POLITIE

0-meting Privacy & Security by Design

BOSZ

10.2.e

Definitief

Versie 1.00

Versie datum 16 april 2019

Rubricering **Politie Intern**

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	30-01-2018	Opzet template rapport
0.8	22-11-2018	Reviewen
0.9	19-12-2018	Aanpassingen verwerkt
0.92	12-04-2019	Reactie op toepassen standaarden verwerkt.
1.00	16-04-2019	Rapport definitief gemaakt na wederzijds akkoord

Review commentaar

Versie	Wanneer	Wie	Afdeling / Functie
0.8	22-11-2018	10.2.e	Gegevensautoriteit
0.9	19-12-2018	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 BOSZ 5

Algemeen 5

Doel 5

Doelgroep 5

Aanwezigen 0-meting 5

BOSZ 6

Soorten verwerkingen van politiegegevens 6

Verwerkingsgrondslag 7

Eindscore BOSZ 8

1.1 Eenmalige vastlegging 9

1.2 PDCA-cyclus 9

1.3 Doelbinding 9

1.4 Verantwoording 10

1.5 Autorisatie 10

1.6 Metagegevens 11

1.7 Kwaliteitszorg 11

1.8 Bewaren en vernietigen 12

1.9 Informatiebeveiliging 12

1.10 Privacy by default 13

1.11 Toepassen standaarden 13

1.12 Verantwoordelijkheden belegd 14

2. Verantwoording toetsing 15

Toetsingscriteria 15

Disclaimer 17

Bijlage 1: Uitgangspunt bij compliance 18

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 BOSZ. 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 BOSZ.
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 BOSZ

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 v2.0 wat in april 2018 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 BOSZ	10.2.e	Product Owner BOSZ
	10.2.e	Analist BOSZ
	10.2.e	Senior BE IM
	10.2.e	Product Owner BVH
	10.2.e	Product Owner Formulieren

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

Gespreksdatum	Nummer meting	Toelichting
10/07/2018	2018071001	De analyse is uitgevoerd op basis van de criteria afkomstig uit het uitvoeringskader **Privacy & Security by Design versie 2.0.**

BOSZ

Betere Opsporing door Sturing op Zaken (BOSZ) is een landelijk systeem voor de coördinatie van onderzoeken. Het is de applicatie voor sturing in opsporingsonderzoeken voor de politieagent en het Openbaar Ministerie (OM). Deze 0-meting betreft alleen het politie deel. Een politiemedewerker beoordeelt de onderzoeken en stuurt op een correcte en tijdige afhandeling. Zijn doel is effectieve en efficiënte inzet van mens en middel. Op deze wijze kunnen wij onze burgers de beste dienst verlenen.
BOSZ is een satelliet van BVH.

Soorten verwerkingen van politiegegevens

Soort verwerking	X	
Verzamelen	X	
Vastleggen	x	Vrije tekstvelden voor werksturing.
Ordenen	x	Proces indicator
Bewaren	x	
Bijwerken (het ontbrekende aanvullen / bestaande aanvullen)	x	Vrije tekstvelden voor werksturing.
Wijzigen (het bestaande aanpassen)	x	Vrije tekstvelden voor werksturing.
Opvragen	x	
Raadplegen	x	
Gebruiken	x	
Vergelijken		
Verstrekken doormiddel van doorzending of enige vorm van terbeschikkingstelling (exporteren)	x	Onderzoeksdossier met persoonsgegevens wordt beschikbaar gesteld voor het OM.
Samenbrengen	x	Gecombineerd inzenden van dossiers naar het OM.
Met elkaar in verband brengen		
Afscherming	x	
Uitwissen (weghalen/verwijderen zonder vernietigen)	x	Volgt BVH
Vernietigen	x	Volgt BVH bij handmatige vernietiging door functioneel beheer.

Verwerkingsgrondslag

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

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

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

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

Artikel 12 (lid 1) Wpg: verwerking met het oog op de controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens.

