0-meting Privacy & Security by Design

TRIS

10.2.e

10.2.e

Definitief

Versie 1.2

Versie datum 19 februari 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-01-2018	Opzet template rapport	
1.0	06-06-2018	Eerste versie rapport	
1.1	30-11-2018	Aanpassingen op basis van feedback	
1.2	19-2-2019	Met wederzijds akkoord het rapport definitief gemaakt	

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
1.0	22-6-2018	10.2.e	Gegevensautoriteit
1.1	30-11-2018	10.2.e	Gegevensautoriteit
1.2	19-2-2019	10.2.e	Gegevensautoriteit

Inhoudsopgave

Documentinformatie 2

Inhoudsopgave 2

Inleiding 4

0-meting TRIS 5

Algemeen 5

Doel 5

Doelgroep 5

Aanwezigen 0-meting 5

Technische Recherche Informatie Systeem (TRIS) 6

Omschrijving applicatie 6

Soorten verwerkingen van politiegegevens 6

Verwerkingsgrondslag 7

Eindscore 8

1.1 Eenmalige vastlegging 10

1.2 PDCA-cyclus 11

1.3 Doelbinding 12

1.4 Verantwoording 13

1.5 Autorisatie 14

1.6 Metagegevens 15

1.7 Kwaliteitszorg 16

1.8 Bewaren en vernietigen 17

1.9 Informatiebeveiliging 18

1.10 Voldoen aan de wet 18

1.11 Toepassen standaarden 19

1.12 Verantwoordelijkheden belegd 19

2. Verantwoording toetsing 20

Toetsingscriteria 20

Disclaimer 22

Bijlage 1: Uitgangspunt bij compliance 23

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 TRIS. 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 TRIS

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 TRIS	10.2.e	Functioneel beheerder
	10.2.e	Functioneel beheerder
	10.2.e	Materie-deskundige /super-user TRIS

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

Gespreksdatum	Nummer meting	Toelichting
13-02-2018	2018021301	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 1.0.**

Technische Recherche Informatie Systeem (TRIS)

Omschrijving applicatie

TRIS (Technische Recherche Informatiesysteem) is een applicatie voor de forensische opsporing (FO). De medewerker FO registreert in het bronsysteem BVH zijn werkzaamheden, zoals bij misdrijven aangetroffen goederen en sporen. Deze komen via een geautomatiseerd berichtenverkeer over naar TRIS. In TRIS kunnen deze verder worden verrijkt, vergeleken & geanalyseerd.
Op zaaks-, goederen- en spoor-nivo kunnen verbanden worden vastgelegd zodat CSV´s ontstaan (Criminele Samenwerkings {Personen} of Spoor Verbanden). TRIS ondersteunt hiermee binnen de FO het sporenanalyse en –coördinatie proces alsmede bepaalde deskundigheidsgebieden en in het algemeen het informatie- en opsporingsproces.
In TRIS worden ook biologische sporen bijgehouden om deze in batches aan te leveren bij het NFI, om daar in een geautomatiseerd proces te onderzoeken op DNA. Het NFI geeft hierop een terugkoppeling. Waarbij de resultaten weer in TRIS verwerkt kunnen worden en daarbij bijdragen in de samenstelling van de CSV´s.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	Toelichting
Verzamelen	X	
Vastleggen	X	Informatie wordt in BVH geregistreerd en de extra aanvullende informatie staat in TRIS
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	
Wijzigen (het bestaande aanpassen)	X	Volgt BVH, daar wordt gewijzigd
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Naar het NFI, resultaten kunnen in Excel geëxporteerd worden.
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	Als je geen autorisatie hebt, kan je er niet in.
Uitwissen (weghalen/verwijderen zonder vernietigen)		Volgt BVH, maar dossiers blijven lang bewaard ivm verwijdertermijnen uit Sv.
Vernietigen		

