0-meting Privacy & Security by Design

VROS
(Verwijzings-index Recherche Onderzoeken en Subjecten)

10.2.e

Definitief

Versie 1.00

Versie datum 26 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	16-11-2018	Review
0.9	16-11-2018	Aanpassingen verwerkt
0.91-0.94	19-04-2019	Diverse aanpassingen nav review. Vastgesteld dat VROS een Wpg artikel 13 lid 3 verwerking is. (geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon)
0.95	26-04-2019	Laatste tekstuele aanpassingen 10.2.e verwerkt.
1.00	26-04-2019	Rapport definitief gemaakt na wederzijds goedkeuren

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	16-11-2018	10.2.e	Gegevensautoriteit

Inhoudsopgave

Inleiding

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

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

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

Dit document beschrijft het resultaat van de 0-meting welke is uitgevoerd bij applicatie VROS. 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 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
[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 VROS

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 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 VROS	10.2.e	IV coördinator opsporing
	10.2.e	Functioneel beheer
	10.2.e	Privacy functionaris
	10.2.e	Privacy functionaris

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

Gespreksdatum	Nummer meting	Toelichting
04/10/2018	2018100401	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

VROS

Omschrijving applicatie
De VROS (Verwijzingsindex RechercheOnderzoek en Subjecten) applicatie geeft landelijk overzicht van lopende en afgesloten recherche-onderzoeken en betrokken entiteiten. Van elk recherche onderzoek dat langer dan vijf dagen duurt, moet een VROS melding worden gemaakt. Hiervoor wordt een zogenaamde Melding Recherche Onderzoek gemaakt. Entiteitsoorten die aan VROS aangeboden zijn: rechtspersonen, organisaties, locaties, vervoermiddel en telecom.

Door politie en partners aangeleverde (MRO)gegevens(entiteiten) uit Summ-IT worden wekelijks onderling en met de zogenoemde BlackBox(niet MRO entiteiten) gematched. Een treffer wordt aan beide onderzoekende teams (zonder specifieke vraag) gemeld. Indien één van de teams een afgeschermde status heeft, wordt de melding aan het team Inwinning van de betreffende eenheid gedaan. Binnen VROS worden 10.2.c

VROS heeft het servicelevel: Laag .

VROS is een Wpg artikel 13 lid 3 verwerking (geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon).

VROS staat al vijf jaar op de nominatie om uit te faseren. Er is geen technische kennis meer aanwezig en de documentatie is minimaal.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	x	
Vastleggen		
Ordenen	x	Onder andere CA code. MRO of ander subject. MOT,….
Bewaren	x	Black box en MRO entiteiten tot aan de matching.
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)		Nieuwe info, bijvoorbeeld CA codes of status onderzoek worden toegevoegd.
Wijzigen (het bestaande aanpassen)		
Opvragen	x	
Raadplegen	x	MRO entiteiten
Gebruiken	x	Automatisch ten opzichte van verzamelen
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	x	Ter beschikking stellen hits naar politie en BOD'en.
Samenbrengen	x	Bijvoorbeeld combinatie van 2 onderzoeken op dezelfde entiteit.
Met elkaar in verband brengen	x	Matching entiteiten. Hit-no-hit
Afscherming	x	Als entiteiten afgeschermd zijn in Summ-IT dan zorgt VROS voor doorafscherming.
Uitwissen (weghalen/verwijderen zonder vernietigen)	x	Volgt de bron. In VROS wordt Artikel 9 getoond, maar wanneer het valt onder artikel 14 dan staat het niet meer in VROS.
Vernietigen	x	

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8		
Onderzoek rechtsorde bepaald geval	Artikel 9		
Informatiepositie	Artikel 10		
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11		
Informanten	Artikel 12		10.2.c [redacted] Dit is geen artikel 12 verwerking in VROS.
Ondersteunende taken	Artikel 13	x	De verwerkingsgrondslag voor VROS s Wpg artikel 13 lid 3 (geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon)

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 11 (lid 1) Wpg: verwerking teneinde vast te stellen of er verbanden bestaan tussen politiegegevens die worden verwerkt op grond van artikel 8 of 9

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 VROS scoort een volwassenheidsniveau 1. Dit houdt in dat VROS 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 VROS een score van 64% en op de criteria van het politiebeleid een score van 46%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de 'autorisatie' en 'informatiebeveiliging' er erg negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Daarnaast zijn er een aantal aandachtspunten.

