0-meting Privacy & Security by Design

LSV

10.2.e

Definitief

Versie 1.0

Versie datum 22 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
1.0	22-3-2019	Definitief na 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

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 applicatie LSV. 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 LSV

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 LSV 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 LSV	10.2.e	Operationeel specialist
	10.2.e	Functioneel beheerder
	10.2.e	Applicatiebeheerder

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

Gespreksdatum	Nummer meting	Toelichting
13-3-2018	2018031301	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

LSV (Landelijke Sporen Volgsysteem)

Omschrijving LSV

De applicatie Landelijk Sporen Volgen (LSV) ondersteunt het forensische opsporingsproces. Met de informatie die in LSV gezet kan worden kunnen exacte gegevens inzichtelijk worden rond het goed of spoor dat onderwerp is van het opsporingsproces. Met de overzichten die LSV oplevert, kan het zogeheten 'chain of custody' in beeld worden gebracht. Een tweede doel van LSV is het maken van de inzetplanning van de medewerkers forensische opsporing en inzicht krijgen in de werkdruk. Het moedersysteem stond oorspronkelijk bij het NFI, maar is overgenomen door de politie.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Via Excel, Formulieren (Word), Cognos
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	Verwijderen kan maar kan via archivering in alle situaties teruggehaald worden. Als bij BVH gegevens zijn verwijderd dan krijg je in LSV een melding dat de gegevens weg zijn (foutcode)
Vernietigen	X	

Verwerkingsgrondslag

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

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

LSV scoort op volwassenheidsniveau een onvoldoende (niveau 1).Dit houdt in dat LSV 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 LSV 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 'Bewaren en vernietigen', 'Informatiebeveiliging' en 'Toepassing standaarden' er negatief uitspringen. Ons advies is eerst te kijken naar de wetscriteria en daarna naar mogelijke verbeteringen op het politiebeleid. Hieronder staan de wetcriteria.

Advies:

- **(Wet archiefwet): Zorg dat bij verwerkte gegevens er een selectie gemaakt kan worden ten behoeve van bewaren en vernietigen [p8c3].**
- **(Wet art 14 lid 4): Zorg dat LSV daar waar mogelijk gegevens beschikbaar stelt ten behoeve van het duurzaam bewaren van gegevens [p8c9].**
- **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse [p9c2].**
- **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening [p9c3].**

Aandachtspunt:

- 10.2.c . Dit zal het risico vergroten mbt de beveiliging van manipulatie op audittrails. Zorg dat er een weloverwogen besluit genomen gaat worden om de risico's uit te sluiten of in het uiterste geval te beperken.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
LSV	13-3-2018	1.0	64%	62%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	33%	2
PDCA-cyclus	M	-	NVT	38%	1
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	50%	2
Autorisatie	Z	-	100%	80%	2
Metagegevens	Z	-	NVT	50%	2
Kwaliteitszorg	Z	-	NVT	83%	2
Bewaren en vernietigen	Z	-	33%	75%	0
Informatiebeveiliging	Z	-	0%	10%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	100%	3
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.

Op dit moment maakt LSV geen gebruik van referentiegegevens. Er is sprake van een subset die geen directe updates krijgt via de GGB. Op dit moment stelt LSV alleen gegevens ter beschikking via Excel, Word en Cognos. Wanneer gebruik gemaakt kan worden van een gegevensdienstenlaag is er een duidelijker beheer over de gegevens.

Actiepunten:

- (Beleid): Zorg dat indien mogelijk er gebruik wordt gemaakt van vastgestelde referentiegegevens. Hierbij is direct contact met de GGB een vereiste [p1c1].
- (Beleid): Zorg dat LSV gegevens ter beschikking kan stellen via een gegevensdienstenlaag [p1c9].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	33%	2

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.

Binnen LSV is het beheer van gegevens, processen en software deels onderdeel van de PDCA-cyclus. Echter het evalueren van de processen maakt nog onvoldoende deel uit van de PDCA-cyclus. Daarnaast is het leveren van stuurinformatie ten behoeve van de reguliere PDCA-cyclus zeer beperkt.

Actiepunten:

- (Beleid): Zorg dat er meer rapportages met LSV gemaakt kunnen worden, zodat er gestuurd kan worden op beveiligingsincidenten, kwaliteit van gegevens en autorisatie [p2c1].
- (Beleid): Zorg dat binnen LSV de evaluatie een vast onderdeel is van het beheer van de processen [p2c2].
- (Beleid): Zorg dat rapportages t.b.v. de besturing van de gegevensverwerking geautomatiseerd opgeleverd kan worden [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.