Verwerkingsgrondslag

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

TRIS scoort op volwassenheidsniveau een dikke onvoldoende (niveau 0). Dat betekent dat niet alleen niet wordt voldaan aan de eisen van de wet op het gebied van Privacy & Security by Design (PSbD), maar ook niet aan het politiebeleid. Er kan worden gesteld dat er (op dit moment) geen specifieke aandacht is voor PSbD. Vooral op de principes eenmalige vastlegging, metagegevens, bewaren en vernietigen en informatiebeveiliging is direct verbetering nodig. Al deze principes hebben een zware onvoldoende, maar hebben daarnaast ook zware weegfactor op het gebied van PSbD. Ons advies is eerst te kijken naar de wetscriteria en daarna pas naar mogelijke verbeteringen op het politiebeleid. Indien het niet mogelijk is te voldoen aan alle wetscriteria moet goed worden onderbouwd waarom ervoor wordt gekozen om niet aan een bepaald criterium te voldoen. Er moet dan een weloverwogen besluit worden genomen.

Advies (hieronder staan de wettelijke actiepunten opgesomd, de beleidspunten blijken uit het document):

- **(Wet art 4 lid 1): verifieer de gegevens van een kernobject (bv. Personen) in de betreffende basisregistratie.**
- **(Wet art 4 lid 1): zorg dat het terugmelden van onjuistheden of in het geval van 'gerede twijfel' niet alleen is opgenomen in het proces, maar ook in de voorziening.**
- **(Wet art 32): neem de datum einde van de verwerkingstermijn op in het gegevensmodel, of zorg er in ieder geval voor dat het voor elk gegeven duidelijk is onder welke verjaringstermijn die valt.**
- **(Wet art 32a): genereer periodieke rapportages over de audittrail[3].**
- **(Wet art 6): als niet aan kan worden gesloten op IAM, moet er gebruik worden gemaakt van de vastgestelde autorisatierollen van de politie. TRIS moet nagaan of de rollen die zij hanteren voldoen aan de eisen van de politie.**
- **(Wet art 14 lid 4): controleer of de juiste bewaartermijnen zijn opgenomen in de applicatie.**
- **(Wet art 8, 9, 10, 12 en 14): gegevens moeten worden voorzien van een selectie ten behoeve van bewaren en vernietigen.**
- **(Wet archiefwet): de voorziening moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens.**
- **(Wet art 4b en c): stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse**
- **(Wet art 4b en c): stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening.**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
TRIS	13-02-2018	V.1.0	32%	41%	0

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	17%	63%	0
PDCA-cyclus	M	-	NVT	50%	2
Doelbinding	Z	-	67%	100%	1
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	50%	33%	1
Metagegevens	Z	-	NVT	19%	0
Kwaliteitszorg	Z	-	NVT	50%	2
Bewaren en vernietigen	Z	-	0%	0%	0
Informatiebeveiliging	Z	-	0%	0%	0
Voldoen aan de wet	Z	-	NVT	NVT	NVT
Toepassing standaarden	L	-	NVT	50%	2
Verantwoordelijkheden belegd	M	-	NVT	100%	3
Principe is niet actief		-			
TOTALEN TOETSING		-	32%	41%	

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

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 het principe eenmalige vastlegging heeft TRIS een onvoldoende volwassenheidsniveau behaald. TRIS is deels afhankelijk van BVH voor het gebruik van GGB tabellen, maar er wordt wel verwacht dat er vanuit de GGB nog enkele lijsten speciaal voor de Forensische Opsporing worden ontwikkeld. Verbeterpunten voor TRIS zitten onder andere in het verifiëren van gegevens van kernobjecten. Daar waar mogelijk wordt BVH gevolgd, maar er is ook sprake van een handmatige invoer indien gegevens terugkomen van het NFI. Tijdens de 0-meting is aangegeven dat het automatisch invullen van NFI gegevens in kwartaal 2 (Q2) op de backlog staat. Daarnaast zijn er verbeteringen mogelijk op het punt van het terugmelden van onjuistheden of in het geval van 'gerede twijfel'. Op dit moment is er namelijk geen automatisch terugmeldvoorziening, maar zit het vooral in het proces. In het geval van onjuistheden wordt er contact met de betreffende diender opgenomen.

