# 0-meting Privacy & Security by Design

## Fotoconfrontatie-module (FCM)

10.2.e

10.2.e

Definitief

Versie 1.1b

Versie datum 10 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 | |
| 1.0 | 12-7-2018 | Eerste versie rapport | |
| 1.1 | 03-04-2019 | Voortschrijdend inzicht in bewaartermijnen artikel 13 verwerkt. | |
| 1.1a | 10-04-2019 | Aanvulling HKS schoningslijst verwerkt. | |
| 1.1b | 10-04-2019 | Definitieve versie na wederzijds goedkeuren | |

**Review commentaar**

| Versie | Wanneer | Wie | Functie |
|---|---|---|---|
| 1.0 | 22-6-2018 | 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 compliance te realiseren (eerdere programma's hebben niet tot een bevredigend resultaat geleid). Met het meerjarig verbeterplan zijn in maart 2016 politieke toezeggingen gedaan aan de Tweede Kamer.[1]

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

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

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

[1] Verbeterplan Wet Politiegegevens en Informatiebeveiliging
[2] Tranche 2018, Verbeterprogramma Wpg en IB

# 0-meting Fotoconfrontatiemodule (FCM)

## 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 FCM | 10.2.e | IV-expert, product owner FCM |
| | 10.2.e | Functioneel beheerder FCM |
| | 10.2.e | Functioneel beheerder FCM / TRIS |

| | Naam | Functie |
|---|---|---|
| Toetsing | 10.2.e | Adviseur architectuur en modellering |
| | 10.2.e | Programmamanager |
| | 10.2.e | Rijks ICT Trainee |

| Gespreksdatum | Nummer meting | Toelichting |
|---|---|---|
| 21-02-2018 | 2018022101 | De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.** |

## FCM

**Omschrijving applicatie**

De Foto Confrontatie Module (FCM) is ter ondersteuning van de opsporing. Er worden foto's gemaakt van personen die worden verdacht van een misdrijf waar voorlopige hechtenis op staat. De foto's worden vanuit verschillende hoeken gemaakt. Samen met de foto wordt een signalement opgesteld. Het signalement wordt met het fotonummer naar BVH gestuurd. BVH kan zelf geen foto's opslaan. De foto's kunnen worden gebruikt om getuigen of slachtoffers de verdachte aan te laten wijzen. Een serie foto's van personen met hetzelfde soort signalement zal wordt laten zien. Niet alle foto's zijn afkomstig van bestaande personen. Het is mogelijk een figurantenfoto van een niet-natuurlijke persoon te creëren. Er zijn drie statussen.

- Nog te keuren: dan moet het nog goedgekeurd worden en kan er niets mee worden gedaan.
- Goedgekeurd: kan worden gebruikt.
- Afkeuren: wordt niet meegenomen in de confrontaties, maar is wel mogelijk bij andere functies.

**Soorten verwerkingen van politiegegevens**

| Soort verwerking | X | |
|---|---|---|
| Verzamelen | X | |
| Vastleggen | X | Zoekvraag, aanwijzing, foto |
| Ordenen | X | |
| Bewaren | X | |
| Bijwerken (het ontbrekende aanvullen / bestaande aanvullen) | X | Kan ook tijdelijk (bewerken voor tijdens de confrontatie) |
| Wijzigen (het bestaande aanpassen) | X | |
| Opvragen | X | |
| Raadplegen | X | |
| Gebruiken | X | |
| Vergelijken | X | |
| Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren) | X | Om bijv. aan een team te laten zien. Rapporten kunnen ook extern als een rechter daar om vraagt |
| Samenbrengen | X | Combisets maken (vb. mannen en vrouwen) |
| Met elkaar in verband brengen | X | |
| Afscherming | X | Besloten maken, ook beperking qua autorisatie |
| Uitwissen (weghalen/verwijderen zonder vernietigen) | X | |
| Vernietigen | X | |

**Verwerkingsgrondslag**

| Doelbinding | Verwerkingsgrondslag | X | Toelichting |
|---|---|---|---|
| Dagelijkse politietaak | Artikel 8 | | |
| Onderzoek rechtsorde bepaald geval | Artikel 9 | | |
| Informatiepositie | Artikel 10 | | |
| Informanten | Artikel 12 | | |
| Ondersteunende taken | Artikel 13 | X | Gegevens voor FCM komen binnen als art. 8, 9 of 10, maar worden binnen FCM als art. 13 verwerkt.<br>Hiervoor geldt het artikel 13 protocol voor FCM dat in werking is getreden op 1 mei 2003. |

**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

FCM scoort een volwassenheidsniveau 1. Dit houdt in niet wordt voldaan aan de eisen van de wet op het gebied van Privacy & Security by Design (PSbD), maar ook niet aan het politiebeleid. Op het gebied van volwassenheid zijn er op de principes verantwoording, metagegevens, informatiebeveiliging en toepassing standaarden direct verbetering nodig. Echter ons advies is om eerst te kijken naar de wettelijke actiepunten zoals deze hieronder beschreven staan.