Binnen VROS worden belangrijke gegevens verwerkt over lopende en afgesloten recherche-onderzoeken en mede daarom staat het op de highrisk lijst. Echter het is een legacy applicatie waarvan de ontwikkeling al jaren stilstaat en er nagenoeg technische kennis meer beschikbaar is. Een kleine storing kan er toe leiden dat er wekenlang geen VROS meldingen zijn en dat recherche onderzoeken naar eenzelfde subject niet van elkaars bestaan weten. Er zal op korte termijn een beslissing moeten worden genomen hoe er op korte termijn verbetering of vervanging kan plaatsvinden.

Actiepunten:

- **(Wet, art 6) Zolang er nog geen aansluiting is op IAM draag er dan zorg voor dat VROS voor het verlenen van toegang gebruik maakt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- **(Wet, art 4a) Zorg dat de gebruikers van VROS geïnstrueerd zijn m.b.t. de voor hen geldende autorisatieregels. [p5c6]**
- **(Wet, art 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. [P5c8]**
- **(Wet art 4a lid 2) Zorg dat de informatiebeveiligingseisen mede bepaald worden op basis van de resultaten van de risicoanalyse. [p9c2]**
- **(Wet art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in VROS. [p9c3]**

Aandachtspunten[4]:

- Voor VROS is er nagenoeg of nauwelijks of moeilijk beschikbare technische kennis aanwezig, waardoor bij een kleine storing het systeem (onnodig lang) niet beschikbaar is. Zorg dat er gekeken wordt naar de mogelijkheden om dit te verbeteren.
- Het model instellingsprotocol voor VROS is al geruime tijd niet aangepast. In de eigenschappen van het document is zichtbaar dat de laatste aanpassing op 15 juni 2011 is geweest. [p3]
- Vanuit het bronsysteem Summ-IT is er geen koppeling met het RDW. Hierdoor worden voertuiggegevens niet geautomatiseerd geverifieerd en ontstaat mogelijk vervuiling in de data van VROS. [p2]
- VROS is afhankelijk van de bronsystemen voor de bewaartermijn. Fouten in de bron werken door in VROS. [p8c2]
- Er is geen test of acceptatie omgeving voor VROS. Dat betekent dat productiedata gebruikt wordt voor het testen van nieuwe versies of dat er vooraf niet getest wordt. Zorg voor een andere oplossing dan testen met productiedata. [p10]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
VROS	04/10/2018	2.0	64%	46%	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	-	NVT	NVT	NVT
PDCA-cyclus	M	-	NVT	25%	0
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	0%	60%	0
Metagegevens	Z	-	100%	40%	2
Kwaliteitszorg	Z	-	NVT	40%	1
Bewaren en vernietigen	Z	-	100%	NVT	3
Informatiebeveiliging	Z	-	0%	10%	0
Privacy by default	Z	-	100%	100%	3
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	67%	2
TOTALEN TOETSING		-	64%	46%	

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.
Voor de principes “Kwaliteitszorg”, “Toepassing standaarden” en “Verantwoordelijkheden belegd” zijn er geen wettelijke criteria. 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.

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.

De gegevens in VROS worden overgenomen uit de bronsystemen Summ-IT. De criteria voor eenmalige vastlegging zijn daarom vooral van toepassing op Summ-IT en niet op VROS. Het principe eenmalige vastlegging is daardoor beoordeeld als 'Niet van toepassing'.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	NVT	NVT	NVT

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.

Doordat VROS al vijf jaar op de nominatie staat voor uitfaseren is de applicatie uit beeld geraakt. Er is geen budget en nagenoeg geen beheer meer. Er zijn wel wensen voor verbeteringen. Het is niet bekend of en wanneer de functionaliteiten van VROS overgenomen wordt door OPP (Operationeel Politie Platform) of een ander systeem. Hierdoor wordt een slechte score gehaald op de beleidscriteria. De wetscriteria (uitvoeren GEB) zijn niet van toepassing omdat er geen nieuwe ontwikkelingen op het programma staan.

Actiepunten:

- (Beleid) Zorg dat de rapportages (bijvoorbeeld cognos rapportage 1242) ten behoeve van de besturing van de gegevensverwerking periodiek worden opgeleverd. [p2c2]
- (Beleid) Zorg dat het beheer van de processen weer deel uit gaat maken van de PDCA cyclus [p2c3]
- (Beleid) Zorg dat het beheer van de software weer deel uit gaat maken van de PDCA cyclus [p2c3]
- (Beleid) Zorg dat de beleidsverantwoordelijke een koers uitzet voor de uitfasering en opvolging van VROS. [p2c7]

Aandachtspunten:

- Vanuit het bronsysteem Summ-IT is er geen koppeling met het RDW en NHR. Hierdoor worden voertuiggegevens en rechtspersonen niet geautomatiseerd geverifieerd en ontstaat mogelijk vervuiling in de data van VROS. [p2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	13%	0

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.

