0-meting Privacy & Security by Design

Verificatie module

10.2.e

Concept

Versie 1.00

Versie datum 2 mei 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
0.8	12-3-2019	Rapport ingevuld op basis van resultaten uit de 0-meting	
0.9	22-3-2019	Review aanpassingen doorgevoerd	
0.92	19-04-2019	Review aanpassingen doorgevoerd.	
0.93	25-04-2019	Review aanpassingen doorgevoerd.	
0.94	02-05-2019	Tekstuele aanpassing doorgevoerd	
1.0	02-05-2019	Rapport definitief gemaakt na wederzijds goedkeuren	

Review commentaar

Versie	Wanneer	Wie	Afdeling
0.9	22-3-2019	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 Verificatiemodule. 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 Verificatiemodule

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 Verificatiemodule	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
13/02/2019	2019021301	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

Verificatiemodule

Omschrijving applicatie

De verificatiemodule is een applicatie om het BRP te bevragen. Hiermee kan een zoekvraag worden gesteld op basis van het BRP. Na een vraag geeft de verificatiemodule slechts 10 resultaten weer, dus het is van belang dat er specifieke vragen worden gesteld. Op basis van een speciale autorisatie kunnen er ook historische vragen worden gesteld. Er worden geen gegevens opgeslagen. Burgers zelf kunnen opvragen welke instantie hun gegevens heeft opgevraagd, tenzij er gebruik is gemaakt van een geheime opvraging. Het verschil met de personenserver is dat de personenserver geen uitgebreide bevraging heeft en de user interface bij de verificatiemodule heel anders is. Elke medewerker moet apart inloggen. Het verschil met BVI-IB is d10.2.c Er zijn ook verschillende zoekvelden. 10.2.c

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen		
Vastleggen		
Ordenen		
Bewaren		
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)		
Wijzigen (het bestaande aanpassen)		
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	Identiteitsbewijs, of als er een inval wordt gedaan (wie woont er allemaal op dat adres).
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)		
Samenbrengen		
Met elkaar in verband brengen		
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	Logging wordt na 5 jaar vernietigd. 10.2.g .

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9	X	
Informatiepositie	Artikel 10	X	
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11		
Informanten	Artikel 12	X	
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 verificatiemodule 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 verificatiemodule een score van 50% en op de criteria van het politiebeleid een score van 33%. Dat geeft aan dat er verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'Informatiebeveiliging', Autorisatie' en 'Doelbinding' er bijzonder negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen.
Daarnaast is er een aandachtspunt met betrekking tot de portefeuillehouder

Advies:

- **(Wet, Art. 4 lid 1) Zorg dat indien er sprake is van 'gerede twijfel' over een gegeven dat dit aan de bronhouder wordt teruggemeld. Hiervoor moet eerst het "Uitvoeringskader terugmelden" worden voltooid en daarna geaccordeerd door de portefeuillehouder. In het uitvoeringskader wordt onder andere de positionering van een centraal loket bepaald. [p1c5]**
- **(Wet, art 3 lid 1) Zorg dat de verwerkingsgrondslag bij een persoonsgegeven in de verificatiemodule kan worden opgenomen (tenzij deze automatisch afgeleid kan worden). [p3c1]**
- **(Wet, art. 6) Zorg dat, zolang de verificatiemodule nog geen gebruik maakt van IAM, voor het verlenen van toegang gebruik wordt gemaakt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- **(Wet, art. 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. [p5c8]**
- **(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:

- Vanaf 1/1/2019 is de Wpg onder andere aangevuld met artikel 6b voor het onderscheid tussen verschillende categorieën van betrokkenen. Voor zover mogelijk moet duidelijk onderscheid gemaakt worden tussen politiegegevens betreffende verschillende categorieën van betrokkenen. 10.2.c
- Zorg dat, indien de verificatiemodule niet meer onder de portefeuille identiteit valt, de applicatie wordt overgedragen aan de nieuwe portefeuillehouder. [p2c8]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Verificatiemodule	13/02/2019	2.0	50%	33%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	0%	NVT	0
PDCA-cyclus	M	-	NVT	13%	0
Doelbinding	Z	-	50%	0%	1
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	33%	10%	0
Metagegevens	Z	-	NVT	17%	0
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	100%	NVT	3
Informatiebeveiliging	Z	-	0%	20%	0
Privacy by default	Z	-	100%	75%	2
Toepassing standaarden	L	-	NVT	50%	2
Verantwoordelijkheden belegd	M	-	NVT	38%	1
TOTALEN TOETSING		-	50%	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.

