0-meting Privacy & Security by Design

ZUIS

10.2.e

Definitief

Versie 2.0

Versie datum 20 maart 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
0.9	1-6-2018	Eerste versie	
1.0	29-6-2018	Conceptversie na review	
1.1	20-9-2018	Aanpassingen gedaan nav gesprek op 5 september 2018 met 10.2.e en 10.2.e	
2.0	20-3-2019	Definitief na wederzijds akkoord	

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
1.0	29-6-2018	10.2.e	Gegevensautoriteit
1.1	20-9-2018	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 ZUIS. 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 ZUIS

Algemeen

Omschrijving ZUIS
Het Zeescheepvaart Uitbreidbaar Integraal Systeem (ZUIS) is in 2011 operationeel geworden en wordt door de Zeehavenpolitie (onderdeel van de Nationale Politie eenheid Rotterdam) en de Koninklijke Marechaussee gebruikt als ondersteuning bij het proces van grenstoezicht. In dit systeem worden gegevens van opvarende van zeeschepen vastgelegd en gecontroleerd (NCIS en documenten).

De bemanningslijsten en passagierslijsten moeten verplicht geleverd worden. Op basis van een controle en risicoprofielen (bijvoorbeeld gevaarlijke en niet-gevaarlijke landen) wordt een risico-inschatting gemaakt om de doelgroep te creëren om controles uit te voeren. Op basis van ZUIS kan gecontroleerd worden wie aan land gingen, wie terug aan boord gingen en wie er 'verdwenen'. Je kan controleren wie er zijn, of ze terecht de grens zijn overgestoken en of ze terecht aanwezig zijn. In de tool zitten aansturingsmogelijkheden, maar ook de geschiedenis van de gegevens, waardoor profielen aangepast kunnen worden aan de hand van analyses. Zieke mensen (ongelukken of iets dergelijks) werden naar het Havenziekenhuis gebracht, maar dan moet je weten of deze persoon visumplichtig is. Voortgang wordt gemonitord en staat in het systeem, tot de persoon naar huis gaat. Registreren, monitoren en controleren zijn de functies van het systeem. Registreren is tegenwoordig minimaal, alleen controleren op schepen waar mensen afmonsteren. Men is nu bezig de informatie digitaal binnen te krijgen. Gegevens komen via RWS (wordt gesplitst naar belasting, douane of ZHP). Grote mogelijkheden zijn verkleind naar aanleiding van veranderende wetgeving en werking. Wordt alleen gebruikt door ZHP Rotterdam. ZUIS is specifiek voor zeeschepen. Voor cruiseschepen wordt ZUIS ook gebruikt, zowel voor bemanning als passagiers. Doel: wat komt er binnen, wat gaat er weg, wat blijft er weg. Dit geldt alleen voor Rotterdam.

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 ZUIS	10.2.e	Functioneel beheer ZUIS
	10.2.e	Kernlid Competence Center Privacy (CCP)
	10.2.e	Adviseur Informatiemanagement
	10.2.e	Functioneel beheer

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

Gespreksdatum	Nummer meting	Toelichting
17-1-2018	2018012018/ ZUIS Toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Soort verwerking	X	Toelichting
Verzamelen	X	
Vastleggen (registreren)	X	
Ordenen (vb. in categorieën plaatsen)	X	Onderscheid bemanningsleden, passagiers, verstekelingen. 10.2.c
Bewaren (opslaan)	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	Automatisch ingelezen lijst: als daar fouten / typefouten in zitten, kan worden aangepast.
Opvragen (ophalen van gegevens)	X	Koppeling met de applicatie 10.2.c
Raadplegen (bekijken van gegevens)	X	
Gebruiken	X	
Vergelijken (bv ter verificatie)		Paspoorten worden wel gecontroleerd, kaarten samengevoegd als persoon twee keer in systeem staat.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)		Kopie naar database waarop Cognos rapporten kunnen worden gedraaid (managementinformatie).
Samenbrengen (samenvoegen)	X	Als iemand op meerdere kaarten, meerdere keren is binnen gekomen, wordt dat tot een enkele persoonskaart samengebracht.
Met elkaar in verband brengen (vanuit de applicatie)	X	Als persoon twee keer is ingevuld dan voegt het systeem het samen tot een enkele persoonskaart.
Afscherming (minder zichtbaar of toegankelijk maken ter bescherming van)	X	Er zijn 18 autorisatieprofielen (Van beheerder tot alleen lezen)
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	Er zijn geen backups, als het systeem crasht wordt de data opnieuw ingevoerd. Van de applicatie worden geen back-ups gemaakt. Informatie van schepen en scheepbewegingen worden opnieuw ingelezen.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	NVT	
Onderzoek rechtsorde bepaald geval	Artikel 9	NVT	
Informatiepositie	Artikel 10	NVT	
Informanten	Artikel 12	NVT	
Ondersteunende taken	Artikel 13	NVT	
Vreemdelingenwet 2000		X	
AVG*		X	*Pas later van toepassing, omdat nieuwe Wpg richtlijnen op dit moment nog niet zijn afgehandeld in de politiek

