0-meting Privacy & Security by Design

AGORA

10.2.e

Concept

Versie 1.00

Versie datum 13 maart 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	21-9-2018	Reviewen
0.9	26-9-2018	Aanpassingen verwerkt
0.91	30-1-2019	Aanpassingen betrokken Agora verwerkt
1.00	13-3-2019	Rapport definitief (wederzijds akkoord)

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	21-9-2018	10.2.e	Gegevensautoriteit
0.9	26-9-2018	10.2.e	Gegevensautoriteit
0.91	30-1-2019	10.2.e	Gegevensautoriteit

Inhoudsopgave

Inleiding

Eind 2015 heeft de Auditdienst Rijk (ADR) gerapporteerd over uitgevoerde (externe) privacy audit en dat heeft aangetoond dat er op het gebied van Privacy en Security verbeteringen nodig zijn. Het verbeterprogramma Wpg en IB is daarna gestart om compliancy te realiseren (eerdere programma's hebben niet tot een bevredigend resultaat geleid). Met het meerjarig verbeterplan zijn in maart 2016 politieke toezeggingen gedaan aan de Tweede Kamer.[1]

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

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

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

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 Agora	10.2.e	Business expert
	10.2.e	Business expert
	10.2.e	Applicatiemanager
	10.2.e	Functioneel Beheerder
	10.2.e	Applicatiemanager

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

Gespreksdatum	Nummer meting	Toelichting
15-2-2018 en 1-3-2018	2018010301	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

AGORA

Omschrijving applicatie

Agora is Grieks voor (dorps)plein ofwel het verzamelpunt waar, in ieder geval in de oudheid, de belangstellenden de laatste nieuwtjes uitwisselden. Op het SharePoint 2013 platform is Agora een verzameling sites. Met Agora kun je met een team samenwerken en makkelijk documenten met elkaar delen. Er zijn drie soorten websites: open (iedereen die bij kantoorautomatisering kan, kan op Agora), besloten (projectpagina's, is vastgesteld obv groepen), gesloten (obv individuele uitnodiging).

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	Geen registratie zoals in een registratiesysteem
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen		
Raadplegen	X	
Gebruiken	X	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen	X	
Met elkaar in verband brengen		
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	
Vernietigen	X	

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9		Politiechef kan wel art. 9 gegevens in Agora zetten, maar de verwerking op Agora is dan obv art. 8 Wpg Bijvoorbeeld een verdachte oppakken (art. 8 Wpg) tbv een groot onderzoek (art. 9).
Informatiepositie	Artikel 10		
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

Agora heeft een volwassenheidsniveau van 1. Dit houdt in dat Agora onvoldoende compliant is op het gebied van Privacy & Security by Design (PSbD). Er is wel specifiek aandacht op het gebied van PSbD, maar die is vooralsnog niet toereikend om te voldoen aan de wet (Wpg) en op basis van het politiebeleid. Op de wetscriteria heeft Agora een score van 64% en op de criteria van het politiebeleid een score van 62%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'autoriseren' en 'bewaren en vernietigen' er negatief uitspringen. Daarnaast heeft Agora een probleem met het waarborgen van de kwaliteit, omdat de content een bepaling is van de sitebeheerder. Inmiddels zijn er meer dan duizend sitebeheerders waardoor ons advies is om het principe kwaliteitszorg extra aandacht te geven. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen.

Advies:

- **(Wet art 32a): Genereer periodieke rapportages over de audittrail. [p4c4]*****
- **(Wet artikel 4a): Gebruikers moet voldoende worden geïnstrueerd mb.t de voor hen geldende autorisatieregels. [p5c6]**
- **(Wet artikel 4a): Controleer ook toegang- en gebruikersrechten bij gesloten pagina's [p5c8]*****
- **(Wet: artikel 14): Zorg dat er daar waar mogelijk gebruik wordt gemaakt van de generieke selectielijst en daarmee kan worden voldaan aan artikel 14 van de Wpg. [p8c1]**
- **(Wet: artikel 8, 9, 10 en 14): Zorg dat Agora voldoet aan de wettelijke bepalingen m.b.t. het bewaren, vernietigen en archiveren van gegevens. [p8c2]**
- **(Wet artikel 14 lid 4) Zorg dat Agora het beschikbaar stellen van de gegevens aan de voorziening ondersteunt ten behoeve van duurzaam bewaren. Archiveren is niet meegenomen tijdens deze 0-meting, maar is zeker een facet waar in de toekomst rekening mee zal moeten worden gehouden. Gezien het feit dat het aantal pagina's zal toenemen is duurzaam bewaren echt van belang. [p8c9]**

