0-meting Privacy & Security by Design

ANPR / Falcon-i

10.2.e

Definitief

Versie 1.0

Versie datum 20 maart 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	02-11-2018	Reviewen
0.9	16-11-2018	Aanpassingen op basis van review
1.0	20-3-2019	Definitief na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.9	02-11-2018	10.2.e	Gegevensautoriteit

Inhoudsopgave

Inleiding

Eind 2015 heeft de Auditdienst Rijk (ADR) gerapporteerd over uitgevoerde (externe) privacy audit en dat heeft aangetoond dat er op het gebied van Privacy en Security verbeteringen nodig zijn. Het verbeterprogramma Wpg en IB is daarna gestart om 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 Falcon-i van ANPR (Automatic Number Plate Recognition). 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 ANPR/Falcon-i

Algemeen

Doel
Het doel van de PSbD 0-meting is het transparant in beeld brengen wat de actuele volwassenheid van highriskapplicaties op het gebied van PSbD. Vanuit deze 0-meting kan er op basis van de actiepunten toegewerkt worden naar een applicatie die PSbD compliant (Wpg compliant in het bijzonder) is. Om dit doel te bereiken is er gebruik gemaakt van uitvoeringskader PSbD wat in april 2018 is vastgesteld.

Doelgroep
De landelijke portefeuillehouder kan dit document gebruiken om maatregelen te nemen om de applicatie PSbD compliant te maken. De gegevensautoriteit heeft op 22 november 2017 een brief naar de landelijke portefeuillehouder gestuurd omtrent het PSbD compliant maken van applicaties. Het portefeuilleteam voert in overleg met de portefeuillehouder de maatregelen uit. Waarbij de productowner de actiepunten prioriteert en verwerkt op de productbacklog.

Aanwezigen 0-meting

	Naam	Functie
Directe betrokkenen 0-meting ANPR/Falcon-i	10.2.e	Afdeling Programmamanagement (Directie Operatien)
	10.2.e	Functioneel beheer
	10.2.e	Privacy functionaris
	10.2.e	Programmamanager ANPR
	10.2.e	Technisch projectleider
	10.2.e	Ondersteuner privacy functionaris

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

Gespreksdatum	Nummer meting	Toelichting
20-06-2018	2018062001	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

ANPR/Falcon-i

Omschrijving applicatie:
ANPR-camera's scannen kentekens op het wegennet in Nederland. Als een kenteken voorkomt in een referentiebestand geeft dit systeem een hit. Een hit is bijvoorbeeld een gestolen auto of een openstaande boete. ANPR is daarmee een zeer efficiënt opsporing- en handhavingsmiddel.
ANPR bestaat uit camera's, infrastructuur langs de weg, distributie naar partners, toegang naar het politie netwerk, opslag en uiteindelijk de backoffice applicatie. De backoffice applicatie is Falcon-i van de firma NorthGate. Deze 0-meting betreft de applicatie Falcon-i.

Er wordt gewerkt aan een opvolger van Falcon-i genaamd Arendsoog. Deze is niet meegenomen in de 0-meting.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	x	
Vastleggen	X	Gaan ook naar BVI (Falcon-I heeft geen analyse) en live alarm.
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	Hit opvolging en analyse
Vergelijken	X	Hit-no-hit
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Naar BVI Exhibit document wordt handmatig bij PV gevoegd. Live alarm via falcon of app
Samenbrengen		
Met elkaar in verband brengen		
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Referentielijsten kunnen na verwijderen weer hersteld worden aan de hand van de excel lijsten van aanvrager.
Vernietigen	X	

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	X	Alleen 13.1

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

Falcon-i scoort een volwassenheidsniveau 1. Dit houdt in dat Falcon-i 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 Falcon-i een score van 46% en op de criteria van het politiebeleid een score van 60%. 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' en 'informatiebeveiliging' er zeer negatief uitspringen. Daarnaast hebben de principes 'autorisatie' en 'metagegevens' ook lage volwassenheidsniveau 's.

Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen.

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

- **(Wet, art. 4. Lid 1) De gegevens van de kernobjecten (voertuigen met een kentekenplaat die een camera gepasseerd zijn) zouden geverifieerd moeten worden in het kentekenregister van de RDW. [p1c3]**
- **(Wet, art 3 lid 1) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) de verwerkingsgrondslag van de verwerkte gegevens wordt opgenomen. Deze zou aangeleverd kunnen worden vanuit de bronsystemen zoals BVH, Summ-IT en OPP. [p3c1]**
- **(Wet, art 3 lid 1) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) meerdere verwerkingsgrondslagen per verwerkt gegeven opgenomen kunnen worden. [p3c2]**
- **(Wet, art 32a) Zorg dat het metagegeven met betrekking tot de verwerkingsgrondslag en de verwerkingstermijn het gegeven blijft begeleiden naar de data-analyse omgeving (de BVI) zodat daar ook de gegevens op de juiste wijze getoond of juist verwijderd worden. [p3c10]**
- **(Wet, art 4a) Zorg dat de toegangs- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. [p5c8]**
- **(Wet, art 4a) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) alle kenmerken van de te verwerken gegevens worden vastgelegd. In Falcon-i wordt al wel de volgende kenmerken vastgelegd: datum, doel, herkomst. In Falcon-i worden nog geen kenmerken vastgelegd zoals de Wpg grondslag van de verwerking. [p6c6]**
- **(Wet art. 4a lid 2) Zorg dat de informatiebeveiligingseisen mede op basis van de risicoanalyse bepaald worden. [p9c2]**
- **(Wet art. 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van realisatie in Falcon-i. [p9c3]**

Aandachtspunten:

- **(Wet, art. 4c) Zorg dat bij de ontwikkeling van Arendsoog getoetst wordt of er een GEB (Gegevensbescherming Effect Beoordeling) uitgevoerd moet worden en neem zo nodig maatregelen. Bijvoorbeeld in verband met de grootschalige gegevensverwerking. [p2c4]**
    - Nieuwe technologieën/projecten waarbij persoonsgegevens gebruikt worden (AVG en/of Wpg) zal altijd een GEB voor uitgevoerd moeten worden.
- (Beleid) Zorg dat de definities en bedrijfsbegrippen zoals die binnen de dienstverlening Falcon-i zijn afgestemd gedeeld worden met de afdeling GGB. [p6c1]
- **(Wet, art 14) Zorg dat bij de ontwikkeling van Arendsoog de gegevensverwerkende processen geanalyseerd worden op basis van de generieke selectielijst. [p8c1]**
- **(Wet, art 8/9/10/12/14) Toets of het vernietigen van alle gegevens na 1 jaar wellicht verruimd kan worden. [p8c2]**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
ANPR/Falcon-i	20-06-2018	1	46%	60%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	50%	100%	1
PDCA-cyclus	M	-	NVT	13%	0
Doelbinding	Z	-	0%	17%	0
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	50%	75%	1
Metagegevens	Z	-	50%	75%	1
Kwaliteitszorg	Z	-	NVT	56%	2
Bewaren en vernietigen	Z	-	100%	100%	3
Informatiebeveiliging	Z	-	0%	60%	0
Privacy by default	Z	-	100%	50%	2
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	79%	2
TOTALEN TOETSING		-	46%	60%	

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 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 het principe van eenmalige vastlegging heeft Falcon-i volwassenheidsniveau één behaald. Als de gegevens van de voertuigen gecontroleerd zouden worden in het kentekenregister van RDW zou Falcon-i de maximale score halen. Daarnaast is er een aandachtspunt voor kenobjecten in Arendsoog.