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

ZUIS heeft op dit moment een volwassenheidsniveau van 1. Dit geeft aan dat ZUIS onvoldoende compliant is op het gebied van Privacy & Security by Design (PSbD). 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. Op het moment van de 0-meting viel ZUIS nog onder de Wpg binnenkort zal dat verschuiven naar de AVG. Op de wetscriteria heeft ZUIS een score van 44% en op de criteria van het politiebeleid scoort ZUIS 40%. Dat is een matige score, wat aangeeft dat er nog wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij generieke terugmeldvoorziening (eenmalige vastlegging), informatiebeveiliging, verwerkingsgrondslag (doelbinding), duurzaam bewaren (bewaren en vernietigen) en metagegevens er negatief uitspringen. Daarnaast is het zorgelijk dat het beheer van ZUIS (qua kennis) vooral in handen is van één persoon 10.2.e .

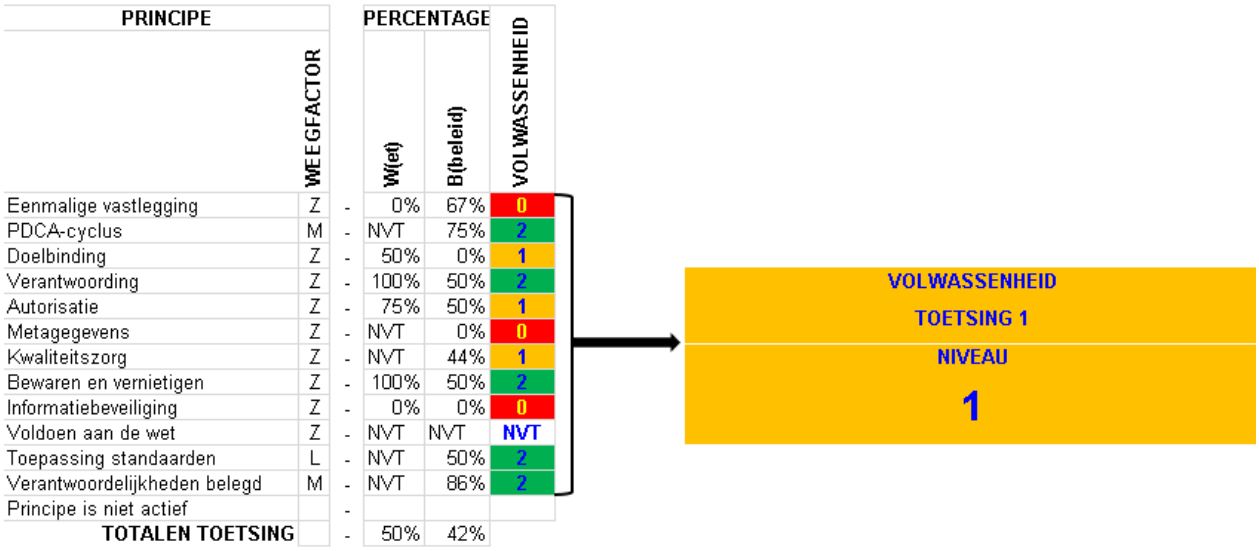
Advies:

- **(Wet art 4 lid 1): Zorg dat ZUIS de uitvoeringsverantwoordelijke (automatisch) ondersteunt bij het terugmelden van een gegeven, indien er gerede twijfel bestaat over het gegeven (alleen vanuit Wpg verplicht bij een externe bronhouder) [p1c6].**
- **(Wet art 3 lid 1 Wpg): Zorg dat de verwerkingsgrondslag van de in ZUIS verwerkte gegevens in de voorziening is opgenomen (art. 5 lid 1 sub d AVG; juistheid van gegevens) [p3c1].**
- **(Wet art 6 Wpg): Zorg dat ZUIS gebruik maakt van de vastgestelde autorisatierollen van de politie (art. 5 lid 1 sub f AVG) [p5c2].**
- **(Wet art 4 lid 3): Zorg dat er op basis van de resultaten uit de risicoanalyse de informatiebeveiligingseisen vastgesteld kunnen worden (art. 5 lid 1 sub f AVG) [p9c2].**
- **(Wet art 4 lid 3): Beoordeel de impact van de informatiebeveiligingseisen op de realisatie van de voorziening (art. 5 lid 1 sub f AVG) [p9c3].**

