



0-meting Privacy & Security by Design



Hansken

10.2.e

Concept

Versie 0.9

Versie datum 21 december 2018

Rubricering **Politie Intern**

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	21-12-2018	Reviewen
0.9	21-12-2018	Aanpassingen op basis van review

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.9	21-12-2018	10.2.e	Gegevensautoriteit

© Politie, all rights reserved.

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

Documentinformatie	2
Inhoudsopgave	2
Inleiding	4
0-meting Hansken	5
Algemeen	5
Doel	5
Doelgroep	5
Aanwezigen 0-meting	5
Hansken	6
Omschrijving applicatie	6
Soorten verwerkingen van politiegegevens	6
Verwerkingsgrondslag	7
Eindscore	8
1.1 Eenmalige vastlegging	10
1.2 PDCA-cyclus	10
1.3 Doelbinding	11
1.4 Verantwoording	11
1.5 Autorisatie	12
1.6 Metagegevens	12
1.7 Kwaliteitszorg	13
1.8 Bewaren en vernietigen	13
1.9 Informatiebeveiliging	14
1.10 Privacy by default	14
1.11 Toepassen standaarden	15
1.12 Verantwoordelijkheden belegd	15
2. Verantwoording toetsing	16
Toetsingscriteria	16
Disclaimer	18
Bijlage 1: Uitgangspunt bij compliance	19

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 Hansken. 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 Hansken

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 Hansken	10.2.e	10.2.e

	Naam	Functie
Toetsing	10.2.e	10.2.e

Gespreksdatum	Nummer meting	Toelichting
15-11-2018	2018111501	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader Privacy & Security by Design versie 2.0.

Hansken

Omschrijving applicatie

Hansken is een landelijke applicatie die in samenwerking met het NFI is ontwikkeld. In 2015 is Hansken in productie gegaan. Met Hansken kan een onderzoeksteam snel en efficiënt zoeken in grote hoeveelheden in beslaggenomen gegevensdragers als computers en mobiele telefoons. Er wordt nog verder ontwikkeld aan het uitlezen van gegevens in een voertuig zoals navigatie en het adresboek. De gegevens worden aangeleverd als een image van een drager. De images worden versleuteld en met een niet herleidbare bestandsnaam per eenheid opgeslagen op het netwerk bij de onderzoeksmap. Dit valt buiten de scope van Hansken.

Op alles wat relevant kan zijn, kan worden gezocht, bijvoorbeeld op woorden en namen of eigenschappen van sporen zoals chatberichten, e-mails of foto's al dan niet gemaakt met een bepaalde camera. Rechercheurs kunnen met de forensische dienst de zoekresultaten blijven filteren tot uit miljoenen sporen een selectie ontstaat, waarvan de sporen één voor één te bekijken zijn. Hansken wordt gehost door politie. Het Operationeel beheer ligt nog bij het NFI.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	Data wordt ingelezen van versleutelde images van de devices. Per project.
Ordenen	X	Alle typen gegevens.
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	Toevoegen sporen van buitenaf aan images. Engelse vertaling van Russische mailtjes.
Wijzigen (het bestaande aanpassen)	X	Alleen wat zelf aangevuld is. Images kunnen nooit gewijzigd.
Opvragen	X	
Raadplegen	X	
Gebruiken	X	
Vergelijken	X	Gebruiker kan gegevens laten vergelijken.
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	Hansken genereert rapport van aangemerkte onderdelen. Eventueel aparte omgeving met geselecteerde data voor raadplegen door externe.
Samenbrengen	X	Binnen project worden de images ingeladen, maar deze worden niet samengevoegd.
Met elkaar in verband brengen		
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)		Hansken kent geen poortwachter constructie.
Vernietigen	X	Er wordt geen backup gemaakt van de data in Hansken.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8		
Onderzoek rechtsorde bepaald geval	Artikel 9	x	
Informatiepositie	Artikel 10		
Geautomatiseerd vergelijken en in combinatie zoeken	Artikel 11		In Hansken kan niet over meerdere zaken heen gezocht worden
Informanten	Artikel 12		
Ondersteunende taken	Artikel 13		

