0-meting Privacy & Security by Design

DCS

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	18-10-2018	Reviewen
0.9	19-10-2018	Aanpassingen verwerkt
1.0	19-2-2019	Na wederzijds akkoord definitief gemaakt

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	18-10-2018	10.2.e	Gegevensautoriteit
0.9	19-10-2018	10.2.e	Gegevensautoriteit
1.0	19-2-2019	10.2.e	Gegevensautoriteit

Inhoudsopgave

Documentinformatie 2

Inhoudsopgave 2

Inleiding 4

0-meting DCS 5
Algemeen 5
Doel 5
Doelgroep 5
Aanwezigen 0-meting 5
DCS 6
Omschrijving applicatie 6
Soorten verwerkingen van politiegegevens 6
Verwerkingsgrondslag 7
Eindscore 8
1.1 Eenmalige vastlegging 10
1.2 PDCA-cyclus 11
1.3 Doelbinding 12
1.4 Verantwoording 13
1.5 Autorisatie 14
1.6 Metagegevens 15
1.7 Kwaliteitszorg 16
1.8 Bewaren en vernietigen 17
1.9 Informatiebeveiliging 18
1.10 Privacy by default 18
1.11 Toepassen standaarden 19
1.12 Verantwoordelijkheden belegd 19

2. Verantwoording toetsing 20
Toetsingscriteria 20
Disclaimer 22

Bijlage 1: Uitgangspunt bij compliance 23

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 DCS. 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 DCS

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 DCS	10.2.e	Functioneel beheer DCS
	10.2.e	Voorzitter landelijk gebruikersoverleg DCS
	10.2.e	Ontwikkelaar / Technisch beheer DCS
	10.2.e	Functioneel beheer DCS (backup)
	10.2.e	Functioneel beheer (coördinator)
	10.2.e	Privacyfunctionaris Landelijke eenheid

	Naam	Functie
Toetsing	10.2.e	Adviseur architectuur en modellering
	10.2.e	Programmamanager
	10.2.e	Trainee (onderzoekopdracht PSbD)

Gespreksdatum	Nummer meting	Toelichting
8-8-2018	2018080801	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

DCS

Omschrijving applicatie

DCS is een webbased analysevoorziening voor de 10.2.c . 10.2.f 10.2.c . 10.2.c , is in principe beschikbaar voor alle gebruikers van DCS, mits op het juiste niveau geautoriseerd 10.2.c

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	x	Histo's worden ingelezen, geüniformeerd en opgeslagen in de database. Hiermee wordt het mogelijk om analyses uit te voeren.
Vastleggen	x	
Ordenen	x	
Bewaren	x	Bewaren ook door export (Mappenstandaard niet afgedwongen en Summ-IT)
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	x	10.2.c
Wijzigen (het bestaande aanpassen)	x	Medewerkers kunnen eigen gebruiker(namen)lijst aanleveren 10.2.c Bron Histo's zelf kunnen niet gewijzigd worden. 10.2.c . Wel in het vervolgtraject/bestanden
Opvragen	x	Opvragen DCS onderzoeken binnen DCS
Raadplegen	x	Ingelezen histo's worden geanalyseerd Onderling vergelijken is ook een optie.
Gebruiken	x	
Vergelijken	x	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	x	10.2.c
Samenbrengen	x	Betreft een analysetool voor historische telefoniegegevens, 10.2.c
Met elkaar in verband brengen	x	
Afscherming	x	Artikel 10 embargo onderzoeken; plus eenmalige afslag gemaakt in 2014 (niet onderhouden)

Uitwissen (weghalen/verwijderen zonder vernietigen)	x	Gegevens kunnen verwijderd worden zonder verzoek tot vernietiging. Iedere medewerker die toegang heeft tot de applicatie kan dit voor de gegevens van zijn eigen onderzoek doen. Functioneel beheer heeft de mogelijkheid tot vernietiging Er komen geen vernietigingsverzoeken (126 cc) vanuit het OM waardoor gegevens de maximale termijn (5jr) bewaard blijven (langer dan nodig). Ook bij politie is geen afhandelproces afgesproken (zou onderzoekseigenaar moeten zijn)
Vernietigen	x	Backups van DCS worden maximaal 30 dagen bewaard en zijn indien verwijderd (weg voor de applicatie) daadwerkelijk na 30 dagen vernietigd.