Advies:

- **(Wet art 4): zorg voor een optimalisering van het proces om onjuistheden van gegevens van kernobjecten aan de bronhouder terug te melden.**
- **(Wet art 4): optimaliseer het terugmelden in geval van 'gerede twijfel' over een gegeven.**
- **(Wet art 32): neem de datum einde verwerkingstermijn op in het gegevensmodel.**
- **(Wet art 32): zorg dat een audittrail kan worden geregistreerd.**
- **(Wet art 4): stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse**
- **(Wet art 4): stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening.**

| Eindscore | Datum toetsing | 0-meting versie | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|---|
| FCM | 21-2-2018 | v1.0 | 55% | 59% | 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 | 100% | 3 |
| Doelbinding | Z | - | 50% | 100% | 1 |
| Verantwoording | Z | - | 0% | 0% | 0 |
| Autorisatie | Z | - | 100% | 50% | 2 |
| Metagegevens | Z | - | NVT | 33% | 0 |
| Kwaliteitszorg | Z | - | NVT | 89% | 2 |
| Bewaren en vernietigen | Z | - | 100% | 0% | 2 |
| Informatiebeveiliging | Z | - | 0% | 0% | 0 |
| Voldoen aan de wet | Z | - | NVT | NVT | NVT |
| Toepassing standaarden | L | - | NVT | 33% | 0 |
| Verantwoordelijkheden belegd | M | - | NVT | 100% | 3 |
| Principe is niet actief | | - | | | |
| TOTALEN TOETSING | | - | 55% | 59% | |


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.

**Nieuwe regelgeving Wpg januari 2019 (buiten de 0-meting)**

Binnenkort zijn er nieuwe richtlijnen van toepassing voor de Wpg. Voor FCM geldt dat direct voor de volgende criteria:

- **(Beleid --> wet januari 2019): maak het mogelijk om (periodiek) een rapportage van de audittrail te genereren.**

## 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.

FCM heeft een volwassenheidsniveau van niveau 1 (onvoldoende) op het principe eenmalige vastlegging. Er wordt volledig aan het politiebeleid voldaan. Echter er zitten verbeterpunten in het terugmelden van onjuistheden. Vaak worden de onjuistheden of gevallen waarin sprake is van 'gerede twijfel' per e-mail gemaild. De meldingen komen alleen op verschillende plekken binnen, waardoor het verder verloop onduidelijk is. Tijdens de 0-meting is aangegeven dat de fout buiten FCM ligt, maar wel onderdeel is van het proces. Zaak is om ervoor te zorgen dat het proces aan de kant van FCM zo optimaal mogelijk is.

Actiepunten:

- **(Wet art 4): zorg voor een optimalisering van het proces om onjuistheden van gegevens van kernobjecten aan de bronhouder terug te melden.**
- **(Wet art 4): optimaliseer het terugmelden in geval van 'gerede twijfel' over een gegeven.**

| 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.

De score van FCM op het principe PDCA-cyclus is maximaal, namelijk 100%. Er worden periodiek rapportages opgeleverd die worden gebruikt als stuurinformatie ten behoeve van de PDCA-cyclus. Het is belangrijk om dergelijke rapportages (periodiek) op te leveren. Op die manier kan de ontwikkeling van (het gebruik van) de applicatie worden bijgehouden. Minder gewenste ontwikkelingen zijn dan snel zichtbaar en dan kan er daar op worden gestuurd. Het beheer van processen, gegevens en software bij FCM is ook onderdeel van de PDCA-cyclus.