VROS is een Wpg artikel 13 lid 3 verwerking (geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon). Tevens is er een model instellingsprotocol (Versie 15/06/2011) aanwezig. Hierdoor voldoet VROS aan alle criteria van dit principe. Er is alleen een aandachtspunt met betrekking tot de actualiteit van het model instellingsprotocol.

Aandachtspunten:

- Het model instellingsprotocol voor VROS is al geruime tijd niet aangepast. In de eigenschappen van het document is zichtbaar dat de laatste aanpassing op 15 juni 2011 is geweest. [p3]

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.

De audittrail wordt geregistreerd en het is mogelijk om een rapportage daar van te genereren. De voorwaarden voor het loggen van gegevens staan beschreven in het beleidskader Logging. Waar nog naar kan worden gekeken is naar de mogelijkheid tot manipulatie van de audittrail. Bij sommige databases (Oracle) is er een speciale audit functionaliteit die (tegen licentiekosten) aan kan worden gezet waarbij de acties van o.a. de database administrator kunnen worden geregistreerd. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten Het is van belang dat VROS bekend is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's).

Actiepunten:

- (Beleid) Zorg dat het niet mogelijk is om een audittrail te wijzigen. Ook niet door een 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.

Er is rechtstreekse toegang tot VROS en er is toegang via Summ-IT. Voor de rechtstreekse toegang is er een autorisatie per gebruiker. Daarnaast is er vanuit elk onderzoek in Summ-IT, dat voldoet aan de MRO criteria, toegang tot VROS. In dit laatste geval wordt gebruik gemaakt van de autorisatie van de gebruiker in Summ-IT. De score van het criterium "Autorisatie" is gebaseerd op de rechtstreekse toegang vanuit Summ-IT.
VROS haalt voor autorisatie de laagst mogelijke score. Er wordt geen gebruik gemaakt van de standaarden voor autorisatie en er is te weinig toezicht op de huidige autorisaties.

Actiepunten:

- (Beleid) Zorg dat VROS voor het verlenen van toegang gebruik van de generieke IAM- voorziening voor het verifiëren van identiteiten gaat maken. [p5c1]
- **(Wet, art 6) Zolang er nog geen aansluiting is op IAM draag er dan zorg voor dat VROS voor het verlenen van toegang gebruik maakt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- (Beleid) Zorg dat VROS voor het verlenen van toegang gebruik maakt van de generieke autorisatietool voor leidinggevenden als er afwijkende autorisaties nodig zijn. [p5c4]
- **(Wet, art 4a) Zorg dat de gebruikers van VROS geïnstrueerd zijn m.b.t. de voor hen geldende autorisatieregels. [p5c6]**
- **(Wet, art 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers periodiek worden gecontroleerd. [P5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	0%	60%	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.

Bij de ontwikkeling van VROS is geen gebruik gemaakt van vastgestelde bedrijfsbegrippen of modellen zoals het Toepassingsprofiel Metagegevens Rijk (TMR) of het Politie Gegevensmodel (PGM). Maar er is wel gebruik gemaakt van metagegevens. Dat zorgt gezamenlijk voor een volwassenheidsscore van 2.

Actiepunten:

- (Beleid) Zorg dat de lijst met vastgestelde definities voor bedrijfsbegrippen, in overleg met GGB, wordt bijgewerkt. De huidige lijst is al 5 jaar niet meer aangepast. [p6c1]
- (Beleid) Onderzoek of het Toepassingsprofiel Metagegevens Rijk (TMR) van toepassing is voor VROS en neem zo nodig maatregelen. [p6c4]
- (Beleid) Onderzoek of het Politie Gegevensmodel (PGM) toegepast kan worden voor VROS en neem zo nodig maatregelen. [p6c5]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	100%	40%	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.

Ondanks dat de kwaliteitseisen van de gegevens al in het bronsysteem zitten zijn er een beperkt aantal kwaliteitseisen die door VROS gehanteerd worden. De kwaliteitsissues die daar uit voort komen worden niet structureel opgelost. Daardoor haalt VROS voor dit principe volwassenheidsniveau 1.

Actiepunten:

- (Beleid) Zorg dat de bestaande bedrijfsregels voor kwaliteitsmeting gedeeld worden met de aanleverende partijen van de MRO's [p7c6].
- (Beleid) Zorg dat er een rapport ontwikkeld wordt waarmee de kwaliteit van gegevens, op basis van de bedrijfsregels, gemeten kan worden. Deze gegevens kunnen nu alleen met veel inspanning handmatig verzameld worden[p7c7].
- (Beleid) Zorg dat de kwaliteitscontroles en de resultaten bewaard worden [p6c8].
- (Beleid) Zorg dat er een terugkoppeling aan de aanleverende partij komt als gegevens door VROS geweigerd worden op basis van de kwaliteitseisen [p6c9].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[5]	40%	1

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.