Verwerkingsgrondslag

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

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

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

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

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

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

Eindscore

DCS scoort een volwassenheidsniveau 1. Dit houdt in dat DCS 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 het politiebeleid. Op de wetscriteria heeft DCS een score van 41% en op de criteria van het politiebeleid een score van 37%. Dat geeft aan dat er verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria die hieronder beschreven staan. Daarnaast is het opvallend dat de principes 'eenmalige vastlegging', 'PDCA-cyclus', 'bewaren en vernietigen', 'informatiebeveiliging' en 'toepassen standaarden' heel negatief scoren.

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

- **(Wet artikel 32a Wpg): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden. [p3c10]**
  - **Zorg dat de koppeling met** 10.2.c **voldoet aan de verwerkingsgrondslag en verwerkingstermijn per gegeven wat geanalyseerd wordt.**
  - **Brief korpsleiding geeft zelfs aan dat gegevens niet andere systemen geregistreerd mogen worden[3].**
- **(Wet art 32a): Zorg dat er bij de queries een volledige rapportage van de audittrail laten zien. [p4c4]**
  - **Zorg dat de query niet alleen gegevens opvraagt binnen** 10.2.c **, maar ook in** 10.2.c **.**
- **(Wet artikel 6): Zorg dat DCS gebruik maakt van de vastgestelde autorisatie rollen van de politie (vervalt bij in gebruik name IAM-voorziening) [p5c2]**
- **(Wet artikel 14 Wpg): Zorg dat DCS de gegevensverwerkende processen geanalyseerd heeft op basis van de generieke selectielijst. Indien dit niet mogelijk is moet er in ieder geval worden voldaan aan artikel 14 lid 4. [p8c1]**
- **(Wet artikel 8, 9, 10, 12 en 14 Wpg): Zorg dat er wordt voldaan aan de wettelijke bepalingen omtrent bewaren, vernietigen en archiveren van (persoons)gegevens.[p8c2]**
  - **Expiratiedatum van onderzoek is standaard 31-12-2099**
  - **Onderzoeken die geen expiratiedatum bevatten worden niet verwijderd**
- **(Wet archiefwet): Bij verwerkte gegevens moet er een selectie gemaakt kunnen worden ten behoeve van bewaren en vernietigen. [p8c3]**
- **(Wet art 14 lid 4): DCS moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens. [p8c9]**
  - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse. [p9c2]**
  - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**

Aandachtspunten:

- Vanuit het productiehuis willen ze de DevOps-teams volledige rechten geven (dus ook op de database). Dit vergt extra risico en dient meegenomen te worden in de overweging mbt de beveiliging van het manipuleren van de audittrail.
- Leidinggevende geven gebruikers via ATL toegang, terwijl ze daarvoor niet de kennis en kunde hebben.
- 11.1
- Er is een te brede gebruikersgroep binnen DCS wat een risico kan zijn voor onjuist gebruik. Zorg voor een specifieke opleiding

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
DCS	8-8-2018	2.0	41%	37%	1

[3] Brief maatregelen DCS, Maatregelen DCS, 2015/07298

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	33%	0
PDCA-cyclus	M	-	NVT	33%	0
Doelbinding	Z	-	50%	33%	1
Verantwoording	Z	-	75%	0%	1
Autorisatie	Z	-	67%	60%	1
Metagegevens	Z	-	100%	33%	2
Kwaliteitszorg	Z	-	NVT	44%	1
Bewaren en vernietigen	Z	-	0%	0%	0
Informatiebeveiliging	Z	-	0%	20%	0
Privacy by default	Z	-	100%	100%	3
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	50%	2
TOTALEN TOETSING		-	41%	37%	

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.