Artikel 8 (lid 1) Wpg: verwerking met het oog op de uitvoering van de dagelijkse politietaak

Artikel 9 (lid 1) Wpg: gerichte verwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval

Artikel 10 (lid 1) Wpg: gerichte verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde

Artikel 11 (lid 1) Wpg: verwerking teneinde vast te stellen of er verbanden bestaan tussen politiegegevens die worden verwerkt op grond van artikel 8 of 9

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

De applicatie Hansken scoort een volwassenheidsniveau 1. Dit houdt in dat Hansken onvoldoende voldoet 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 Hansken een score van 60% en op de criteria van het politiebeleid een score van 63%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria, waarbij de principes 'informatiebeveiliging', 'PDCA-cyclus' en 'autorisatie' er negatief uitspringen. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Daarnaast zijn er een aantal aandachtspunten.

Hansken is geen registratief systeem. De data wordt geleverd vanuit de in beslaggenomen gegevensdragers. Deze worden automatisch overgenomen in Hansken. Daardoor wordt voldaan aan veel criteria, of zijn criteria juist niet van toepassing. Een gevolg hiervan is dat criteria die wel van toepassing zijn maar waar een actiepoint uit volgt het volwassenheidsniveau snel omlaag trekken. Een actiepoint dat wordt opgelost zal het volwassenheidsniveau daar in tegen weer snel omhoog trekken.

Actiepunten:

- (Wet, art 4c) Borg dat bij iedere nieuwe ontwikkeling getoetst wordt doormiddel van een pre-GEB en indien nodig een GEB uitgevoerd gaat worden. Hansken is nog vol op in ontwikkeling en de kans is groot dat de ontwikkelingen GEB waardig zijn. [p2c4] [p2c5]
- (Wet, art 6c lid 2) Zorg dat, zolang het operationeel beheer nog niet is overgedragen naar politie, er een overeenkomst is tussen politie en het NFI voor het operationeel beheer van Hansken. Als dit niet valt onder een bestaande generieke overeenkomst dan moet er een nieuwe overeenkomst opgesteld worden. De nieuwe overeenkomst zou ook aan kunnen sluiten bij Wpg artikel 6 lid 4, het autoriseren van personen die geen politie ambtenaar zijn.
- (Wet, art 6) Zorg dat, zolang nog geen gebruik gemaakt wordt van IAM, voor het verlenen van toegang gebruik gemaakt wordt van de vastgestelde autorisatie rollen van de politie. [p5c2]
- (Wet art 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers regelmatig gecontroleerd worden. [p5c8]

Aandachtspunten:

- Hansken volgt voor de bewaartermijnen het systeem Summ-IT. Als in Summ-IT de verwerkingen niet voorzien wordt van een waardering en selectie ten behoeve van bewaren en vernietigen dan werkt dat door in Hansken (garbage in, garbage out). [p8]
- Support voor Hansken moet nog overgedragen worden van het NFI naar politie.

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
Hansken	15-11-2018	2.0	60%	63%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR	PERCENTAGE		VOLWASSENHEID
		W(wet)	B(beleid)	
Eenmalige vastlegging	Z -	NVT	NVT	NVT
PDCA-cyclus	M -	25%	75%	0
Doelbinding	Z -	100%	NVT	3
Verantwoording	Z -	100%	0%	2
Autorisatie	Z -	33%	38%	0
Metagegevens	Z -	NVT	50%	2
Kwaliteitszorg	Z -	NVT	100%	3
Bewaren en vernietigen	Z -	100%	NVT	3
Informatiebeveiliging	Z -	0%	20%	0
Privacy by default	Z -	100%	100%	3
Toepassing standaarden	L -	NVT	100%	3
Verantwoordelijkheden belegd	M -	NVT	100%	3
TOTALEN TOETSING	-	60%	63%	

VOLWASSENHEID
TOETSING 1
NIVEAU
1

In de afbeelding hierboven staan de volwassenheidsniveaus per principe beschreven. De eerste kolom geeft de weegfactor van het principe op de eindscore weer. De tweede en derde kolom geven het behaalde percentage van de beleids- en wetscriteria weer. Tot slot staat het volwassenheidsniveau per principe weergegeven. Dit niveau is gebaseerd op de score van alle principes van deze toets.

