POLITIE

0-meting Privacy & Security by Design

iBase

10.2.e

Concept

Versie 1.00

Versie datum 2 mei 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-1-2018	Opzet template rapport
0.8	16-11-2018	Eerste review
0.9	23-11-2018	Aanpassingen voor laatste controle
0.91	05-04-2019	Aanpassingen naar aanleiding van review verwerkt.
0.92	30-04-2019	Aanpassingen naar aanleiding van review verwerkt. - Artikel 11 en 12 verwijderd bij verwerkingsgrondslag omdat deze niet deze lijst thuishoren. - Bij principe 3 Wpg artikel 11 geformuleerd als handelingsbevoegdheid.

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	16-11-2018	10.2.e	Gegevensautoriteit
0.9	23-11-2018	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 compliance 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) compliance 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 compliance.

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 iBase. 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[3]. 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
[3] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

0-meting iBase

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 iBase	10.2.e	Functioneel beheer
	10.2.e	Coördinator LE methodes & tooling voor analyse
	10.2.e	IV-Expert intelligence
	10.2.e	BICC LE (Bluebase import tool)
	10.2.e	Team KVI DLIO
	10.2.e	Analist team criminele inlichtingen

	Naam	Functie
Toetsing	10.2.e	Programmamanager
	10.2.e	Beleidsadviseur

Gespreksdatum	Nummer meting	Toelichting
2018/10/09	2018100901	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

iBase

iBase is een data-analysetool die gemaakt is door IBM en via de firma Data Expert wordt geleverd. Het is een krachtige relationele database omgeving voor het vastleggen en doorzoeken van (onderzoek)gegevens uit o.a. BVI en SummIT . iBase wordt vooral gebruikt in het kader van veiligheids- en zaakanalyses.
Voor de teams Analyse & Onderzoek (A&O) is een landelijke omgeving ingericht onder de naam SIAN (Standaardisatie en Implementatie Analysetools). Alle ruim 650 analisten uit deze teams hebben de beschikking over een gestandaardiseerde toolset (iBase, Analyst Notebook, MapInfo) en kunnen hiermee in een landelijke mappenstructuur samenwerken. Er is strikte scheiding aangebracht tussen de domeinen A&O (reguliere analyses op basis van artikel 8 en 9 WPG), TCI (artikel 10 WPG), TOOI (artikel 10 WPG), Thema-onderzoeken CTER, Mensenhandel, Mensensmokkel (artikel 10 WPG), onderzoeken die plaatsvinden i.k.v. artikel 13.2 WPG en Embargo-onderzoeken. Per domein wordt een landelijk register bijgehouden van actuele databases . Om toegang te krijgen tot één van de domeinen moet men expliciet worden geautoriseerd. Hierbij geldt het zogenaamde 4-ogen principe voor de TCI, TOOI en Thema-onderzoeken (zowel teamchef A&O als de teamchef Inwinning moet toestemming geven). Om bovendien toegang te krijgen tot de data in een specifieke analysedatabase (onderzoek), moet men ook nog op (individueel) onderzoekniveau worden geautoriseerd. Tot slot zijn er voor SIAN 3 aparte SQL-databasesservers ingericht zodat de verschillende regimes ook fysiek gescheiden zijn.
iBase wordt ook gebruikt door gebruikers die organisatorisch niet zijn ingedeeld bij één van de teams Analyse & Onderzoek. Voor deze gebruikersgroep is eveneens een aparte SQL-databaseserver ingericht. De eenheid Den Haag en een aantal afdelingen van de Landelijke Eenheid hebben hier databases in gebruik. Deze afdelingen gebruiken ieder een eigen afgeschermde mappenstructuur en hebben geen toegang tot de landelijke SIAN-omgeving van de teams A&O.
De eenheid Rotterdam maakt als enige gebruik van zgn. cases binnen iBase. Hiermee wordt het mogelijk om meerdere dataverzamelingen binnen één onderzoeken logisch te onderscheiden. In deze gevallen is het mogelijk om in één zoekslag alle dataverzamelingen in het betreffende onderzoek te raadplegen.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	X	Bijvoorbeeld info uit buitenland of verrijken van data.
Ordenen	X	
Bewaren	X	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	X	Bijvoorbeeld telefoonnummers ontdubbelen of personen ontdubbelen.
Wijzigen (het bestaande aanpassen)	X	
Opvragen	X	
Raadplegen	X	
Gebruiken	X	Analyse en onderzoek
Vergelijken	X	
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	X	
Samenbrengen	X	
Met elkaar in verband brengen	X	
Afscherming	X	
Uitwissen (weghalen/verwijderen zonder vernietigen)	X	
Vernietigen	X	Nog niet gebaseerd op termijnen.

