



0-meting Privacy & Security by Design

**Personen
server**

10.2.e

Definitief

Versie 2.0

Versie datum 25 april 2019

Rubricering **Politie Intern**

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
1.0	26-04-2018	Eerste versie rapport
1.8	21-12-2018	Nieuwe versie nav veranderde omstandigheden van de personenserver
1.9	21-12-2018	Aanpassingen op basis van review
2.0	25-04-2019	Rapport definitief gemaakt na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
1.9	21-12-2018	10.2.e	Gegevensautoriteit

© Politie, all rights reserved.

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

Documentinformatie	2
Inhoudsopgave.....	2
Inleiding.....	4
0-meting Personenserver	5
Algemeen.....	5
Doel	5
Doelgroep	5
Aanwezigen 0-meting	5
Personenserver.....	6
Omschrijving applicatie.....	6
Soorten verwerkingen van politiegegevens	6
Verwerkingsgrondslag	7
Eindscore	8
1.1 Eenmalige vastlegging	10
1.2 PDCA-cyclus	10
1.3 Doelbinding.....	11
1.4 Verantwoording.....	11
1.5 Autorisatie.....	12
1.6 Metagegevens	12
1.7 Kwaliteitszorg	13
1.8 Bewaren en vernietigen	13
1.9 Informatiebeveiliging.....	14
1.10 Privacy by default	14
1.11 Toepassen standaarden	15
1.12 Verantwoordelijkheden belegd	15
2. Verantwoording toetsing.....	16
Toetsingscriteria.....	16
Disclaimer	18
Bijlage 1: Uitgangspunt bij compliance	19

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 de Personenserver. 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 Personenserver

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

Directe betrokkenen	Naam	Functie
0-meting Personenserver	10.2.e	Team GGB
	10.2.e	Team software ontwikkeling

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

Gespreksdatum	Nummer meting	Toelichting
21/11/2018	2018112101	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader Privacy & Security by Design versie 2.0.

Personenserver

Omschrijving applicatie

Het doel van de Personenserver is tweeledig:

- Verifiëren van persoonsgegevens d.m.v. online bevestigingen bij de BRP. 10.2.c
- Het eenmalig vastleggen van persoonsgegevens binnen de politie in de database van de Personenserver. Indien mogelijk worden de persoonsgegevens geverifieerd bij de BRP. Als er vervolgens wijzigingen zijn in de gegevens bij de BRP worden deze wijzigingen door de BRP doorgegeven aan de Personenserver. De Personenserver geeft deze wijzigingen dan op haar beurt weer door aan de op de Personenserver aangesloten applicaties. 10.2.c

De Personenserver heeft geen schermen voor eindgebruikers. Verschillende applicaties zoals BV, Summ-IT, Verona, BVI-IB, OPP, Politie.nl, KMAR (met HKS) en PSH-TM wisselen berichten uit met de Personenserver. De BRP bevat gegevens uit de gemeentelijke GBA's en uit het Register Niet-Ingezetenen (RNI). BVID (De zuil) levert identificatie gegevens aan de Personenserver.

10.2.c, 10.2.g

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	Ook niet geverifieerde personen komen direct in de personenserver van uit BVH.
Vastleggen	X	
Ordenen		
Bewaren		
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	Vanuit GBA. Bijv. 10.2.c
Wijzigen (het bestaande aanpassen)	X	Mutaties zoals verhuisberichten nav notificatie.
Opvragen	X	Personenserver vraagt een bevestiging op bij het GBA
Raadplegen	X	Personenserver raadpleegt het GBA
Gebruiken	X	
Vergelijken	X	Gegevens worden geverifieerd in het GBA
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Bijvoorbeeld aan HKS van de KMAR.
Samenbrengen	X	Als BVI er achter komt dat één persoon meerdere keren is opgevraagd worden die gegevens samengevoegd.
Met elkaar in verband brengen		
Afscherming	X	Er zijn verschillende soorten bevestiging mogelijk. Regulier, gevoelig en geheim.
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	De afnemende applicatie bepaalt of iets vernietigd wordt. Als alle applicaties de registratie van de persoon vernietigd hebben dan de persoon vernietigd in de personenserver.