Enkele criteria waren tijdens de 0-meting nog niet van toepassing, waaronder het uitvoeren van de gegevensbeschermingseffectbeoordeling (GEB). Deze is sinds mei 2018 verplicht en geldt alleen als er sprake is van een *nieuwe* verwerking. Op het moment van de 0-meting stond er nog niets op de planning bij FCM. Indien in de toekomst een nieuwe functionaliteit wordt toegevoegd die ook een nieuwe verwerking inhoudt, moet er door middel van een korte vragenlijst worden vastgesteld of het nodig is een GEB uit te voeren. Het is aan te raden om deze dan uit te voeren met behulp van de privacy functionaris.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| PDCA-cyclus | Middel (M) | NVT | 100% | 3 |

## 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.

Alle verwerkingen van politiegegevens in FCM gebeuren op grond van artikel 13 Wpg, dus als duidelijk is dat een gegeven afkomstig is uit FCM dan is ook meteen duidelijk wat de verwerkingsgrondslag is. Aangezien het een artikel 13 verwerking is, moet er een artikel 13 protocol zijn opgesteld. Deze is aanwezig[3], maar het is niet duidelijk of de datum einde verwerkingstermijn opgenomen is in het gegevensmodel. Dit is wel verplicht.

Actiepunten:

- **(Wet art 32): neem de datum einde verwerkingstermijn op in het gegevensmodel.**

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Doelbinding | Zwaar (Z) | 50% | 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.

Op het principe verantwoording voldoet FCM niet. Er wordt geen audittrail geregistreerd. Het is van belang dat als een audittrail wordt geregistreerd dat deze is beveiligd tegen manipulatie. Dit betreft niet alleen manipulatie door de gebruiker, maar ook de manipulatie door een databasebeheerder. Voor dat laatste bestaat bij Oracle een aparte audit functionaliteit. Deze kan worden aangezet, maar daar zijn wel licentiekosten aan verbonden. Er moet een afweging worden gemaakt tussen de kosten en baten van een dergelijke functionaliteit. Ook moet het mogelijk zijn om een rapportage van de audittrail te genereren. Dit was tijdens de 0-meting nog politiebeleid, maar is sinds mei 2018 wet. Ook hiervoor geldt dat het belangrijk is dergelijke rapportages bij te houden om de ontwikkelingen in de gaten te houden.

Actiepunten:

- **(Wet art 32): zorg dat een audittrail kan worden geregistreerd.**
- (Beleid): beveilig de audittrail tegen manipulatie door zowel gebruikers als (database)beheerders.
- **(Beleid --> wet art 32 vanaf juni/juli 2018): maak het mogelijk om (periodiek) een rapportage van de audittrail te genereren.**

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Verantwoording | Zwaar (Z) | 0% | 0% | 0 |

[3] Artikel 13 protocol voor FCM dat in werking is getreden op 1 mei 2003.

## 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.

FCM maakt geen gebruik van de IAM-voorziening. Het probleem hierbij is dat voor het gebruik van FCM een aparte opleiding moet worden gevolgd, maar die rollen zijn in IAM niet aanwezig. De LFNP-functies zijn te ruim omschrijven voor de rollen die FCM nodig heeft. Het gebruik van de generieke autorisatietool voor leidinggevende kan beter worden uitgewerkt. De profielen van FCM sluiten niet goed aan op de ATL. Tijdens de 0-meting kwam naar voren dat FCM een keuze zou moeten maken tussen IAM en de ABAC (zie ook de Uitvoering autorisatiebeleid politie 2016-2020). Een laatste verbeterpunt op het principe autorisatie is het verbeteren van de controle op toegangs- en gebruiksrechten. Nu gebeurt dat incidenteel handmatig, maar het zou zo geautomatiseerd mogelijk en veel regelmatiger moeten zijn. FCM voldoet aan de (wettelijke) eis dat de gebruikers worden geïnstrueerd met betrekking tot de voor hen geldende autorisatieregels. Niet alleen bij de opleiding, maar ook in de applicatie wordt de gebruiker op verschillende manieren geïnformeerd.

Actiepunten:

- (Beleid): zorg dat FCM gebruik gaat maken van IAM inclusief de mogelijkheden tot het meenemen van opleidingscertificaten.
    - (Beleid): indien er geen gebruik gemaakt kan worden van IAM zorg dat FCM het ABAC ondersteunt
- (Beleid): werk de profielen voor de ATL beter uit.
- (Beleid): zorg voor een periodieke geautomatiseerde controle van toegangs- en gebruikersrechten.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Autorisatie | Zwaar (Z) | 100% | 50% | 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.