Aandachtspunten:

- **Het is het zorgelijk dat het beheer van ZUIS (qua kennis) vooral in handen is van één persoon 10.2.e .**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
ZUIS	17-01-2018	V1.0	50%	42%	1



PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	0%	67%	0
PDCA-cyclus	M	-	NVT	75%	2
Doelbinding	Z	-	50%	0%	1
Verantwoording	Z	-	100%	50%	2
Autorisatie	Z	-	75%	50%	1
Metagegevens	Z	-	NVT	0%	0
Kwaliteitszorg	Z	-	NVT	44%	1
Bewaren en vernietigen	Z	-	100%	50%	2
Informatiebeveiliging	Z	-	0%	0%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	50%	2
Verantwoordelijkheden belegd	M	-	NVT	86%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	50%	42%	

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.

ZUIS scoort onvoldoende op het principe eenmalige vastlegging meervoudig gebruik. Er wordt geen gebruik gemaakt van vastgestelde referentiegegevens. Het is binnen ZUIS mogelijk om bijvoorbeeld de landentabel aan te passen (bijvoorbeeld om NED te wijzigen in HOL). Er worden eigen tabellen gebruikt die niet in contact staan met de GGB (Gegevens, Gebruik en Beheer).
Door de samenwerking met de Kmar en het Maritiem single window loket voor scheepgegevens en persoonsgegevens worden o.a. persoonsgegevens via de koppeling in ZUIS ingelezen, alleen bij een correctie wordt er nog handmatig gewerkt. Daarnaast wordt er bij het ontbreken van data wel een technische signalering gemeld, maar zal de terugkoppeling handmatig moeten worden gedaan in plaats van automatisch.

Actiepunten:

- (Beleid): Zorg dat ZUIS gebruik maakt van vastgestelde referentiegegevens. Maak hier voor contact met de GGB [p1c1].
- **Wet art 4 lid 1): Zorg dat ZUIS de uitvoeringsverantwoordelijke (automatisch) ondersteunt bij het terugmelden van een gegeven, indien er gerede twijfel bestaat over het gegeven (alleen vanuit Wpg verplicht bij een externe bronhouder) [p1c6].**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	0%	67%	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.

Op het gebied van sturing wordt er geen gebruik gemaakt van stuurinformatie uit ZUIS. Daarnaast worden er geen rapportages t.b.v. de besturing van gegevensverwerking (geautomatiseerd) opgeleverd. Er zou wel een query gemaakt kunnen worden waar een rapport uit gemaakt zou kunnen worden.

Actiepunten:

- (Beleid): Zorg dat ZUIS stuurinformatie aanlevert, zodat er gestuurd kan worden op basis van de informatie vanuit ZUIS [p2c1].
- (Beleid): Zorg dat er rapportages (automatisch) worden op geleverd t.b.v. de besturing van de gegevensverwerking [p2c7].

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

1.3 Doelbinding

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

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

Op dit moment wordt de verwerkingsgrondslag van verwerkte gegevens niet in ZUIS opgenomen. Dit is een essentieel onderdeel om de doelbinding van een verwerkte gegeven vast te kunnen stellen. Het verwerken van de verwerkingsgrondslag staat op de backlog, maar het advies is om dit een hogere prioriteit te geven.

Actiepunten:

- **(Wet art 3 lid 1 Wpg): Zorg dat de verwerkingsgrondslag van de in ZUIS verwerkte gegevens in de voorziening is opgenomen (art. 5 lid 1 sub d AVG; juistheid van gegevens) [p3c1].**
- (Beleid): Zorg dat de verwerkingsgrondslag is opgenomen in het gegevensmodel van ZUIS [p3c2].
- (Beleid): Zorg dat de verwerkingsgrondslag automatisch kan worden herleid [p3c4].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	50%	0%	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.