DCS scoort een onvoldoende op het principe eenmalige vastlegging. Op dit moment wordt er geen gebruik gemaakt van referentietabellen van de GGB. Daarnaast is het invullen van een onderzoeksnummer een vrij-veld waar geen koppeling in zit met de bestaande onderzoeken in BVH en Summ-IT. Hierdoor is het mogelijk om meerdere onderzoeken onder hetzelfde onderzoeksnummer te starten.

Actiepunten:

- (Beleid): Zorg dat de referentiegegevens bijgewerkt zijn. Neem hiervoor contact op met de GGB. [p1c1]
- (Beleid): Zorg dat het Summ-IT en BVH onderzoeksnummer wordt gecontroleerd (dmv een koppeling) bij het opvoeren van een DCS onderzoek. [p1c9]
- (Beleid): Voorkom de mogelijkheid tot het starten van meerdere onderzoeken onder hetzelfde onderzoeksnummer. [p1c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	NVT	33%	0

1.2 PDCA-cyclus

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

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

DCS scoort op het principe 'PDCA-cyclus' een zware onvoldoende. Op het moment van de meting was bij de betrokkenen niet duidelijk wie de portefeuillehouder was. De senior Coördinerend Business Expert is vanwege drukte niet bereikbaar. Daarnaast functioneer het ProductGroepOverleg (PGO) niet zoals het hoort. Leden in het overleg nemen geen beslissing of er wordt van de beslissing afgeweken binnen de eenheid.

Op dit moment werkt de managementfunctie van DCS niet, omdat zodra deze aangezet wordt er performanceproblemen ontstaan. Hierdoor levert DCS onvoldoende rapportages op het gebied van stuurinformatie.

Actiepunten:

- (Beleid) Zorg dat er gebruik wordt gemaakt van de functionaliteit om een rapport op te leveren waarmee stuurinformatie geleverd kan worden ten behoeve van de PDCA cyclus. [p2c1]
- (Beleid) Zorg dat naast de servicedeskrapportage en autorisatierapportage betreffende rapporten periodiek opgeleverd wordt ten behoeve van de gegevensverwerking. [p2c2]
    - Risicoanalyses
    - Aantal onderzoeken
    - Audits
- (Beleid) Zorg dat het beheer van de processen via PDCA-cyclus gaat verlopen. [p2c3]
    - Een eenheid moet met mandaat toegesproken worden indien er onjuist afgeweken wordt
    - Landelijke beslissingen moeten met mandaat binnen het PGO genomen kunnen worden
    - Afgevaardigde per eenheid van het PGO moeten hier een mandaat voor hebben.
- (Beleid) Zorg dat het beheer van gegevens via PDCA-cyclus gaat verlopen. [p2c3]
    - Zorg dat afloopberichten retour komen en worden verwerkt.
    - Zorg dat oude DCS onderzoeken een expiratiedatum krijgen
- (Beleid) Zorg dat de beleidsverantwoordelijke regie, op definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens voert. [p2c7]
    - Zorg dat er een aanspreekpunt is in de SUO (Senior User Overleg)
    - Zorg voor een structureel contact met de senior Coördinerend Business Expert.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	33%	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.

DCS scoort op het principe doelbinding (volwassenheidsniveau 1) een onvoldoende. In DCS 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. Op dit moment is er een koppeling met [redacted] 10.2.c , terwijl in de brief van korpsleiding aangegeven wordt dat gegevens niet in andere systemen geregistreerd mogen worden.