Actiepunten:

- **(Wet, art. 4. Lid 1) De gegevens van de kernobjecten (voertuigen met een kentekenplaat die een camera gepasseerd zijn) zouden geverifieerd moeten worden in het kentekenregister van de RDW. [p1c3]**

Aandachtspunten:

- (Beleid) De gegevens van de kernobjecten moeten in de opvolger van Falcon-i (Arendsoog) worden vastgelegd volgens het model van kernobjecten.[p1c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	50%	100%	1

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 Falcon-i volwassenheidsniveau 0 behaald. Dat is een zware onvoldoende. Dat wordt veroorzaakt door een slechte score op de criteria van beleid. Tijdens de 0-meting is aangegeven dat de betreffende actiepunten deels pas opgelost kunnen worden in de opvolger van Falcon-i (Arendsoog) en deels nog in de huidige situatie. De criteria vanuit de wet zijn niet van toepassing op Falcon-i maar in de toekomst wellicht wel voor Arendsoog.

Actiepunten:

- (Beleid) Zorg dat de opvolger van Falcon-i (Arendsoog) stuurinformatie in de reguliere plan- en rapportageproducten zoals jaarplannen en jaarverslagen ook onderdelen bevatten 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 opvolger van Falcon-i (Arendsoog) periodiek rapportages ten behoeve van de besturing van de gegevensverwerking oplevert. [p2c2]
- (Beleid) Zorg dat het beheer van processen onderdeel uit gaat maken van de PDCA cyclus. Er is aangegeven dat hier gewerkt wordt door een oprichting van een landelijke coördinatieteam Falcon-i. [p2c3]
- (Beleid) Zorg dat er vanuit strategische niveau meer strategie komt op verbeteringen en kwaliteit. [p2c7]

Aandachtspunten:

- **(Wet, art. 4c) Zorg dat bij de ontwikkeling van Arendsoog getoetst wordt of er een GEB (Gegevensbescherming Effect Beoordeling) uitgevoerd moet worden en neem zo nodig maatregelen. Bijvoorbeeld in verband met de grootschalige gegevensverwerking. [p2c4]**
    - Nieuwe technologieën/projecten waarbij persoonsgegevens gebruikt worden (AVG en/of Wpg) zal altijd een GEB voor uitgevoerd moeten worden. Een voorbeeld wat niet tijdens de 0-meting is besproken is de proeftuin in Roermond met het puntensysteem.

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.

In Falcon-i 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. Falcon-i heeft op dit principe een volwassenheidsniveau 0 behaald. Dat is een zware onvoldoende.

Actiepunten:

- **(Wet, art 3 lid 1) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) de verwerkingsgrondslag van de verwerkte gegevens wordt opgenomen. Deze zou aangeleverd kunnen worden vanuit de bronsystemen zoals BVH, Summ-IT en OPP. [p3c1]**
- **(Wet, art 3 lid 1) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) meerdere verwerkingsgrondslagen per verwerkt gegeven opgenomen kunnen worden. [p3c2]**
- (Beleid) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) de verwerkingsgrondslag, als deze niet wordt aangeleverd door het bronsysteem, zo mogelijk automatisch bepaald wordt. [p3c3]
- (Beleid) Zorg dat in (de opvolger van) Falcon-i (Arendsoog) de automatisch afgeleide verwerkingsgrondslag (als dat mogelijk is) door de gebruiker aangepast kan worden. [p3c4]
- (Beleid) Onderzoek of in Falcon-i de aanwezige Engelse verwerkingsgrondslag gebruikt worden als alternatieve vastlegging. [p3c5]
- **(Wet, art 32a) Zorg dat het metagegeven met betrekking tot de verwerkingsgrondslag en de verwerkingstermijn het gegeven blijft begeleiden naar de data-analyse omgeving (de BVI) zodat daar ook de gegevens op de juiste wijze getoond of juist verwijderd worden. [p3c10]**

