0-meting Privacy & Security by Design

Raffinaderij

10.2.e

Definitief

Versie 1.0

Versie datum 19 februari 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	21-12-2018	Reviewen
0.9	21-12-2018	Aanpassingen op basis van review
1.0	19-2-2019	Rapport definitief gemaakt na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.9	21-12-2018	10.2.e	Gegevensautoriteit
1.0	19-2-2019	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 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 Raffinaderij. 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 Raffinaderij

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 Raffinaderij	10.2.e	Product Owner
		Programmamanager
		10.2.e
		Dienst IM, Team advies
		10.2.e

	Naam	Functie
Team Auditing en Kwaliteit (aanwezig als gast)	10.2.e	Auditor

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

Gespreksdatum	Nummer meting	Toelichting
29/11/2018	2018112901	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

Raffinaderij

Omschrijving applicatie

De politie wordt in het opsporingsproces steeds vaker geconfronteerd met grote hoeveelheden gestructureerde en ongestructureerde data waaruit nuttige informatie kan worden verkregen.
Raffinaderij biedt rechercheurs en analisten de mogelijkheid om snel grote hoeveelheden politiegegevens in samenhang met elkaar te analyseren en visualiseren. Zo kan data uit opsporingsonderzoeken (denk aan bijvoorbeeld 10.2.c eenvoudig worden ontsloten en geanalyseerd. Door inzicht te hebben in het geheel (er kan worden gekeken over verschillende onderzoeken heen en door de verschillende data heen in plaats van alleen te kijken naar óf OSINT informatie óf digitaal beslag óf de registratie in politiesystemen etc.), kunn10.2.c juist in een vroeg stadium worden ontkracht.
De afgelopen jaren heeft Raffinaderij als pilot gedraaid op een aantal landelijke dossiers. Vanwege de positieve ervaringen die zijn opgedaan wordt Raffinaderij de komende jaren stapsgewijs verder geïmplementeerd en geborgd in de organisatie. Het belangrijkste achterliggende doel is om het proces van waarheidsvinding in de opsporing te versnellen en verbeteren en inbreuken op de rechtsorde door bepaalde vormen van (zware) criminaliteit te voorkomen en/of op effectievere wijze aan te pakken.

Raffinaderij bestaat uit 10.2.c De raffinaderij wordt nu ingezet binnen thema's 10.2.c .
De raffinaderij heeft nu bijna 170 gebruikers en maximaal 40 gelijktijdige gebruikers.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen		
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	Alleen voor eigen onderzoek. Aanpassing vindt plaats in de bron.
Wijzigen (het bestaande aanpassen)	X	Alleen voor eigen onderzoek. Aanpassing vindt plaats in de bron
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Bijvoorbeeld Graph in PDF of Excel via mail.
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	Autorisatie obv Summ-IT
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Autorisatie kan dichtgezet worden.
Vernietigen	X	Brondata kan niet vernietigd worden. Een investigation kan wel vernietigd worden.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9	X	
Informatiepositie	Artikel 10	10b	
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11	X	
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13	X	FIU verdachte transacties

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 raffinaderij scoort een volwassenheidsniveau 1. Dit houdt in dat de raffinaderij 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 raffinaderij een score van 74% en op de criteria van het politiebeleid een score van 72%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'bewaren en vernietigen', 'eenmalige vastlegging' en 'doelbinding' er negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Daarnaast zijn er een aantal aandachtspunten.

De raffinaderij is geen registratief systeem. De gegevens worden overgenomen uit de bronsystemen. Daardoor zijn de meeste actiepunten vanuit de wet ook gericht op het volgen van de bron.

Actiepunten:

- **(Wet, art 32a Wpg) Zorg dat zodra de gegevens uit de raffinaderij via een gegevensdienstenlaag ter beschikking worden gesteld (p1c8) de metagegevens met betrekking tot de verwerkingsgrondslag en verwerkingstermijn de gegevens begeleiden. [p3c10]**
- **(Wet, art 8, 9, 10, 12, 14) Zorg dat de raffinaderij de bronsystemen volgt voor het vernietigen van gegevens. Op dit moment wordt alleen het verwijderen in de bronsystemen gevolgd. [p8c1] [p8c2] [p8c5]**
- **(Wet, art 8) Onderzoek of het gewenst is om gegevens die verwijderd zijn in een bronsysteem direct te vernietigen in de raffinaderij en neem zo nodig maatregelen. [p8c10]**
- **(Wet, art 8) Zorg dat de poortwachter als enige toegang krijgt tot de verwijderde gegevens. [p8c10]**

Aandachtspunten:

- Zorg dat bij nieuwe ontwikkeling wordt het politiegegevensmodel (PGM) wordt toegepast. [p6c5]
- Bij terugkerende problemen met import bestanden moet naar een structurele oplossing worden gezocht. [p7c5].
- De raffinaderij gebruikt nu 10.2.c .