Vanuit ZUIS kan er nog worden gekeken naar de mogelijkheid tot manipulatie van de audittrail. Er is een speciale audit functionaliteit die (tegen licentiekosten) aan kan worden gezet waarbij de acties van onder andere 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 ZUIS bewust is met het risico en dat het risico is geminimaliseerd of is geaccepteerd (restrisico's).

Actiepunten:

- (Beleid): Zorg dat de audittrail van ZUIS beveiligd is tegen manipulatie van gebruikers en beheerders [p4c3].

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

ZUIS maakt (nog) geen gebruik van de generieke IAM-voorziening. Om de autorisatie centraal onder controle te hebben is het aan te raden om gebruik te maken van de generieke IAM-voorziening. Daarnaast is het aan te raden om rapporten te generen op het gebied van autorisaties. Op dit moment is het wel raadpleegbaar door de functioneel beheerder, maar kan het dus niet in een rapport gegenereerd worden.

Actiepunten:

- (Beleid): Zorg dat ZUIS gebruik gaat maken van de generieke IAM-voorziening [p5c1].
    - **(Wet art 6 Wpg): Zorg dat ZUIS gebruik maakt van de vastgestelde autorisatierollen van de politie (art. 5 lid 1 sub f AVG) [p5c2].**
    - (Beleid): Zorg dat ZUIS Audit Based Access Control ondersteunt (alleen van toepassing indien er geen gebruik gemaakt gaat worden van de IAM-voorziening) [p5c5].
- (Beleid): Zorg dat ZUIS rapporten genereert op het gebied van autorisaties [p5c7].

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

Het eerder benoemde ontbreken van de verwerkingsgrondslag en het niet gebruiken van enige vorm van metagegevens zorgen ervoor dat de juistheid en rechtmatigheid van het gebruik van ZUIS moeilijk is vast te stellen. Metagegevens die daarvoor in aanmerking zouden geautomatiseerd of niet geautomatiseerd moeten kunnen worden afgeleid en vastgelegd. Binnen ZUIS is dat op dit moment niet mogelijk

Actiepunten:

- (Beleid): Zorg dat ZUIS effectief gebruik gaat maken van het verwerken van metagegevens. Hieronder staan de kenmerken die van de verwerkte gegevens worden verwacht [p6c7]:
    - Identificatiekenmerken,
    - Wettelijke verwerkingsgrondslag
    - Kenmerken die noodzakelijk zijn voor het verwerken van gegevens binnen het politieproces en/of binnen de keten, voorbeelden zijn 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 is dit verplicht),
    - Logginggegevens, zoals tijd en datum en wie met welke taak is ingelogd.
- (Beleid): Zorg dat ZUIS metagegevens die daarvoor in aanmerking komen geautomatiseerd of niet geautomatiseerd kan afleiden en vastleggen [p6c8] [p6c9].
- (Beleid): Zorg dat ZUIS gebruik maakt van metagegevens voor bijvoorbeeld het verlenen van toegang, bewaartermijnen, audittrails of managementrapportages [p6c10].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	0%	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.

ZUIS zal meer aandacht moeten besteden aan de waarborging van de kwaliteit van de gegevensverwerking. Er zijn geen bedrijfsregels geformuleerd om de kwaliteit van de gegevens te meten. Het is onduidelijk welke geautomatiseerde controles zijn ingebouwd. Daarnaast is het niet mogelijk om een rapport op te stellen over de kwaliteit van gegevens.

Actiepunten:

- (Beleid): Zorg dat er bedrijfsregels geformuleerd zijn om de kwaliteit van gegevens te meten [p7c5].
- (Beleid): Zorg dat er duidelijkheid komt over welke geautomatiseerde controles zijn ingebouwd om de gegevens kwaliteit te meten [p7c6].
- (Beleid): Zorg dat er rapporten kunnen worden samengesteld over de kwaliteit van gegevens [p7c7].
    - (Beleid): Zorg ervoor dat de resultaten uit uitgevoerde kwaliteitsrapporten worden bewaard [p7c8].
- (Beleid): Zorg ervoor dat gebruikers geattendeerd worden op kwaliteitsafwijkingen (op basis van geformuleerde kwaliteitseisen) [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.

ZUIS zal moeten kijken hoe het omgaat met het duurzaam bewaren en toegankelijkheid van gegevens. Zeker nu het in de toekomst vervangen zal gaan worden. Daarnaast is er op moment vervuiling in ZUIS wat niet geautomatiseerd verwijderd wordt (dat gebeurt nu handmatig).

