0-meting Privacy & Security by Design

Internet-aangifte

10.2.e

Definitief

Versie 1.00

Versie datum 11 april 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	2-10-2018	Aanpassingen verwerkt
0.91	22-3-2019	Aanpassingen nav feedback betrokkenen
1.00	11-04-2019	Rapport definitief na wederzijds goedkeuren

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	21-9-2018	10.2.e	Gegevensautoriteit
0.9	2-10-2018	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 de applicatie Internetaangifte. 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 Internetaangifte.
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 Internetaangifte

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 Internetaangifte	10.2.e	Adviseur Proces- en informatiemanagement
	10.2.e	Functioneel beheerder Internetaangifte
	10.2.e	Business expert
	10.2.e	Business expert
	10.2.e	Privacy functionaris
	10.2.e	IV expert
	10.2.e	IV expert

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

Gespreksdatum	Nummer meting	Toelichting
29-1-2018 & 3-4-2018	2018040301	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Internetaangifte

Omschrijving applicatie

Internetaangifte is een webapplicatie waarbij het voor het burger mogelijk is om een aangifte via internet te doen. Dit kan de burger doen op www.politie.nl. Op www.politie.nl wordt de aangever gevraagd wat deze precies wil en dat kan leiden tot het doen van Internetaangifte. Bij de keuze voor internetaangifte wordt de burger via DigiD met tweefactor-authenticatie geïdentificeerd. Zijn/haar gegevens worden aan de aangifte toegevoegd d.m.v. het BSN en een raadpleging van de personenserver. Via de website kunnen bij de volgende situaties gebruik worden gemaakt van de Internetaangifte webapplicatie:

- Diefstal
- Sommige vormen van (internet) oplichting
- Vernieling

Soorten verwerkingen van politiegegevens

Soort verwerking	X	toelichting
Verzamelen	X	
Vastleggen (registreren)	X	
Ordenen (vb. in categorieën plaatsen)	X	Persoonsgegevens apart, goederen apart, soort aangifte, etc.
Bewaren (opslaan)	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	Aanvullen (bijvoorbeeld als de aangifte niet compleet is wordt er contact met burger opgenomen). Een aangifte mag na afsluiten niet meer gewijzigd worden. Aanvullen op het bestaande mag wel.
Wijzigen (het bestaande aanpassen)	X	Als het adres bijvoorbeeld niet strookt met locatie dan kan dat worden gewijzigd (alléén door politie).
Opvragen (ophalen van gegevens)	X	Persoonsgegevens uit personenserver, openbare gegevens mbt kenteken. Er is geen link met KvK.
Raadplegen (bekijken van gegevens)	X	
Gebruiken	X	
Vergelijken (bv ter verificatie)	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Aangifte wordt aan burger teruggegeven, maar ook aan BVH. KMar heeft ook toegang en neemt in sommige gevallen aangiftes over.
Samenbrengen (samenvoegen)	X	Als een persoon meerdere keren aangifte heeft gedaan, dan wordt dit samengevoegd tot een persoonskaart.
Met elkaar in verband brengen (vanuit de applicatie)	X	Afhankelijk van de pleegplaats gaat aangifte (automatisch) naar betreffende eenheid.
Afscherming (minder zichtbaar of toegankelijk maken ter bescherming van)	X	Verschillende inlogmogelijkheden met verschillende autorisaties.
Uitwissen (weghalen/verwijderen zonder vernietigen)		
Vernietigen	X	Via internet is een aangifte 365 dagen zichtbaar, daarna wordt de aangifte vernietigd. Globale gegevens worden bewaard (aantallen etc). ***Back ups moeten worden gecontroleerd, niet duidelijk wanneer deze precies vernietigd worden***

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	Het is intake, dus pas als daarna blijkt dat het moet veranderen kan het in BVH naar een ander artikel overgaan.
Onderzoek rechtsorde bepaald geval	Artikel 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

Internetaangifte scoort een volwassenheidsniveau 1. Dit houdt in dat Internetaangifte 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 Internetaangifte een score van 78% 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 'Verantwoording' en 'Metagegevens' er negatief uitspringen.

Advies:

- **(Wet art 32a): Zorg dat een audittrail kan worden geregistreerd. [p4c1]**
- **(Beleid --> wet art 32a vanaf januari 2019): Maak het mogelijk om (periodiek) een rapportage van de audittrail te genereren. [p4c4]*****
- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening Internetaangifte. [p9c3]**

Aandachtspunten:

- **(Wet): Op dit moment worden IP-adressen van burgers 30 dagen opgeslagen. De vraag is of er een doel is gesteld om de IP-adressen van de burgers op te slaan. Indien er geen doel is dan mogen de IP-adressen niet worden opgeslagen en dient dat worden stopgezet.**
- Als een internetaangifte niet in behandeling wordt genomen dan wordt de (internet) aangifte teruggegeven aan de burger. Een voorbeeld hiervan is het verkeerde kanaal kiezen, dan krijgt de burger een brief met het verzoek om naar een bureau te gaan. Op dit moment worden niet aangenomen aangiftes niet als mutatie opgenomen, waardoor een burger alles opnieuw moet doen. Zorg ervoor dat niet aangenomen aangiftes worden geregistreerd.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Internetaangifte	3-4-2018	1.0	87%	62%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	100%	60%	2
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	0%	0%	0
Autorisatie	Z	-	100%	25%	2
Metagegevens	Z	-	NVT	29%	0
Kwaliteitszorg	Z	-	NVT	72%	2
Bewaren en vernietigen	Z	-	100%	50%	2
Informatiebeveiliging	Z	-	75%	80%	1
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	100%	3
Verantwoordelijkheden belegd	M	-	NVT	100%	3
Principe is niet actief		-			
TOTALEN TOETSING		-	87%	62%	

VOLWASSENHEID TOETSING 1 NIVEAU **1**

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.

***LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar is vanaf januari 2019 van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).**

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.

Internetaangifte heeft de maximale score op het principe eenmalige vastlegging behaald. Er is veel contact met de GGB over het gebruik van bronnen. Denk hierbij o.a. aan referentiegegevens en het terugmelden bij de bron indien gegevens niet juist zijn.

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.

Internetaangifte levert op verschillende manieren stuurinformatie ten behoeve van de PDCA-cyclus. Cijfers over aangiftes worden periodiek d.m.v. Cognos aangeleverd, maar daar wordt in beperkte mate sturing op gegeven. Daarnaast wordt er niet via een periodiek proces gerapporteerd over de kwaliteit van gegevens. Op het moment van de 0-meting werd er een gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd voor Internetaangifte.

Actiepunten:

- (Beleid): Zorg dat Internetaangifte periodiek een rapportage (stuurinformatie) oplevert op het gebied van kwaliteit van gegevens [p2c1].
- (Beleid): Zorg dat de GEB is afgerond [p2c3]
- (Beleid): Zorg dat er meer sturing komt t.b.v. van de besturing van de gegevensverwerking [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	100%	60%	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.

Internetaangifte voldoet op zowel de wet als beleid aan alles wat binnen de mogelijkheden ligt op het gebied van doelbinding. De doelbinding van Internetaangifte valt onder artikel 8 (handhaving).

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.

Op het principe verantwoording voldoet Internetaangifte niet. Er wordt op dit moment geen audittrail geregistreerd. Het is alleen mogelijk om in de historie te zien welke beoordelaar de aanvraag heeft behandeld. Echter het gaat hierbij alleen om de laatste persoon die beoordeelding heeft behandeld.

Het is van belang dat als een audittrail wordt geregistreerd dat deze is beveiligd tegen manipulatie. Dit betreft niet alleen manipulatie door de gebruiker, maar ook de manipulatie door een databasebeheerder. Er moet een afweging worden gemaakt tussen de kosten en baten van een dergelijke functionaliteit. Ook moet het mogelijk zijn om een rapportage van de audittrail te genereren, waarbij het belangrijk is om dergelijke rapportages bij te houden om de ontwikkelen in de gaten te houden. Dit was tijdens de 0-meting nog politiebeleid, maar zal vanaf Q4 2018 wet worden.

Actiepunten:

- **(Wet art 32a): Zorg dat een audittrail kan worden geregistreerd [p4c1].**
- (Beleid): Beveilig de audittrail tegen manipulatie door zowel gebruikers als (database)beheerders [p4c3].
- **(Beleid --> wet art 32a vanaf januari 2019): Maak het mogelijk om (periodiek) een rapportage van de audittrail te genereren [p4c4] .**

Aandachtspunt:

- **(Wet): Op dit moment worden IP-adressen van burgers 30 dagen opgeslagen. De vraag is of er een doel is gesteld om de IP-adressen van de burgers op te slaan. Indien er geen doel is dan mogen de IP-adres niet worden opgeslagen en dient dat worden stopgezet.**

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

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.

Internetaangifte maakt op dit moment geen gebruik van de generieke IAM-voorziening. Het staat op termijn wel op de planning om ingevoerd te worden. Daarnaast is het is op dit moment onduidelijk of Internetaangifte gebruik maakt van de ATL voorziening.

Actiepunten:

- (Beleid): Zorg dat Internetaangifte gebruik gaat maken van de IAM-voorziening van de politie [p5c1].
    - (Beleid): Zorg dat indien nodig Internetaangifte gebruik maakt van ATL voorziening als onderdeel van IAM. [p5c4]
- (Beleid): Zorg voor een periodieke geautomatiseerde controle van toegangs- en gebruikersrechten doormiddel van een geautomatiseerde rapportage op het gebruik van autorisaties [p5c7].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	25%	2

1.6 Metagegevens

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

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

Internetaangifte scoort een onvoldoende (niveau 0) op het gebied van metagegevens. Bij de ontwikkeling van Internetaangifte is nog niet bewust rekening gehouden met het gebruik van metagegevens. Het toepassingsprofiel metagegevens Rijk (TMR) is nog niet bekend. Metagegevens worden op dit moment niet bewust gebruikt.

