POLITIE

Vooronderzoek PSbD compliancy

Privacy & Security by Design compliancy van highrisk applicaties

Wpg en IB verbeterprogramma

Versie 1.1

3-11-2017

« waakzaam en dienstbaar »

1 Documentinformatie

Brondocumentatie

#	Document	Versie	Datum	PTB
1	Programmaplan concept versie	0.1	20-09-2017	Ja/nee
2				Ja/nee
3				Ja/nee
4				Ja/nee

Afstemmatrix

#	Naam	Versie	Datum
1		0.1	17-09-2017
2		0.2	20-09-2017
3		0.3	27-09-2017
4		0.4	27-09-2017
5		1.0	26-10-2017
6		1.1	3-11-2017

2 Inhoudsopgave

3 Achtergrond en inleiding

Een externe audit in 2015 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 verbeterprogramma van 2015 zijn politieke toezeggingen gedaan aan de Tweede Kamer.

Het project 'Privacy & Security by Design (PSbD) compliancy van highrisk applicaties' is onderdeel van het verbeterprogramma Wpg en IB. 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 geeft in grote lijnen het totale traject weer dat nodig is om een tot een compliant applicatie te komen. Onder de verantwoording van het programma valt het vooronderzoek. Dit wordt voorgelegd aan de portefeuillehouders. Op initiatief van de portefeuillehouders volgt uitwerking en borging bij de dienst IM en ICT. Gezien de scope van het programma focust dit plan zich op het vooronderzoek.

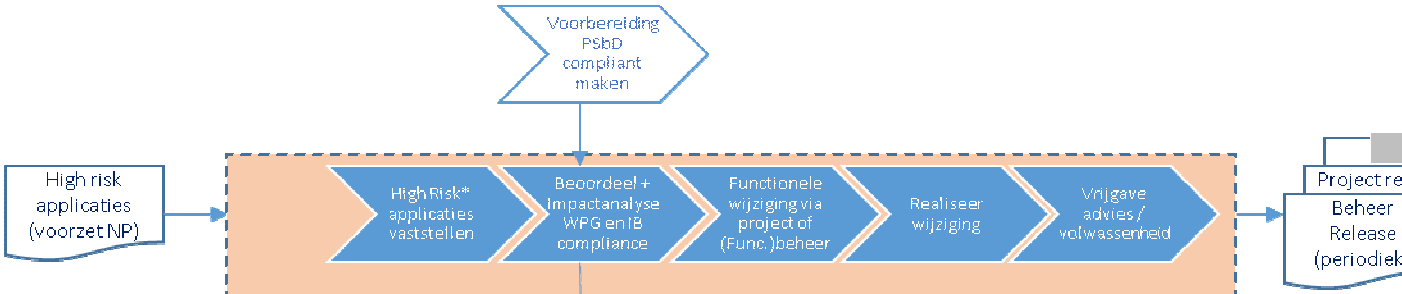
4 De opdracht

De opdracht is om met behulp van het PSbD uitvoeringskader de highrisk applicaties PSbD compliant te maken. De highrisk applicaties moeten per 25 mei 2018 Wpg en IB compliant dan wel met een toelichting en een plan (minimaal transparant zijn).

In 2018 worden de nieuwe privacy regelgevingen van kracht. Per 6 mei 2018 moet aan alle bepalingen van de (nieuwe) Wet politiegegevens (Wpg) worden voldaan. De Algemene Verordening Gegevensbescherming (AVG) vervangt de huidige Wet bescherming persoonsgegevens (Wbp) en is per 25 mei 2018 van kracht.

Het is niet haalbaar om alle applicaties binnen de informatievoorziening per mei 2018 compliant te maken volgens het PSbD uitvoeringskader. Om te kunnen voldoen aan de nieuwe privacy regelgevingen is er een selectie gemaakt van de potentieel highrisk applicaties op het gebied van privacy naast BVH, SUMMIT en [redacted] De grootste politie applicaties (BVH en SUMMIT) gaan via [redacted] vervangen worden waarbij bij de ontwikkel al rekening zal worden gehouden met PSbD. De te doorlopen stappen staan in het onderstaande schema.