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Raffinaderij	29/11/2018	2.0	76%	72%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	50%	2
PDCA-cyclus	M	-	100%	75%	2
Doelbinding	Z	-	83%	100%	1
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	100%	60%	2
Metagegevens	Z	-	100%	80%	2
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	13%	NVT	0
Informatiebeveiliging	Z	-	100%	60%	2
Privacy by default	Z	-	100%	67%	2
Toepassing standaarden	L	-	NVT	NVT	NVT
Verantwoordelijkheden belegd	M	-	NVT	80%	2
TOTALEN TOETSING		-	76%	72%	

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.

Het grootste deel van de gegevens van onderzoeken in de raffinaderij is afkomstig uit de politiesystemen. Dat betekent dat de raffinaderij afhankelijk is van de kwaliteit van de gegevens in die systemen. De meeste criteria van dit principe zijn daardoor niet van toepassing.

Actiepunten:

- (Beleid) Zorg dat de gegevens uit de raffinaderij niet meer ter beschikking worden gesteld via bestanden in email maar via een gegevensdienstenlaag. [p1c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	50%	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.

De raffinaderij voldoet deels aan de criteria voor de PDCA-cyclus. Maar de rapportages en het beheer van gegevens moeten nog uitgebreid worden. Er is in 2014 al een GEB uitgevoerd.

Actiepunten:

- (Beleid) Zorg dat naast de huidige rapportages voor aantallen gebruikers er ook rapportage ontwikkeld worden op basis van proces indicatoren om het effect van de raffinaderij te meten. [p2c1]
- (Beleid) Borg dat met het verlaten van de pilot fase het beheer van de processen onderdeel wordt van de PDCA cyclus. [p2c3]
- (Beleid) Onderzoek of vernietigen toegevoegd moet worden aan de logging van objecten en borg zo nodig de maatregelen. [p2c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	100%	75%	2

1.3 Doelbinding

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

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

De raffinaderij is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsysteem wordt de doelbinding geregistreerd. Deze wordt automatisch overgenomen in de raffinaderij. Hierdoor voldoet de raffinaderij aan bijna alle criteria.
Als er datasets worden ingelezen die vallen onder artikel 13 dan ligt de verantwoordelijkheid voor het artikel 13 protocol bij de leverancier van de dataset. Dit is bijvoorbeeld het geval bij 10.2.c

Actiepunten:

- **(Wet, art 32a Wpg) Zorg dat zodra de gegevens uit de raffinaderij via een gegevensdienstenlaag ter beschikking worden gesteld (p1c8) de metagegevens met betrekking tot de verwerkingsgrondslag en verwerkingstermijn de gegevens begeleiden. [p3c10]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	83%	100%	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.

Waar nog naar kan worden gekeken is naar de mogelijkheid tot manipulatie van de audittrail. Er is een speciale audit functionaliteit die (tegen licentiekosten) aan kan worden gezet 10.2.c waarbij de acties van o.a. de database administrator kunnen worden geregistreerd. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten Het is van belang dat de raffinaderij bekend is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's).

Actiepunten:

- (Beleid) Zorg dat de audittrail door niemand gemuteerd kan worden. Ook niet door ontwikkelaars of 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 beheerslast op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

De raffinaderij is nog niet beschikbaar in de KA omgeving. Op dit moment wordt nog gebruik gemaakt van de transferium omgeving. Er is daardoor ook geen aansluiting mogelijk met IAM en ATL. Afgezien van deze twee punten voldoet de raffinaderij aan alle criteria voor autorisatie.

Actiepunten:

- (Beleid) Zorg dat, zodra de raffinaderij beschikbaar komt voor de KA omgeving, voor het verlenen van toegang gebruik gaat maken van de generieke IAM- voorziening voor het verifiëren van identiteiten. [p5c1]
- (Beleid) Zorg dat, zodra de raffinaderij beschikbaar komt voor de KA omgeving, voor het verlenen van toegang afwijkend van IAM gebruik gemaakt gaat worden van de generieke autorisatietool voor leidinggevenden. [p5c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	60%	2

1.6 Metagegevens

"*Gegevens worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de juistheid en de rechtmatigheid van de gegevensverwerking te waarborgen*"

Om de juistheid en de rechtmatigheid van het gebruik te kunnen waarborgen worden metagegevens vastgelegd over bijvoorbeeld de context, inhoud, structuur, vorm en gedrag evenals het beheer en gebruik. Deze metagegevens bepalen de wijze waarop deze gegevens (mogen) worden verwerkt.

