a.v. review 10.2.	
0.91	18-12-2018	Aanpassingen n.a.v. feedback betrokkenen Servicemodule	
0.92	22-3-2019	Aanpassingen n.a.v. feedback betrokkenen Servicemodule	
1.00	11-4-2019	Rapport definitief na wederzijds goedkeuren	

Review commentaar

Versie	Wanneer	Wie	Afdeling
0.8	11-9-2018	10.2.e	Gegevensautoriteit
0.9	19-9-2018	10.2.e	Gegevensautoriteit
0.91	18-12-2018	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 de Servicemodule. 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 Servicemodule

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 Servicemodule	10.2.e	Adviseur Proces- en informatiemanagement
	10.2.e	Privacy functionaris
	10.2.e	IV expert
	10.2.e	Functioneel beheer

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

Gespreksdatum	Nummer meting	Toelichting
15-5-2018	2018051501	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Servicemodule

Omschrijving applicatie

De servicemodule is een applicatie voor de intake van klantverzoeken aan de Politie. Deze komen binnen via de telefoon, aan de balie, via www.politie.nl , via mail en via Social Media. Het Regionaal Service Center in iedere eenheid registreert de klantverzoeken in de servicemodule. Na triage en verder uitvraag worden de klantverzoeken vertaald naar 4 politieproducten: de melding, het terugbelverzoek, het informatieverzoek en de afspraak.
Later-meldingen en terugbelverzoeken worden na registratie vooralsnog via de mail doorgezet naar het basisteam.
De spoed- en de nu-meldingen gaan naar het Operationeel Centrum (meldkamer). Spoed-meldingen via de telefoon, nu-meldingen, na registratie in de Servicemodule, geautomatiseerd naar GMS. Van de spoed-meldingen wordt alleen de naam en het telefoonnummer geregistreerd(voor het geval de telefoonverbinding verbreekt), de nu- en later-meldingen worden volledig binnen de servicemodule geregistreerd. De verdeling spoed, nu en later is gerelateerd aan de reactietijden op de meldingen.
De informatieverzoeken en de afspraken worden met de persoonsgegevens van de verzoekers geregistreerd binnen de servicemodule. Over informatieverzoeken en het maken van afspraken is afgesproken dat deze binnen het RSC en dus de servicemodule worden opgepakt en afgehandeld.

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	Persoonskaart
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	Adhv het telefoonnummer wordt gekeken of de persoon al vaker heeft gebeld (belhistorie wordt meegegeven). De codes zijn niet geverifieerd en bedoeld voor eventuele koppeling met andere toepassingen. Niet om personen makkelijk terug te vinden.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Terugbelberichten gaan niet naar GMS. Die blijven binnen de servicemodule en worden daar door de OPCO-functie verdeeld. De medewerker wordt via de mail met de inhoud van het verzoek op de hoogte gesteld. Op termijn wordt dit een link. Alles gaat binnen de politie. Geen verstrekkingen naar externe partijen.
Samenbrengen	X	Belhistorie van de beller
Met elkaar in verband brengen	X	Telefoonnummer en alle belhistorie
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	Als een registratie 25 maanden niet wordt geactualiseerd, dan wordt de registratie na een maand vernietigd. Als er een zaak van wordt gemaakt wordt de informatie overgezet naar bronsystemen zoals BVH.

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		Het kan zijn dat personen die bellen een bepaalde melding krijgen. Bijvoorbeeld als ze in een bepaald aangewezen gebied wonen, vuurwapengevaarlijk zijn, precedenten, onderzoeksfocus van basisteams. Dit is niet meer dan een signaal uit BVH op basis van de locatiegegevens. Deze gegevens worden niet opgenomen in de de servicemodule. Daarmee vervalt o.i. deze verwerkingsgrondslag
Overige wetgeving	Wbp/AVG	X	Sommige vragen zijn puur informatief van aard (hoe laat zijn de winkels open, mag mijn caravan zo lang geparkeerd staan etc)

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

Servicemodule scoort een volwassenheidsniveau van 1. Dit houdt in dat de Servicemodule onvoldoende voldoet 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 heeft de Servicemodule een score van 58% en op de criteria van het politiebeleid een score van 60%. 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', 'informatiebeveiliging' en 'toepassen standaarden' er negatief uitspringen. Hieronder staan de wetscriteria.

