0-meting Live Journaal Politie (module Journaal)

PSbD compliancy

10.2.e

Definitief

Versie 1.3

Versie datum 25 april 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-11-2017	Concept formaat document	
1.0	5-3-2018	Laatste review en scores aangepast	
1.1	14-11-2018	Aanpassingen op basis van gesprekken en feedbackformulier	
1.2	30-11-2018	Aanpassingen nav feedback 10.2.e	
1.3	25-04-2019	Rapport definitief gemaakt na wederzijds akkoord	

Review commentaar

Versie	Wanneer	Wie	Afdeling
1.0	2-3-2018	10.2.e	PPI
1.1	14-11-2018	10.2.e	Gegevensautoriteit
1.2	30-11-2018	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[1] zijn in maart 2016 politieke toezeggingen gedaan aan de Tweede Kamer.

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 Live Journaal Politie (LJP) en dan specifiek de module Journaal. 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 Live Journaal Politie (module Journaal)

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 bij de 0-meting

	Naam	Functie
Direct betrokkenen 0-meting Live Journaal Politie	10.2.e	Ontwikkelaar LJP / Operationeel specialist
	10.2.e	ICT IV expert
	10.2.e	Operationeel specialist
	10.2.e	ICT IV expert
	10.2.e	Sr. Coördinerend business expert

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

Gesprek datum	Nummer meting	Toelichting
29-11-2017 & 9-1-2017	20171011900/Basis Voorziening Informatie-LJP Toetsing 1	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader Privacy & Security by Design versie 1.0.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Opmerking
Verzamelen	X	
Vastleggen	X	
Ordenen	X	
Bewaren	X	
Bijwerken (toevoegen aan iets bestaands)	X	
Wijzigen (aanpassen van een bestaand gegeven)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling	X	Palantier is eenmalig voorgekomen. Ook handmatig dmv een rapportage
Samenbrengen	X	
Met elkaar in verband brengen		Niet geautomatiseerd
Afscherming (niet ter beschikking stellen van)	X	
Uitwissen (verwijderen zonder vernietigen)	X	
Vernietigen	X	

Verwerkingsgrondslag Live Journaal Politie

Doelbinding	Verwerkingsgrondslag	X
Dagelijkse politietaak	Artikel 8	X
Onderzoek rechtsorde bepaald geval	Artikel 9	X
Informatiepositie	Artikel 10	X
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

Tijdens de 0-meting is qua resultaten alleen gekeken naar de module Journaal, omdat dit de basis is van de applicatie. Live Journaal Politie (LJP) scoort een volwassenheid van niveau 1. Op het gebied van Privacy & Security by Design voldoet LJP nog onvoldoende. Om te voldoen aan de Wpg is het belangrijk dat er extra aandacht besteed gaat worden op het gebied van informatiebeveiliging en de autorisatierollen die buiten de politie staan. Daarnaast is er onvoldoende geregeld op het gebied van duurzaam bewaren. Wat daarnaast opvalt, is dat Live Journaal niet onder politie architectuur is gemaakt. Dit zorgt ervoor dat LJP op veel facetten van het (politie)beleid achterblijft. Indien er met LJP doorontwikkeld zal worden dan dienen er op het gebied van architectuur opnieuw naar applicatie gekeken moeten worden.

De eenvoud en makkelijke manier van gebruik is de kracht van LJP, maar tevens ook het grootste gevaar. Het gemak zit in de eenvoud waarbij er in de basis gebruik wordt gemaakt van een vrij tekstveld in een gecentraliseerd systeem. Waarbij voorheen gegevens zeer gefragmenteerd werden bijgehouden in allerlei applicaties zoals o.a. Excel, Access, Word en mail (Outlook). Met LJP is er nu beter zicht op de informatie, op de inhoud en is het (mits geautoriseerd) eenvoudig toegankelijk. Daarnaast is er geprobeerd met software functionaliteiten de privacy & security gevaren tot het minimum te beperken en geprobeerd waar mogelijk te voldoen aan de Wpg.

