0-meting Privacy & Security by Design

Amazone

10.2.e

Definitief

Versie 1.0

Versie datum 2 april 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	
0.9	03-08-2018	Review aanpassingen verwerkt	
0.91	02-11-2018	Aanpassingen nav feedback verwerkt	
1.0	02-04-2019	Rapport definitief gemaakt na wederzijds akkoord	

Review commentaar

Versie	Wanneer	Wie	Functie
0.9	3-8-2018	10.2.e	Adviseur Architectuur en modellering
0.91	2-11-2018	10.2.e	Adviseur Architectuur en modellering

© 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

Inleiding

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

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

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

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

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 Amazone	10.2.e	IV Expert
	10.2.e	Functioneel beheer
	10.2.e	Functioneel beheer
	10.2.e	Product owner
	10.2.e	Software ontwikkelaar

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

Gespreksdatum	Nummer meting	Toelichting
30/05/2018	2018053001	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

Amazone

Amazone is een registratiesysteem voor veelplegers en andere doelgroepen. Veelplegers worden in dit monitoringsysteem van doelgroepen geregistreerd en vervolgens gegroepeerd tot een doelgroep. Dit biedt de politie tal van voordelen op het gebied van de aanpak van criminaliteit en monitoren.

Amazone wordt medio 2019 opgenomen in 'Vernieuwend registreren'.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Toelichting
Verzamelen	x	
Vastleggen	x	
Ordenen	x	
Bewaren	x	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	x	
Wijzigen (het bestaande aanpassen)	x	
Opvragen	x	
Raadplegen	x	
Gebruiken	x	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	x	OM, reclassering, gemeenten. Verstrekking kan ook gebeuren door email adressen zijn buiten overheid. Op dit moment worden er bij 8 eenheden gegevens verstrekt aan gemeenten.
Samenbrengen	x	
Met elkaar in verband brengen		
Afscherming	x	Onder andere beslotenheid
Uitwissen (weghalen/verwijderen zonder vernietigen)	x	Er zijn back-ups, maar deze zijn nog nooit gebruikt.
Vernietigen	x	Vernietigen door functioneel beheer ongeveer 1 maand na verwijderen vanuit archiveren door gebruiker.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	x	
Onderzoek rechtsorde bepaald geval	Artikel 9	x	
Informatiepositie	Artikel 10	x	
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13		

Artikel 8 (lid 1) Wpg: verwerking met het oog op de uitvoering van de dagelijkse politietaak

Artikel 9 (lid 1) Wpg: gerichte verwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval

Artikel 10 (lid 1) Wpg: gerichte verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde

Artikel 12 (lid 1) Wpg: verwerking met het oog op de controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens.

Artikel 13 Wpg: de politiegegevens van artikel 8, 9 en 10 Wpg mogen verder worden verwerkt ten behoeve van de ondersteuning van de politietaak

Eindscore

Amazone scoort een volwassenheidsniveau 1. Dit houdt in dat Amazone 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 Amazone een score van 42% en op de criteria van het politiebeleid een score van 67%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'doelbinding', 'bewaren en vernietigen' en 'informatiebeveiliging' er negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Gezien overgang van Amazone naar 'Vernieuwend registeren' in 2019 raden we ook aan om af te wegen in welke applicatie de actiepunten gerealiseerd moeten worden.

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

- **(Wet, art 3 lid 1) De verwerkingsgrondslag van de verwerkte gegevens moet vastgelegd worden. [p3c1]**
- **(Wet, art 3 lid 1) Er moeten meerdere verwerkingsgrondslagen van een verwerkt gegevens vastgelegd kunnen worden. [p3c2]**
- **(Wet, art 32) De volledige audittrail moet worden geregistreerd. Voor de migratie naar OPP moet rekening gehouden worden met het nieuwe auditbeleid. [p4c1]**
- **(Wet, art 6) Toets of aparte autorisatie op basis van ATL voor bepaalde groepen gebruikers en/of voor bepaalde functionaliteit noodzakelijk is en draag zorg voor realisatie. [p5c2]**
- **(Wet, art 4a) Zorg dat alle kenmerken van de te verwerken gegevens worden vastgelegd. [p6c6]**
- **(Wet, art 14) Maak een analyse van de gegevensverwerkende proces op basis van de generieke selectielijst. [p8c1]**
- **(Wet, art 8/9/10/12/14) Er moet voldaan worden aan de wettelijke bepalingen met betrekking tot het bewaren vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- **(Wet, archiefwet) De verwerkte gegevens moeten voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen. [p8c3]**
- **(Wet, art 14 lid 4) Amazone moet gegevens beschikbaar stellen aan voorzieningen ten behoeve van het duurzaam bewaren. [p8c9]**
- **(Wet, art 4a lid 2) Alleen de poortwachter mogen toegang hebben tot de verwijderde gegevens. [p8c10]**
- **(Wet, art 4a lid 2) Zorg dat er informatiebeveiligingseisen worden opgesteld mede aan de hand van de resultaten uit de risicoanalyse. [p9c2]**
- **(Wet, art 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt. [p9c3]**