Actiepunten:

- (Beleid) Indien mogelijk moet een er een automatische herleiding zijn van de verwerkingsgrondslag. [p3c3]
- (Beleid) De automatisch afgeleide verwerkingsgrondslag moet aangepast kunnen worden door de gebruiker. [p3c4]
- **(Wet artikel 32a Wpg): Zorg dat een metagegeven met betrekking tot de verwerkingsgrondslag en verwerkingstermijn het gegeven blijft begeleiden. [p3c10]**
    - **Zorg dat de koppeling met 10.2.c [redacted] voldoet aan de verwerkingsgrondslag en verwerkingstermijn per gegeven wat geanalyseerd wordt.**
    - **Brief korpsleiding geeft zelfs aan dat gegevens niet andere systemen geregistreerd mogen worden[5].**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	50%	33%	1

[4] 10.2.c [redacted]
[5] Brief maatregelen DCS, Maatregelen DCS, 2015/07298

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 DCS 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. 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 DCS bekend is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's). Daarnaast is het van belang dat indien er een audittrail opgevraagd wordt de meest volledige rapportage aangeleverd wordt.

Actiepunten:

- (Beleid): Zorg dat de audittrail beveiligd is tegen manipulatie door ook de logging van de DBA'ers aan te zetten. Indien dit niet mogelijk is zorg dat het risico geminimaliseerd en geaccepteerd is. [p4c3]
  - Extra risico: audittrail zit in dezelfde database als operationele gegevens.
- **(Wet art 32a): Zorg dat er bij de queries een volledige rapportage van de audittrail laten zien. [p4c4]**
  - **Zorg dat de query niet alleen gegevens opvraagt binnen** 10.2.c **, maar ook in** 10.2.c

Aandachtspunt:

- Vanuit het productiehuis willen ze de DevOps-teams volledige rechten geven (dus ook op de database). Dit vergt extra risico en dient meegenomen te worden in de overweging mbt de beveiliging van het manipuleren van de audittrail.

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

1.5 Autorisatie

"*Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van noodzaak voor de uitvoering van de hen opgedragen werkzaamheden*"

Door de toegang en het gebruik van informatie en systemen te koppelen aan de werkzaamheden waarvoor deze nodig zijn, hoeven autorisaties niet meer op de persoon of het systeem te worden toegekend en wordt het mogelijk om de rechten vanuit de registratie van functies en werkzaamheden te organiseren en te beheren. Dit levert een reductie in beheerslast op, een beter overzicht op uitstaande gebruiksrechten en het wordt gemakkelijker om centraal autorisatiebeleid door te voeren.

DCS voldoet op dit moment niet op het principe autorisatie. Op dit moment maakt DCS bewust geen gebruik van de generieke IAM-voorziening van de politie. Er is op dit moment autorisatie via certificaat beschikbaar en dat maakt het onverantwoord om op basis van autoriteitsrollen toegang te geven tot DCS. Deze situatie doet zich nu ook al voor bij ATL waarbij gebruikers toegang krijgen via hun leidinggevende zonder enige kennis van de DCS. Door de maandelijkse controle op nieuwe autorisaties (rapport) wordt dit nu onder controle gehouden.

Actiepunten:

- (Beleid): Zorg dat DCS gebruik maakt van de generieke IAM-voorziening voor het verifiëren van identiteiten. Hierin zal meegenomen moeten worden dat autorisatie alleen mogelijk is via een certificaat na een 5-daagse opleiding 'Histo analyse'. [p5c1]
    - (Beleid): Zorg dat er een 5-daagse 'Histo analyse' opleiding met toetsing ontwikkeld is. [p5c1]
- **(Wet artikel 6): Zorg dat DCS gebruik maakt van de vastgestelde autorisatie rollen van de politie (vervalt bij in gebruik name IAM-voorziening) [p5c2]**
- (Beleid): Zorg dat DCS Access Control Toegang ondersteunt (vervalt bij in gebruik name IAM-voorziening). [p5c5]

Aandachtspunt:

- Leidinggevende geven gebruikers via ATL toegang, terwijl ze daarvoor niet de kennis en kunde hebben.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	67%	60%	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.