Het gevaar ligt bij de gegevensverwerker waar een grote verantwoordelijkheid in de omgang van gegevens ligt. Dit is ook wat in de Wpg-notitie terugkomt[3]. De vraag is of de vrije manier van verwerking van gegevens volstaat (doelbinding) bij zo'n grote groep gebruikers (36.000+, waarbij er gemiddeld 450 gebruikers per maand bij komen). Met zulke grote aantallen gebruikers is inhoudelijk niet meer te controleren of de gegevensverwerker de gegevens correct verwerkt (zonder koppeling met een bronsysteem). Daarnaast is tijdens de gesprekken ook naar voren gekomen dat in sommige gevallen LJP gebruikt wordt als bron-systeem (eerste en soms enige registratiesysteem). Dit zou te allen tijde voorkomen dienen te worden.

Actiepunten:
Het belangrijkste wat nu ieder geval moet gebeuren is zo snel mogelijk de actiepunten aan te pakken die voor de wet vereist zijn. Indien de onderstaande punten opgepakt worden dan stijgt direct het volwassenheidsniveau en voldoet LJP aan de Wpg.

- **Wet: Vanwege de werking van LJP (gebruik van een vrij tekstveld) is het niet mogelijk om basisregistraties te verifiëren [p1c3].**
- **Wet: Onjuistheden in de gegevens van een kernobject worden niet direct aan de bronhouder van het betreffende register teruggemeld [p1c5]**.
- **Wet: Het is mogelijk om de gegevens duurzaam te bewaren, maar op dit moment is dat nog niet geregeld. Om duurzaam te bewaren in gang te brengen kan er contact opgenomen worden met DIV [p8c9].**
- **Wet: Er moet een uitgebreidere risicoanalyse komen op het gebied van informatiebeveiliging. Op basis hiervan moeten informatiebeveiligingseisen worden bepaald. Dit zal uitgevoerd moeten worden door team informatiebeveiliging (dienst IM) en team veiligheid en continuïteit (dienst ICT) [p9c1] en [p9c2].**
- **Wet: De impact van de informatiebeveiligingseisen moet beoordeeld worden ten aanzien van LJP [p9c3].**

Aandachtspunten buiten de 0-meting:

- Ontwikkeling van LJP zou niet onder één persoon moeten vallen
- Beslissingen over verbeteringen van applicatie moeten breder afgestemd worden.
- Beperken van het gebruik als bronsysteem
- Koppeling maken met bronsysteem indien dit vereist is (indien Journaal gaat over politiegegevens)

Eindscore	Peildatum	Checklist PSbD	Wet (Wpg)	Beleid (PSbD)	Volwassenheid
Live Journaal Politie	9-1-2018	1.0	74%	37%	1

[3] 11.1

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	33%	25%	0
PDCA-cyclus	M	-	NVT	88%	2
Doelbinding	Z	-	100%	20%	2
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	100%	17%	2
Metagegevens	Z	-	100%	38%	2
Kwaliteitszorg	Z	-	NVT	33%	0
Bewaren en vernietigen	Z	-	90%	75%	1
Informatiebeveiliging	Z	-	0%	40%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	0%	0
Verantwoordelijkheden belegd	M	-	NVT	83%	2
Principe is niet actief		-			
TOTALEN TOETSING		-	74%	37%	

In de afbeelding hierboven staan de volwassenheidsniveaus per principe beschreven. Waarbij de eerste kolom de weegfactor aangeeft van het principe op de eindscore. De tweede en derde kolom geeft het percentage aan van criteria in Wet en Beleid waarin is voldaan. Tot slot staat indien van toepassing een volwassenheidsniveau beschreven. Dit niveau is gebaseerd op de score van de toets criteria bij alle principes van deze toets. In de volgende paragrafen worden de resultaten per principe nader toegelicht.