Voor de principes "Kwaliteitszorg", "Toepassing standaarden" en "Verantwoordelijkheden belegd" zijn er geen wettelijke criteria benoemd. Deze worden daardoor standaard met "NVT" gewaardeerd. Voor alle andere resultaten geldt dat deze alleen "NVT" krijgen als alle betreffende criteria niet van toepassing zijn.

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.

Dit principe is niet van toepassing voor Hansken aangezien de gegevens in de bronsystemen worden geclassificeerd. Hansken neemt deze gegevens één op één over.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	NVT	NVT	NVT

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.

Hansken levert periodiek stuurinformatie voor de PDCA cyclus. De capaciteit voor deployment van nieuwe releases is echter nog onvoldoende. De kans is groot dat bij nieuwe ontwikkelingen een GEB en eventueel raadpleging van de autoriteit persoonsgegevens noodzakelijk is. En als laatste is het van belang dat de beleidsverantwoordelijke goed in positie wordt gebracht.

Actiepunten:

- (Beleid) Zorg dat er meer capaciteit beschikbaar komt voor deployment van nieuwe releases. Dit is nu een bottleneck. [p2c3]
- **(Wet, art 4c) Borg dat bij iedere nieuwe ontwikkeling getoetst wordt doormiddel van een pre-GEB en indien nodig een GEB uitgevoerd gaat worden. Hansken is nog vol op in ontwikkeling en de kans is groot dat de ontwikkelingen GEB waardig zijn. [p2c4] [p2c5]**
- **(Wet, art 6c lid 2) Zorg dat, zolang het operationeel beheer nog niet is overgedragen naar politie, er een overeenkomst is tussen politie en het NFI voor het operationeel beheer van Hansken. Als dit niet valt onder een bestaande generieke overeenkomst dan moet er een nieuwe overeenkomst opgesteld worden. De nieuwe overeenkomst zou ook aan kunnen sluiten bij Wpg artikel 6 lid 4, het autoriseren van personen die geen politie ambtenaar zijn. [p2c6]**
- (Beleid) Zorg dat de beleidsverantwoordelijke een visie vaststelt voor Hansken en zorg dat de beleidsverantwoordelijke goed in positie wordt gebracht zodat hij adequaat kan reageren op problemen bij het gebruik van Hansken. [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	25%	75%	0

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.

Alle projecten in Hansken zijn gekoppeld aan een artikel 9 onderzoek. De project in Hansken vallen ook onder artikel 9. Hierdoor voldoet Hansken aan de wet en zijn alle andere criteria niet van toepassing.

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

De audittrail wordt door Hansken bewaard en er kan een rapportage van de trail gemaakt worden. Er is een actiepunt voor de beveiliging van de audittrail en een actiepunt voor de retentie van de audittrail.

Actiepunten:

- (Beleid) Zorg dat de audittrail door niemand gemanipuleerd kan worden. Ook niet door een database administrator. Er is door het NFI al gewerkt aan een logging framework waar de audittrail veilig vastgelegd kan worden. Deze moet nog getoetst worden aan het loggingskader. [p4c3]
- (Beleid) Onderzoek of gegevens uit de audittrail automatisch worden vernietigd na een bepaalde periode. Als dat zo is, onderzoek dan of dat schadelijk is voor de verantwoording en borg zo nodig de maatregelen. [p4c3]

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.