Advies:

- **(Wet artikel 4a): Controleer op een periodieke basis de toegang- en gebruikersrechten van de servicemodule. [p5c8]**
  LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).
- **(Wet, art 8) Zorg dat in de Servicemodule voldaan wordt aan de wettelijke bepalingen met betrekking tot het bewaren, vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse op het gebied van informatiebeveiliging. [p9c2]**
- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**

Aandachtspunt:

- Tijdens de 0-meting is aangegeven dat een terugbelbericht en/of reguliere meldingen via de email verzonden wordt aan de desbetreffende politiemedewerker. Hier staan persoonsgegevens in die niet via de mail verstuurd zouden mogen worden. Er werd al aangegeven dat dit opgelost kan worden door in de mail alleen een hyperlink mee te geven met een verwijzing naar de applicatie. Zorg dat gegevens altijd binnen de applicatie blijven.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Servicemodule	16-4-2018 en 15-5-2018	1.0	58%	60%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	100%	3
PDCA-cyclus	M	-	NVT	75%	2
Doelbinding	Z	-	100%	50%	2
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	100%	60%	2
Metagegevens	Z	-	NVT	58%	2
Kwaliteitszorg	Z	-	NVT	92%	2
Bewaren en vernietigen	Z	-	50%	0%	1
Informatiebeveiliging	Z	-	0%	25%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	17%	0
Verantwoordelijkheden belegd	M	-	NVT	88%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	58%	60%	

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

Nieuwe regelgeving Wpg januari 2019 (buiten de 0-meting)
Vanaf januari 2019 is de nieuwe Wpg van toepassing. Enkele criteria die in deze 0-meting nog als beleid zijn aangemerkt worden vanaf dat moment wet. Daarnaast is het van belang om bij ontwikkeling vast te stellen over sprake is van een nieuwe verwerking. Indien dit het geval is dan dient er een GEB uitgevoerd te voeren.

1.1 Eenmalige vastlegging

"Gegevens worden eenmalig vastgelegd en meervoudig gebruikt"

Naast dat het efficiënter en goedkoper is om gegevens te hergebruiken dan om gegevens opnieuw aan te maken of te verkrijgen zal ook de kwaliteit van gegevens verbeterd worden. Meerdere administratieve registraties van hetzelfde gegeven kunnen zorgen voor onduidelijkheid of inconsistentie van informatie. Bij de inzet van gegevens zal eerst gekeken moeten worden of er een authentieke bron is of dat al gegevens van eenzelfde of aantoonbaar ten minste gelijkwaardige kwaliteit en nauwkeurigheid beschikbaar zijn. In de gevallen waarin de politie met andere partijen samenwerkt, wordt bezien of de benodigde gegevens binnen de operationele en/of bedrijfsvoering keten kunnen worden verkregen.

Voor het principe eenmalige vastlegging voldoet Servicemodule volledig aan zowel de wet als het politiebeleid (100%). De servicemodule gebruikt daar waar mogelijk gebruik van tabellen die vastgesteld zijn door de GGB. Gegevens die binnenkomen bij de servicemodule worden niet standaard geverifieerd, maar dat is vanuit de rol van de applicatie ook niet nodig. Het telefoonnummer is het belangrijkste object binnen de applicatie, waarmee indien nodig de desbetreffende persoon (in nodig) kan worden opgenomen en geverifieerd. Registratie gaat per naam en indien iemand belt met een telefoon van iemand anders dan is dat een aparte registratie (twee registraties van namen bij één telefoonnummer), maar zal dit wel gekoppeld worden aan de belhistorie (telefoonnummer).

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

1.2 PDCA-cyclus

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

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

Voor het principe PDCA-cyclus scoort de Servicemodule een volwassenheidsniveau van 2. Het is van belang dat er aandacht besteed gaat worden aan periodieke basis van rapportages t.b.v. de besturing van de gegevensverwerking. Daarnaast is tijdens de sessie aangegeven dat de beleidsverantwoordelijke meer regie zou moeten voor de Servicemodule.