Nieuwe regelgeving WPG Q1 2019 (buiten de 0-meting)
Om voorbereid te zijn op de nieuwe regelgeving mbt WPG welke vanaf januari 2019 van kracht gaat is er ook gekeken of buiten de eerder genoemde actiepunten nog meer punten zijn die voor LJP aangepast moeten worden om te voldoen aan de wet. Er zijn drie actiepunten wat nu benoemd is als beleid wat in januari 2019 onderdeel zal zijn van de wet.

- (Wet): Een GEB moet worden uitgevoerd indien er sprake is van een nieuwe verwerking en als is voldaan aan een van de volgende criteria: er wordt gebruik gemaakt van een nieuwe technologie en/of er is sprake van een hoog risico [p2c3].

- (Beleid --> Vanaf Q1 2019 Wet): Er zijn geen metagegevens mbt de verwerkingsgrondslag en verwerkingstermijn die het gegeven begeleiden. Het begeleiden van metagegevens bij verstrekking is van belang indien er bijvoorbeeld gebruik gemaakt gaat worden van data-analyseomgevingen. Er kan dan bepaald worden of het rechtmatig is om een bepaald gegeven nog te gebruiken (denk aan bewaren en vernietigen). Dit is vanaf januari 2019 verplicht volgens art 32a. Wpg [p3c11].

- (Beleid --> Vanaf Q1 2019 Wet): Op dit moment worden toegang- en gebruikersrechten van gebruikers niet regelmatig gecontroleerd. Nu worden gebruikers als er twee jaar geen activiteit is gearchiveerd. Bij het gebruik van IAM zal dat vaker gecontroleerd worden [p5c6].

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.

Live Journaal Politie (module: Journaal) wordt in de basis niet gezien als een bronsysteem zoals SUMMIT en BVH, maar als een werkprocessysteem waarin wel persoonsgegevens geregistreerd kunnen worden. Het wordt gebruikt voor overdracht aan collega's en maakt vooral gebruik van ongestructureerde gegevens doormiddel van een vrij tekstveld. Door veelvuldig gebruik van ongestructureerde gegevens is het heel lastig om te voldoen aan het principe eenmalige vastlegging. Om aan de voorwaarden te voldoen zullen de volgende actiepunten aangepakt moeten worden.

Actiepunten:

- (Beleid): LJP maakt geen gebruik van vastgestelde referentiegegevens. Het maakt gebruik van samenvattingen in een vrij tekstveld. Met de opmerking dat het in de basis niet bedoeld is als registratiesysteem. Echter er zijn wel situaties waar de informatie van LJP als eerste bron van informatie geraadpleegd wordt. In het geval van politiegegevens is het van belang om een koppeling te hebben met het bronsysteem, zodat duidelijk is waarmee een Journaal verbonden is. Dit voorkomt ook dat er gegevens dubbel geregistreerd worden [p1c1].
    - **(Wet): Vanwege de werking van LJP (gebruik van een vrij tekstveld) is het niet mogelijk om basisregistraties te verifiëren [p1c3].**
    - **(Wet): Onjuistheden in de gegevens van een kernobject worden niet direct aan de bronhouder van het betreffende register terug gemeld [p1c5].**
    - (Beleid): Er wordt niet gecontroleerd of gegevens al bestaan, indien gegevens geregistreerd worden [p1c10].
- (Beleid): Binnen LJP kan het wijzigen van informatie verkregen (of geregistreerd) uit het bronsysteem zonder opdracht van de bron. Het gevolg is dat in LJP informatie staat welk in het bronsysteem gewijzigd is en omgekeerd (mede door gebruik van vrij tekstvelden) [p1c8].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	33%	25%	0

1.2 PDCA-cyclus

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

Om in de managementverantwoordelijkheid te kunnen voorzien is het belangrijk dat de informatievoorziening stuurinformatie levert zodat er zicht is op de gegevenskwaliteit en de informatiebeveiliging.