TRIS zou het ter beschikking stellen van gegevens via een gegevensdienstenlaag moeten ondersteunen. Op dit moment worden de gegevens van het berichtenverkeer van BVH naar TRIS gestuurd. Op het moment van de 0-meting stond het ter beschikking stellen van veredelde data aan BVI op de planning. Als laatste zou er verbetering mogelijk zijn op het controleren of gegevens al bestaan bij registratie. Momenteel is BVH leidend en daar wordt wel geverifieerd, maar in TRIS niet.

Actiepunten:

- **(Wet art 4 lid 1): verifieer de gegevens van een kernobject (bv. Personen) in de betreffende basisregistratie.**
- **(Wet art 4 lid 1): zorg dat het terugmelden van onjuistheden of in het geval van 'gerede twijfel' niet alleen is opgenomen in het proces, maar ook in de voorziening.**
- (Beleid): zorg dat gegevens via een gegevensdienstenlaag ter beschikking worden gesteld aan andere voorzieningen (het staat wel op de planning om data ter beschikking te stellen aan BVI).
- (Beleid): voer controles in of gegevens al bestaan op het moment van registratie.

Aandachtspunten:

- Neem contact op met de GGB over het ontwikkelen van lijsten mbt Forensische Opsporing.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	17%	63%	0

1.2 PDCA-cyclus

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

Om in de managementverantwoordelijkheid te kunnen voorzien is het belangrijk dat de informatievoorziening stuurinformatie levert zodat er zicht is op de gegevenskwaliteit en de informatiebeveiliging. Het is aan de betreffende verantwoordelijke managers om keuze te maken op basis van de stuurinformatie.

TRIS levert slechts beperkte stuurinformatie. Er worden wel rapportages over het aantal gebruikers opgeleverd, maar daar wordt niet specifiek op gestuurd. Daarnaast zouden er ook rapportages over ander zaken zoals de omvang van de gegevensverwerking, de aantallen verstrekkingen en het beheer van autorisaties moeten worden opgeleverd. De managementmodule is uit TRIS gehaald omdat de bron moest worden gevolgd. Het beheer van gegevens, software en de processen gaat deels volgens de PDCA-cyclus. Aangezien BVH wordt gevolgd voor het verwijderen en vernietigen heeft TRIS niet de gehele levenscyclus van een gegeven in de hand. Het is op dit moment niet mogelijk periodieke rapportages (geautomatiseerd) op te leveren. Het is wel belangrijk dit te doen, omdat periodieke rapportages het mogelijk maken de ontwikkeling omtrent een applicatie bij te houden. Indien er sprake is van ongewenste ontwikkelingen kan daar tijdig op worden ingegrepen.

Tijdens de 0-meting kwamen ook vragen over de gegevensbeschermingseffectbeoordeling (GEB) en de verwerkers overeenkomst naar voren. Het uitvoeren van een GEB is vanaf januarie 2019 verplicht. Aangezien een GEB alleen uitgevoerd dient te worden in het geval van een nieuwe verwerking is dit voor TRIS alleen van toepassing als er een nieuwe functionaliteit wordt toegevoegd die ook daadwerkelijk een nieuwe verwerking inhoudt. Hierbij moet worden gedacht aan een functionaliteit die iets met gegevens kan dat op dit moment nog niet wordt gedaan. Een andere eis is daarbij of er sprake is van een hoog risico of een nieuwe technologie. Voor de beantwoording van die vragen zou moeten worden gekeken naar het kader Gegevensbeschermingseffectbeoordeling Model Wpg-verwerking. Hierin staat een lijst van tien vragen die langsgelopen moet worden om vast te stellen of een GEB moet worden uitgevoerd.