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

Eindscore BOSZ

De interviews voor de 0-metingen van BVH en BOSZ zijn op verzoek van de product owner gecombineerd en uiteindelijk in minder dan de helft van het normale tijdsbestek afgenomen. Dit heeft geleid tot een 0-meting met een beperkte diepgang en het risico dat details met betrekking tot privacy en security niet behandeld zijn.

BOSZ scoort een volwassenheidsniveau 1. Dit houdt in dat BOSZ onvoldoende compliant is op het gebied van Privacy & Security by Design (PSbD). Er is wel specifiek aandacht op het gebied van PSbD, maar die is vooralsnog niet toereikend om te voldoen aan de wet (Wpg) en op basis van het politiebeleid. Op de wetscriteria heeft BOSZ een score van 94% en op de criteria van het politiebeleid een score van 70%. Dat geeft aan dat er nog wel wat verbeteringen nodig zijn. Ons advies is om eerst te kijken naar de wetscriteria bij het principe 'autorisatie'. Hieronder staan de wetcriteria waarbij ons advies is hier direct wat aan te gaan doen. Er is maar één actiepunt wat opgelost moet worden om tot volwassenheidsniveau 2 te komen.

Actiepunten:

- **(Wet art 4a) Zorg dat de toegang- en gebruiksrechten van politiemedewerkers regelmatig worden gecontroleerd. [p5c8]**

Aandachtspunten:

- De verwerkingsgrondslag van een registratie kan in BOSZ worden geregistreerd. Maar daar wordt nog geen gebruik van gemaakt. Dit betreft dan alleen de misdrijven. Overtredingen worden niet in BOSZ geregistreerd. In de 0-meting van BVH is een actiepunt opgenomen voor criterium 5 van principe 3 om te onderzoeken in hoeverre BOSZ gebruikt kan worden voor het registreren van de verwerkingsgrondslag.
- Toets of de BRL-scan nog steeds voldoet aan alle aspecten van de Wpg en PSbD. [p9]

Eindscore	Datum toetsing	0-meting versie	Wet	Beleid	Volwassenheid
BOSZ	10/07/2018	2018071001	94%	70%	1

Tabel 1: Resultaat TOETSING 1 PSbD

PRINCIPE	WEEGFACTOR		PERCENTAGE W(et)	PERCENTAGE B(beleid)	VOLWASSENHEID
Eenmalige vastlegging	Z	-	NVT	100%	3
PDCA-cyclus	M	-	NVT	88%	2
Doelbinding	Z	-	NVT	100%	3
Verantwoording	Z	-	100%	0%	2
Autorisatie	Z	-	75%	50%	1
Metagegevens	Z	-	NVT	75%	2
Kwaliteitszorg	Z	-	NVT	56%	2
Bewaren en vernietigen	Z	-	100%	NVT	3
Informatiebeveiliging	Z	-	100%	100%	3
Privacy by default	Z	-	100%	NVT	3
Toepassing standaarden	L	-	NVT	50%	2
Verantwoordelijkheden belegd	M	-	NVT	75%	2
TOTALEN TOETSING		-	94%	70%	



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. 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.

BOSZ haalt voor dit principe het hoogste volwassenheidsniveau. Het grootste deel van de gegevens is afkomstig uit BVH. Er worden in BOSZ maar een beperkt aantal gegevens wordt vastgelegd. En deze gegevens worden conform het principe van "eenmalige vastlegging" verwerkt.

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

BOSZ haalt voor dit principe volwassenheidsniveau 2. Om te komen tot het hoogste volwassenheidsniveau moet het beheer van processen en gegevens volledig opgenomen in de PDCA cyclus.

Actiepunten

- (Beleid) Zorg dat het beheer van processen volledig onderdeel uit gaat maken van de PDCA cyclus. Op dit moment is het beperkt tot IV gerelateerde issues. [p2c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
PDCA-cyclus	Middel (M)	NVT	88%	2

1.3 Doelbinding

"Persoonsgegevens worden alleen verwerkt als daar een gerechtvaardigd doel voor bestaat en ze worden niet verder verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel."