1. Highrisk applicaties vaststellen (verbeterprograma Wpg en IB, samen met senior coördinerend business expert)
2. Beoordeel + impactanalyse (senior coördinerend business expert /functioneel beheer)
3. Functionele wijziging via project of (Func.) beheer (senior coördinerend business expert / functioneel beheer)
4. Realiseer wijziging (senior coördinerend business expert / functioneel beheer)
5. Vrijgave advies/volwassenheid (IM)



5 Aanpak en uitvoering

5.1 Doelgroepen

Het vooronderzoek is in de eerste plaats bedoeld voor de direct betrokkenen bij het PSbD compliant maken van de 'highrisk applicaties'.:

- Portefeuillehouders
- Portefeuilleteam
- Privacy functionaris
-
- Functioneel beheer

Ook die niet betrokken zijn bij 'highrisk applicaties' vormen een belangrijke doelgroep. Uiteindelijk zullen de normale applicaties (via werkproces) ook PSbD compliant moeten zijn. De die niet betrokken zijn bij 'highrisk applicaties' zullen een presentatie krijgen over PSbD en op welke manier het uitvoeringskader toegepast kan worden. Daarnaast is het vooronderzoek bedoeld voor andere geïnteresseerden (dIMers en dICTers) die de stappen willen weten welke er moeten worden doorlopen om een applicatie PSbD compliant te krijgen.

Overzicht van de doelgroepen per eenheid staat in bijlage 2.

Fout! Ongeldige koppeling.

5.2 Planning

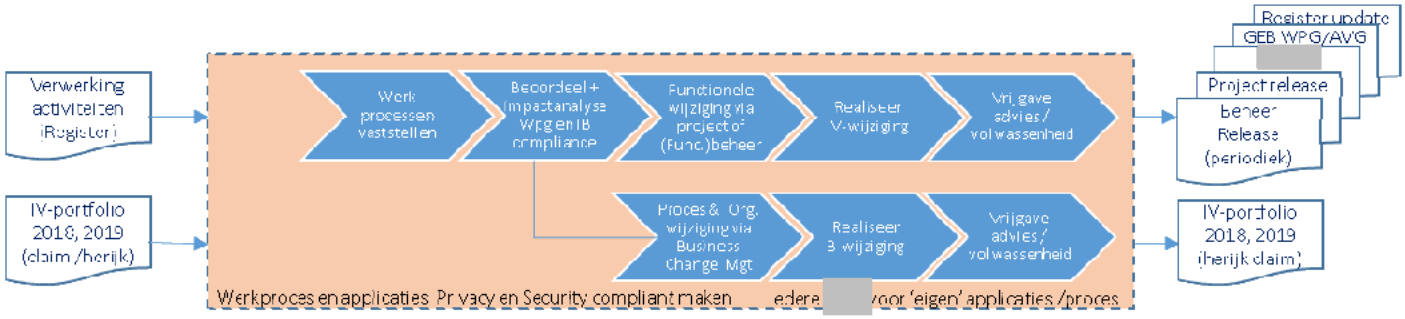
In de planning staat beschreven welke opdrachten er uitgevoerd moeten worden om highrisk applicaties compliant te maken. Waarbij de eerste twee opdrachten (Highrisk applicaties vaststellen en voorbereiding PSbD compliant) in één keer uitgevoerd worden. De andere opdrachten worden uitgevoerd naar het aantal Highrisk applicaties. In bijlage 2 staat een uitleg van de resultaten die bij de planning staan.