Actiepunten:

- (Beleid): TRIS levert slechts beperkt stuurinformatie. Er is gekozen om de managementmodule uit TRIS te halen, omdat de bron (BVH) gevolgd moest worden. Er zal onderzocht moeten worden of hiermee voldoende sturing wordt gegeven aan TRIS.
- (Beleid): Doordat BVH gevolgd wordt voor het verwijderen en vernietigen heeft TRIS niet de gehele levenscyclus in hand. Er zal gekeken moeten worden of de bewaartermijnen op specifieke gegevens vanuit TRIS gelijk zijn aan de bewaartermijnen die nu gebruikt worden bij de bron (BVH).
- (Beleid): Er worden binnen TRIS geen rapportages opgeleverd t.b.v. de besturing van de gegevensverwerking. Het is van belang om bij de managementrapportages een paragraaf op te nemen over de gegevensverwerking, zodat indien nodig hierop bijgestuurd kan worden.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	50%	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.

De verwerkingsgrondslag van TRIS is artikel 13 Wpg. Alle verwerkingen binnen TRIS vallen hier onder. Het is momenteel niet mogelijk dat een metagegeven met de verwerkingsgrondslag een gegeven blijft begeleiden. Dit is in de toekomst wel nodig als TRIS gekoppeld aan BVI wordt. Voor TRIS is een goedgekeurd artikel 13 protocol opgesteld. Niet duidelijk werd tijdens de 0-meting of de datum einde verwerkingstermijn is opgenomen in het gegevensmodel. Het is belangrijk om duidelijk te maken welke verjaringstermijn bij welk gegeven hoort.

Actiepunten:

- **(Wet art 32): neem de datum einde van de verwerkingstermijn op in het gegevensmodel, of zorg er in ieder geval voor dat het voor elk gegeven duidelijk is onder welke verjaringstermijn die valt.**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Doelbinding	Zwaar (Z)	67%	100%	1

1.4 Verantwoording

"De politie moet verantwoording kunnen afleggen over zijn taakuitvoering en over de gegevensverwerking die daarbij plaatsvindt."

De politie moet over zijn taakuitvoering verantwoording kunnen afleggen. Dit is vooral van belang voor gegevensverwerking in strafzaken en de inzet van opsporings- en geweldsbevoegdheden maar geldt ook voor de bedrijfsvoering in brede zin. De informatievoorziening moet het daarom mogelijk maken dat de politie verantwoording aflegt over handelingen en de totstandkoming van besluiten. De verantwoording ten aanzien van gegevensverwerking vormt het sluitstuk van de besturing van de informatievoorziening. De verantwoording zorgt tevens dat invulling gegeven kan worden aan de rechten van betrokkenen wiens persoonsgegevens verwerkt worden.

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

Actiepunten:

- **(Wet art 32a): genereer periodieke rapportages over de audittrail.**
  LETOP: Dit viel tijdens de 0-meting nog onder beleid, maar dit is inmiddels van toepassing op de wet (bij de berekening van de 0-meting valt dit nog onder beleid).
- (Beleid): beveilig de audittrail tegen manipulatie. Dit geldt voor manipulatie mogelijk door gebruikers, maar ook door beheerders. Het moet een bewuste keuze zijn om de audittrail ook voor beheerders te beschermen tegen manipulatie (kosten/baten)

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.

Op het principe autorisatie heeft TRIS een volwassenheidsniveau van 1 (onvoldoende). TRIS is deels aangesloten op IAM, maar het probleem is dat de LFNP-rollen niet aansluiten op de rollen die bij TRIS nodig zijn. De functieomschrijving LFNP is te ruim voor de specifieke rollen van TRIS. Op het moment van de 0-meting werd gewerkt aan een voorstel aan het portefeuilleteam. Het is daarbij niet duidelijk of er gebruik wordt gemaakt van de vastgestelde autorisatierollen van de politie. Er zal nagegaan moeten worden of TRIS op dit onderdeel overeenstemt met de wet. TRIS maakt geen gebruik van toegangsverlening op gegevensniveau, maar op applicatieniveau. Het risico hierbij is dat gegevens tegenwoordig vaak via meerdere applicaties geraadpleegd kunnen worden. Als toegang wordt verleend op applicatieniveau kan het zijn dat gegevens die in de ene applicatie niet toegankelijk zijn, dat wel worden via een andere applicatie. Bij toegang op gegevens niveau is dat niet het geval.