Hansken maakt gebruik van een eigen autorisatiemodel met toegangsverlening op gegevensniveau. De gebruikers zijn op de hoogte van de voor hen geldende autorisatieregels. Hansken moet gebruik gaan maken van de generieke IAM voorziening of, tijdelijk, van de vastgestelde autorisatirollen met daarbij een goed controle proces en sanctiebeleid. Voor autorisaties buiten de standaardrollen om moet gebruik gemaakt gaan worden van de autorisatietool voor leidinggevend. Daarnaast moet er een regelmatige controle zijn op de autorisaties.

Actiepunten:

- (Beleid) Zorg dat Hansken voor het verlenen van toegang gebruik gaat maken van de generieke IAM-voorziening voor het verifiëren van identiteiten. Hansken gebruikt nu een eigen identity provider. [p5c1]
- **(Wet, art 6) Zorg dat, zolang nog geen gebruik gemaakt wordt van IAM, voor het verlenen van toegang gebruik gemaakt wordt van de vastgestelde autorisatirollen van de politie. [p5c2]**
- (Beleid) Zorg dat Hansken voor het verlenen van toegang gebruik gaat maken van de generieke autorisatietool voor leidinggevend. [p5c4]
- (Beleid) Zorg dat Hansken, zolang IAM nog niet ondersteund wordt, Audit Based Acces (ABA) ondersteund. Dat wil zeggen dat er een goed controle (audit) proces en sanctiebeleid is. Zie het autorisatiebeleid 2016-2020. [p5c5]
- **(Wet art 4a) Zorg dat de toegang- en gebruiksrechten van gebruikers regelmatig gecontroleerd worden. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	33%	38%	0

1.6 Metagegevens

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

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

Hansken is geen registratief systeem. De data wordt geleverd vanuit de in beslaggenomen gegevensdragers. In de gegevensdragers worden de metagegevens geregistreerd. Deze worden automatisch overgenomen in Hansken. De meeste criteria zijn daardoor niet van toepassing. Er is één actiepunt. Dit betreft een toets of het toepassingsprofiel metagegevens Rijk (TMR) meerwaarde heeft voor Hansken.

Actiepunten:

- (Beleid) Bestudeer de mogelijkheden van het toepassingsprofiel metagegevens Rijk (TMR) en pas dat indien mogelijk toe, totdat het Toepassingsprofiel Metagegevens Politie beschikbaar is [p6c4].

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.

De kwaliteitseisen voor Hansken zijn gericht op het inlezen en het interpreteren van de gegevens uit de in beslag genomen gegevensdragers. Daarbij is het Inception raamwerk van het NFI leidend. Hansken voldoet aan al deze eisen.

Er kunnen geen kwaliteitseisen gesteld worden aan de in beslag genomen gegevens zelf.

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

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.

Een onderzoek in Hansken moet vernietigd worden zodra het gerelateerde onderzoek in Summ-IT wordt verwijderd. Bij het verwijderen van het onderzoek in Summ-IT hoort ook het verwijderen van de gegevens in de map van de mappenstandaard. De images van de in beslag genomen gegevensdragers staan ook in deze map. De images blijven dus nog vijf jaar toegankelijk voor de poortwachter. Gegevens in Hansken vallen niet onder archivering.

Er is geen geautomatiseerde koppeling tussen Summ-IT en Hansken. Zolang het support van Hansken nog bij het NFI ligt zal het verwijderbericht dus naar het NFI verstuurd moeten worden waar het handmatig verwerkt wordt. Aangezien de bewaartermijn bewaakt wordt in Summ-IT zijn de meeste criteria voor "Bewaren en vernietigen" niet van toepassing voor Hansken. Maar er wordt voldaan aan de wettelijke eisen met betrekking tot bewaren, vernietigen en archiveren en aan het volgen van de bron.

Aandachtspunten:

- Hansken volgt voor de bewaartermijnen het systeem Summ-IT. Als in Summ-IT de verwerkingen niet voorzien wordt van een waardering en selectie ten behoeve van bewaren en vernietigen dan werkt dat door in Hansken (garbage in, garbage out). [p8]
- Support voor Hansken moet nog overgedragen worden van het NFI naar politie. [p8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	100%	NVT	3

³ Er zijn voor dit principe geen wettelijke criteria benoemd.