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

Binnen Falcon-i is de audittrail nog niet optimaal beveiligt tegen manipulatie. Binnen de applicatie kunnen de gebruikers de audittrail niet manipuleren. Echter het is nu nog wel mogelijk dat een ontwikkelaar en/of beheerder de audittrail kan wijzigen zonder dat dit opgemerkt wordt. Een beheerder en/of ontwikkelaar moet een audittrail niet kunnen wijzigen zonder dat hiervan iets geregistreerd wordt. De registratie van handelingen moet beveiligd worden tegen manipulatie en moet waarborg bieden voor bewaring en goede toegankelijkheid. Het uiteindelijke doel is ervoor te zorgen dat de bewijskracht voor het verantwoordingsdoel niet in gevaar komt. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten. Het is van belang dat Falcon-i bekend is met het risico en dat het risico is geminimaliseerd en is geaccepteerd (restrisico's).

Actiepunten:

- (Beleid) Zorg dat de audittrail beveiligd is tegen manipulatie en indien dat niet mogelijk is zorg er dan voor dat het risico geminimaliseerd en geaccepteerd is. Dit staat op de backlog voor de nieuwe applicatie (Arendsoog). [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.

Op het principe autorisatie heeft ANPR een volwassenheidsniveau 1 gehaald. Dat wordt veroorzaak doordat er geen rapportagemogelijkheden zijn op het gebruik van autorisaties en er daardoor ook geen sturing mogelijk is op het gebruik van autorisaties is.

Actiepunten:

- (Beleid) Zorg dat in de opvolger van Falcon-i (Arendsoog) rapportages op het gebruik van autorisaties bevat. [p5c7]
- **(Wet, art 4a) Zorg dat de toegangs- en gebruiksrechten van gebruikers regelmatig worden gecontroleerd. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	50%	75%	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.

Op het principe metagegevens heeft Falcon-i volwassenheidsniveau 1 gehaald. Om te komen tot het volgende niveau moet aan het wettelijke criterium voldaan worden dat alle kenmerken van de verwerkte gegevens worden vastgelegd. Daarnaast is er het aandachtspunt om de definities en bedrijfsbegrippen te delen met de afdeling GGB.

Actiepunten:

- (Beleid) Zorg dat in de opvolger van Falcon-i (Arendsoog) het toepassingsprofiel metagegevens rijk (TMP) wordt toegepast. [p6c4]
- **(Wet, art 4a) Zorg dat in de opvolger van Falcon-i (Arendsoog) alle kenmerken van de te verwerken gegevens worden vastgelegd. In Falcon-i wordt al wel de volgende kenmerken vastgelegd: datum, doel, herkomst. In Falcon-i worden nog geen kenmerken vastgelegd zoals de Wpg grondslag van de verwerking. [p6c6]**
- (Beleid) Zorg dat metagegevens onderdeel uit gaan maken van de managementrapportages. [p6c9]

Aandachtspunten:

- (Beleid) Zorg dat de definities en bedrijfsbegrippen zoals die binnen de dienstverlening Falcon-i zijn afgestemd gedeeld worden met de afdeling GGB. [p6c1]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	50%	75%	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.

Voor het principe kwaliteitszorg zijn er alleen criteria vanuit beleid. De applicatie Falcon-i heeft hiervoor een volwassenheidsniveau 2 behaald. Om te komen tot het hoogste niveau moeten de kwaliteitseisen geformaliseerd, en gerealiseerd worden inclusief rapportages. Daarnaast is er een aandachtspunt met betrekking tot de stabiliteit van de verbindingen.