LSV voldoet op zowel wet als beleid aan alles wat binnen de mogelijkheden ligt op het gebied van doelbinding. De doelbinding van LSV valt onder artikel 13 (Forensische opsporing) en hiervoor is een goedgekeurd artikel 13 protocol aanwezig. Er is rekening gehouden met de datum einde verwerkingstermijn en die is opgenomen in het gegevensmodel.

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.

Binnen LSV is de audittrail nog niet optimaal beveiligt tegen manipulatie. Binnen de applicatie kunnen de gebruikers de audittrail niet manipuleren. Echter het is nu nog wel mogelijk dat een ontwikkelaar en/of beheerder de audittrail kan wijzigen zonder dat dit opgemerkt wordt. Een beheerder en/of ontwikkelaar moet een audittrail niet kunnen wijzigen zonder dat hiervan iets geregistreerd wordt. De registratie van handelingen moet beveiligd worden tegen manipulatie en moet waarborg bieden voor bewaring en goede toegankelijkheid. Het uiteindelijke doel is om ervoor te zorgen dat de bewijskracht voor het verantwoordingsdoel niet in gevaar komt. Er is een speciale audit functionaliteit die (tegen licentiekosten) aangezet kan worden (Oracle) waarbij de acties van o.a. de database administrator kunnen worden geregistreerd. Er zal hierbij wel een afweging moeten worden gemaakt tussen de kosten en baten Het is van belang dat LSV bekend is met het risico en dat het risico is geminimaliseerd en is geaccepteerd (restrisico's).

Actiepunten:

- (Beleid): Zorg dat de audittrail beveiligd is tegen manipulatie en indien niet mogelijk dat het risico geminimaliseerd en geaccepteerd is [p4c3].

Aandachtspunt:

- 10.2.c . Dit zal het risico vergroten mbt de beveiliging van manipulatie op audittrails. Zorg dat er een weloverwogen besluit genomen gaat worden om de risico's uit te sluiten of in het uiterste geval te beperken.

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.

LSV maakt voor de basis gebruik van IAM. De landelijke rollen zijn geïmplementeerd en uniform. Echter de exclusieve rollen zijn voor verbetering vatbaar (niet via IAM). LSV controleert één keer per jaar de toegang en gebruikersrechten, maar kijkt niet naar hoelang een gebruiker inactief is geweest.

Actiepunten:

- (Beleid): Zorg dat de exclusieve autorisatie rollen beter worden ingericht [p5c3].
- (Beleid): Het toegang- en gebruikersrechten van gebruikers moet regelmatig (periodiek) gecontroleerd worden. Zorg dat het personeel wat langere tijd inactief is gecontroleerd gaat worden [p5c8].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	80%	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.

Op dit moment maakt LSV voor een deel gebruik van vastgestelde bedrijfsbegrippen. In het gegevensmodel zijn er afspraken gemaakt omtrent bedrijfsbegrippen, maar op bedrijfsprocessen niveau is dit niet vastgelegd. Het lastige als een applicatie geen gebruik maakt van de vastgestelde definities voor bedrijfsbegrippen is dat het uitwisselen van gegevens bemoeilijkt wordt. De metagegevens die daarvoor in aanmerking komen zouden geautomatiseerd afgeleid en vastgelegd moeten worden. Dit is belangrijk om de juistheid en rechtmatigheid te kunnen waarborgen.

Actiepunten:

- (Beleid): LSV moet binnen de gehele applicatie en gerelateerde bedrijfsprocessen dezelfde bedrijfsbegrippen hanteren. Zorg dat dit is vastgelegd [p6c1].
- (Beleid): Zorg dat zolang het Toepassingsprofiel Metagegevens Politie (TMP) in ontwikkeling is er gebruik gemaakt worden van het Toepassingsprofiel Metagegevens Rijk (TMR) bij het opstellen van de requirements voor metagegevens [p6c4].
- (Beleid): Zorg dat metagegevens die daarvoor in aanmerking komen geautomatiseerd afgeleid en vastgelegd worden [p6c8].
- (Beleid): Gebruik metagegevens om toegang te verlenen, bewaartermijnen bij te houden en voor audittrails en managementrapportages [p6c10].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	50%	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.