DCS voldoet op het gebied van de Wpg aan het principe 'metagegevens', maar op het gebied van politiebeleid PSbD zijn er verbeteringen nodig. DCS maakt geen gebruik van één vastgestelde lijst van definities voor bedrijfsbegrippen. Hierdoor kunnen er onduidelijkheden ontstaan zoals 10.2.c (voorbeeld genoemd tijdens de 0-meting).
Al een lange tijd is bekend dat DCS technisch achterhaald is en dat er een fundamentele verbeterslag nodig is. Performance gaat achteruit en de applicatie valt dagelijks uit. De knelpunten zijn bekend, maar er is nog geen actie.
Op dit moment maakt DCS geen gebruik van het toepassingsprofiel Metagegevens Rijk (in afwachting van het toepassingsprofiel Metagegevens politie). Daarnaast worden er bij DCS op dit moment geen metagegevens gebruikt voor audittrails en managementrapportages.
Metagegevens worden bij een export niet meegeleverd, daarnaast is het onbekend welke metagegevens meegaan met de analyseapplicatie Raffinaderij.

Actiepunten:

- (Beleid): Zorg dat er binnen DCS gebruik gemaakt gaat worden van één vastgestelde lijst van definities voor bedrijfsbegrippen (vb. exportpaal, cellid, mast, etc.). [p6c1]
- (Beleid): Kijk naar de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is [p6c4].
- (Beleid) Zorg dat DCS geschikt is om onder de hedendaagse architectuur te kunnen werken.[p6c5]
    - Knelpunten zijn bekend bij de (technische) experts van DCS.
        - Performance
        - Stabiliteit
        - Technisch verouderd
- (Beleid) Zorg dat metagegevens die daar voor in aanmerking komen geautomatiseerd worden afgeleid en vastgelegd. [p6c7]
- (Beleid): Zorg dat DCS gebruik maakt van metagegevens voor het gebruik van audittrails en managementrapportages [p6c9].
- (Beleid): Zorg dat metagegevens meegeleverd worden bij koppelingen voor verwerking in andere voorzieningen. [p6c10]
    - Metagegevens gaan niet mee in de export die gemaakt wordt (Excel)
    - Zoek uit welke metagegevens meegaan met de applicatie 10.2.c

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	100%	33%	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.

Bij het principe 'kwaliteitszorg' zijn vooral verbeteringen nodig in de afstemming. De senior Coördinerend Business Export is niet tot nauwelijks bereikbaar (vanwege de drukte). Het is lange tijd onduidelijk geweest wie de portefeuillehouder is. Daarnaast is er op dit moment geen rapport over de kwaliteit van gegevens, waardoor er geen duidelijk beeld is over de kwaliteit van gegevens. Echter tijdens de PGO-gesprekken is wel duidelijk dat eenheden op verschillende manieren reageren op kwaliteitsafwijkingen.

Actiepunten:

- (Beleid): Zorg dat er een lijst met kwaliteitseisen wordt opgesteld. [p7c1]
- (Beleid): Zorg met de beleidsverantwoordelijke dat de kwaliteitseisen beter afgestemd worden [p7c2]
    - Contact met senior Coördinerend Business Expert verloopt moeizaam
    - Lange tijd onduidelijkheid over wie de portefeuillehouder van DCS is
- (Beleid): Zorg dat naast het handmatig aanpassen van afwijkingen in de gegevenskwaliteit dat structurele oplossingen die voor handen zijn opgelost worden [p7c4]
    - Voorbeeld: naamgeving onderzoek
- (Beleid): Zorg dat er een rapport over de kwaliteit van gegevens kan worden samengesteld. [p7c7]
- (Beleid): Zorg dat uitgevoerde kwaliteitscontroles en het resultaat daarvan bewaard worden. [p7c8]
- (Beleid): Zorg dat binnen elke eenheid op dezelfde manier gereageerd wordt op kwaliteitsafwijkingen.[p7c9]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	44%	1