Bij TRIS wordt gebruik gemaakt van de generieke autorisatietool voor leidinggevenden, maar er komen vanuit de uitvoering geluiden dat TRIS niet in de tool kan worden gevonden. Het is niet duidelijk waar het hier precies mis gaat.

Ook op het gebied van autorisaties zouden regelmatig rapportages moeten worden opgesteld. Het is dan goed bij te houden of er sprake is van afwijkende aantallen geautoriseerden. Het controleren van toegangs- en gebruiksrechten gebeurt nu 1x per jaar. De vraag die bij de 0-meting langskwam was wat precies regelmatig is. Dat is afhankelijk van de applicatie, het aantal gebruikers en de doorloop daarvan. Als er veel gebruikers zijn of als de doorloop heel hoog is, dan is het belangrijker dat er vaker wordt gecontroleerd. Het is aan TRIS om te bepalen wat geschikt is voor hun situatie.

Actiepunten:

- (Beleid): Er zal gekeken moeten worden wat er nodig is om op de generieke informatievoorziening van IAM aangesloten te kunnen worden.
    - **(Wet art 6): als niet aan kan worden gesloten op IAM, moet er gebruik worden gemaakt van de vastgestelde autorisatierollen van de politie. TRIS moet nagaan of de rollen die zij hanteren voldoen aan de eisen van de politie.**
    - (Beleid): indien niet kan worden aangesloten bij IAM moet de voorziening de Audit Based Access Control ondersteunen. Zie hiervoor ook de Uitvoering Autorisatiebeleid politie 2016-2020.
- (Beleid): toegang zou moeten worden verleend op gegevensniveau en niet op applicatieniveau.
- (Beleid): zoek uit waar het mis gaat in de uitvoering met de generieke autorisatietool voor leidinggevenden.
- (Beleid): genereer rapportages over het gebruik van de autorisaties.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	50%	33%	1

1.6 Metagegevens

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

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

Vanwege het verschil in FO expertise zijn er verschillende soorten classificaties (bijvoorbeeld een schoenafdruk met zigzag of rondjespatroon) van bepaalde zaken. Het lastige als een applicatie geen gebruik maakt van de vastgestelde definities voor bedrijfsbegrippen is dat het uitwisselen van gegevens bemoeilijkt wordt. Een deel van de bedrijfsbegrippen is echter wel overgenomen, want daarvoor is BVH leidend. De metagegevens die daarvoor in aanmerking komen zouden geautomatiseerd afgeleid en vastgelegd moeten worden. De vastgelegde metagegevens moeten ook mee worden geleverd met koppelingen voor de verwerking in andere voorzieningen. Dit is belangrijk om de juistheid en rechtmatigheid te kunnen waarborgen.

Actiepunten:

- (Beleid): op dit moment maakt TRIS voor een deel gebruik van de vastgestelde bedrijfsbegrippen die vanuit BVH zijn overgenomen. Echter er kan per deskundige-eenheid verschillende soorten classificaties zijn (bijvoorbeeld 10.2.c). Hierin zouden duidelijke afspraken moeten worden gemaakt in samenspraak met GGB.
- (Beleid): stel vast of TRIS onder architectuur is ontwikkeld. Indien dit niet geval is dan dient er beoordeeld te worden of het nog past onder de huidige architectuur.
- (Beleid): Zorg dat er gebruik gemaakt gaat worden van metagegevens, zodat de juistheid en rechtmatigheid gewaarborgd kunnen worden.
    - (Beleid): zolang het Toepassingsprofiel Metagegevens Politie in ontwikkeling is dient er gebruik te worden gemaakt van het Toepassingsprofiel Metagegevens Rijk (TMR) voor het opstellen van de requirements voor metagegevens.
    - (Beleid): zorg dat metagegevens die daarvoor in aanmerking komen geautomatiseerd worden afgeleid en vastgelegd.
    - (Beleid) zorg dat metagegevens die niet geautomatiseerd worden vastgelegd op andere manieren worden ingevuld.
    - (Beleid): gebruik de metagegevens om toegang te verlenen, bewaartermijnen bij te houden en voor audittrails en managementrapportages.
    - (Beleid): lever metagegevens mee bij koppeling voor verwerkingen in andere voorzieningen.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	19%	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.