Actiepunten:

- (Beleid): Zorg dat de beleidsverantwoordelijke regie op definities, beleid, koers en strategie worden vastgesteld voor de verwerking van gegevens. De regie moet meer terug naar de portefeuillehouder [p2c6]
- (Beleid): Zorg dat er binnen de Servicemodule op periodieke basis rapportages opgeleverd worden ten behoeve van de besturing van de gegevensverwerking. Het is van belang om bij de managementrapportages een paragraaf op te nemen over de gegevensverwerking, zodat indien nodig hierop bijgestuurd kan worden. Bijvoorbeeld voor het vaststellen van het verloop van aantallen [p2c7].

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.

Voor het principe "Doelbinding" scoort de Servicemodule een volwassenheidsniveau van 2. Op dit moment wordt de verwerkingsgrondslag van verwerkte gegevens niet in de Servicemodule opgenomen. Dit is een essentieel onderdeel om de doelbinding van een verwerkte gegeven vast te kunnen stellen. Het is dus van belang dat de verwerkingsgrondslag direct herleidt kan worden. Echter het is bij de servicemodule de vraag of bij elke melding/bericht het noodzakelijk is om persoonsgegevens te registreren indien er ook algemene vragen gesteld kunnen worden. Het is daarom van belang om in overeenstemming met de privacyfunctionaris een juiste balans te vinden tot het registeren van persoonsgegevens en het beantwoorden van algemene vragen.

Actiepunten:

- (Beleid): Zorg dat de verwerkingsgrondslag is opgenomen in het gegevensmodel van de Servicemodule en daarmee bij elke intakeproces duidelijk is. [p3c2]

Aandachtspunt:

- Stem af met de privacyfunctionaris in welk stadium er persoonsgegevens geregistreerd mogen worden (bijvoorbeeld voor de eerste vraag of na de eerste vraag afhankelijk van het soort vraag).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	100%	50%	2

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.

Voor het principe "Verantwoording" scoort de Servicemodule een volwassenheidsniveau van 2. Vanuit de Servicemodule kan er nog worden gekeken naar de mogelijkheid tot manipulatie van de audittrail. Er is een speciale audit functionaliteit die (tegen licentiekosten) aan kan worden gezet waarbij de acties van onder andere de database administrator kunnen worden geregistreerd. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten Het is van belang dat de beleidsverantwoordelijke van de Servicemodule bewust is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's). Daarnaast is het van belang dat er een rapport van de audittrail gegenereerd kan worden.

Actiepunten:

- (Beleid): Zorg dat de audittrail van de Servicemodule beveiligd is tegen manipulatie van gebruikers en beheerders [p4c3].
- (Beleid): Zorg dat het mogelijk moet zijn een rapportage van de audittrail te genereren [p4c4].

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 de Servicemodule is op het moment van meten een voldoende behaald op het gebied van autorisatie.
Echter er is vanuit de wet een verplicht onderdeel bij gekomen wat ervoor zorgt dat verbeteringen nodig zijn. Het is verplicht dat er regelmatig een controle is op de toegangs- en gebruiksrechten van de Servicemodule. Daarnaast is het van belang dat er een rapport gegenereerd kan worden op het gebied van autorisaties. Op dit moment is de toepassing zo opgezet dat een relatief kleine groep werkt aan de registratie van meldingen. Een vergelijkbaar kleine groep verdeelt de meldingen. Een forse groep maakt afspraken via de servicemodule. Daartoe moet een zeer grote groep geautoriseerd worden voor de servicemodule voor een relatief klein onderdeel. De combinatie functionaliteit en autorisatie verdient enig onderzoek en mogelijke verbetering.

Actiepunten:

- (Beleid): Zorg dat de Servicemodule rapporten genereert op het gebied van autorisaties [p5c7].
- **(Wet artikel 4a): Controleer op een periodieke basis de toegang- en gebruikersrechten van de servicemodule. [p5c8]**
  LETOP: 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).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	60%	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.

Het eerder benoemde ontbreken van de verwerkingsgrondslag en het niet gebruiken van enige vorm van metagegevens zorgen ervoor dat de juistheid en rechtmatigheid van het gebruik van de Servicemodule moeilijk is vast te stellen. Metagegevens die daarvoor in aanmerking zouden geautomatiseerd moeten kunnen worden afgeleid en vastgelegd. Binnen de Servicemodule is dat op dit moment niet mogelijk