Actiepunten:

- (Beleid) Zorg dat in de opvolger van Falcon-i (Arendsoog) requirements met betrekking tot de kwaliteit van gegevens worden meegenomen. [p7c1]
- (Beleid) Zorg dat voor de opvolger van Falcon-i de nieuwe kwaliteitseisen zijn afgestemd met de beleidsverantwoordelijke. [p7c2]
- (Beleid) Zorg dat voor de opvolger van Falcon-i de realisatie van de nieuwe kwaliteitseisen geborgd wordt. [p7c3]
- (Beleid) Zorg dat er geautomatiseerd een rapport over de kwaliteit van gegevens kan worden samengesteld. [p7c7]
- (Beleid) Zorg dat uitgevoerde kwaliteitscontroles en de resultaten opgeslagen worden. [p7c8]

Aandachtspunten

- (Beleid) Volg de aanbevelingen op die uit het onderzoek van de dienst ICT komen naar de kwaliteit van de verbindingen. Hiermee wordt voorkomen dat metingen vernietigd worden omdat er meer dat n 10 minuten zit tussen de hit en de cameraregistratie.[p7c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[3]	56%	2

[3] 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 dit principe heeft Falcon-i het hoogst mogelijke volwassenheidsniveau.
Er zijn alleen aandachtspunten met betrekking tot de generieke selectielijst en het toetsen of de bewaartermijn van 1 jaar wellicht verruimd kan worden.

Aandachtspunten:

- **(Wet, art 14) Zorg dat bij de ontwikkeling van Arendsoog de gegevensverwerkende processen geanalyseerd worden op basis van de generieke selectielijst. [p8c1]**
- **(Wet, art 8/9/10/12/14) Toets of het vernietigen van alle gegevens na 1 jaar wellicht verruimd kan worden. [p8c2]**

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

Op dit principe heeft Falcon-i het laagst mogelijke volwassenheidsniveau behaald. Dat is een zware onvoldoende.
Om te komen tot een hoger volwassenheidsniveau moet er een risicoanalyse uitgevoerd worden. Als daar nieuwe informatiebeveiligingseisen uit komen dan zullen deze gerealiseerd moeten worden of als restrisico periodiek beheerd moeten worden.
NB: Tijdens het interview is er gerefereerd naar een recente risicoanalyse. Deze blijkt echter niet te bestaan.

Actiepunten:

- (Beleid) Voer een risicoanalyse uit voor de verwerking in Falcon-i. [p9c1]
- **(Wet art. 4a lid 2) Zorg dat de informatiebeveiligingseisen mede op basis van de risicoanalyse bepaald worden. [p9c2]**
- **(Wet art. 4a lid 2) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van realisatie in Falcon-i. [p9c3]**
- (Beleid) Zorg dat de restrisico's in de beveiliging van Falcon-i die uit de risicoanalyse naar voren gekomen zijn periodiek beheerd worden. [p9c7]

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

1.10 Privacy by default

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

Voor dit principe is volwassenheidsniveau 2 behaald. Om te komen tot het hoogste volwassenheidsniveau moet onderzocht worden of er PET (Privacy Enhancement Technology) hulpmiddelen toegevoegd kunnen worden.

Actiepunten:

- (Beleid) Zorg dat voor in de opvolger van Falcon-i (Arendsoog) gebruik gemaakt wordt van PET (Privacy Enhancement Technology) hulpmiddelen zoals pseudonimiseren, anonimiseren of versleutelen. [p10c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Voldoen aan de wet	Zwaar (Z)	100%	50%	2

1.11 Toepassen standaarden

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

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

Voor dit principe is het hoogst mogelijke volwassenheidsniveau behaald.

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

[4] 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

Voor dit principe zijn er alleen criteria vanuit beleid. Hiervoor is volwassenheidsniveau 2 behaald. Om te komen tot het hoogste niveau zijn er een drietal actiepunten.

Actiepunten:

- (Beleid) Zorg dat de definities, richtlijnen en kwaliteitseisen voor de verwerking van gegevens vastgesteld worden. Deze hebben nu nog een concept status. [p12c2]
- (Beleid) Zorg dat alle uitvoeringsverantwoordelijken (teamchefs) een plan maken voor het gebruik van Falcon-i. [p12c3]
- (Beleid) Zorg dat de verwerkingsgrondslag wordt opgenomen in de referentielijst waarna deze ook overgenomen kan worden in Falcon-i. [p12c4],[p12c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[5]	79%	2

[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