Op één na alle criteria van dit principe zijn niet van toepassing omdat de gegevens betrokken worden uit de BRP. Alleen het criterium betreffende gerede twijfel over een gegeven is van toepassing.

Actiepunten:

- **(Wet, Art. 4 lid 1) Zorg dat indien er sprake is van 'gerede twijfel' over een gegeven dat dit aan de (externe) bronhouder wordt teruggemeld. Hiervoor moet eerst het "Uitvoeringskader terugmelden" worden voltooid en daarna geaccordeerd door de portefeuillehouder. In het uitvoeringskader wordt onder andere de positionering van een centraal loket bepaald. [p1c5]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	0%	NVT	0

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.

Alle criteria die, voor dit principe, van toepassing zijn op de verificatiemodule leveren een actiepunt op. Dat houdt in dat de PDCA cyclus nog niet goed is ingericht. De criteria voor een GEB, raadplegen van de autoriteit persoonsgegevens en een verwerkersovereenkomst zijn niet van toepassing. Daarnaast is er aan aandachtspunt over de portefeuille waaronder de verificatiemodule valt.

Actiepunten:

- (Beleid) Zorg dat de verificatiemodule 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. [p2c1]
- (Beleid) Zorg dat de rapportages t.b.v. de besturing van de gegevensverwerking periodiek opgeleverd worden. [p2c2]
- (Beleid) Zorg dat het autorisatieproces onderdeel wordt van de PDCA cyclus. [p2c3]
- (Beleid) Zorg dat de portefeuillehouder een beleidsverantwoordelijke voor de gegevens die verwerkt worden aanstelt. Zorg dat deze regie gaat voeren op definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens. [p2c7]

Aandachtspunten:

- Zorg dat, indien de verificatiemodule niet meer onder de portefeuille identiteit valt, de applicatie wordt overgedragen aan de nieuwe portefeuillehouder. [p2c8]

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.

Aangezien de verificatiemodule alleen de raadpleging van de gegevens in de BRP omvat zijn de meeste criteria niet van toepassing. Er is bijvoorbeeld geen artikel 13 protocol van toepassing. De criteria voor de verwerkingsgrondslag zijn wel van toepassing.

Actiepunten:

- **(Wet, art 3 lid 1) Zorg dat de verwerkingsgrondslag bij een persoonsgegeven in de verificatiemodule kan worden opgenomen (tenzij deze automatisch afgeleid kan worden). [p3c1]**
- (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]
- (Beleid) Zorg dat de automatisch afgeleide verwerkingsgrondslag door de gebruiker kan worden aangepast. [p3c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	50%	0%	1

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 politie kan verantwoording afleggen over gegevensverwerkingen als er een correct toegepaste audittrail is. De verificatiemodule houdt een audittrail bij en het mogelijk om een rapportage daar van te genereren. Het is van belang dat als een audittrail wordt geregistreerd dat deze is beveiligd tegen manipulatie. Dit betreft niet alleen manipulatie door de gebruiker, maar ook de manipulatie door een databasebeheerder. Er moet een afweging worden gemaakt tussen de kosten en baten van een dergelijke functionaliteit.

Actiepunten:

- (Beleid): Beveilig de audittrail tegen manipulatie door zowel gebruikers als (database)beheerders [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 beheer last op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

De gebruikers van de verificatiemodule worden in het startscherm geïnformeerd over de autorisatieregels. Maar de autorisatie zelf verloopt buiten alle generieke voorzieningen en controle mechanismen om.

Actiepunten:

- (Beleid) Zorg dat de verificatiemodule voor het verlenen van toegang gebruik gaat maken van de generieke IAM- voorziening voor het verifiëren van identiteiten. Voor de verificatiemodule loopt dit nu nog via de autorisatiedesk. [p5c1]
- **(Wet, art. 6) Zorg dat, zolang de verificatiemodule nog geen gebruik maakt van IAM, voor het verlenen van toegang gebruik wordt gemaakt van de vastgestelde autorisatierollen van de politie. [p5c2]**
- (Beleid) Zorg dat de verificatiemodule gebruik maakt van toegangsverlening op gegevensniveau (in plaats van uitsluitend op applicatieniveau). [p5c3]
- (Beleid) Zorg dat de verificatiemodule voor het verlenen van toegang gebruik maakt van de generieke autorisatietool voor leidinggevenden. [p5c4]
- (Beleid) Zorg dat, zolang de verificatiemodule 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]
- (Beleid) Zorg dat de verificatiemodule rapportages genereert op het gebruik van autorisaties. [p5c7]
- **(Wet, art. 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	33%	10%	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 meeste criteria van dit principe zijn niet van toepassing omdat de gegevens betrokken worden uit de BRP. Er zijn wel actiepunten over de afleiding van een aantal gegevens, het toepassen van het TMR en over het gebruik van metagegevens bij nieuwe functionaliteiten.