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 DCS niet aan het principe 'Bewaren en vernietigen'. Er wordt niet voldaan aan de bewaartermijnen (artikel 14 Wpg). Er is geen koppeling met BVH/Summ-IT m.b.t. onderzoeksnummers, waardoor het niet mogelijk is om gegevens te verwijderen en vernietigen wanneer dit noodzakelijk is. Daarnaast is bij veel onderzoeken de expiratiedatum onduidelijk, hierdoor wordt er niet verwijderd en vernietigd.

Afloopberichten komen niet aan en als de afloopberichten aankomen dan worden ze niet via de geautomatiseerde weg overgenomen. De ketensamenwerking met het OM zal verbeterd moeten worden om meer afloopberichten mee te laten komen in DCS.

DCS voldoet niet aan de kwaliteitseisen van de DUTO standaard. Dit is van belang om overheidsgegevens duurzaam beschikbaar en toegankelijk te houden. In het verlengde daarvan moet DCS de gegevens beschikbaar stellen ten behoeve van het duurzaam bewaren van gegevens.

Actiepunten:

- **(Wet artikel 14 Wpg): Zorg dat DCS de gegevensverwerkende processen geanalyseerd heeft op basis van de generieke selectielijst. Indien dit niet mogelijk is moet er in ieder geval worden voldaan aan artikel 14 lid 4. [p8c1]**
- **(Wet artikel 8, 9, 10, 12 en 14 Wpg): Zorg dat er wordt voldaan aan de wettelijke bepalingen omtrent bewaren, vernietigen en archiveren van (persoons)gegevens.[p8c2]**
    - **Expiratiedatum van onderzoek is standaard 31-12-2099**
    - **Onderzoeken die geen expiratiedatum bevatten worden niet verwijderd**
- **(Wet archiefwet): Bij verwerkte gegevens moet er een selectie gemaakt kunnen worden ten behoeve van bewaren en vernietigen. [p8c3]**
- (Beleid): Zorg dat gegevens op basis van de geldende termijnen geautomatiseerd worden verwijderd en vernietigd. [p8c4]
    - Voorbeeld de gegevens die niet automatisch worden vernietigd nadat een bepaalde termijn (artikel 8) die wel zonder afloopbericht vernietigd kan worden.
- (Beleid): Zorg dat er een koppeling is met het bronsysteem, zodat verwijdering en vernietiging van het bronsysteem gevolgd kan worden [p8c5]
- (Beleid): Zorg dat afloopberichten langs de geautomatiseerde weg kunnen worden overgenomen. [p8c6]
    - Ketensamenwerking met het OM op basis van afloopbericht moet verbeterd worden
        - Afloopbericht komt niet aan
- (Beleid): Zorg dat een beslissing van een afloopbericht automatisch wordt verwerkt. [p8c7]
- (Beleid): DCS moet waar mogelijk voldoen aan de kwaliteitseisen van DUTO [p8c8]
- **(Wet art 14 lid 4): DCS moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens. [p8c9]**

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

1.9 Informatiebeveiliging

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

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

DCS heeft recent geen risico analyse uitgevoerd. Het is belangrijk om 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 al kan zijn achterhaald. Het advies hier luidt om een risico analyse uit te laten voeren. Naar aanleiding van de resultaten uit de analyse moet worden gekeken welke informatiebeveiligingseisen moeten worden genomen en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's in beeld zijn en in beheer zijn.