LJP werkt op gegevensniveau nog onvoldoende op cyclische terugkoppeling. Gegevens worden niet gedurende de gehele levenscyclus beheerd volgens de levenscyclus van gegevensverwerking.
Om de risico's in kaart te brengen op gebied van verwerkingen is het van belang om een gegevensbeschermingseffectbeoordeling (GEB) uit te voeren. De GEB Wpg is op het moment van de toetsing nog niet beschikbaar, maar zodra de GEB Wpg volledig beschikbaar is dan zal dit direct uitgevoerd gaat worden. Vanaf januari 2019 is dit verplicht vanuit de wet.

Actiepunten:

- (Beleid): Binnen LJP is het beheer van gegevens, processen en software deels onderdeel van de PDCA-cyclus. Voor gebruikers is er een mogelijkheid om een melding te plaatsen die de gehele PDCA-cyclus doorloopt. Echter de gegevens worden niet gedurende de gehele levenscyclus beheerd volgens de levenscyclus van gegevensverwerking (blz 28 uitvoeringskader PSbD) [p2c2].
    - Besturing
    - Uitvoering
    - Terugkoppeling

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	88%	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 de doelbinding te bepalen. Op basis van de doelbinding kan worden gerechtvaardigd waarom (politie)gegevens verwerkt mogen worden.

LJP (module: Journaal) voldoet op dit moment aan alle punten vanuit de wet wat binnen de mogelijkheden ligt op het gebied van doelbinding. De voorziening neemt vooraf de verwerkingsgrondslag van de te verwerken gegevens op. Echter de verwerkingsgrondslag van een persoonsgegeven wordt niet als metagegeven opgenomen in het gegevensmodel van de voorziening. Vanaf januari 2019 is het vanuit de wet van belang dat een metagegeven mbt de verwerkingsgrondslag en verwerkingstermijn het gegeven gaan begeleiden. Dat betekent dat de verwerkingsgrondslag en verwerkingstermijn als metagegeven in de voorziening moeten worden opgenomen.

Actiepunten:

- (Beleid): De verwerkingsgrondslag van een persoonsgegeven is niet als metagegeven opgenomen in het gegevensmodel van de voorziening. Het is van belang om de indien er persoonsgegevens worden verwerkt dat dit als metagegeven wordt aangegeven. Aangezien het in de voorziening vooral om een vrij tekstveld gaat zal het gebruik van persoonsgegevens afgeraden worden, omdat er geen specifieke doelbinding aan de persoonsgegevens gegeven kan worden. In de basis zal een persoonsgegeven moeten worden verwerkt in de bronsysteem en mogelijk met een koppeling naar LJP overgenomen worden [p3c2].
- (Beleid): Een verwerkingsgrondslag kan niet automatisch worden herleid en kan daarmee ook niet door de gebruiker worden aangepast. Het moet mogelijk zijn om per vrij tekstveld de verwerkingsgrondslag aan te kunnen passen [p3c5].
- (Beleid): Bij een artikel 13-verwerking moet de datum einde verwerkingstermijn kunnen worden gewijzigd (bijvoorbeeld voor gevarenclassificatie) [p3c9].
- **(Beleid --> Vanaf Q1 2019 Wet): Er zijn geen metagegevens mbt de verwerkingsgrondslag en verwerkingstermijn die het gegeven begeleiden. Het begeleiden van metagegevens bij verstrekking is van belang indien er bijvoorbeeld gebruik gemaakt gaat worden van data-analyseomgevingen. Er kan dan bepaald worden of het rechtmatig is om een bepaald gegeven nog te gebruiken (denk aan bewaren en vernietigen). Dit is vanaf januari 2019 verplicht volgens art 32a. Wpg [p3c11].**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	100%	20%	2

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 het 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 LJP is het mogelijk voor een controlerende instantie vast te stellen wie, wanneer welke handelingen heeft verricht en hoe besluiten tot stand zijn gekomen. Kortom een audittrail wordt geregistreerd. Op dit moment is de auditrail niet optimaal beveiligd tegen manipulatie. Ontwikkelaar en beheerder kunnen de audittrail wijzigen zonder dat het opgemerkt wordt.