TRIS voldoet aan de helft van de criteria van kwaliteitszorg, maar er is nog wel verbetering nodig. Door achterstallig onderhoud zijn nog niet alle kwaliteitseisen uit het ontwerp al gerealiseerd. Dit stond voor het 2e kwartaal op de planning. Ook zijn niet alle kwaliteitseisen afgestemd met de beleidsverantwoordelijke. Op service niveau is de beleidsverantwoordelijke bekend met de kwaliteitseisen. Daarnaast zijn er nog geen bedrijfsregels opgesteld om de kwaliteit van gegevens te meten. Net zoals bij eerdere principes al is genoemd, is het belangrijk ook hier rapportages op te stellen. Als de kwaliteit van gegevens wordt bijgehouden, kunnen afwijkingen sneller worden opgemerkt en daar vervolgens naar worden gehandeld. 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): stem de kwaliteitseisen uit het ontwerp af met de beleidsverantwoordelijke. Op dit moment worden er wel eisen doorgevoerd, maar niet aan de hand van kwaliteitseisen. De beleidsverantwoordelijke is hier op serviceniveau mee bekend.
    - (Beleid): realiseer de vastgestelde kwaliteitseisen.
- (Beleid): formuleer bedrijfsregels om de kwaliteit van gegevens te meten.
- (Beleid): zorg dat een rapport kan worden samengesteld over de kwaliteit van gegevens.
- (Beleid): voer kwaliteitscontroles uit en bewaar de resultaten hiervan.
- (Beleid): zorg dat de applicatie (automatisch) de gebruiker attendeert op kwaliteitsafwijkingen. Nu gebeurt dat allen nog handmatig en op werkprocesniveau.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT	50%	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 TRIS niet op het gebied van bewaren en vernietigen. Aan de ene kant is BVH de leidende applicatie op het gebied van bewaren en vernietigen, maar vanwege het FO karakter van TRIS moeten de verjaringstermijnen van het Wetboek van Strafvordering worden gevolgd. Het is op dit moment nog niet duidelijk of al deze termijnen goed zijn opgenomen in TRIS. De gegevens in TRIS worden niet voorzien van een selectie ten behoeve van bewaren en vernietigen. Ook voldoet de voorziening 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 TRIS de gegevens beschikbaar stellen ten behoeve van het duurzaam bewaren van gegevens.

Actiepunten:

- **(Wet art 14 lid 4): controleer of de juiste bewaartermijnen zijn opgenomen in de applicatie.**
- **(Wet art 8, 9, 10, 12 en 14): gegevens moeten worden voorzien van een selectie ten behoeve van bewaren en vernietigen.**
- (Beleid): de voorziening moet voldoen aan de kwaliteitseisen van DUTO.
- **(Wet archiefwet): de voorziening moet ondersteunen dat gegevens beschikbaar worden gesteld ten behoeve van het duurzaam bewaren van gegevens.**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	0%	0%	0

1.9 Informatiebeveiliging

"*De informatievoorziening wordt beveiligd met een adequaat stelsel van maatregelen op basis van risicobeheersing*"

Het belang van informatiebeveiliging is op basis van risicobeheersing al mogelijke schadelijke gevolgen door bedreigingen van de informatievoorziening op een bewuste manier afweegt tegen kosten en belemmeringen van beveiligingsmaatregelen. Met daarbij in acht nemen dat de politie een verantwoordelijkheid en verplichting heeft om de gegevens van de burgers te beschermen.

TRIS 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 in beheer zijn.