Verwerkingsgrondslag

Doelbinding	Verwerkingsgrondslag	X	Toelichting
Dagelijkse politietaak	Artikel 8	X	
Onderzoek rechtsorde bepaald geval	Artikel 9	X	
Informatiepositie	Artikel 10	X	
Ondersteunende taken	Artikel 13	X	13.1 of 13.2 verwerking afkomstig uit bronsystemen.

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 13 Wpg: de politiegegevens van artikel 8, 9 en 10 Wpg mogen verder worden verwerkt ten behoeve van de ondersteuning van de politietaak

Eindscore

Deze 0-meting is uitgevoerd voor het gebruik van iBase conform de landelijke werkwijze. De applicatie iBase scoort een volwassenheidsniveau 1. Dit houdt in dat iBase 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 iBase een score van 61% en op de criteria van het politiebeleid een score van 77%. 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', 'bewaren en vernietigen' 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.

Actiepunten:

- **(Wet, art 4a) Zorg dat de naleving van de autorisatieregels in de werkinstructies goed wordt geborgd. [p5c6]**
- **(Wet art 8,9,10,14) Zorg dat gegevens die in de bron zijn verwijderd (alleen nog toegankelijk voor de poortwachter) ook in iBase verwijderd worden. [p8c1] [p8c2] [p8c5].**
- **(Wet art 8,9,10,14) Zorg dat gegevens die in de bron zijn vernietigd ook in iBase vernietigd worden. [p8c1] [p8c2] [p8c5].**
- **(Wet art 4a lid 2) Stel de informatiebeveiligingseisen vast op basis van de resultaten uit de risicoanalyse. [p9c2]**
- **(Wet art 4a lid 2) Beoordeel de impact van de informatiebeveiligingseisen ten behoeve van realisatie. [p9c3]**

Aandachtspunten[4]:

1. De doelbinding moet in de bronsystemen goed geregistreerd worden. In BVH bijvoorbeeld worden alle verwerkingen nu beschouwd als artikel 8, terwijl er ook artikel 9, 10 en13 verwerkingen tussen zitten. [p3]
2. De doelbinding en de einddatum voor de verwerkingstermijn kunnen in iBase gewijzigd worden. Maar dat is geen gewenste functionaliteit. Wijzigingen moeten gemaakt worden in het bronsysteem. [p3]
3. **(Wet, art 4a) Er is een risico dat via ATL gebruikers geautoriseerd worden voor een andere doelgroep. [p5c6]**
4. **iBase is niet bedoeld als registratiesysteem maar biedt daar wel mogelijkheden toe. In de praktijk wordt iBase in uitzonderlijke gevallen ook voor registratie toegepast en dat wordt gedoogd. [p7]**
5. iBase volgt voor de bewaartermijnen de bronsystemen. Als in een bronsysteem de verwerkingen niet voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen dan werkt dat door in iBase (garbage in, garbage out). [p8]
6. Met iBase kunnen gegevens geëxporteerd worden om in andere applicatie verder te verwerken. Het is ook mogelijk om de geëxporteerde gegevens te verstrekken. Dit laatste kan rechtmatig zijn. Maar er zijn geen (technische) beperkingen tegen een onrechtmatige verstrekking. Onderzoek of dit nog verbeterd kan worden. [p12]
7. **De eenheid Den Haag heeft een eigen server voor iBase. De onderzoeken op deze server zijn niet zichtbaar in de landelijke mappenstructuur. Daarnaast is er geen toezicht op navolging van de landelijke werkwijze.. De landelijke eenheid maakt voor de onderzoeken die niet onder "Analyse en onderzoek" vallen ook gebruik van de server van Den Haag.**