Aandachtspunt:

- Er moet structureel getoetst worden op het gebruik van de standaarden.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Amazone	30/05/2018	2.0	42%	65%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	83%	2
PDCA-cyclus	M	-	NVT	63%	2
Doelbinding	Z	-	0%	33%	0
Verantwoording	Z	-	75%	0%	1
Autorisatie	Z	-	83%	70%	1
Metagegevens	Z	-	50%	50%	1
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	17%	0%	0
Informatiebeveiliging	Z	-	0%	33%	0
Privacy by default	Z	-	100%	100%	3
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	86%	2
TOTALEN TOETSING		-	42%	65%	

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

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 tenminste 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 het principe van eenmalige vastlegging heeft Amazone volwassenheidsniveau 2 behaald. Amazone voldoet volledig aan de aan de wet (Wpg), maar nog niet volledig aan het (politie)beleid. Om te voldoen aan het beleid moet Amazone gebruik gaan maken van referentiegegevens voor de lijst met organisatorische eenheden. Er zal hiervoor contact moeten worden opgenomen met de afdeling GGB.

Actiepunten:

- (Beleid) Voor de organisatorische eenheden moet gebruik gemaakt worden van referentiegegevens in plaats van een eigen lijst. [p1c1]

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

1.2 PDCA-cyclus

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

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

Op het principe voor de PDCA-Cyclus heeft Amazone volwassenheidsniveau 2 behaald. Dat houdt in dat er volledig wordt voldaan aan de aan de wet (Wpg), maar dat er nog niet volledig wordt voldaan aan het (politie)beleid. Hiervoor zal er meer aandacht moeten komen voor stuurinformatie uit Amazone, beheer van processen en daarnaast het structureel controleren van de doelgroepen.

Actiepunten:

- (Beleid) Er moet stuurinformatie geleverd worden voor de reguliere PDCA cyclus. De stuurinformatie moet informatie bevatten over de omvang van de gegevensverwerking, de kwaliteit van gegevens, aantallen gebruikers, aantallen verstrekkingen, het beheer van autorisaties, beveiligingsmaatregelen en –incidenten. [p2c1]
- (Beleid) Richt een structurele controle in op de doelstelling en de actualiteit van doelgroepen en gekoppelde VSA's. [p2c2]
- (Beleid) Zoek voor het beheer van processen aansluiting bij bedrijfsarchitectuur en procesbeheer. [p2c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	63%	2

1.3 Doelbinding

"*Persoonsgegevens worden alleen verwerkt als daar een gerechtvaardigd doel voor bestaat en ze worden niet verder verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel.*"

Voor elke verwerking is het van belang om te bepalen voor welk doel de gegevens worden verwerkt. Op basis van de doelbinding kan worden gerechtvaardigd waarom (politie)gegevens verwerkt mogen worden.

Amazone scoort op het principe doelbinding (volwassenheidsniveau 0) een onvoldoende. In Amazone worden gegevens verwerkt die vallen onder de Wpg grondslagen 8, 9 en 10. Het is belangrijk om onderscheid te kunnen maken naar deze grondslagen omdat ze verschillende maximale verwerkingstermijnen kennen. Om te kunnen voldoen aan de Wpg mogen gegevens nooit langer verwerkt worden als de maximale verwerkingstermijn.

Actiepunten:

- **(Wet, art 3 lid 1) De verwerkingsgrondslag van de verwerkte gegevens moet vastgelegd worden. [p3c1]**
- **(Wet, art 3 lid 1) Er moeten meerdere verwerkingsgrondslagen van een verwerkt gegevens vastgelegd kunnen worden als dat van toepassing is. [p3c2]**
- (Beleid) Indien mogelijk moet een er een automatische herleiding zijn van de verwerkingsgrondslag. [p3c3]
- (Beleid) De automatisch afgeleide verwerkingsgrondslag moet aangepast kunnen worden door de gebruiker. [p3c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	0%	33%	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.

Op dit principe is een volwassenheidsniveau 1 gemeten. Dat wordt veroorzaakt doordat in Amazone niet de volledige audittrail wordt geregistreerd. Daarnaast is de database administrator in staat om de audittrail te wijzigen.

Actiepunten:

- **(Wet, art 32) De volledige audittrail moet worden geregistreerd. Voor de migratie naar OPP moet rekening gehouden worden met het nieuwe auditbeleid. [p4c1]**
- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. Ook niet door een database administrator. [p4c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	75%	0%	1

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.