Voor elke verwerking is het van belang om te bepalen voor welk doel de gegevens worden verwerkt. Op basis van de doelbinding kan worden gerechtvaardigd waarom (politie)gegevens verwerkt mogen worden.

BOSZ haalt voor dit principe de hoogst mogelijke score. Dat komt omdat BOSZ een satelliet van BVH is. Er is echter wel een aandachtspunt.

Aandachtspunten:

- De verwerkingsgrondslag van een registratie kan in BOSZ worden geregistreerd. Maar daar wordt nog geen gebruikt van gemaakt. Dit betreft dan alleen de misdrijven. Overtredingen worden niet in BOSZ geregistreerd. In de 0-meting van BVH is een actiepunt opgenomen voor criterium 5 om te onderzoeken in hoeverre BOSZ gebruikt kan worden voor het registreren van de verwerkingsgrondslag.

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

BOSZ haalt voor dit principe volwassenheidsniveau 2. Om te komen tot het hoogste volwassenheidsniveau is er één actiepunt.

Actiepunten:

- (Beleid) Zorg dat de audittrail door niemand gewijzigd kan worden. Op dit moment zijn er ongeveer tien database administrators die de audittrail aan zouden kunnen passen. Met de komst van DevOps wordt dat aantal nog groter. [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.

BOSZ haalt voor dit principe volwassenheidsniveau 1. Dat is een dikke onvoldoende. Om te komen tot in niveau 2 moeten alleen de toegang- en gebruiksrechten regelmatig worden gecontroleerd. Voor het hoogste volwassenheidsniveau moeten de actiepunten vanuit beleid uitgevoerd worden.

Actiepunten:

- (Beleid) Onderzoek of voor autorisaties binnen BOSZ (de toegang tot BOSZ loopt via BVH) ook gebruikt gemaakt kan worden van IAM en borg zo nodig de implementatie.[p5c1]
- (Beleid) Onderzoek of de rol van autorisatiedesk toegevoegde waarde heeft voor autorisaties die via de ATL (Autorisatie Tool Leidinggevenden) worden aangevraagd en neem zo nodig maatregelen. [p5c4]
- (Beleid) Zorg dat BOSZ een rapportage krijgt waarmee het gebruik van autorisaties getoetst kan worden. [p5c7]
- **(Wet art 4a) Zorg dat de toegang- en gebruiksrechten van politiemedewerkers regelmatig worden gecontroleerd. [p5c8]**

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Autorisatie	Zwaar (Z)	75%	50%	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.

BOSZ haalt voor dit principe volwassenheidsniveau 2. Om te komen tot het hoogste volwassenheidsniveau moeten alleen de definities voor de bedrijfsbegrippen worden vastgesteld.

Actiepunten:

- (Beleid) Zorg dat de definities voor bedrijfsbegrippen conform de leidraad, en in overleg met de afdeling GGB (Gegevens Gebruik en Beheer), worden vastgesteld. Op onderdelen zijn de bedrijfsbegrippen nu al vastgesteld. Bijvoorbeeld voor de maatschappelijke klassen. [p6c1]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Metagegevens	Zwaar (Z)	NVT	75%	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 kwaliteitszorg zijn er alleen criteria vanuit beleid. BOSZ haalt voor dit principe volwassenheidsniveau 2. Om te komen tot het hoogste volwassenheidsniveau moeten onderstaande actiepunten uitgevoerd worden.

Actiepunten:

- (Beleid) Onderzoek welke requirements met betrekking tot de kwaliteit van gegevens opgenomen kunnen worden in BOSZ en borg de realisatie. [p7c1]
- (Beleid) Zorg dat de kwaliteitseisen, die nog niet zijn opgenomen in het beleidskader BOSZ, afgestemd worden met de beleidsverantwoordelijke. [p7c2]
- (Beleid) Zorg dat de kwaliteitseisen die op de backlog staan gerealiseerd worden. [p7c3]
- (Beleid) Onderzoek welke soorten afwijkingen in de gegevenskwaliteit nu niet handmatig aangepast kunnen worden en borg de realisatie. [p7c4]
- (Beleid) Onderzoek welke aanvullende bedrijfsregels geformuleerd kunnen worden om de kwaliteit van de gegevens te meten. [p7c5]
- (Beleid) Zorg dat de uitgevoerde kwaliteitscontroles (inclusief het resultaat) worden vastgelegd [p7c8]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Kwaliteitszorg	Zwaar (Z)	NVT[3]	56%	2

[3] Er zijn voor dit principe geen wettelijke criteria.