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		
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 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 personenserver scoort een volwassenheidsniveau 1. Dit houdt in dat de personenserver 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 personenserver een score van 37% en op de criteria van het politiebeleid een score van 33%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'PDCA-cyclus', 'Autorisatie' en 'Informatiebeveiliging' er bijzonder negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Daarnaast is er een aandachtspunt.

De personenserver is geen normale applicatie maar een tussenstation voor de gegevens uit de BRP. Een deel van de criteria is daardoor niet van toepassing. Dat maakt dat de criteria die wel van toepassing zijn, maar waar niet aan voldaan wordt, een grote invloed hebben op het volwassenheidsniveau. Zodra een actiepoint wordt opgelost heeft dit ook direct een grote invloed op het volwassenheidsniveau.

Deze 0-meting vervangt de eerdere meting van 10/01/2018. De vorige meting ging nog uit van een levensduur van minder dan 2 jaar. Achteraf bleek dat er nog een langere levensduur verwacht wordt. De criteria zijn opnieuw beoordeeld vanuit deze optiek. Tevens zijn de criteria beoordeeld door andere betrokkenen

Advies:

- (Wet art 6c lid 2) Zorg dat de verwerkersovereenkomst voor 10.2.g periodiek wordt getoetst en borg zo nodig de aanpassingen. De huidige verwerkersovereenkomst wordt jaarlijks stilzwijgend verlengd. [p2c6]
- (Wet, art 3 lid 1) Zorg dat de verwerkingsgrondslag bij een persoonsgegeven in de personenserver kan worden opgenomen (tenzij deze automatisch afgeleid kan worden). [p3c1]
- (Wet, art 3 lid 1) Onderzoek of er meerdere verwerkingsgrondslagen kunnen zijn bij een persoon in de personenserver en borg zo nodig de maatregelen. [p3c2]
- (Wet, art 6) Zorg dat, zolang de personenserver nog niet is aangesloten op het autorisatiebeheersysteem IAM, er gebruik gemaakt wordt van de vastgestelde autorisatirollen van de politie. [p5c2]
- (Wet, art 4a) Borg dat de beheerders, bijvoorbeeld door opleidingen, altijd op de hoogte zijn van de voor hen geldende autorisatieregels. Er zijn geen gewone gebruikers voor de personenserver. [p5c6]
- (Wet art 8, 9, 10, 12 en 14) Zorg dat de personenserver naast het vernietigen van gegevens op aangeven van de bron ook het verwijderen van gegevens (toegang beperkt tot de poortwachter) op aangeven van de bron gaat ondersteunen. [p8c2] [p8c5]
- (Wet art 8) Zorg dat, zodra de personenserver het verwijderen van gegevens ondersteunt, de poortwachter toegang krijgt tot de verwijderde gegevens. [p8c10]
- (Wet art 4a lid 2) Stel de informatiebeveiligingseisen vast op basis van de resultaten uit de risicoanalyse. [p9c2]
- (Wet art 4a lid 2) Beoordeel de impact van de informatiebeveiligingseisen ten behoeve van realisatie. [p9c3]

Aandachtspunten:

- Bij wijzigingen van een verwerking wordt de historie niet gelogd. Er worden alleen notificaties verstuurd naar de gerelateerde applicaties. We raden aan om te onderzoeken of dit mechanisme voldoende is en, zo nodig, de maatregelen te borgen. [p2c3]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Personenserver	21/11/2018	2.0	37%	33%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR	PERCENTAGE		VOLWASSENHEID
		W(et)	B(beleid)	
Eenmalige vastlegging	Z	100%	100%	3
PDCA-cyclus	M	0%	25%	0
Doelbinding	Z	25%	0%	0
Verantwoording	Z	100%	0%	2
Autorisatie	Z	0%	0%	0
Metagegevens	Z	NVT	0%	0
Kwaliteitszorg	Z	NVT	19%	0
Bewaren en vernietigen	Z	17%	NVT	0
Informatiebeveiliging	Z	0%	30%	0
Privacy by default	Z	100%	50%	2
Toepassing standaarden	L	NVT	100%	3
Verantwoordelijkheden belegd	M	NVT	33%	0
TOTALEN TOETSING		37%	33%	



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 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.