Actiepunten:

- (Beleid): er moet een nieuwe risicoanalyse voor de verwerkingen uitgevoerd worden.
    - **(Wet art 4b en c): stel de informatiebeveiligingseisen op naar aanleiding van de resultaten van de risico analyse.**
    - **(Wet art 4b en c): stel vast wat de impact van de te nemen informatiebeveiligingseisen is op de voorziening.**
    - (Beleid): gebruik waar mogelijk de standaard informatiebeveiligingsdiensten. Als dat niet mogelijk is, neem passende maatregelen.
    - (Beleid): beheer de restrisico's.

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

1.10 Voldoen aan de wet

"*Gegevensverwerking door de politie voldoet aan de daarvoor geldende wettelijke kaders*"

Dit principe is niet besproken aangezien dit in de volgende versie verwijderd gaat worden en de vragen omtrent wetgeving verweven zitten in de andere principes.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Voldoen aan de wet	Zwaar (Z)	NVT	NVT	NVT

1.11 Toepassen standaarden

"*Bij de gegevensverwerking wordt gebruik gemaakt van bestaande overheids- en ketenstandaarden*"

Door het gebruik van bestaande overheids- en ketenstandaarden bevordert de samenwerking tussen de organisaties en de interoperabiliteit van systemen. In de basis is het ban belang om waar mogelijk gebruik te maken van standaardisatie en uniformiteit binnen een informatievoorziening. Indien een organisatie hierin een eigen keuze maakt en afwijkt van standaarden zullen er afspraken gemaakt moeten worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

TRIS maakt gebruikt van bestaande overheids- en ketenstandaarden. De verantwoordelijkheid voor het uitvoeren van toetsen op de toepasselijke standaarden ligt bij DICT, maar sinds 2015 is hier niet meer naar gekeken. Dat is ook afhankelijk van het scrum team. Het is niet duidelijk of in het geval van afwijkingen een motivatie is gegeven door de verwerkingsverantwoordelijke.

Actiepunten:

- (Beleid): voer toetsen uit op de toepasselijke standaarden.
- (Beleid): in het geval van afwijkingen van standaarden moet er een motivatie zijn die is geaccepteerd door de verwerkingsverantwoordelijke (pas toe of leg uit)

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

1.12 Verantwoordelijkheden belegd

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

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

TRIS voldoet volledig aan het politiebeleid van het principe verantwoordelijkheden belegd. Er zijn bij dit principe geen wetscriteria actief dus TRIS heeft de maximale volwassenheidsscore van 100%.

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.
- 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[4].

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.

[4] Bijlage 1: Uitgangspunt bij compliance

Bedrijfsregels volwassenheidsniveau
Als de criteria zijn beoordeeld als “niet van toepassing” dan zijn er geen criteria benoemd of de criteria zijn niet van toepassing gebleken voor de applicatie.

Niveau 0: Een volwassenheidsniveau 0 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan minder dan 35% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan minder dan 35% van de beleidscriteria wordt voldaan.

Niveau 1: Een volwassenheidsniveau 1 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan ten minste 35% maar minder dan 100% van de wettelijke criteria wordt voldaan
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 35% maar minder dan 50% van de beleidscriteria wordt voldaan.

Niveau 2: Een volwassenheidsniveau 2 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria, en aan niet alle van de beleidscriteria wordt voldaan.
b: de wettelijke criteria zijn niet van toepassing, en aan ten minste 50% maar minder dan 100% van de beleidscriteria wordt voldaan.

Niveau 3: Een volwassenheidsniveau 3 moet worden toegekend, indien een van de volgende voorwaarden van toepassing is:

a: aan alle wettelijke criteria en aan alle beleidscriteria wordt voldaan
b: aan alle wettelijke criteria wordt voldaan en de beleidscriteria zijn niet van toepassing
c: de wettelijke criteria zijn niet van toepassing, en aan alle beleidscriteria wordt voldaan

NVT : Een volwassenheidsniveau NVT moet worden toegekend, indien de volgende voorwaarde van toepassing is:

a: de wettelijke criteria en de beleidscriteria zijn niet van toepassing

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