Amazone heeft voor het raadplegen geen eigen autorisatiestructuur. Er wordt gebruik gemaakt van de autorisaties in de BVH en de BVI. De rollen coördinator en functioneel beheer (alle rollen met meer rechten dan raadplegen) lopen via de ATL tool. Dat maakt dat Amazone voor dit principe niet volledig voldoet aan de wettelijke eisen. Daarnaast heeft Amazone geen eigen rapportage mogelijkheid voor het gebruik van de autorisaties.

Actiepunten:

- (Beleid) Toets of aparte autorisatie op basis van IAM voor bepaalde groepen gebruikers en/of voor bepaalde functionaliteit noodzakelijk is en draag zorg voor realisatie. [p5c1]
- **(Wet, art 6) Toets of aparte autorisatie op basis van ATL voor bepaalde groepen gebruikers en/of voor bepaalde functionaliteit noodzakelijk is en draag zorg voor realisatie. [p5c2]**
- (Beleid) Toets of na het aanpassen van de BVI de besloten doelgroepen niet meer getoond worden. [p5c3]
- (Beleid) Ontwikkel naast gebruikerslogging in BVH ook een standaard rapportage voor Amazone. [p5c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	83%	70%	1

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.

In Amazone worden nog niet alle kenmerken van de te verwerken gegevens vastgelegd. Dat zorgt voor een score van 50% voor het voldoen aan de wet. Daarnaast zijn er een aantal actiepunten om te voldoen aan het beleid. Dit betreft het gebruik van TMR, het geautomatiseerd afleiden en vastleggen van metagegevens en als laatste het daadwerkelijk gebruik van de metagegevens.

Actiepunten:

- (Beleid) Pas het Toepassingsprofiel Metagegevens Politie (TMP) toe zodra dit gereed is. Tot die tijd moet het Toepassingsprofiel Metagegevens Rijk (TMR) gebruikt worden. [p6c4]
- (Beleid) Borg dat het Toepassingsprofiel Metagegevens Rijk (TMR) wordt toegepast bij de migratie van Amazone naar OPP. [p6c4]
- **(Wet, art 4a) Zorg dat alle kenmerken van de te verwerken gegevens worden vastgelegd. [p6c6]**
- (Beleid) Zorg dat metagegevens die daar voor in aanmerking komen geautomatiseerd worden afgeleid en vastgelegd. [p6c7]
- (Beleid) Zorg dat metagegevens daadwerkelijk gebruikt worden voor audittrails en managementrapportages. [p6c9]

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

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.

Amazone voldoet aan alle beleidscriteria voor kwaliteitszorg. Er zijn geen wettelijke eisen voor kwaliteitszorg. Dat maakt dat Amazone voor kwaliteitszorg het hoogste volwassenheidsniveau heeft behaald.

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

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.

Amazone heeft voor dit principe het laagste mogelijke volwassenheidsniveau gehaald. Ten aanzien van de wettelijke eisen geldt dat Amazone alleen aan de eis voldoet dat de bron (BVH) gevolgd moet worden als daar een gegeven verwijderd of vernietigd wordt. Amazone voldoet aan geen enkele wettelijke of beleidsmatige eis als het gaat om de bewaartermijnen van de doelgroepen.

Actiepunten:

- **(Wet, art 14) Toets of de huidige vernietigingstermijn in Amazone, 14 dagen na verwijderen, toereikend is. Vanuit de Wpg is de termijn voor vernietigen maximaal 5 jaar. [p8c1]**
- **(Wet, art 8/9/10/12/14) Er moet voldaan worden aan de wettelijke bepalingen met betrekking tot het bewaren vernietigen en archiveren van (persoons)gegevens. [p8c2]**
- **(Wet, archiefwet) De verwerkte gegevens moeten voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen. [p8c3]**
- (Beleid) Gegevens moeten op basis van de geldende termijnen geautomatiseerd worden verwijderd en vernietigd. [p8c4]
- (Beleid) Toets of de DUTO standaard (Duurzame toegankelijkheid) van toepassing is op Amazone. Als deze van toepassing is borg dan dat Amazone voldoet aan de DUTO standaard. [p8c8]
- **(Wet, art 14 lid 4) Amazone moet gegevens beschikbaar stellen aan voorzieningen ten behoeve van het duurzaam bewaren. [p8c9]**
- **(Wet, art 8) Alleen de poortwachter mogen toegang hebben tot de verwijderde gegevens. [p8c10]**

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

1.9 Informatiebeveiliging

"*De informatievoorziening wordt beveiligd met een adequaat stelsel van maatregelen op basis van risicobeheersing*"

Het belang van informatiebeveiliging is op basis van risicobeheersing al mogelijke schadelijke gevolgen door bedreigingen van de informatievoorziening op een bewuste manier afweegt tegen kosten en belemmeringen van beveiligingsmaatregelen. Met daarbij in acht nemen dat de politie een verantwoordelijkheid en verplichting heeft om de gegevens van de burgers te beschermen.