Actiepunten:

- (Beleid): Zorg dat gegevens op basis van de geldende termijnen geautomatiseerd verwijderd en vernietigd worden [p8c4].
- (Beleid): Zorg dat ZUIS voldoet aan de kwaliteitseisen van de DUTO standaard [p8c8]
    - Hieronder staat in het kort beschreven aan welke eisen het vooralsnog niet doet:
        - Eis 1 Er is een informatiemodel waarin alle informatieobjecten zijn beschreven die de organisatie ontvangt en creëert.
        - Eis 2 Informatieobjecten zijn ingedeeld in risicoklassen. Per risicoklasse is het toegankelijkheidsniveau bepaald waaraan de betreffende informatieobjecten moeten voldoen.
        - Eis 3 Er is een vastgestelde Selectielijst waarin is beschreven hoe lang informatieobjecten bewaard worden.
        - Eis 9 Informatieobjecten zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen. Conform de geldende standaarden voor informatiebeveiliging.
        - Eis 12 Informatieobjecten worden niet eerder en niet later vernietigd dan is aangeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	100%	50%	2

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 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 is niet meer goed genoeg is. ZUIS heeft op dit moment nog helemaal geen risicoanalyse uitgevoerd op het gebied van informatiebeveiliging. Daarnaast zijn de potentiele risico's van ZUIS niet in beheer.

Actiepunten:

- (Beleid): Zorg dat een nieuwe risicoanalyse uitgevoerd gaat worden [p9c1].
    - **(Wet art 4 lid 3): Zorg dat er op basis van de resultaten uit de risicoanalyse de informatiebeveiligingseisen vastgesteld kunnen worden (art. 5 lid 1 sub f AVG [p9c2].**
    - **(Wet art 4 lid 3): Beoordeel de impact van de informatiebeveiligingseisen op de realisatie van de voorziening (art. 5 lid 1 sub f AVG [p9c3].**
    - (Beleid): Maak indien mogelijk gebruik van de generieke voorzieningen voor informatiebeveiliging [p9c4].
    - (Beleid): Bekijk of het mogelijk is alle informatiebeveiligingseisen te realiseren met de standaard informatiebeveiligingseisen [p9c5].
    - (Beleid): Zorg dat er maatregelen zijn genomen om informatiebeveiligingseisen te realiseren die niet door de standaard informatiebeveligingsdiensten zijn gerealiseerd [p9c6].
    - (Beleid): Stel een lijst van restrisico's op en zorg dat de ze beheerd zullen worden [p9c7].

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.

ZUIS maakt op basis van XML gebruik van een API koppeling en koppeling 10.2.c Het is van belang om controle te houden op afwijkingen van de geldende standaarden.

Actiepunten:

- (Beleid): Zorg dat afwijkingen van geldende standaarden worden voorzien van een motivatie die geaccepteerd is door de verwerkingsverantwoordelijke [p11c3].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT	50%	2

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

De verantwoordelijkheden binnen ZUIS zijn goed belegd. Echter het is het zorgelijk dat het beheer van ZUIS (qua kennis) vooral in handen is van één persoon die binnenkort met pensioen gaat.

Actiepunten:

- (Beleid): Zorg dat de uitvoeringsverantwoordelijke binnen ZUIS voldoende zal worden ondersteunt met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid [p12c4].

Aandachtspunten:

- **Het is het zorgelijk dat het beheer van ZUIS (qua kennis) vooral in handen is van één persoon** 10.2.e

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

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 compliancy van de informatievoorziening.

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

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

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

Bij het bepalen van de volwassenheid wordt er gekeken naar de huidige situatie van ZUIS. Er kan hierbij onderscheid gemaakt worden tussen ontwikkeling, invoering en uitvoering. Om de volwassenheid te bepalen wordt er gekeken in hoeverre vereiste functionaliteiten de status van uitvoering hebben gekregen. Hiermee kan het dus voorkomen dat er actiepunten genoteerd staan die wel al ‘in ontwikkeling’ en/of ‘ ingevoerd worden’ staan[3].

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

[3] Bijlage 1: Uitgangspunt bij compliance

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

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

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

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

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

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

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

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

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

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

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

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

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

Aandachtspunten
1: Volwassenheidsniveau 1:

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

2: Beleidscriteria:

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

3: Privacy functionaris:

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

Disclaimer

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

Bijlage 1: Uitgangspunt bij compliance

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

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