1.9 Informatiebeveiliging

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

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

Het is van belang regelmatige de informatiebeveiliging te laten controleren. In de snel veranderende wereld om ons heen kan het betekenen dat de informatiebeveiliging van vandaag voldoende is, maar morgen is achterhaald. Hansken haalt voor dit principe het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt doordat er geen risicoanalyse is uitgevoerd. Hansken maakt wel gebruik van de generieke voorzieningen voor informatiebeveiliging. Er is door het NFI wel een security audit uitgevoerd op de programmacode van Hansken. Daarnaast is er door het NFI ook een penetratietest uitgevoerd.

Actiepunten:

- (Beleid) Zorg dat er een risicoanalyse voor de verwerking wordt uitgevoerd. [p9c1]
 - (Beleid) Zorg dat de informatiebeveiligingseisen mede bepaald worden op basis van de resultaten van de risicoanalyse. [p9c2]
 - (Beleid) Zorg dat de impact van de informatiebeveiligingseisen beoordeeld wordt ten behoeve van de realisatie in Hansken. [p9c3]
 - (Beleid) Toets of alle informatiebeveiligingseisen gerealiseerd kunnen worden door de standaard informatiebeveiligingsdiensten. [p9c5]
 - (Beleid) Toets of er maatregelen genomen kunnen worden om informatiebeveiligingseisen te realiseren die niet door de standaard informatiebeveiligingsdiensten kunnen worden gerealiseerd. [p9c6]
 - (Beleid) Zorg dat de restrisico's in de beveiliging van Hansken worden beheerd. [p9c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Informatiebeveiliging	Zwaar (Z)	0%	20%	0

1.10 Privacy by default

"De verwerking van persoonsgegevens is standaard zo beperkt mogelijk ingericht"

Zowel de AVG als de Wpg bevatten Privacy by Default en Privacy by Design als verplichte principes. Deze dienen ertoe om gegevensbescherming vanaf het moment van ontwikkeling van informatiediensten tot aan het laatste gebruik zoveel mogelijk in de gegevensverwerking te integreren. Daar waar Privacy by Design vooral toeziet op ontwerpkeuzes bij de *ontwikkeling* van informatiediensten is Privacy by Default van belang bij keuzemomenten tijdens *gebruik* van de informatiediensten. Dit principe verplicht organisaties om de privacy van betrokkenen zo veel mogelijk te beschermen door de verwerking van persoonsgegevens standaard (by default) op de meest privacy vriendelijke stand te zetten.

De verwerking van persoonsgegevens in Hansken bevat geen overbodige informatie en de gegevens zijn relevant voor het doel van onderzoek. Een opt-in regime en Privacy Enhancement Technology (PET) hulpmiddelen zijn niet van toepassing. Hierdoor wordt aan alle criteria voldaan.

De images van de gegevensdragers die staan opgeslagen in een map van de mappenstandaard zijn overigens versleuteld. Maar dat valt buiten de scope van Hansken.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	100%	100%	3

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 van 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.

Afgezien van een paar basale standaarden zoals JSON (JavaScript Object Notation) zijn er geen standaarden van toepassing voor Hansken.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT ⁴	100%	3

1.12 Verantwoordelijkheden belegd

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

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

De beleidsverantwoordelijke is bekend met Hansken en heeft ook de definities, beleid, koers en strategie vastgesteld. De uitvoeringsverantwoordelijke kan zo nodig gegevens corrigeren en verstrekken. Dit samen maakt dat Hansken voldoet aan alle criteria voor "Verantwoordelijkheden belegd".

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT ⁵	100%	3

⁴ Er zijn voor dit principe geen wettelijke criteria benoemd.

⁵ Er zijn voor dit principe geen wettelijke criteria benoemd.

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-26_Uitvoeringskader_Privacy en Security by Design_v2.0'. 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 compliance 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' staan⁶.

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.

⁶ 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

Weefactor

Van ieder principe is een weefactor 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 weefactoren is als volgt:

Weefactor	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