Aandachtspunten:

- Agora is niet bedoeld als registratiesysteem en er zal daardoor niet of beperkt gecontroleerd kunnen worden of gegevens al bestaan. Dat is verklaarbaar, maar zorg dat het proces wat wel en niet op Agora kan mbt politiegegevens actiever in de gaten zal worden gehouden (hiervoor zijn meer middelen nodig).
- Zorg dat het mogelijk is om de doelbinding van de verwerkte gegevens (binnen de pagina's) te controleren, ondanks de procedurele afspraken (art 8) die zijn voorgelegd aan de beheerders van Agora pagina's.

UPDATE 30-1-2019

Tussen de 0-meting en de definitieve versie van het rapport zat meer dan 6 maanden. Hierdoor zijn veel actiepunten die genoemd zijn tijdens de 0-meting al opgelost. De huidige situatie van de actiepunten zal in het feedbackformulier aangegeven worden.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Agora	1-3-2018	V1.0	64%	62%	1

***LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar dit is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).**

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	NVT	38%	1
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	25%	2
Autorisatie	Z	-	0%	70%	0
Metagegevens	Z	-	100%	67%	2
Kwaliteitszorg	Z	-	NVT	40%	1
Bewaren en vernietigen	Z	-	0%	0%	0
Informatiebeveiliging	Z	-	100%	80%	2
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	80%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	64%	62%	

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.

Bij het principe eenmalige vastlegging scoort Agora een volwassenheidsniveau van 3. Dit principe is merendeel niet van toepassing voor Agora aangezien het niet gezien kan worden als een registratiesysteem. Echter doordat er wel politiegegevens op Agora gezet worden is hier goed naar gekeken. Bij onjuistheid van informatie heeft de gebruiker de mogelijkheid om een reactie te geven (die bij de beheerder zichtbaar is). Desondanks moet worden voorkomen dat politiegegevens onnodig (lang) op Agora terecht komen. Er zal dus actiever gekeken moeten worden naar het proces wat wel en wat niet op Agora kan.

Aandachtspunt:

- Agora is niet bedoeld als registratiesysteem en er zal daardoor niet of beperkt gecontroleerd kunnen worden of gegevens al bestaan. Dat is verklaarbaar, maar zorg dat het proces wat wel en niet op Agora kan mbt politiegegevens actiever in de gaten gehouden zal worden (hiervoor zijn meer middelen nodig).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	100%	3

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.

Agora levert slechts beperkte stuurinformatie. Er is wel maandelijks een vlootschouw waarin wekelijks rapportages worden besproken. Echter binnen het team is er onvoldoende capaciteit beschikbaar om alles te kunnen behandelen en te voldoen aan de vereiste kwaliteit. Het beheer van een pagina (gegevens) komt pas in beeld indien deze niet meer wordt gebruikt (daarvoor niet). Er worden geen rapportages van risicoanalyses opgeleverd t.b.v. de besturing van de gegevensverwerking. Daarnaast zijn de portefeuillehouders en politiechefs die verantwoordelijk zijn voor regie op definities, beleid, koers en strategie inhoudelijk niet voldoende op de hoogte.

Actiepunten:

- (Beleid): Zorg dat Agora stuurinformatie levert t.b.v. de PDCA-cyclus. [p2c1]
- (Beleid): Agora moet zorgen voor eerder (automatisch) beheer op de gegevens van pagina's. [p2c2]
- (Beleid): De portefeuillehouders en politiechefs moeten meer inhoudelijk op de hoogte zijn om regie, beleid, koers en strategie te kunnen bepalen. [p2c6]
- (Beleid): Agora moet rapportages van risicoanalyses (geautomatiseerd) opleveren t.b.v. de besturing van de gegevensverwerking. [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	38%	1

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.