Actiepunten:

- (Beleid): Er moet een nieuwe risicoanalyse voor de verwerkingen uitgevoerd worden. [p9c1]
    - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse. [p9c2]**
    - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening. [p9c3]**
    - (Beleid): Zorg dat daar waar mogelijk de informatiebeveiligingseisen gerealiseerd kunnen worden door de standaard informatiebeveiligingsdiensten [p9c5]
    - (Beleid): Gebruik waar mogelijk de standaard informatiebeveiligingsdiensten. Als dat niet mogelijk is, neem passende maatregelen. [p9c6]
    - (Beleid): Zorg dat het beheer van de restrisico's op periodieke basis gebeurt. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	20%	0

1.10 Privacy by default

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

Zowel de AVG als de Wpg bevatten Privacy by Default en Privacy by Design als verplichte principes. Deze dienen ertoe om gegevensbescherming vanaf het moment van ontwikkeling van informatiediensten tot aan het laatste gebruik zoveel mogelijk in de gegevensverwerking te integreren. Daar waar Privacy by Design vooral toeziet op ontwerpkeuzes bij de *ontwikkeling* van informatiediensten is Privacy by Default van belang bij keuzemomenten tijdens *gebruik* van de informatiediensten. Dit principe verplicht organisaties om de privacy van betrokkenen zo veel mogelijk te beschermen door de verwerking van persoonsgegevens standaard (by default) op de meest privacyvriendelijke stand te zetten.

Voor het principe 'Privacy by Default' is het hoogste volwassenheidsniveau 3 gemeten. De persoonsgegevens zijn zo beperkt mogelijk gehouden en binnen de DCS worden alleen persoonsgegevens verzameld die voor het doel betreffend zijn.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	100%	3

1.11 Toepassen standaarden

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

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

Het is op dit moment onbekend in hoeverre DCS gebruik maakt van bestaande overheids- en ketenstandaarden. Dat is ook meteen de reden dat DCS hier heel laag op scoort.

Actiepunten:

- (Beleid): Het is onduidelijk op welke manier binnen DCS gebruik wordt gemaakt van bestaande overheids- en ketenstandaarden. Zorg dat het duidelijk is welke overheids- en ketenstandaarden er binnen DCS gebruikt worden [p11c1]
    - (Beleid): Voer toetsen uit op de toepasselijke standaarden. [p11c2]
    - (Beleid): In het geval van afwijkingen van standaarden moet er een motivatie zijn die is geaccepteerd door de verwerkingsverantwoordelijke (pas toe of leg uit). [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	0%	0

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

DCS voldoet voor het grootste deel aan beleidsmatige eisen van PSbD (volwassenheidsniveau 2). Echter de samenwerking tussen beleidsverantwoordelijke en de uitvoeringsverantwoordelijke werkt. Het beleid, koers en strategie zijn eenmalig (2014) vastgesteld, maar daarna niet meer. Het lijnmanagement is onvoldoende op de hoogte hoe gegevens via DCS verwerkt worden.

Actiepunten:

- (Beleid) Zorg dat er regelmatig afstemming (beleidsverantwoordelijke en uitvoering) plaatsvindt op basis van beleid, koers en strategie. [p12c2]
- (Beleid) Zorg dat het lijnmanagement voldoende op de hoogte is met welke gegevens er verwerkt worden binnen DCS [p12c3]

Aandachtspunten:

- Het is onduidelijk wie (DCS) gegevens (incl. histo en exports) gebruikt buiten de applicatie. Zorg dat duidelijk is wie welke gegevens gebruikt buiten DCS.
- Er is een te brede gebruikersgroep binnen DCS wat een risico kan zijn voor onjuist gebruik. Zorg voor een specifieke opleiding

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	50%	2

2. Verantwoording toetsing

Toetsingscriteria

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

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van 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[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
Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien de voorziening of het principe aan geen enkel wettelijk criterium voldoet

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

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

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

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

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

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

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

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

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

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

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

Weegfactor	Licht (L)	Middel (M)	Zwaar (Z)
Aantal	1	3	9

Aandachtspunten
1: Volwassenheidsniveau 1:

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

2: Beleidscriteria:

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

3: Privacy functionaris:

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

Disclaimer

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

Bijlage 1: Uitgangspunt bij compliance

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

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