FCM scoort een 0 op het gebeid van metagegevens. Het lastige als een applicatie geen gebruik maakt van de vastgestelde definities voor bedrijfsbegrippen is dat het uitwisselen van gegevens bemoeilijkt wordt. Hetzelfde is van toepassing op de kenmerken van verwerkte gegevens. Alleen op die manier kan de juistheid en rechtmatigheid gewaarborgd worden. Daarnaast kunnen metagegevens gebruikt worden om toegang te verlenen, te bepalen of een bewaartermijn verstreken is, handelingen te bestuderen op basis van een audittrail en om te rapporteren aan het management.

Actiepunten

- (Beleid): FCM maakt nog geen gebruik van vastgestelde definities en bedrijfsbegrippen. Dit zou in overeenstemming met GGB geregeld moeten worden
- (Beleid): FCM maakt bij het gebruik van metagegevens nog geen gebruik van het toepassingsprofiel metagegegevens Rijk (TMR). Zolang het Toepassingsprofiel Metagegevens Politie nog niet beschikbaar is kan hier het beste naar gekeken worden.
- (Beleid): Voor FCM is het belangrijk dat verwerkte gegevens bepaalde kenmerken (metagegevens) bevatten:
    - Identificatiekenmerken
    - Wettelijke verwerkingsgrondslag
    - Kenmerken die noodzakelijk zijn voor het verwerken van gegevens binnen het politieproces en/of binnen de keten (bijvoorbeeld transactie/event, datum, status, vorm)
    - Kenmerken die noodzakelijk zijn voor het verwerken van gegevens in de keten
    - De herkomst van de gegevens (verplicht voor art 9 en 10 gegevens)
    - De wijze van verkrijging (verplicht voor art 9 en 10 gegevens)
    - Logginggegevens zoals tijd en datum, en wie met welke taak is ingelogd
- (Beleid): FCM maakt geen gebruik van metagegevens voor het gebruik van het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages.

Aandachtspunt:

- Controleer de huidige architectuur aangezien het onduidelijk is of het nog voldoet.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Metagegevens | Zwaar (Z) | NVT | 29% | 0 |

## 1.7 Kwaliteitszorg

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

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

De score van FCM op het principe kwaliteitszorg is hoog (89%) en het verbeterpunt zit in de kwaliteitscontroles. Deze werden vroeger wel gedaan, maar de afgelopen 3 jaar niet meer. Kwaliteitscontroles moeten periodiek worden uitgevoerd om bij te kunnen houden of bepaalde zaken met betrekking tot kwaliteit sterk afwijken van de norm. Daarom moeten de resultaten ook worden bewaard, aangezien je op die manier kan vaststellen of een kwaliteitsresultaat daadwerkelijk afwijkt.

Actiepunten:

- (Beleid): voer periodiek kwaliteitscontroles uit en bewaar de resultaten.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Kwaliteitszorg | Zwaar (Z) | NVT | 89% | 2 |

## 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 moment voldoet FCM niet op het gebied van vernietigen. Ook voldoet FCM niet aan de kwaliteitseisen van de DUTO standaard.

Actiepunten:

- (Beleid): Er worden geen gegevens op basis van geldende termijnen geautomatiseerd vernietigd op basis van het artikel 13 protocol voor FCM dat in werking is getreden op 1 mei 2003.[4]
- (Beleid): FCM voldoet niet aan de kwaliteitseisen van de DUTO standaard

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Bewaren en vernietigen | Zwaar (Z) | 100% | 0% | 2 |

[4] Voor de uitfasering van HKS werd de HKS schoningslijst gebruikt om gegevens te vernietigen.

## 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.

De uitgevoerde risico analyse van FCM was niet recent genoeg om deze op te kunnen voeren. Het is van belang regelmatig de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. Vandaar dat de risico analyse niet wordt meegenomen. Het advies voor dit principe luidt om opnieuw een risico analyse uit te laten voeren. Naar aanleiding van die resultaten moet worden gekeken welke informatiebeveiligingseisen moeten worden genomen en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Daar waar mogelijk moet gebruik worden gemaakt van de standaard informatiebeveiligingsdiensten. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's worden beheerst.

Actiepunten:

- (Beleid): voer een risico analyse uit.
- **(Wet art 4b en c): stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse**
- **(Wet art 4b en c): stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening.**
- (Beleid): gebruik waar mogelijk de standaard informatiebeveiligingsdiensten. Als dat niet mogelijk is, neem passende maatregelen.
- (Beleid): beheer de restrisico's.