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 personenserver geeft informatie van de BRP ongewijzigd door naar de aangesloten applicaties. De criteria voor terugmelden zijn van toepassing op deze applicaties en niet op de personenserver. Aan alle andere criteria wordt voldaan. Dit zijn: gebruik van referentiegegevens, verificatie in basisregistratie, gebruik van model kernobjecten, gebruik van een gegevensdienstenlaag en het voorkomen van dubbele registraties.

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.

Het beheer van gegevens, processen en software is onderdeel van de PDCA cyclus. Een GEB (gegevensbeschermingseffectbeoordeling) is niet van toepassing evenmin als toetsing door de autoriteit persoonsgegevens.

Er zijn wel actiepunten voor het (periodiek) leveren van stuurinformatie ten behoeve van de reguliere PDCA cyclus, voor een verwerkersovereenkomst ten behoeve van 10.2.g en voor de beleidsverantwoordelijke.

Actiepunten:

- (Beleid) Zorg dat de voorziening stuurinformatie levert ten behoeve van de reguliere PDCA cyclus. Bijvoorbeeld over de omvang van de gegevensverwerking, de kwaliteit van gegevens, aantallen gebruikers, aantallen verstrekkingen, het beheer van autorisaties, beveiligingsmaatregelen en –incidenten. Er wordt nu alleen op incidenten geacteerd (piepsysteem). [p2c1]
- (Beleid) Zorg dat de rapportages t.b.v. de besturing van de gegevensverwerking periodiek opgeleverd worden. [p2c2]
- **(Wet art 6c lid 2) Zorg dat de verwerkersovereenkomst voor 10.2.g periodiek wordt getoetst en borg zo nodig de aanpassingen. De huidige verwerkersovereenkomst wordt jaarlijks stilzwijgend verlengd. [p2c6]**
- (Beleid) Zorg dat duidelijk wordt wie de beleidsverantwoordelijke is voor de personenserver. [p2c7]
- (Beleid) Zorg dat de beleidsverantwoordelijke definities, beleid, koers en strategie voor de verwerking van gegevens gaat vaststellen en vervolgens regie gaat voeren op de borging. [p2c7]

Aandachtspunten:

- Bij wijzigingen van een verwerking wordt de historie niet gelogd. Er worden alleen notificaties verstuurd naar de gerelateerde applicaties. We raden aan om te onderzoeken of dit mechanisme voldoende is en, zo nodig, de maatregelen te borgen. [p2c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	0%	25%	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.

In de personenserver wordt gebruik gemaakt van de classificaties regulier, gevoelig en geheim. Deze classificaties worden aangeleverd door de BRP. Verwerkingen ten behoeve van de vergunningen module vallen onder regulier. Deze vallen niet onder de Wpg maar onder de AVG. Het is niet duidelijk of de classificaties "Gevoelig" en "Geheim" gebruikt kunnen worden om de Wpg verwerkingsgrondslag af te leiden. Er moet onderzocht worden hoe de verwerkingsgrondslag automatisch kan worden herleid en daarna opgeslagen kan worden bij de verwerking.

Actiepunten:

- **(Wet, art 3 lid 1) Zorg dat de verwerkingsgrondslag bij een persoonsgegeven in de personenserver kan worden opgenomen (tenzij deze automatisch afgeleid kan worden). [p3c1]**
- **(Wet, art 3 lid 1) Onderzoek of er meerdere verwerkingsgrondslagen kunnen zijn bij een persoon in de personenserver en borg zo nodig de maatregelen. [p3c2]**
- (Beleid) Onderzoek hoe de verwerkingsgrondslag automatisch afgeleid kan worden en borg de maatregelen. Bijvoorbeeld door gebruik te maken van de classificaties "Gevoelig" en "Geheim" die verstrekt worden door de BRP. [p3c3]

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

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 in de personenserver geregistreerd en er kan een rapportage van de audittrail gemaakt worden. Er is slechts één actiepunt en dat betreft de manipuleerbaarheid van de trail.