LSV voldoet aan bijna alle punten op het gebied van kwaliteitszorg. Een rapport over de kwaliteit van de gegevens kan ad-hoc via een query uitgevoerd worden, maar niet periodiek. Als er kwaliteitscontroles worden uitgevoerd is het ook aan te raden de resultaten hiervan te bewaren of op te nemen in de rapportages. Alleen op basis hiervan kan met regelmaat de kwaliteit gecontroleerd worden.

Actiepunten:

- (Beleid): Zorg dat er periodiek een rapport wordt samengesteld over de kwaliteit van gegevens. [p7c7]
- (Beleid): Voer de kwaliteitscontroles uit en bewaar de resultaten hiervan. [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	83%	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 LSV niet op het gebied van bewaren en vernietigen. LSV voldoet niet aan de kwaliteitseisen van de DUTO standaard. Dit is van belang om overheidsgegevens duurzaam beschikbaar en toegankelijk te houden. In het verlengde daarvan moet LSV de gegevens beschikbaar stellen ten behoeve van het duurzaam bewaren van gegevens. Daarnaast is er een selectielijst opgesteld aan de hand van taak- en bedrijfsprocessen. De processen zijn daarin ingedeeld naar een drietal hoofdcategorieën: Besturen, Uitvoeren en Ondersteunen. In de selectielijst wordt per proces een waardering toegekend aan de informatie die uit dat proces voortvloeit in de zin van bewaren (B) of (op termijn) vernietigen (V). Binnen LSV is het (nog) niet mogelijk om bij verwerkte gegevens een selectie te maken tussen bewaren of op termijn vernietigen. Om deze punten te verbeteren kan er contact worden opgenomen DIV (Documentaire informatievoorziening). De contactpersonen daar zijn 10.2.e en 10.2.e

Actiepunten:

- **(Wet archiefwet): Zorg dat bij verwerkte gegevens er een selectie gemaakt kan worden ten behoeve van bewaren en vernietigen [p8c3].**
- (Beleid): LSV moet voldoen aan de kwaliteitseisen van DUTO [p8c8].
- **(Wet art 14 lid 4): LSV moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens [p8c9].**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	33%	75%	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.

LSV heeft recent geen risico analyse uitgevoerd. Het is belangrijk om regelmatig de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen al kan zijn achterhaald. Het advies hier luidt om een risico analyse uit te laten voeren. Naar aanleiding van de resultaten uit de analyse moet worden gekeken welke informatiebeveiligingseisen moeten worden genomen en welke impact deze op de voorziening hebben als ze worden gerealiseerd. Daar waar mogelijk moet er gebruik worden gemaakt van de standaard informatiebeveiligingsdiensten. Als er risico's overblijven die niet kunnen worden weggenomen, moeten deze restrisico's in beeld zijn en periodiek beheert worden.

Actiepunten:

- (Beleid): Zorg dat er een nieuwe risicoanalyse op het gebied van informatiebeveiliging uitgevoerd gaat worden [p9c1].
    - **(Wet art 4b en c): Stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse [p9c2].**
    - **(Wet art 4b en c): Stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening [p9c3].**
    - (Beleid): Zorg dat LSV gebruik maakt van de aanwezige generieke voorziening voor informatiebeveiliging [p9c4].
    - (Beleid): Zorg dat daar waar mogelijk de informatiebeveiligingseisen gerealiseerd kunnen worden door de standaard informatiebeveiligingsdiensten [p9c5].
    - (Beleid): Zorg dat LSV waar mogelijk de standaard informatiebeveiligingsdiensten gebruikt. In dit niet mogelijk is dan dienen er passende maatregelen te worden genomen[p9c6].
    - (Beleid): Zorg dat de restrisco's periodiek beheert worden [p9c7].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	10%	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.

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

Actiepunten:

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

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

1.12 Verantwoordelijkheden belegd

"*De verantwoordelijkheden voor de zorgvuldige en rechtmatige verwerking van gegevens zijn eenduidig belegd*"

Het is van belang dat de verantwoordelijkheden voor gegevensverwerking belegd zijn om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen

LSV voldoet aan alle gestelde criteria op het gebied van 'verantwoordelijkheden belegd'. De definities, beleid, koers en strategie zijn vastgesteld voor het verwerken van gegevens. LSV ondersteunt de uitvoeringsverantwoordelijke met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. Door gebruik te maken van IAM wordt de rechtmatigheid van gegevensverwerking gewaarborgd.

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 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