VROS voldoet voor dit principe aan alle criteria. Voor verwijdering en de vernietiging wordt het registratieve bronsysteem gevolgd. De bronsystemen zijn zelf verantwoordelijk voor de bewaartermijnen van de gegevens. Daardoor is het grootste deel van de criteria niet van toepassing voor VROS. Er is wel een aandachtspunt.

Aandachtspunten:

- VROS is afhankelijk van de bronsystemen voor de bewaartermijn. Fouten in de bron werken door in VROS. [p8c2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	100%	NVT	3

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

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.

VROS haalt voor dit principe het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt doordat er geen risicoanalyse is uitgevoerd. VROS maakt deels gebruik van de generieke voorzieningen voor informatiebeveiliging. Echter het is onduidelijk wat de actuele status is van de informatiebeveiliging.

Actiepunten:

- (Beleid) Zorg dat er een risicoanalyse voor de verwerking wordt uitgevoerd. [p9c1]
    - **(Wet art 4a lid 2) Zorg dat de informatiebeveiligingseisen mede bepaald worden op basis van de resultaten van de risicoanalyse. [p9c2]**
    - **(Wet art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in VROS. [p9c3]**
    - (Beleid) Toets of alle informatiebeveiligingseisen gerealiseerd kunnen worden door de standaard informatiebeveiligingsdiensten. [p9c5]
        - (Beleid) Toets of er maatregelen genomen kunnen worden om informatiebeveiligingseisen te realiseren die niet door de standaard informatiebeveiligingsdiensten kunnen worden gerealiseerd? [p9c6]
    - (Beleid) Zorg dat de restrisico's in de beveiliging van VROS periodiek worden beheerd. [p9c7]
- (Beleid) Onderzoek in hoeverre het Vax-VMS platform waar VROS op draait risico's met zich mee brengt en neem zo nodig maatregelen. [p9c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	10%	0

1.10 Privacy by default

"De verwerking van persoonsgegevens is standaard zo beperkt mogelijk ingericht"

Zowel de AVG als de Wpg bevatten Privacy by Default en Privacy by Design als verplichte principes. Deze dienen ertoe om gegevensbescherming vanaf het moment van ontwikkeling van informatiediensten tot aan het laatste gebruik zoveel mogelijk in de gegevensverwerking te integreren. Daar waar Privacy by Design vooral toeziet op ontwerpkeuzes bij de *ontwikkeling* van informatiediensten is Privacy by Default van belang bij keuzemomenten tijdens *gebruik* van de informatiediensten. Dit principe verplicht organisaties om de privacy van betrokkenen zo veel mogelijk te beschermen door de verwerking van persoonsgegevens standaard (by default) op de meest privacyvriendelijke stand te zetten.

VROS voldoet aan alle criteria voor de principe voor Privacy by Default. Echter tijdens de 0-meting is aangegeven dat er geen test of acceptatieomgeving is voor VROS. Hierdoor wordt er getest met productiedata wat de nodige risico's met zich meebrengt.

Aandachtspunten:

- Er is geen test of acceptatie omgeving voor VROS. Dat betekent dat productiedata gebruikt wordt voor het testen van nieuwe versies of dat er vooraf niet getest wordt. Zorg voor een andere oplossing dan testen met productiedata. [p10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	100%	3

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.

Er zijn geen actiepunten voor dit principe. Voor de encryptie van de bestanden met MRO's wordt gebruik gemaakt van de standaarden PGP en GPG.

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

Ondanks dat de verantwoordelijkheden voor VROS goed zijn belegd is er toch een actiepunt voor de uitvoering van de verantwoordelijkheid.

Actiepunten:

- (Beleid) Zorg dat de definities, beleid, koers en strategie voor de verwerking van gegevens in VROS opgesteld en vastgesteld worden. [p12c2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[7]	67%	2

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

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-26_Uitvoeringskader_Privacy en Security by Design_v2.0'. 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[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
Als de criteria zijn beoordeeld als “niet van toepassing” dan zijn er geen criteria benoemd of de criteria zijn niet van toepassing gebleken voor de applicatie.

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

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

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

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

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

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

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

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

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

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

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

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

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

Aandachtspunten
1: Volwassenheidsniveau 1:

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

2: Beleidscriteria:

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

3: Privacy functionaris:

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

Disclaimer

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

Bijlage 1: Uitgangspunt bij compliance

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

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