Agora voldoet aan de doelbinding omdat binnen de applicatie van te voren is vastgelegd wat de verwerkingsgrondslag is waarop politiegegevens worden geregistreerd. Er is afgesproken dat alles op Agora mbt politiegegevens valt onder artikel 8. Indien er politiegegevens erop gezet worden die niet onder artikel 8 vallen, dan wordt de beheerder van de pagina hierop aangesproken en dient het van de pagina te worden gehaald.

Aandachtspunt:

- Het is onvoldoende mogelijk om de doelbinding van alle verwerkte gegevens (binnen de pagina's) te controleren ondanks de procedurele afspraken (art 8) die zijn gemaakt voor beheerders van Agora pagina's.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	100%	100%	3

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.

Agora voldoet volledig aan de wetscriteria gesteld in het principe verantwoording, want er wordt een audittrail geregistreerd. Echter het is niet mogelijk om een rapportage van deze audittrail te genereren. Hiervoor werd het belang van periodieke rapportages ook al aangegeven. Naast dat periodieke rapportages kunnen helpen bij het anticiperen op bepaalde ontwikkelingen is het bij de audittrail ook van belang als een toezichthouder inzicht in de applicatie wil krijgen. Vanaf januari 2019 is het daarom ook verplicht om een rapportage van de audittrail te kunnen genereren. Daarnaast moet de audittrail beter worden beveiligd tegen manipulatie. Het gaat hier niet alleen om manipulatie door gebruikers, maar ook door (database)beheerders. Bij Oracle bestaat er een speciale audit functionaliteit die tegen licentiekosten aan kan worden gezet. Het is aan de productowner van Agora om de afweging te maken tussen de kosten en de baten.

Actiepunten

- (Beleid): Agora moet een weloverwogen keuze maken in het beveiligen van een audittrail tegen manipulatie. [p4c3]
  - Bescherm de mogelijkheid van manipulatie niet alleen voor gebruikers maar ook door beheerders.
  - Maak een bewuste keuze om de audittrail ook voor beheerders te beschermen tegen manipulatie (kosten/baten)
- **(Wet art 32a): Genereer periodieke rapportages over de audittrail. [p4c4]**
  LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar dit is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	25%	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.

Binnen Agora is de aandacht bij autorisatie vooral gefocust op de paginabeheerder en minder op de gebruiker. Gebruikers zijn onvoldoende geïnstrueerd mb.t de voor hen geldende autorisatieregels (Wpg). Daarnaast kunnen er binnen Agora wel rapporten opgeleverd worden voor het gebruik van autorisaties, maar wordt dit op dit moment niet gedaan.

Gebruikers en toegangsrechten voor besloten en open pagina's worden gecontroleerd d.m.v. Active Directory (AD). Echter de gesloten pagina's worden niet gecontroleerd d.m.v. AD. De gesloten pagina's gaan via persoonlijke uitnodiging en dit zorgt ervoor dat er geen controle is op de toegang- en gebruiksrechten tenzij de beheerder van de pagina's dit op zich neemt. Indien er bij een gesloten pagina gebruik zal worden gemaakt van politiegegevens, dan zal dit gecontroleerd moeten worden.

Actiepunten:

- **(Wet artikel 4a): Gebruikers moet voldoende worden geïnstrueerd mb.t de voor hen geldende autorisatieregels. [p5c6]**
- (Beleid): Agora moet rapportages opleveren voor het gebruik van autorisaties. [p5c7]
- **(Wet artikel 4a): Controleer ook toegang- en gebruikersrechten bij gesloten pagina's. [p5c8]**
  LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar dit is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	0%	70%	0

1.6 Metagegevens

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

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

De wettelijke criteria voor het principe metagegevens zijn niet van toepassing op Agora. Op de beleidscriteria scoort Agora 67%, waarmee het een voldoende volwassenheid score is behaald. Het Toepassingsprofiel Metagegevens Rijk wordt nog niet toegepast bij verdere ontwikkeling van Agora.

Actiepunten:

- Zorg dat er gebruik gemaakt gaat worden van metagegevens, zodat de juistheid en rechtmatigheid gewaarborgd kunnen worden.
    - (Beleid): Gebruik zolang het Toepassingsprofiel Metagegevens Politie in ontwikkeling is het Toepassingsprofiel Metagegevens Rijk (TMR) voor het opstellen van de requirements voor metagegevens. [p6c4]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	67%	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.