Actiepunt:

- (Beleid): De audittrail is 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 [p4c3].
- (Beleid): Het is niet mogelijk om een rapportage te genereren van een audittrail [p4c4].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoording	Zwaar (Z)	100%	0%	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.

LJP voldoet op dit moment nog niet op het gebied van autorisatie. Er is aangegeven dat vanaf begin maart 2018 gebruik gemaakt gaat worden van de generieke IAM-voorziening. Zodra de generieke IAM-voorziening in uitvoering is zullen veel van de onderstaande punten opgelost zijn.

Actiepunt:

- (Beleid): Er wordt geen gebruik gemaakt van een generieke IAM-voorziening voor het verifiëren van identiteiten. Het is belang om gebruik te maken van de generieke IAM-voorziening om het autorisatiebeheer eenvoudig en efficiënt in te richten volgens geautomatiseerde procedures. Vanaf begin maart 2018 zullen er aanpassingen gedaan worden waardoor dit wel mogelijk is [p5c1].
- (Beleid): De voorziening maakt geen gebruik van toegangsverlening op gegevensniveau, maar op werkprocesniveau. Met de ontwikkeling van kernregisters en gegevensdiensten komt het echter steeds vaker voor dat dezelfde gegevens via meerdere applicaties geraadpleegd en verwerkt kunnen worden. Het is daarbij van belang dat gebruikers die niet geautoriseerd zijn voor het raadplegen en verwerken van gegevens via de ene applicatie ook niet onbedoeld via een andere applicatie bij dezelfde gegevens kunnen. Op dit moment wordt dit gewaarborgd door de autorisaties voor verschillende applicaties te baseren op dezelfde autorisatieregels. Voor LJP is het van belang om aan te sluiten bij de bestaande autorisatieregels[4] omtrent toegangsverlening [p5c3].
- (Beleid): LJP maakt geen gebruik van de generieke autorisatietool voor leidinggevende [p5c4].
- (Beleid): LJP ondersteunt geen Audit Based Access Control toegang. Als IAM in werking is, dan is dit punt niet meer van toepassing [p5c5].
- **(Beleid --> Vanaf januari 2019 wet): Op dit moment worden toegang- en gebruikersrechten van gebruikers niet regelmatig gecontroleerd. Nu worden gebruikers als er twee jaar geen activiteit is gearchiveerd. Bij het gebruik van IAM zal dat vaker gecontroleerd worden [p5c6].**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	100%	17%	2

[4] Autorisatiebeleid 2016 – 2020, 21 april 2016

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.

Metagegevens zijn gegevens die nodig zijn voor de ontsluiting en beheer van andere gegevens. Het zijn de eigenschappen van gegevens en zorgen ervoor dat er van gegevens betekenisvolle informatie gemaakt worden. Bij het ontwerp en ontwikkeling van LJP ongeveer 14 jaar geleden is een eigen invulling gegeven aan tabellen, hierbij is er geen rekening gehouden met vastgestelde definities van bedrijfsbegrippen. Gezien het gebruik van een vrij tekstveld zal er strakker gekeken moeten omgang en gebruik van metagegevens. Indien er koppeling gelegd moeten worden met bestaande bronsystemen is het van belang om de basis van Politiegegevensmodel (PGM) te gebruiken.

Actiepunten:

- (Beleid): LJP maakt geen gebruik van vastgestelde definities voor bedrijfsbegrippen. Het is van belang dat er vastgestelde definities voor bedrijfsbegrippen gedefinieerd worden zodat de betekenis van woorden die gebruikt worden bij de uitvoering van het werk eenduidig is beschreven. Dit zal in overleg met het Gegevens-, Gebruik en Beheer (GGB) besproken moeten worden [p6c1].
- (Beleid): LJP (14 jaar geleden gecreëerd) maakt niet gebruik van het PGM. Het is van belang om te laten controleren hoe LJP gegevensmodel op dit moment past binnen de architectuur van de politie [p6c5].
- (Beleid): Bij LJP zijn de metagegevens niet vastgesteld. Hierdoor kan er niet gekeken worden of de metagegevens die daarvoor in aanmerking komen geautomatiseerd afgeleid en vastgelegd. Of op een andere manier worden vastgelegd. Op dit moment zijn er geen koppelingen met andere systemen, maar als deze er gemaakt worden is het van belang om metagegevens mee te leveren [p6c8], [p6c9] en [p6c11].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	100%	38%	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.