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
iBase	09/10/2018	2.0	61%	77%	1

[4] Als er algemene verbeterpunten besproken zijn die niet direct gerelateerd kunnen worden aan de criteria uit PSbD dan worden deze opgenomen als aandachtspunten. Deze tellen niet mee in de berekening van de scores.

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	100%	100%	3
PDCA-cyclus	M	-	NVT	25%	0
Doelbinding	Z	-	100%	100%	3
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	50%	100%	1
Metagegevens	Z	-	NVT	100%	3
Kwaliteitszorg	Z	-	NVT	100%	3
Bewaren en vernietigen	Z	-	25%	NVT	0
Informatiebeveiliging	Z	-	0%	20%	0
Privacy by default	Z	-	NVT	100%	3
Toepassing standaarden	L	-	NVT	NVT	NVT
Verantwoordelijkheden belegd	M	-	NVT	100%	3
TOTALEN TOETSING		-	61%	77%	

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.

Het grootste deel van de gegevens van onderzoeken in iBase is afkomstig uit de politiesystemen. Dat betekent dat iBase afhankelijk is van de kwaliteit van de gegevens in die systemen. De criteria van dit principe zijn daardoor niet van toepassing.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Eenmalige vastlegging	Zwaar (Z)	100%	100%	3

1.2 PDCA-cyclus

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

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

Er is geen besturing van iBase mogelijk op basis van periodieke rapportages omdat deze ontbreken. Daarnaast is niet duidelijk of er voldoende beleid wordt gevoerd vanuit de beleidsverantwoordelijke en de betrokken gremia. De applicatie iBase haalt hierdoor voor dit principe het laagst mogelijke volwassenheidsniveau.

Actiepunten:

- (Beleid) Onderzoek of iBase voldoende rapportage mogelijkheden heeft voor de reguliere PDCA cyclus en neem zo nodig maatregelen. Bijvoorbeeld rapportages over de omvang van de gegevensverwerkingen, kwaliteit van de gegevens, aantallen gebruikers en beheer van autorisaties. [p2c1]
- (Beleid) Zorg dat de rapportages periodiek worden opgeleverd. [p2c2]
- (Beleid) Zorg dat het beheer van gegevens beter wordt geborgd. Dit is nu afhankelijk van de persoonlijke invulling van de analisten. [p2c3]
- (Beleid) Onderzoek of de beleidsverantwoordelijke en de gremia rondom iBase voldoende betrokken zijn en neem zo nodig maatregelen. Voeren zij voldoende beleid op definities, beleid, koers en strategie voor de verwerking van gegevens? Als gremia worden genoemd: "Landelijk productgroep overleg", "Platform analyse en onderzoek" en de "Stuurgroep analyse". [p2c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	25%	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.

iBase is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsysteem wordt de doelbinding geregistreerd. Deze wordt automatisch overgenomen in iBase. Hierdoor voldoet iBase aan alle criteria. Ten behoeve van Wpg artikel 9 of 10 verwerkingen worden er analyses gemaakt in iBase. De analyse is een handelingsbevoegdheid die valt onder Wpg artikel 11 (geautomatiseerd vergelijken en in combinatie zoeken). Het resultaat van de analyse is een Wpg artikel 9 of 10 verwerking.