Actiepunten:

- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. Nu heeft een database administrator daar de mogelijkheden voor zonder traceerbaarheid. [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.

De personenserver heeft slechts 4 beheerders die toegang hebben. Er zijn geen gewone gebruikers. Hierdoor is een deel van de criteria niet van toepassing. Voor autorisatie van de beheerders moet de personenserver nog aangesloten worden op IAM. Zolang er nog aansluiting is op IAM moet er gebruik gemaakt worden van de vastgestelde autorisatie rollen en moet er een goed controle (audit) proces en sanctiebeleid ingeregeld worden. Daarnaast moet de opleiding van de beheerders geborgd worden.

Actiepunten:

- (Beleid) Zorg dat de personenserver toegang verleent aan de beheerders op basis van de generieke IAM-voorziening voor het verifiëren van identiteiten. Er zijn geen gewone gebruikers voor de personenserver. [p5c1]
- **(Wet, art 6) Zorg dat, zolang de personenserver nog niet is aangesloten op het autorisatiebeheersysteem IAM, er gebruik gemaakt wordt van de vastgestelde autorisatie rollen van de politie. [p5c2]**
- (Beleid) Zorg dat, zolang de personenserver nog niet is aangesloten op het autorisatiebeheersysteem IAM, er gebruik gemaakt wordt van Audit Based Access Control. Dat wil zeggen een goed controle (audit) proces en sanctiebeleid. Zie hiervoor ook het autorisatiebeleid 2016-2020. [p5c5]
- **(Wet, art 4a) Borg dat de beheerders, bijvoorbeeld door opleidingen, altijd op de hoogte zijn van de voor hen geldende autorisatieregels. Er zijn geen gewone gebruikers voor de personenserver. [p5c6]**

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

De personenserver is ontwikkeld voordat standaarden als PGM en TMR bestonden. Daarnaast worden metagegevens bijgehouden in de bronsystemen. Dit samen maakt dat alleen het criterium voor de bedrijfsbegrippen van toepassing is voor de personenserver.

Actiepunten:

- (Beleid) Onderzoek of de personenserver in voldoende mate gebruik maakt van vastgestelde bedrijfsbegrippen en borg zo nodig de maatregelen. [p6c1]

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

Er is recent een handmatige controle uitgevoerd om de gegevens in de personenserver te vergelijken met de gegevens in de gekoppelde applicaties. Maar er zijn nog geen kwaliteitseisen bepaald voor de gegevens in de personenserver. Hierdoor volgt uit de meeste criteria voor kwaliteitszorg een actiepunten.

Actiepunten:

- (Beleid) Zorg dat er kwaliteitseisen worden opgesteld en dat deze vervolgens afgestemd worden met de beleidsverantwoordelijke. [p7c2]
- (Beleid) Zorg dat de kwaliteitseisen worden gerealiseerd. [p7c3]
- (Beleid) Zorg dat er bedrijfsregels worden geformuleerd om de kwaliteit van gegevens te meten. [p7c5]
- (Beleid) Onderzoek of de bedrijfsregels vertaald kunnen worden naar geautomatiseerde controles en borg zo nodig de maatregelen. [p7c6]
- (Beleid) Zorg dat een rapport over de kwaliteit van de gegevens kan worden samengesteld. [p7c7]
- (Beleid) Zorg dat de uitgevoerde kwaliteitscontroles en het resultaat daarvan bewaard worden. [p7c8]
- (Beleid) Onderzoek of de gebruiker geattendeerd kan worden op kwaliteitsafwijkingen en borg zo nodig de maatregelen. [p7c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT ³	19%	0

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.

De personenserver volgt de bron al voor het vernietigen van gegevens. Als de personenserver ook de bron gaat volgen voor het verwijderen van gegevens en als de poortwachter toegang krijgt tot de verwijderde gegevens dan wordt aan alle criteria voldaan.