Nummer	Opdracht	Resultaten	Actiehouder	Einddatum	Status
1	Highrisk applicaties vaststellen	• Lijst highrisk applicaties creëren en vaststellen	GA	Juli 2017	Klaar
		• [redacted] kunnen de lijst met goede onderbouwing nog uitbreiden.	[redacted]	November 2017	
2	Voorbereiding PSbD compliant maken	• Criteria PSbD vaststellen	GA/ Inrichtingsgroep [redacted]	September 2017	Klaar
		• Brief sturen portefeuillehouders	GA	September/ oktober 2017	
		• Opname in architectuurkader productiehuis (Emergent design)	GA [redacted]	Oktober 2017	
		• Bezoek cSBE per portefeuillehouder o PSbD uitleggen doormiddel van een presentatie.	GA	November 2017	
		• Inregelen toets op PSbD	Initieel GA Structuree[redacted] PSbD	Januari 2018	
		• [redacted] geschikt maken voor registratie volwassenheid PSbD	GA	December 2017	
		• Competentie afspraken maken binnen Dienst IM en Dienst ICT	Bedrijfsplan IM en ICT	November 2017 – Januari 2018	
		• Opleiding	Bedrijfsplan IM en ICT	Februari 2018	
3	Beoordeel impactanalyse PSbD	• 0-meting applicaties op basis van PSbD criteria gereed	[redacted]/GA	Januari 2018	
		• Impactanalyse van de noodzakelijke wijzigingen gereed	[redacted]/FB	Mei 2018	
4	Functionele wijziging via project of (funct.) beheer	• PSbD compliancy van bestaande applicaties via beheer gereed	[redacted]/FB	Mei 2018	
		• PSbD compliancy van lopende en nieuwe projecten via het project gereed	[redacted]/FB	Mei 2018	
5	Realiseer wijziging	• Realiseren van wijzigingen tbv PSbD compliance	[redacted]/FB	Eind 2018 (highrisk appl.)	
6	Vrijgave advies/volwassenheid	• Volwassenheid opnieuw toetsen	[redacted] PSbD	nntb	
		• Volwassenheid bijwerken in [redacted]	[redacted] PSbD	2018	
		• Volwassenheid als indicator op het [redacted]	GA [redacted]	Nntb	
		• Volwassenheid visueel weergeven bij de servicelijn van het [redacted]	[redacted] PSbD/ [redacted]	Mei 2018	

6 Buiten Scope

Buiten scope valt het compliant maken van de 'normal' risk applicaties (via werkprocessen). Hieronder staat een schema hoe dat proces moet verlopen.

PSbD compliant maken van normal risk applicaties



Nr.	Buiten scope	Actiehouder	Actie / afspraak
B1	PSbD compliant maken van normal risk applicaties	dIM en diCT	Eerst highrisk applicaties en daarna Normal(/Low/No Risk) applicaties. Het doel is om deze applicaties uiterlijk 2020 compliant gemaakt te hebben.
B2		Politiechefs	Politiechefs krijgen het verzoek om compliant te maken.
B3	AVG		Compliancy-plan is afgesproken op het MT PDC
B4	Impactanalyse PSbD	Sr. Coördinerend Business expert	Is onderdeel van het IV-portfolio (10% claim)
B5	Opdracht voor functionele wijzigingen	Sr. Coördinerend Business expert	Is onderdeel van het IV-portfolio (10% claim)
B6	Realiseren van functionele wijzigingen	Sr. Coördinerend Business expert	Is onderdeel van het IV-portfolio (10% claim)
B7	Bedrijfsplan (opleiding)	Steller Bedrijfsplan IM ( ) en ICT)	Opleiden van 150 IMers en 450 ICTers
B8		Steller Bedrijfsplan IM ( ) en ICT ( )	Inrichten en in beheer nemen van het
B9	Uitvoeringskader PSbD	Gegevensautoriteit	Het beheer van het uitvoeringskader

7 Afhankelijkheden en Randvoorwaarden

In de tabel hieronder staan de afhankelijkheden en randvoorwaarden beschreven die minimaal nodig zijn om een applicatie compliant te maken.

Nr.	Randvoorwaarde / Afhankelijkheid	Op welke manier?
R1	Medewerking van	Het overbrengen van PSbD
R2	Toekennen van 20% niet gealloceerde ruimte in het portfolio	Geen ruimte toegekend voor het compliant maken
R3	Medewerking ontwikkelteam	Naleven criteria
R4	Medewerking managementlijn	Belang van PSbD op de juiste waarde inzien.
R5	Kennis voor uitvoering	Er moet voldoende kennis overgebracht worden tijdens de opleiding om applicaties te laten voldoen aan de PSbD
R6	Vastgestelde criterialijst PSbD	Goedgekeurd door inrichtingsgroep en redactie uitvoeringskader PSbD
R7	Opdrachtverstrekking van	Tijd en geld in IV-portfolio Verslaglegging besluitvorming over het al dan niet wijzigen in de notulen van het portefeuilleteamoverleg (comply or explain)
R8	Volwassenheidsscore	De volwassenheidscore wordt gebaseerd op het formeel vastgestelde uitvoeringskader PSbD.