Actiepunten:

- (Beleid) Zorg dat de afleiding[3] van de woonplaats met behulp van de postcode en het huisnummer wordt gedocumenteerd. De documentatie moet daarna wordt overgedragen naar GGB. Zie ook p11c1. [p6c1]
- (Beleid) Toets in hoeverre de gegevens die door de BRP worden verstrekt aan de verificatiemodule voldoen aan TMR (Toepassingsprofiel Metagegevens Rijk) en borg zo nodig de maatregelen. Dit zou in theorie moeten kloppen, maar het is niet bekend of het al een keer getoetst is. [p6c4]
- (Beleid) Zorg dat de metagegevens ook daadwerkelijk gebruikt voor de te ontwikkelen functionaliteiten zoals: verlenen van toegang, bewaartermijnen, audittrails en managementrapportages. [p6c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	17%	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.

De meeste criteria van dit principe zijn niet van toepassing omdat de gegevens betrokken worden uit de BRP. De criteria die wel van toepassing zijn leiden niet tot actiepunten aangezien er voldaan wordt aan de gestelde kwaliteitseisen (format huisnummer en dergelijke) en omdat de gebruiker geattendeerd wordt op kwaliteitsafwijkingen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[4]	100%	3

[3] De woonplaats wordt niet rechtstreeks overgenomen van de BRP, maar wordt afgeleid met behulp van de postcode tabel van de door de BRP verstrekte postcode en huisnummer. Dit is ontstaan omdat het gebruik van de BAG b j de start van de personenserver niet verplicht was. De GBA's maakten geen gebruik van de "Woonplaats". In de verificatiemodule wordt de "Woonplaats" afgeleid met behulp van de postcodetabel. Sinds 1 juli 2011 is het gebruik van de BAG verplicht. De BRP levert de "Woonplaats" nu wel aan, maar de verificatiemodule is daar niet op aangepast.

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

1.8 Bewaren en vernietigen

"*Gegevens worden niet langer verwerkt dan is toegestaan en worden vernietigd zodra ze niet langer noodzakelijk zijn*"

De politie mag alleen gegevens verwerken indien en voor zolang daar een wettelijke grondslag voor bestaat. Als die grondslag komt te vervallen moeten de gegevens worden verwijderd of vernietigd. Ook voor gegevens waarvan blijkt dat ze onjuist zijn geldt dat ze moeten worden vernietigd of gecorrigeerd. De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden.

Op één na alle criteria van dit principe zijn niet van toepassing omdat de gegevens betrokken worden uit de BRP. Er wordt voldaan aan het criterium voor de bewaartermijnen omdat de logging automatisch na 5 jaar wordt vernietigd.

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

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 alle mogelijke schadelijke gevolgen door bedreigingen van de informatievoorziening op een bewuste manier af te wegen 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 verificatiemodule haalt voor "Informatiebeveiliging" het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt omdat er geen risicoanalyse is uitgevoerd.

Actiepunten:

- (Beleid) Zorg dat er een risicoanalyse voor de verwerking wordt uitgevoerd. [p9c1]
- **(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%	20%	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 privacy vriendelijke stand te zetten.

De verwerking van persoonsgegevens in de verificatiemodule is zo beperkt mogelijk. Een opt-in of opt-out regime is niet van toepassing. En er wordt gebruik gemaakt van Privacy Enhancement Technology (PET) hulpmiddelen door middel van versleuteling van berichten (als de gebruiker daar voor kiest). Daarnaast heeft de BRP heeft een eigen omgeving voor testen.

Actiepunten:

- (Beleid) Zorg dat berichten altijd versleuteld worden. Nu is het een keuze van de gebruiker. [p10c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	75%	2

1.11 Toepassen standaarden

"*Bij de gegevensverwerking wordt gebruik gemaakt van bestaande overheids- en ketenstandaarden*"

Door het gebruik van bestaande overheids- en ketenstandaarden bevordert de samenwerking tussen de organisaties en de interoperabiliteit van systemen. In de basis is het ban belang om waar mogelijk gebruik te maken van standaardisatie en uniformiteit binnen een informatievoorziening. Indien een organisatie hierin een eigen keuze maakt en afwijkt van standaarden zullen er afspraken gemaakt moeten worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

Er vindt een kleine vertaling plaats van de gegevens uit de BRP. Dat is de enige reden waarom voor dit principe niet het hoogste volwassenheidsniveau gehaald wordt.