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): Zorg dat de Servicemodule effectief gebruik gaat maken van het verwerken van metagegevens. Hieronder staan de kenmerken die van de verwerkte gegevens worden verwacht [p6c7]:
    - Identificatiekenmerken,
    - Wettelijke verwerkingsgrondslag
    - Kenmerken die noodzakelijk zijn voor het verwerken van gegevens binnen het politieproces en/of binnen de keten, voorbeelden zijn transactie/event, datum, status, vorm,
    - Kenmerken die noodzakelijk zijn voor het verwerken van gegevens in de keten,
    - De herkomst van de gegevens (verplicht voor art. 9 en 10-gegevens)
    - De wijze van verkrijging (verplicht voor art. 9 en 10-gegevens is dit verplicht),
    - Logginggegevens, zoals tijd en datum en wie met welke taak is ingelogd.
- (Beleid) Zorg dat metagegevens die daarvoor in aanmerking komen geautomatiseerd worden afgeleid en vastgelegd. [p6c8]
- (Beleid): Zorg dat de Servicemodule gebruik maakt van metagegevens voor bijvoorbeeld het verlenen van toegang, bewaartermijnen, audittrails of managementrapportages [p6c10].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	58%	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.

Bij het principe Kwaliteitszorg zijn er geen wettelijke criteria van toepassing. Op beleidscriteria scoort de Servicemodule 92%. Er is één punt van verbetering op het gebied van kwaliteitszorg. Afwijkingen van de gegevenskwaliteit worden op dit moment handmatig aangepast. Op dit moment wordt in deze situatie niet gekeken naar structurele aanpassingen om dit te verbeteren.

Actiepunten:

- (Beleid) Zorg dat er bij afwijkingen in de gegevenskwaliteit naast handmatig aanpassen ook gekeken wordt naar een structurele oplossing. [p7c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	92%	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 de Servicemodule niet op het gebied van bewaren en vernietigen. Het verwijderen gebeurt nu naar operationele behoefte na 25 maanden, maar voor het vernietigen van gegevens wordt hier niet aan voldaan. Er wordt op dit moment niet gekeken naar geldende termijnen om de gegevens geautomatiseerd te verwijderen en vernietigen.

Actiepunten:

- **(Wet, art 8) Zorg dat in de Servicemodule voldaan wordt aan de wettelijke bepalingen met betrekking tot het bewaren, vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- (Beleid): Zorg dat gegevens op basis van de geldende termijnen geautomatiseerd verwijderd en vernietigd worden [p8c4].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	50%	0%	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.

De Servicemodule heeft recent geen risico analyse uitgevoerd. 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. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's in beeld zijn en in beheer zijn.

Actiepunten:

- (Beleid): Er moet 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 op te volgen informatiebeveiligingseisen voor de voorziening. [p9c3]**
    - (Beleid): Maak indien mogelijk gebruik van de generieke voorzieningen voor informatiebeveiliging [p9c4].
    - (Beleid): Controleer periodiek de restrisico's . [p9c7]

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

De Servicemodule maakt vooral veel gebruik van open source en de rest is maatwerk. Het is op dit moment niet duidelijk in hoeverre er gebruik wordt gemaakt van bestaande overheids- en ketenstandaarden. Dat is ook meteen de reden dat de Servicemodule hier heel laag op scoort. Er is tijdens de 0-meting aangegeven dat het een bewuste keuze is om geen gebruik te maken van bestaande overheids- en keten standaarden. Hier dient een verklaring voor gegeven te worden.

Actiepunten:

- (Beleid): Zorg dat duidelijk is binnen de servicemodule in hoeverre er gebruik wordt gemaakt van bestaande overheids- en ketenstandaarden en indien dit niet van toepassing is, dan verklaren waarom deze keuze gemaakt is. [p11c1]
    - (Beleid): Voer indien mogelijk 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). [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	17%	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 Servicemodule voldoet bijna in zijn geheel aan het principe 'Verantwoordelijkheden belegd'. Echter de werking op technisch niveau (zoals het gebruikt moet worden zoals bedoeld) komt niet overeen met de werking in de praktijk. Meldingen kunnen door een operationeel coördinator afgeboekt worden zonder dat het in BVH is opgenomen (voorbeeld voor kwaliteitszorg [p7c4]). Hierdoor wordt niet alles BVH geregistreerd.

Actiepunten:

- (Beleid) Zorg dat er regelmatig afstemming (beleidsverantwoordelijke en uitvoering) plaatsvindt op basis van beleid, koers en strategie. [p12c2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	88%	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
- 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