Bijlage 1: Doelgroepen

Rol	Naam	Applicatie
		AVR

Rol	Naam	Applicatie

Rol	Naam	Applicatie
		FCM
		HAVANK
		LSV
		PSH-VM
		TRIS

Rol	Naam	Applicatie
		Live Journaal Politie

Rol	Naam	Applicatie
		BVID 2.0
		PSH-V
		Verificatiemodule
		ZUIS

Rol	Naam	Applicatie
		BVI – IB
		BVI – BlueSpot
		BVI – Blueview 4.0

Rol	Naam	Applicatie
		PSH-TM
		VROS
		Amazone

Rol	Naam	Applicatie

Rol	Naam	Applicatie
		BVH-BOSZ

Rol	Naam	Applicatie
		Internetaangifte
		Servicemodule
		MEOS-TM (bestaat uit meerdere applicaties)

Rol	Naam	Applicatie
[redacted]	[redacted]	[redacted]
		SBV
		[redacted]
		SMC
		ANPR
		DCS
		Orion+
		[redacted]

Rol	Naam	Applicatie
[redacted]	[redacted]	

Rol	Naam	Applicatie
[redacted]	[redacted]	[redacted]
		Agora
		KA / schijven en mappen

Bijlage 2: Toelichting op de planning

Op de planning staan de resultaten benoemd die binnen afzienbare tijd behaald moeten worden. In deze bijlage staat de resultaatomschrijving gedetailleerder beschreven. Daarnaast is het duidelijker wat de inhoud is van de resultaten die bereikt moeten worden m.b.t. PSbD compliancy.

1. Highrisk applicaties vaststellen

Als eerste dient er worden vastgesteld welke applicaties onder de highrisk applicaties vallen. Het gaat hierbij om applicaties die een potentieel hoge privacy risico hebben en daarnaast veel gebruikt worden door het uitvoerende deel van de politie. BVH en SUMMIT zijn buiten deze selectie gelaten vandaar de term 'Highrisk applicaties'. De basislijst is gecreëerd op basis van parate kennis en de weging op het gebeid van de criteria zoals deze hieronder beschreven staan[1].

criteria	*waarde*	
Labeling	er wordt al gelabeld	0
	weinig risico/afleidbaar	1
	risicovol	2
Verwijderen&vernietigen	volgens wetgeving	0
	er zijn enkele maatregelen	1
	risicovol	2
Logging	hoeft niets mee	0
	behoeft aandacht	1
	risicovol	2
Autoriseren	risico zeer beperkt	0
	weinig risico	1
	risicovol	2
Verstrekken	handmatig	0
	geautomatiseerd kleine aantallen	1
	geautomatiseerd grote aantallen	2
Risico-opslag	los van overige criteria	0
	een kwalitatief oordeel	1
	van de groep	2
Aantal users	veel: 10.000-50.000 users	4
	weinig: 1000- 10.000 users	2
	Zeer weinig < 1000 users	1
Lifecycle	uitfasering in 2017	disqualified
	vervangen voor 2019	1
	vervanging binnen 6 jaar	2
	toekomstvast /	3

Vervolgens kunnen de van de diverse portefeuilleteams nog aangeven (met onderbouwing) of er nog applicaties ontbreken aan de lijst 'Highrisk applicaties'. Op basis van deze gesprekken wordt de lijst definitief vastgesteld. De lijst van highrisk applicaties bestaat op dit moment uit 35 applicaties (zie de lijst in de paragraaf hieronder)

- Highrisk applicaties creëren en vaststellen
- kunnen de lijst met een goede onderbouwing nog uitbreiden.

[1] Memo Wpg en IB risicoanalyse applicaties

ications (voorlopig)

Applicatie	Toelichting
AVR	Verhoorregistratie
Livejournaal politie	ntern bulletin board tbv SGBO/DGBO
Servicemodule	
IA	Internet Aangifte
FCM	Foto Confrontatie Module
HAVANK	Het Automatisch Vingerafdrukkensysteem Nederlandse Kollectie
LSV	Landelijk Sporen Volgen
TRIS	Technische Recherche Informatie Systeem
BVID	Basisvoorziening Identiteitsmanagement
Agora	In beschreven als
BVI-IB	Integrale Bevraging
BVI-Blueview 4.0	
BVI-BlueSpotMonitor	
SBV	Sirene Berichten Verkeer
SMC	
MEOS	
PSH-TM	Politie Suite Handhaving – Transactie Module
PSH-VM	Artikel 13 Wpg, vergunningen
Orion	
DCS	Digitale Communicatie Sporen (DCS).
ANPR	Nummerplaatherkenning
VROS	
BOSZ	BOSZ en BOSZ
Amazone	Doelgroepen
Verificatiemodule	
ZUIS	Zeescheepvaart Uitbreidbaar Integraal Systeem
PSH-V	Vreemdelingen-module
KA / schijven en mappen	staat niet in