Het gegevensmodel van Internetaangifte is nog niet afgestemd met het politiegegevensmodel (PGM). Er is tijdens de 0-meting wel aangegeven dat dit zal gebeuren zodra de HOS (Handhaving ontsluiting service) is geïmplementeerd.

Actiepunten

- (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 Internetaangifte het gegevensmodel afstemt op het politie gegevensmodel (PGM) [p6c5]
- (Beleid): Kijk naar de mogelijkheden om metagegevens die niet geautomatiseerd worden vastgelegd op andere manieren in te vullen [p6c9]
- (Beleid): Zorg dat Internetaangifte gebruik maakt van metagegevens voor het gebruik van het verlenen van toegang, bewaartermijnen, audittrails en managementrapportages [p6c10].
- (Beleid): Zorg dat metagegevens meegeleverd worden bij koppelingen voor verwerking in andere voorzieningen. [p6c11]

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

1.7 Kwaliteitszorg

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

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

Internetaangifte voldoet op het gebied van kwaliteitszorg, maar er zijn nog wel verbeteringen door te voeren. Kwaliteitseisen worden met de dienst IM kort gesloten, maar niet altijd bijgehouden in Jira. Er kan op dit moment geen rapport over de kwaliteit van gegevens worden samengesteld. Zodra dat rapport kan worden samengesteld is het van belang dat die uitgevoerde kwaliteitscontroles bewaard worden om te sturen op kwaliteitsverbeteringen. Dit zou ook beter afgestemd kunnen worden met de GGB.

Actiepunten:

- (Beleid): Zorg dat kwaliteitseisen worden bijgehouden, zodat indien nodig er een formeel akkoord gegeven kan worden door de beleidsverantwoordelijke [p7c2]
- (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]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	72%	2

1.8 Bewaren en vernietigen

"*Gegevens worden niet langer verwerkt dan is toegestaan en worden vernietigd zodra ze niet langer noodzakelijk zijn*"

De politie mag alleen gegevens verwerken indien en voor zolang daar een wettelijke grondslag voor bestaat. Als die grondslag komt te vervallen moeten de gegevens worden verwijderd of vernietigd. Ook voor gegevens waarvan blijkt dat ze onjuist zijn geldt dat ze moeten worden vernietigd of gecorrigeerd. De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden.

Op dit moment voldoet Internetaangifte niet aan het principe 'Bewaren en vernietigen'. Bij het team verantwoordelijk voor Internetaangifte is de DUTO standaard niet bekend en daardoor is het onduidelijk of Internetaangifte voldoet aan de kwaliteitseisen van de DUTO (indien van toepassing). Dit is van belang om overheidsgegevens duurzaam beschikbaar en toegankelijk te houden.

Actiepunten:

- (Beleid): Kijk in hoeverre Internetaangifte voldoet aan de DUTO en in welke mate dit van toepassing is. [p8c8]

Aandachtspunt:

- Als een internetaangifte niet in behandeling wordt genomen dan wordt de (internet) aangifte teruggegeven aan de burger. Een voorbeeld hiervan is het verkeerde kanaal kiezen, dan krijgt de burger een brief met het verzoek om naar een bureau te gaan. Op dit moment worden niet aangenomen aangiftes niet als mutatie opgenomen, waardoor een burger alles opnieuw moet doen.

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 regelmatige de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. Internetaangifte moet naar aanleiding van de risicoanalyse de impact opnemen van de te nemen informatiebeveiligingseisen. Daarnaast is het van belang om risico's die niet opgevangen zijn (restrisico's) te beheren en op periodieke basis vast te stellen of de restrisico's nog steeds verantwoord zijn.

Actiepunten:

- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening Internetaangifte. [p9c3]**
- (Beleid): Zorg dat het beheer van de restrisico's op periodieke basis gebeurt. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	75%	80%	1

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.

Internetaangifte voldoet aan het principe toepassen standaarden. Er wordt onder andere gebruik gemaakt van DigID en NOREA. Indien er afgeweken wordt van toepasbare standaarden dan zal dit eerst worden besproken met architecten en worden voorzien van een motivatie.

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

Het principe verantwoordelijkheden belegd heeft geen wetscriteria. Internetaangifte voldoet volledig aan het politiebeleid en heeft daarom een volwassenheidsniveau 3.

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

2. Verantwoording toetsing

Toetsingscriteria

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

Doel analyserapport
Het analyserapport geeft een cijfermatige analyse van de uitgevoerde toetsing met als doel om voor iedere informatievoorziening eenzelfde interpretatie van de toetsresultaten te genereren. Het resultaat van de analyse moet in samenhang met de bijzonderheden van de toetsing worden beschouwd. Alleen op deze manier ontstaat een compleet beeld van de mate van 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 compliance van de getoetste voorziening gegeven. Tevens wordt geen enkele garantie gegeven inzake de juistheid of volledigheid van de checklist als gevolg van veranderende wet- of regelgeving.

Bijlage 1: Uitgangspunt bij compliance

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

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