Actiepunten:

- (Wet art 8, 9, 10, 12 en 14) Zorg dat de personenserver naast het vernietigen van gegevens op aangeven van de bron ook het verwijderen van gegevens (toegang beperkt tot de poortwachter) op aangeven van de bron gaat ondersteunen. [p8c2] [p8c5]
- (Wet art 8) Zorg dat, zodra de personenserver het verwijderen van gegevens ondersteunt, de poortwachter toegang krijgt tot de verwijderde gegevens. [p8c10]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	17%	NVT	0

³ Er zijn voor dit principe geen wettelijke criteria benoemd.

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 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 is achterhaald.

De personenserver haalt voor "Informatiebeveiliging" het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt omdat er geen volledige risicoanalyse is uitgevoerd. In 2016 is een risicoanalyse uitgevoerd, maar deze was niet gericht op informatiebeveiliging.

Actiepunten:

- **(Wet art 4a lid 2) Stel de informatiebeveiligingseisen vast op basis van de resultaten uit de risicoanalyse. [p9c2]**
- **(Wet art 4a lid 2) Beoordeel de impact van de informatiebeveiligingseisen ten behoeve van realisatie. [p9c3]**
- (Beleid) Toets of alle informatiebeveiligingseisen gerealiseerd zijn door de standaard informatiebeveiligingsdiensten en borg zo nodig alsnog de realisatie. [p9c5]
- (Beleid) Onderzoek of er informatiebeveiligingseisen gerealiseerd zijn buiten de standaard informatiebeveiligingsdiensten en neem zo nodig maatregelen. [p9c6]
- (Beleid) Zorg dat de restrisico's in de beveiliging beheerd worden. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0	30%	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.

De afnemersindicatie wordt nu automatisch geplaatst bij alle personen in BVH en nooit meer verwijderd. Er is nieuw beleid gemaakt om dat te beperken. Maar dat beleid moet nog vastgesteld en uitgevoerd worden.

Actiepunten:

- (Beleid) Zorg dat het nieuwe beleid voor de afnemersindicatie wordt vastgesteld. [p10c3]
- (Beleid) Zorg dat het nieuwe beleid voor de afnemersindicatie wordt toegepast in de personenserver. [p10c3]

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 van belang om waar mogelijk gebruik te maken van standaardisatie en uniformiteit binnen een informatievoorziening. Indien een organisatie hierin een eigen keuze maakt en afwijkt van standaarden zullen er afspraken gemaakt moeten worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

Voor de personenserver zijn alleen de standaarden van de GBA van toepassing. Daar wordt aan voldaan. Alleen als voldaan wordt aan de standaarden werkt de koppeling naar de GBA.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT ⁴	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. Ook als er onzekerheid is over de levensduur van de personenserver.

Actiepunten:

- (Beleid) Zorg dat er, naast de aandachtsgebiedhouder, ook een portefeuillehouder benoemd wordt voor de personenserver. [p12c1]
- (Beleid) Zorg dat de definities, beleid, koers en strategie voor de verwerking van gegevens worden vastgesteld. [p12c2]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT ⁵	33%	0

⁴ Er zijn voor dit principe geen wettelijke criteria benoemd.

⁵ 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'. 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' staan⁶.

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.

⁶ 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.

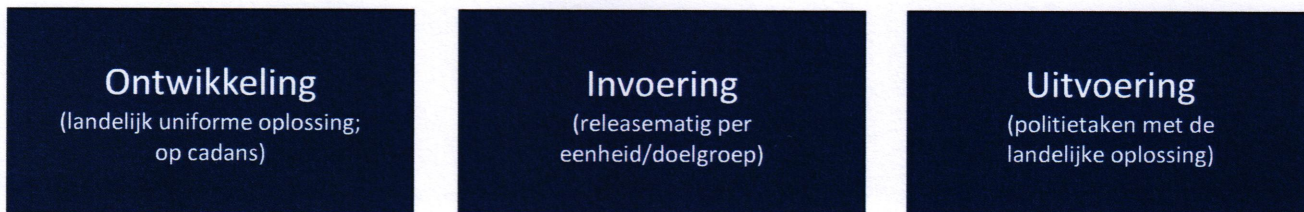
3: Privacy functionaris:

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 Portefuillehouder 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 Portefuillehouder.

Bij compliance van de landelijke uniforme oplossing gaat het óók om de invoering