Aandachtspunten:

- De doelbinding moet in de bronsystemen goed geregistreerd worden. In BVH bijvoorbeeld worden alle verwerkingen nu beschouwd als artikel 8, terwijl er ook artikel 9, 10 en13 verwerkingen tussen zitten. [p3]
- De doelbinding en de einddatum voor de verwerkingstermijn kunnen in iBase gewijzigd worden. Maar dat is geen gewenste functionaliteit. Wijzigingen moeten gemaakt worden in het bronsysteem. [p3]

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

1.4 Verantwoording

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

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

Voor dit principe is er slechts één actiepunt vanuit beleid. Er zijn geen actiepunten vanuit de wet. Als het actiepunt opgelost wordt haalt iBase voor "Verantwoording" het hoogst mogelijke volwassenheidsniveau.

Actiepunten:

- (Beleid) Toets of verhoging van het audit level in iBase toegevoegde waarde heeft. Het huidige level is 3. Met level 4 en 5 wordt er minder geregistreerd bij een bulk import en meer bij raadplegen van gegevens. [p4c1]
- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. Op dit moment kan de audittrail gewijzigd worden door twee database administrators. [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.

Voor dit principe is er slechts één actiepunt vanuit de wet. Er wordt voldaan aan alle actiepunten vanuit beleid omdat gebruik gemaakt wordt van IAM, ATL en toegangsverlening op gegevensniveau. Als het openstaande actiepunt opgelost wordt haalt iBase voor "Autorisatie" het hoogst mogelijke volwassenheidsniveau.

Actiepunten:

- **(Wet, art 4a) Zorg dat de naleving van de autorisatieregels in de werkinstructies goed wordt geborgd. [p5c6]**

Aandachtspunten:

- **(Wet, art 4a) Er is een risico dat via ATL gebruikers geautoriseerd worden voor een andere doelgroep. [p5c6]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	50%	100%	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.

iBase is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsystemen worden de metagegevens geregistreerd. Deze worden automatisch overgenomen in iBase. Hierdoor voldoet iBase aan alle criteria.

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

Voor het principe "Kwaliteitszorg" zijn er alleen criteria vanuit beleid. Hier zijn geen acties uit voortgekomen. Er is wel een aandachtspunt.

Aandachtspunten:

- iBase is niet bedoeld als registratiesysteem maar biedt daar wel mogelijkheden toe. In de praktijk wordt iBase **in uitzonderlijke gevallen** ook voor registratie toegepast en dat wordt gedoogd. [p7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[5]	100%	3

[5] Er zijn voor dit principe geen wettelijke criteria benoemd.

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.

iBase is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsystemen mogen gegevens niet langer worden verwerkt dan is toegestaan en worden ze vernietigd zodra ze niet langer nodig zijn. iBase volgt de bron niet voor vernietigen en verwijderen.

Actiepunten:

- **(Wet art 8,9,10,14) Zorg dat gegevens die in de bron zijn verwijderd (alleen nog toegankelijk voor de poortwachter) ook in iBase verwijderd worden. [p8c1] [p8c2] [p8c5].**
- **(Wet art 8,9,10,14) Zorg dat gegevens die in de bron zijn vernietigd ook in iBase vernietigd worden. [p8c1] [p8c2] [p8c5].**

Aandachtspunt:

- iBase volgt voor de bewaartermijnen de bronsystemen. Als in een bronsysteem de verwerkingen niet voorzien worden van een waardering en selectie ten behoeve van bewaren en vernietigen dan werkt dat door in iBase (garbage in, garbage out). [p8]
- Tijdelijke import/export bestanden moeten direct na gebruik vernietigd worden.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Bewaren en vernietigen	Zwaar (Z)	25%	NVT	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.

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.

iBase haalt voor "Informatiebeveiliging" het laagst mogelijke volwassenheidsniveau. Dat wordt veroorzaakt omdat er geen risicoanalyse is uitgevoerd.