Ook bij het principe Kwaliteitszorg zijn er geen wettelijke criteria van toepassing. Op beleidscriteria scoort Agora 40%. Er zijn bij Agora geen automatische controles ingebouwd om de gegevenskwaliteit te meten. Er is 1x per maand de eerder genoemde (handmatige) vlootschouw, maar in de basis blijft de sitebeheerder verantwoordelijk voor de content op de pagina. Waarbij ook hier gemeld moet worden dat kwaliteitscontroles niet volledig gedaan kunnen worden vanwege capaciteitsproblemen. Er zal meer aandacht (capaciteit/middelen) moeten komen om de kwaliteit te kunnen waarborgen..

Actiepunten:

- (Beleid): Zorg dat er binnen Agora een automatische controles ingebouwd wordt om de gegevenskwaliteit te meten. [p7c6]
- (Beleid): Zorg dat er een rapport opgeleverd/samengesteld kan worden over de kwaliteit van de gegevens. [p7c7]
- (Beleid): Zorg dat er middelen/capaciteit beschikbaar wordt gesteld om de kwaliteitscontroles van de vlootschouw kwantitatief en kwalitatief te verbeteren. [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	40%	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 Agora niet op het gebied van bewaren en vernietigen. Ondanks het gebruik van de vlootschouw is het mogelijk om daarvan af te wijken door de paginabeheerder. Agora voldoet hiermee niet aan artikel 14 van de Wpg. Initieel is Agora geen registratiesysteem, maar er worden wel politiegegevens door paginabeheerders verwerkt. Dat betekent dat Agora niet voldoet aan de wettelijke bepalingen voor zowel het bewaren, vernietigen als voor het archiveren van gegevens.

Actiepunten:

- **(Wet: artikel 14): Zorg dat er daar waar mogelijk gebruik wordt gemaakt van de generieke selectielijst en daarmee kan worden voldaan aan artikel 14 van de Wpg. [p8c1]**
- **(Wet: artikel 8, 9, 10 en 14): Zorg dat Agora voldoet aan de wettelijke bepalingen m.b.t. het bewaren, vernietigen en archiveren van gegevens [p8c2]**
- (Beleid): Zorg dat gegevens op basis van de geldende termijnen geautomatiseerd verwijderd en vernietigd worden. [p8c4]
- **(Wet artikel 14 lid 4): Zorg dat Agora het beschikbaar stellen van de gegevens aan de voorziening ondersteunt ten behoeve van duurzaam bewaren. Archiveren is niet meegenomen tijdens deze 0-meting, maar is zeker een facet waar in de toekomst rekening mee zal moeten worden gehouden. Gezien het feit dat het aantal pagina's zal toenemen is duurzaam bewaren echt van belang. [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.

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. Bij Agora is een risicoanalyse gedaan, maar is er geen beheer op de risico's die wel in beeld zijn. Waarbij het niet duidelijk is of daar bewust en/of onbewust niets mee is gedaan.

Actiepunten:

- (Beleid): Zorg dat restrisico's in de beveiliging van Agora periodiek worden beheerd. [p9c7]

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

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.

Agora maakt daar waar mogelijk is gebruik van bestaande overheids- en ketenstandaarden. Er zijn bij dit principe geen wetscriteria actief dus Agora heeft de maximale volwassenheidsscore van 100%.

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

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 zijn binnen Agora voldoende belegd. Echter er zijn wel verbeteringen te maken in de bewustwording van de verantwoordelijkheden van een uitvoeringsverantwoordelijke (bijvoorbeeld een leidinggevende basisteam of PDC), omdat deze alleen naar de paginabeheerder worden aangegeven. Daarnaast zijn de taken van gegevensverwerkers (individuele politiemedewerker) om gegevens zorgvuldig en rechtmatig te verwerken maar deels ondersteunt. Bijvoorbeeld de afbeeldingsbibliotheek zit de controle er in, maar maak je het zelf aan dan kan er om deze controle heen gewerkt worden.

Actiepunten:

- (Beleid): Zorg dat de uitvoeringsverantwoordelijke voldoende bewust is wat zijn verantwoordelijkheden zijn. [p12c3]
- (Beleid): Zorg dat de taken van gegevensverwerkers om gegevens zorgvuldig en rechtmatig zal worden ondersteunt. [p12c7]

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