Actiepunten:

- (Beleid) Onderzoek hoe de huidige afleiding[5] van de woonplaats uit de door de BRP verstrekte postcode en huisnummer combinatie overbodig gemaakt kan worden en borg de maatregelen. Zie ook p6c1. [p11c1]
- (Beleid) Zorg dat de verwerkingsverantwoordelijk op de hoogte is van het feit dat de woonplaats wordt afgeleid uit de door de BRP verstrekte postcode en huisnummer combinatie. [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[6]	50%	2

[5] De woonplaats wordt niet rechtstreeks overgenomen van de BRP, maar wordt afgeleid met behulp van de postcode tabel van de door de BRP verstrekte postcode en huisnummer. Dit is ontstaan omdat het gebru k van de BAG b j de start van de personenserver niet verplicht was. De GBA's maakten geen gebruik van de "Woonplaats". In de verificatiemodule wordt de "Woonplaats" afgeleid met behulp van de postcodetabel. Sinds 1 juli 2011 is het gebruik van de BAG verplicht. De BRP levert de "Woonplaats" nu wel aan, maar de verificatiemodule is daar niet op aangepast.

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

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 verificatiemodule ondersteund, met uitzondering van het vastleggen van de verwerkingsgrondslag, de uitvoeringsverantwoordelijke voldoende. Maar het is niet bekend wie de beleidsverantwoordelijke is. Er is een architectuur document geaccordeerd waarin de personenserver voorlopig nog blijft bestaan, dit geldt dan ook voor de verificatiemodule. De vernieuwing van de verificatiemodule zit niet in de scope van PVR.

Actiepunten:

- (Beleid) Zorg dat de portefeuillehouder (zie p2c7) een beleidsverantwoordelijke voor de gegevens die verwerkt worden aanstelt. Zorg dat deze bekend gemaakt wordt met de verificatiemodule. [p12c1]
- (Beleid) Zorg dat de beleidsverantwoordelijke definities, beleid, koers en strategie voor de verificatiemodule vaststelt. [p12c2]
- (Beleid) Zorg dat de gegevensverwerkers de verwerkingsgrondslag (zie ook principe 3) kunnen vastleggen. [p12c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[7]	38%	1

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

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-26_Uitvoeringskader_Privacy en Security by Design_v2.0'. Vervolgens zijn er criteria toegevoegd of aangescherpt op basis van documenten waar in het uitvoeringskader naar wordt verwezen. Het resultaat is met de auteurs van het uitvoeringskader besproken. Hun commentaar is verwerkt en nogmaals besproken.

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

Herkomst
De herkomst van de criteria is met een W (wetgeving) en een B (beleid politie) gemarkeerd. Het toevoegen van de herkomst is gebaseerd op de gebruikte brondocumenten. Een W werd toegekend als de herkomst rechtstreeks herleidbaar was naar een wet, anders werd het een B. Tevens kan een criteria een W hebben, terwijl daarvan afgeleide criteria een B hebben gekregen. Ter verduidelijking het voorbeeld van het gebruik van basisregistraties. Voorzieningen moeten van de gegevens in die registraties gebruik maken. De politie heeft besloten om niet iedere voorziening afzonderlijk met een basisregistratie te koppelen, maar hiervoor kernregisters te gaan gebruiken. Het gebruik van de basisregistratie is dan een W, terwijl het gebruik maken van het kernregister een B is.

Volwassenheid:
Het resultaat van de toetsing is uitgedrukt in een volwassenheidsniveau voor de volledige toets en per principe. Het volwassenheidsniveau wordt uitgedrukt in een getal, 0 tot en met 3. De niveaus hebben de volgende betekenis (bron: Vooronderzoek_PSbD_Highrisk_applicaties v1.doc):

- Niveau 0: Er is geen specifieke aandacht voor PSbD op basis van het (politie)beleid.
- Niveau 1: Er is wel specifieke aandacht op het gebied van PSbD, maar die is niet toereikend om te voldoen aan de wet (Wpg) op basis van het (politie)beleid.
- Niveau 2: Er is wel specifieke aandacht op het gebied van PSbD en is afdoende om te voldoen aan de wet (Wpg), maar niet toereikend voor het (politie)beleid.
    - Wpg compliant
- Niveau 3: Het aandacht op het gebied van PSbD voldoet aan de wet en het vastgestelde (politie)beleid.
    - PSbD compliant

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[8].

De betekenis van de volwassenheidsniveau ’s is meetbaar gemaakt door het formuleren van de volgende bedrijfsregels. Het uitgangspunt hierbij is dat wettelijke criteria zwaarder wegen dan beleidscriteria.

[8] Bijlage 1: Uitgangspunt bij compliance

Bedrijfsregels volwassenheidsniveau
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