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

## 1.10 Voldoen aan de wet

"*Gegevensverwerking door de politie voldoet aan de daarvoor geldende wettelijke kaders*"

Dit principe is niet besproken aangezien dit in de volgende versie verwijderd gaat worden en de vragen omtrent wetgeving verweven zitten in de andere principes.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Voldoen aan de wet | Zwaar (Z) | NVT | NVT | NVT |

## 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.

FCM maakt gebruikt van bestaande overheids- en ketenstandaarden. Momenteel wordt er geen toetsing gedaan op de bestaande standaarden. Het is van belang om de toegepaste standaarden in beheer te hebben. Daarnaast is het niet duidelijk of in het geval van afwijkingen een motivatie is gegeven door de verwerkingsverantwoordelijke.

Actiepunten:

- (Beleid): voer toetsen uit op de toepasselijke standaarden.
- (Beleid): in het geval van afwijkingen van standaarden moet er een motivatie zijn die is geaccepteerd door de verwerkingsverantwoordelijke (pas toe of leg uit)

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Toepassen standaarden | Zwaar (Z) | NVT | 33% | 1 |

## 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

Op het principe verantwoordelijkheden belegd zijn er geen wetscriteria. FCM voldoet volledig aan het politiebeleid en heeft daarom een volwassenheidsniveau 3.

| Principe | Weegfactor | Wet | Beleid | Volwassenheid |
|---|---|---|---|---|
| Verantwoordelijkheden belegd | Zwaar (Z) | NVT | 100% | 3 |

# 2. Verantwoording toetsing

## Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2017-07-20_Uitvoeringskader_Privacy en Security by Design_v1.0'. Vervolgens zijn er criteria toegevoegd of aangescherpt op basis van documenten waar in het uitvoeringskader naar wordt verwezen. Het resultaat is met de auteurs van het uitvoeringskader besproken. Hun commentaar is verwerkt en nogmaals besproken.

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

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

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

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

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van de applicatie. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[5].

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.

[5] Bijlage 1: Uitgangspunt bij compliance

**Bedrijfsregels volwassenheidsniveau**
Als de criteria zijn beoordeeld als “niet van toepassing” dan zijn er geen criteria benoemd of de criteria zijn niet van toepassing gebleken voor de applicatie.

Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan minder dan 35% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan minder dan 35% van de beleidscriteria wordt voldaan.

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan ten minste 35% maar minder dan 100% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria, en aan niet alle van de beleidscriteria wordt voldaan.
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria en aan alle beleidscriteria wordt voldaan
b: aan alle wettelijke criteria wordt voldaan en de beleidscriteria zijn niet van toepassing
c: de wettelijke criteria zijn niet van toepassing, en aan alle beleidscriteria wordt voldaan

NVT : Een volwassenheidsniveau NVT moet worden toegekend, indien de volgende voorwaarde van toepassing is:

a: de wettelijke criteria en de beleidscriteria zijn niet van toepassing

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

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

| Weegfactor | Licht (L) | Middel (M) | Zwaar (Z) |
|---|---|---|---|
| Aantal | 1 | 3 | 5 |

**Aandachtspunten**
1: Volwassenheidsniveau 1:

Voor het vaststellen van dit niveau maakt het geen verschil of de voorziening of het principe geheel of deels aan een of alle min 1 wettelijke criteria voldoet.

2: Beleidscriteria:

Met uitzondering van niveau 3 geldt dat de mate waarin de voorziening voldoet aan de beleidscriteria, uitgedrukt in een percentage, niet van invloed is op de vaststelling van het volwassenheidsniveau. Het percentage beleidscriteria bij een principe is wel een indicatie of meer of minder inspanning moet worden geleverd om het principe compliant te krijgen aan het uitvoeringskader. Met name in combinatie met de percentages van de wettelijke criteria bij het volwassenheidsniveau 1 en in combinatie met de weegfactor geeft het inzicht bij het prioriteren van werkzaamheden om de voorziening compliant te maken.

3: Privacy functionaris:

De applicatie specifieke requirements mbt PSbD worden tijdens de ontwikkeling bepaald in samenwerking met de Privacy Functionaris en de business expert. Daarnaast is de privacy functionaris eerste aanspreekpunt mbt vragen over privacy.

## Disclaimer

Aan de resultaten op basis van het gebruik van de 0-meting wordt geen enkele garantie met betrekking tot de mate van compliance van de getoetste voorziening gegeven. Tevens wordt geen enkele garantie gegeven inzake de juistheid of volledigheid van de checklist als gevolg van veranderende wet- of regelgeving.

# Bijlage 1: Uitgangspunt bij compliance


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

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