2. Voorbereiding PSbD compliant maken

Om bij de highrisk applicaties PSbD compliancy vast te stellen moeten er een aantal voorbereidingen worden getroffen. De voorbereiding is erop gericht dat alles klaar staat om meerdere applicaties parallel aan elkaar compliant te kunnen maken op basis van de richtlijnen uit het uitvoeringskaders PSbD.

2.1 Criteria Privacy & Security by Design vaststellen

Vanuit de dienst IM (is er een PSbD criterialijst opgesteld op basis van het uitvoeringskader PSbD in samenwerking met de inrichtingsgroep van en de redactie van het uitvoeringskader. De lijst bestaat uit dertien principes met voor elke principe zijn eigen criteria (zie onderstaande afbeelding). Daarnaast is er onderscheid gemaakt of er in het principe criteria zitten waaraan moet worden voldaan volgens de wet (W) of het beleid (B). De criteria bepalen of een applicatie voldoet aan een principe. Indien er een criteria is wat niet voldoet aan de wet is het niet mogelijk om voldoende te scoren op de betreffende principe. Op basis van de score per per principe kan er een algehele volwassenheid (zie paragraaf 2.7) aangegeven worden.

	OVERZICHT PER PRINCIPE						TOETSING 1																					
							RESULTAAT TOETSING												BEREKENING MINUS CRITERIA BS en NVT										
		HERKOMST CRITERIA						J		N		D		BS		NVT		CRITERIA tbv BEREKENING			TE BEHALEN PUNTEN		TOTAAL	PUNTEN BEHAALD		TOTAAL	PROCENT		TOTAAL	MINIMALE SCORE
PRINCIPES	AANTAL	W	B	WEGING	FACTOR	MAX PUNTEN	AANTAL	W	B	W	B	W	B	W	B	W	B	W	B	AANTAL	W	B		W	B		W	B		
Eenmalige vastlegging	**9**	1	8	Z	5	45	9	0	2	0	1	0	0	1	5	0	0	0	3	**3**	0	15	**15**	0	10	**10**	0%	67%	**67%**	NEE
PDCA-cyclus	**4**	1	3	M	3	12	4	0	1	0	1	1	0	0	1	0	0	1	2	**3**	3	6	**9**	1	3	**4**	33%	50%	**44%**	NEE
Doelbinding	**10**	7	3	Z	5	50	10	0	0	7	3	0	0	0	0	0	0	7	3	**10**	35	15	**50**	0	0	**0**	0%	0%	**0%**	NEE
Verantwoording	**4**	1	3	Z	5	20	4	1	3	0	0	0	0	0	0	0	0	1	3	**4**	5	15	**20**	5	15	**20**	100%	100%	**100%**	JA
Autorisatie	**6**	1	5	Z	5	30	0																							
Metagegevens	**7**	3	4	Z	5	35	0																							
Kwaliteitszorg	**7**	0	7	Z	5	35	0																							
Bewaren en vernietigen	**6**	1	5	Z	5	30	0																							
Informatiebeveiliging	**10**	5	5	Z	5	50	0																							
Voldoen aan de wet	**4**	1	3	Z	5	20	0																							
Toepassing standaarden	**1**	0	1	L	1	1	0																							
Verantwoordelijkheden belegd	**7**	0	7	M	3	21	0																							
Privacy by default	**0**	0	0	M	3	0	0																							
																				TOTAALSCORE	43	51	**94**	6	28	**34**	14%	55%	**36%**	

De criteria worden elk half jaar bijgewerkt naar aanpassing vanuit wet en/of regelgeving, maar ook op basis van aanpassingen in het uitvoeringskader PSbD.

2.2 Brief sturen naar portefeuillehouders

De Gegevens Autoriteit (GA) stuurt een brief naar de portefeuillehouders met daarin het verzoek om aandacht te geven aan het PSbD compliant maken van de applicaties. In deze brief geeft de GA aan dat de portefeuillehouders verantwoordelijk zijn voor het PSbD compliant maken van de applicaties. Dit is van toepassing op de bestaande en nieuwe applicaties binnen de portefeuille.