De huidige werking van LJP zorgt ervoor dat kwaliteitszorg onvoldoende is.

Actiepunten:

- (Beleid): Kwaliteitseisen zijn tijdens het ontwerp (14 jaar) geleden niet afgestemd met de beleidsverantwoordelijke. Het is van belang om nieuwe kwaliteitseisen af te stemmen op basis van het kwaliteitsraamwerk wat kijkt naar de juistheid, doeltreffendheid en controleerbaarheid van gegevens. Een verwijzing hoe een kwaliteitsraamwerk opgesteld moet worden staat op noraonline [p7c2].
- (Beleid): Zodra de kwaliteitseisen zijn opgesteld is het van belang om deze kwaliteitseisen te realiseren [p7c3].
- (Beleid): Er zijn geen bedrijfsregels geformuleerd om de kwaliteit van gegevens te meten [p7c5].
- (Beleid): Er zijn geen geautomatiseerde controles ingebouwd om de gegevenskwaliteit te meten. Dit heeft mede te maken door het gebruik van een vrij tekstveld [p7c6].
- (Beleid): Er kan geen rapport gemaakt worden over de kwaliteit van de gegevens [p7c7].
- (Beleid): Er worden geen resultaten bewaard van uitgevoerde kwaliteitscontroles [p7c8].

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

1.8 Bewaren en vernietigen

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

Het verwerken van gegevens mag alleen indien er een wettelijke grondslag voor bestaat. Op dit moment worden de gegevensverwerkende processen niet geanalyseerd op basis van de generieke selectielijst, maar wordt er gekeken naar Wpg.

Er kunnen geen gegevensverwerkende processen geanalyseerd worden op basis van de generieke selectielijst. Aan de wettelijke bepalingen mbt bewaren, vernietigen en archiveren van (persoons)gegevens wordt voldaan. Echter aan het duurzaam bewaren wordt nog niet voldaan. LJP wil hier graag aan meewerken maar het proces is onduidelijk.

Actiepunten:

- (Beleid): LJP voldoet maar voor een deel aan de eisen van de DUTO-standaard [p8c8].

	Eis	Voldoet niet
Eis 1	Er is een informatiemodel waarin alle informatieobjecten zijn beschreven die de organisatie ontvangt en creëert.	Het is een vr j tekstveld en daardoor niet beschreven
Eis 3	Er is een vastgestelde Selectielijst waarin is beschreven hoe lang informatieobjecten bewaard worden.	Alleen indien het valt onder de Wpg
Eis 9	Informatieobjecten zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen. Conform de geldende standaarden voor informatiebeveiliging.	Niet volgens het informatiebeveiligingsbeleid
Eis 11	De weergave en export van elk informatieobject bevat minimaal volledige en actuele metagegevens zoals voorgeschreven in de Richtlijn Metagegevens Overheidsinformatie.	Niet de volledige en actuele metagegevens
Eis 12	Informatieobjecten worden niet eerder en niet later vernietigd dan is aangeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar.	Er is geen verklaring van vernietiging beschikbaar
Eis 13	Een bl jvend te bewaren informatieobject wordt binnen twintig jaar overgebracht naar een archiefbewaarplaats.	Bij LJP is niet duidelijk hoe dit proces verloopt

- **(Wet): Het is mogelijk om de gegevens duurzaam te bewaren, maar op dit moment is dat nog niet geregeld. Om duurzaam te bewaren in gang te brengen kan er contact opgenomen worden met DIV [p8c9].**

TIP: Het is van belang om de LJP te controleren op basis van de generieke selectielijst.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	90%	75%	1

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.