De bedrijfsbegrippen van de raffinaderij zijn beschikbaar via Agora, de kenmerken van de gegevens worden vastgelegd, metagegevens worden als dat mogelijk is geautomatiseerd afgeleid en de metagegevens worden daadwerkelijk gebruikt. Daarmee voldoet de raffinaderij aan bijna alle criteria. Is slechts één actiepunt en één aandachtspunt.

Actiepunten:

- (Beleid) Bestudeer de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is. [p6c4].

Aandachtspunten:

- Zorg dat bij nieuwe ontwikkeling wordt het politiegegevensmodel (PGM) wordt toegepast. [p6c5]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	100%	80%	2

1.7 Kwaliteitszorg

"*De informatievoorziening waarborgt de kwaliteit van de gegevensverwerking*"

Van de politie wordt verwacht dat de kwaliteitseisen (juistheid, doeltreffendheid, controleerbaarheid) van de te verwerken gegevens van te voren bekend zijn. Waarborgen voor gegevenskwaliteit zijn onmisbaar om de juiste werking van systemen en de integriteit van de informatievoorziening als geheel te waarborgen.

De gegevens in de raffinaderij komen uit de bronsystemen. In de bronsystemen ligt de zorg voor kwaliteit. De raffinaderij doet wel controles op bijvoorbeeld 10.2.d s. Daarmee wordt aan alle criteria voldaan.
Er is wel aandachtspunt omdat problemen met de import nu alleen ad-hoc worden opgelost.

Aandachtspunten:

- Bij terugkerende problemen met import bestanden moet naar een structurele oplossing worden gezocht. [p7c5].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[3]	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.

De raffinaderij is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsystemen mogen gegevens niet langer worden verwerkt dan is toegestaan en worden ze vernietigd zodra ze niet langer nodig zijn. De raffinaderij moet de bron volgen voor het verwijderen en vernietigen van gegevens.

Actiepunten

- **(Wet, art 8, 9, 10, 12, 14) Zorg dat de raffinaderij de bronsystemen volgt voor het vernietigen van gegevens. Op dit moment wordt alleen het verwijderen in de bronsystemen gevolgd. [p8c1] [p8c2] [p8c5]**
- **(Wet, art 8) Onderzoek of het gewenst is om gegevens die verwijderd zijn in een bronsysteem direct te vernietigen in de raffinaderij en neem zo nodig maatregelen. [p8c10]**
- **(Wet, art 8) Zorg dat de poortwachter als enige toegang krijgt tot de verwijderde gegevens. [p8c10]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	10%	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 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.

Er is recent een risico analyse uitgevoerd voor de raffinaderij. Maar er wordt nog niet voldaan aan criteria om er nog geen gebruik wordt gemaakt van IAM en ATL voor autorisatie en omdat er nog verbeteringen mogelijk met het beheer van de restrisico's.

Actiepunten:

- (Beleid) Zorg dat voldaan wordt aan de generieke voorzieningen voor informatie beveiliging door gebruik te gaan maken van IAM en ATL zoals genoemd in de actiepunten p5c1 en p5c2. [p9c4] [p9c5]
- (Beleid) Onderzoek of de restrisico's voldoende worden beheerd en neem zo nodig maatregelen. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	100%	60%	2

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.

Alleen de noodzakelijke gegevens worden ingelezen in de raffinaderij. Er is slechts één actiepunt. De testomgeving moet gebruik maken van data die niet is herleiden naar personen.

Actiepunten:

- (Beleid) Onderzoek of het is toegestaan om onderzoeken die niet meer onder de rechter zijn (onherroepelijk vonnis) te gebruiken als testdata en borg zo nodig de maatregelen. [p10c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	67%	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.

Dit principe is niet van toepassing op de raffinaderij omdat de gegevens ongewijzigd worden overgenomen uit de bronsystemen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[4]	NVT	NVT

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

Er is slechts één actiepunt voor eenduidige belegging van verantwoordelijkheden. En dat betreft de opleiding van 2 weken voor de gebruikers. Het is niet altijd duidelijk voor de uitvoeringsverantwoordelijke waarom dit noodzakelijk is en waarom het niet sneller kan.

Actiepunten:

- (Beleid) Zorg dat de uitvoeringsverantwoordelijkheden goed geïnformeerd worden over de mogelijkheden die de raffinaderij beidt en de opleidingsinspanning die daar bij hoort. [p12c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[5]	80%	2

[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 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.
- 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[6].

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 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