Het is van belang regelmatige de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. Amazone heeft voor dit principe het laagst mogelijk volwassenheidsniveau behaald. Het enige criterium waar aan voldaan wordt is dat er gebruik gemaakt wordt van de aanwezige generieke voorzieningen voor informatiebeveiliging. Het advies hier luidt om een risico analyse uit te laten voeren. Naar aanleiding van de resultaten uit de analyse moet er gekeken worden welke informatiebeveiligingseisen genomen moeten worden en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's in beeld zijn en periodiek beheert worden.

Actiepunten:

- (Beleid): Zorg dat er een nieuwe risicoanalyse op het gebied van informatiebeveiliging uitgevoerd gaat worden [p9c1].
    - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse [p9c2].**
    - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening [p9c3].**
    - (Beleid): Zorg dat de restrisco's periodiek beheert worden [p9c7].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	33%	0

1.10 Privacy by default

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

Amazone haalt hier de maximale score omdat er gebruik gemaakt wordt van de persoonsgegevens uit BVH, alle gegevens binnen het doel van de verzameling vallen, er is sprake van een opt-in regime en er wordt voor de oefen- en testomgevingen gebruikt gemaakt van Privacy Enhancement Technology.

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.

Amazone maakt voor de gegevensuitwisseling gebruik van een standaard formaat in XML. Deze standaard is tot nu toe nog nooit gewijzigd. Er wordt niet structureel gecontroleerd of de standaard overal correct gebruikt wordt. Amazone voldoet hierdoor aan het hoogste volwassenheidsniveau, met een aandachtspunt voor de toetsing.

Aandachtspunt:

- Er moet structureel getoetst worden op het gebruik van de standaarden.

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

Amazone voldoet aan het grootste deel van beleidsmatige eisen. Dit brengt Amazone op een volwassenheidsniveau van 2. De enige actiepunten liggen bij de uitvoeringsverantwoordelijke en het verstrekken buiten het overheidsdomein.

Actiepunten:

- (Beleid) Zorg dat de uitvoeringsverantwoordelijke ondersteund wordt met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. [p12c4]
- (Beleid) Borgen dat er niet verstrekt wordt naar email adressen buiten het overheidsdomein. [p12c6]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	86%	2

2. Verantwoording toetsing

Toetsingscriteria

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

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van compliancy 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[3].

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

[3] Bijlage 1: Uitgangspunt bij compliance

Bedrijfsregels volwassenheidsniveau
Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien de voorziening of het principe aan geen enkel wettelijk criterium voldoet

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

a: aan ten minste 35% van de wettelijke criteria, maar niet alle wordt geheel of ten dele voldaan.
b: Geen wettelijke criteria zijn benoemd en aan tenminste 35% maar minder dan 50% van de wettelijke criteria wordt voldaan.
c: Geen beleidscriteria zijn benoemd en aan tenminste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

a: de voorziening of het principe voldoet aan alle wettelijke criteria, maar niet aan alle beleidscriteria
b: Geen wettelijke criteria zijn benoemd en aan tenminste 50% maar minder dan 100% van de wettelijke criteria wordt voldaan.
c: Geen beleidscriteria zijn benoemd en aan tenminste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien aan een van de volgende voorwaarden wordt voldaan:

a: de voorziening voldoet aan alle wettelijke en aan alle beleidscriteria.
b: de voorziening voldoet aan alle beleidscriteria en er geen wettelijke criteria zijn benoemd
c: de voorziening voldoet aan alle wettelijke criteria en er geen beleidscriteria zijn benoemd

NVT : Een principe of toetsing moet de indicatie NVT krijgen, indien wordt voldaan aan een van de volgende voorwaarden:

a: Alle criteria van een principe of een toetsing zijn met NVT gewaardeerd
b: Alle criteria van een principe of een toetsing zijn met een NVT en/of een BS gewaardeerd

BS : Een principe of toetsing moet de indicatie BS krijgen, indien alle criteria van een principe of een toetsing met BS zijn gewaardeerd.

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

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

Weegfactor	Licht (L)	Middel (M)	Zwaar (Z)
Aantal	1	3	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 compliancy van de getoetste voorziening gegeven. Tevens wordt geen enkele garantie gegeven inzake de juistheid of volledigheid van de checklist als gevolg van veranderende wet- of regelgeving.

Bijlage 1: Uitgangspunt bij compliance

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

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