Op het gebied van informatiebeveiliging voldoet LJP niet. Er is een risicoanalyse[5] uitgevoerd in 2014, maar deze risicoanalyse is niet meer toereikend. In de analyse wordt er gesproken over een gebruikersaantal van 800, terwijl in de recentere Wpg notitie[6] gesproken wordt over 28.000 gebruikers. Daarnaast staat in de risicoanalyse dat de beveiligingsrisico's laag zijn aangezien het om rubriceringsniveau 'Politie Intern' zou gaan. De hogere rubriceringen zijn niet onderzocht, maar vallen wel binnen dezelfde applicatie(module). De risico analyse is te beperkt en daarom moet er een uitgebreidere risicoanalyse gedaan worden. Op basis van een uitgebreidere risico analyse kan vervolgens de impact beter bepaald op het gebied van privacy en security.

Actiepunten:

- **(Wet): Er moet een uitgebreidere risico analyse komen op het gebied van informatiebeveiliging. Op basis hiervan moeten informatiebeveiligingseisen worden bepaald. Dit zal uitgevoerd moeten worden door team informatiebeveiliging (dienst IM) en team veiligheid en continuïteit (dienst ICT) [p9c1] en [p9c2].**
- **(Wet): De impact van de informatiebeveiligingseisen moet beoordeeld worden ten aanzien van LJP [p9c3].**
- (Beleid): Bepaald moet worden of alle informatiebeveiligingseisen gerealiseerd zijn door de standaard informatiebeveiligingsdiensten [p9c5].
- (Beleid): Er moeten maatregelen genomen worden om informatiebeveiligingseisen te realiseren die niet door standaard informatiebeveiligingsdiensten zijn gerealiseerd (op dit moment deels gerealiseerd) [p9c6].
- (Beleid): Restrisico's in de beveiliging van LJP moeten beheerd worden [p9c7].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	40%	0

1 [redacted]
1 [redacted]

1.10 Voldoen aan de wet

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 Toepassing 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.

LJP maakt initieel geen gebruik van bestaande overheids- en ketenstandaarden. In de basis (14 jaar geleden) is LJP niet onder architectuur van de politie ontwikkeld. Dat betekent dat niet is vast te stellen of aan de van toepassing zijnde overheids- en ketenstandaarden wordt voldaan.

Actiepunten:

- (Beleid): LJP maakt initieel geen gebruik van bestaande overheids- en ketenstandaarden. LJP is in de basis niet onder architectuur van de politie ontwikkeld. Er zal gekeken moeten worden hoe er (indien mogelijk) gebruik gemaakt kan worden van bestaande overheids- en ketenstandaarden. Doormiddel van toetsing zal gekeken worden of er wordt voldaan aan de geldende standaarden en indien er van afgeweken wordt zal dat gemotiveerd moet worden (comply or explain). Een verwijzing is te vinden op blz 59 uitvoeringskader PSbD v1.0 en de website van het Rijk. [p11c1], [p11c2] en [p11c3].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassing 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 om de verantwoordelijkheden voor gegevensverwerking belegd zijn om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen.

LJP voldoet op de meeste criteria op het van 'verantwoordelijkheden belegd'. De beleidsverantwoordelijke is bekend met de gegevens die door LJP verwerkt worden. LJP ondersteunt de uitvoeringsverantwoordelijke met het verwerken van de juiste classificatie en metagegevens voor onder meer informatiebeveiliging, vastlegging van de grondslag en de rechtmatigheid. Alleen zijn definities, beleid, koers en strategie niet vastgesteld voor de verwerking van gegevens bij LJP.

Actiepunten:

- (Beleid): Definities, beleid, koers en strategie voor de verwerking van gegevens is niet vastgesteld [p12c2].

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT	83%	2

2 Verantwoording toetsing

2.1 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[7].

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.

[7] 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.

2.2 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