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.

BOSZ is een satelliet van BVH. Voor het bewaren en vernietigen van gegevens is BVH leidend. De meeste criteria zijn daarom als 'niet van toepassing' geregistreerd.

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

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 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 is achterhaald.

BVH/BOSZ is eind 2017 opnieuw getoetst volgens de BRL (Beoordelings RichtLijn). De BRL scan richt zich op het ontwikkelen, beheren en product management van informatiesystemen (inclusief Wpg). BVH/BOSZ zal eind 2018 weer getoetst worden volgens de BRL. De resultaten daar van komen op de backlog van BVH/BOSZ en worden daar beheerd. Daarmee voldoet BVH/BOSZ aan alle criteria voor informatiebeveiliging

Aandachtspunten:

- Toets of de BRL scan nog steeds voldoet aan alle aspecten van de Wpg en PSbD. [p9]

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

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.

BOSZ voldoet aan alle criteria voor het principe "Privacy by default". Dat komt voornamelijk omdat er maar een beperkt aantal gegevens wordt vastgelegd in BOSZ. Het grootste deel van de gegevens is afkomstig van BVH.

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

Voor dit principe zijn er alleen criteria vanuit beleid. BOSZ heeft daarvoor volwassenheidsniveau 0 gehaald. Dat wordt veroorzaakt omdat niet bekend is of er standaarden van toepassing zijn.

Actiepunten:

- (Beleid) Onderzoek of er voldoende gebruik gemaakt wordt van bestaande overheids- of ketenstandaarden die van toepassing zijn op BOSZ. Bijvoorbeeld NORA, ISO/NEN of het "Raamwerk en stappenplan gegevenskwaliteit Strafrechtsketen". Een eerste scan door de product owner leverde op dat hier deels aan voldaan wordt. [p11c1]
- (Beleid) Als er gebruik gemaakt wordt van standaarden voor gegevensverwerking toets dan of deze juist worden toegepast. Een eerste scan door de product owner leverde op dat hier deels aan voldaan wordt. [p11c2]
- (Beleid) Onderzoek of er afwijkingen zijn van geldende standaarden. Leg in dat geval gemotiveerd de motivatie vast en laat deze accepteren door de verantwoordelijke. Een eerste scan door de product owner leverde op dat er wellicht afwijking zijn. [p11c3]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Toepassen standaarden	Zwaar (Z)	NVT[4]	50%	2

[4] Er zijn voor dit principe geen wettelijke criteria.

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

Voor dit principe zijn er alleen criteria vanuit beleid. BOSZ heeft daarvoor volwassenheidsniveau 2 gehaald. Om te komen tot het hoogste volwassenheidsniveau zijn er actiepunten voor het vaststellen van beleid en voor het vastleggen van de verwerkingsgrondslag.

Actiepunten:

- (Beleid) Onderzoek of alle definities, beleid, koers en strategie voor de verwerking van gegevens zijn beschreven, bijvoorbeeld de soorten afhandelingen van een verdachte, en borg dat deze worden vastgesteld door de beleidsverantwoordelijke. [p12c2]
- (Beleid) Onderzoek of alle taken van de gegevensverwerkers om gegevens zorgvuldig en rechtmatig te verwerken door de voorziening ondersteunt worden.[p12c7]

Principe	Weegfactor	Wet	Beleid	Volwassenheid
Verantwoordelijkheden belegd	Zwaar (Z)	NVT[5]	75%	2

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

2. Verantwoording toetsing

Toetsingscriteria

De toetscriteria zijn afgeleid uit het document '2018-04-24_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[6].

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

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