Actiepunten:

- (Beleid) Voor een risicoanalyse uit voor de verwerkingen in iBase. [p9c1]
    - **(Wet art 4a lid 2) Stel de informatiebeveiligingseisen vast op basis van de resultaten uit de risicoanalyse. [p9c2]**
        - **(Wet art 4a lid 2) Beoordeel de impact van de informatiebeveiligingseisen ten behoeve van realisatie. [p9c3]**
        - (Beleid) Toets of alle informatiebeveiligingseisen gerealiseerd zijn door de standaard informatiebeveiligingsdiensten en borg zonodig alsnog de realisatie. [p9c5]
        - (Beleid) Onderzoek of er informatiebeveiligingseisen gerealiseerd zijn buiten de standaard informatiebeveiligingsdiensten en neem zo nodig maatregelen. [p9c6]
    - (Beleid) Zorg dat de restrisico's in de beveiliging beheerd worden. [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 privacyvriendelijke stand te zetten.

Er worden binnen iBase alleen gegevens verwerkt die voor het doel betreffend zijn. Daarnaast wordt er gebruik gemaakt van een opt-in regime. Hiermee voldoet iBase aan alle beleidscriteria. De wettelijke criteria zijn niet van toepassing.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Privacy by default	Zwaar (Z)	NVT	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 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.

iBase is geen registratief systeem. De data wordt geleverd vanuit de bronsystemen. In de bronsystemen worden de standaarden toegepast. Deze worden automatisch overgenomen in iBase. Hierdoor is het principe "Toepassen standaarden" niet van toepassing voor iBase.

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Licht (L)	NVT[6]	NVT	NVT

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

iBase voldoet aan alle criteria voor het principe "Verantwoordelijkheden belegd". Er is één aandachtspunt dat de menselijke factor betreft voor het mogelijk onrechtmatig verstrekken van gegevens.

Aandachtspunten:

- Met iBase kunnen gegevens geëxporteerd worden om in andere applicatie verder te verwerken. Het is ook mogelijk om de geëxporteerde gegevens te verstrekken. Dit laatste kan rechtmatig zijn. Maar er zijn geen (technische) beperkingen tegen een onrechtmatige verstrekking. Onderzoek of dit nog verbeterd kan worden. [p12]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[7]	100%	3

[6] Er zijn voor dit principe geen wettelijke criteria benoemd.
[7] 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' staan[8].

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.

[8] 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	5

Aandachtspunten
1: Volwassenheidsniveau 1:

Voor het vaststellen van dit niveau maakt het geen verschil of de voorziening of het principe geheel of deels aan een of alle min 1 wettelijke criteria voldoet.

2: Beleidscriteria:

Met uitzondering van niveau 3 geldt dat de mate waarin de voorziening voldoet aan de beleidscriteria, uitgedrukt in een percentage, niet van invloed is op de vaststelling van het volwassenheidsniveau. Het percentage beleidscriteria bij een principe is wel een indicatie of meer of minder inspanning moet worden geleverd om het principe compliant te krijgen aan het uitvoeringskader. Met name in combinatie met de percentages van de wettelijke criteria bij het volwassenheidsniveau 1 en in combinatie met de weegfactor geeft het inzicht bij het prioriteren van werkzaamheden om de voorziening compliant te maken.

3: Privacy functionaris:

De applicatie specifieke requirements mbt PSbD worden tijdens de ontwikkeling bepaald in samenwerking met de Privacy Functionaris en de business expert. Daarnaast is de privacy functionaris eerste aanspreekpunt mbt vragen over privacy.

Disclaimer

Aan de resultaten op basis van het gebruik van de 0-meting wordt geen enkele garantie met betrekking tot de mate van compliance van de getoetste voorziening gegeven. Tevens wordt geen enkele garantie gegeven inzake de juistheid of volledigheid van de checklist als gevolg van veranderende wet- of regelgeving.

Bijlage 1: Uitgangspunt bij compliance

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

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