2.3 Opname in architectuurkader

De omschrijving van PSbD en de PSbD-criteria zijn onderdeel van het architectuurkader De PSbD-criteria worden, net als de gecontroleerd bij de start van een nieuw project. Op deze manier wordt er gewaarborgd dat bij elk nieuw project er rekening gehouden wordt met PSbD.

2.4 Bezoek per portefeuillehouder

Om een applicatie PSbD compliant te maken behoort de te weten hoe PSbD werkt. De GA geeft uitleg met een presentatie met daarin ook aandacht voor de PSbD criterialijst. Daarnaast hebben de de mogelijkheid om de highrisk applicaties te kunnen vaststellen.

- Presentatie + uitleggen PSbD criterialijst
- Vaststellen highrisk applicaties

2.5 Competentie afspraken maken

Er komen competentie afspraken gericht op Privacy en Security by Design. Waarbij de doelstelling van de competentie afspraken is om:

- kennis ontwikkelen, borgen en uitdragen doormiddel van 2de lijns ondersteuning (vraagbraak voor)
- opstellen en beheren richtlijnen per doelgroep en rapporteren volwassenheid (in normkader).
- Verlenen ondersteuning aan dIM en dICT-medewerkers op het gebied van PSbD.

De competentie afspraken die gemaakt worden hebben een link met het beheer van het PSdB uitvoeringskader en met de privacyfunctionaris van de Wpg en AVG. De competentie afspraken zijn onderdeel van de bedrijfsplannen dienst IM (dIM) en dienst ICT (dICT).

2.6 Inregelen toets op PSbD

Er moeten afspraken gemaakt worden om het toetsen van de PSbD op een regelmatige basis op te nemen in het beheerproces. Hierbij gaan we uit van een 0-meting en van een nieuwe meting nadat de wijzigingen zijn toegepast. Er moet nog vastgesteld worden wie en op welke manier de toetsing uitvoert. Deze afspraken worden gemaakt in overleg met het dienst IM en dienst ICT.

- Toetsen standaard onderdeel van het proces
- Afspraken 0-meting PSbD in overleg met dienst IM en dienst ICT
- Afspraken opnieuw toetsen PSbD in overleg met dienst IM en dienst ICT

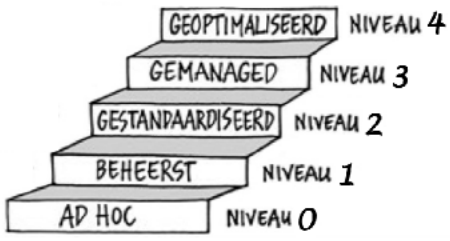
2.7 geschikt maken voor registratie volwassenheid PSbD

In is er een mogelijkheid om de mate van volwassenheid voor PSbD in te vullen in een specifieke kolom. In de voorbereiding maken we afspraken over de weergave van volwassenheid van PSbD, en bespreken we bij wie het beheer van de PSbD volwassenheid in geborgd wordt.

- Weergave volwassenheid PSbD in
- Beheer volwassenheid PSbD in bepalen

Niveau	Betekenis	Toelichting
Niveau 0 = Ad-hoc	Geen plan	Er is geen plan aanwezig. Er is geen specifieke aandacht voor PSbD.
Niveau 1 = Beheerst	Plan (niet toereikend voor de wet)	Er is wel een plan op het gebied van PSbD, maar die is niet toereikend om te voldoen aan de wet (Wpg).
Niveau 2 = Gestandaardiseerd	Wet	Er is een plan op het gebied van PSbD en is afdoende om te voldoen aan de wet (Wpg), maar niet toereikend voor het beleid
Niveau 3 = Gemanaged	Wet + Beleid	Het plan op het gebied van PSbD voldoet aan de wet en beleid
Niveau 4 = Geoptimaliseerd	Wet + Beleid + Laatste ontwikkelingen	Het plan op het gebied van PSbD voldoet aan de wet, beleid en de laatste ontwikkelingen

Het volwassenheidsmodel



2.8 Opleiding

Om alle dIMers en dICTers de benodigde kennis bij te brengen over PSbD krijgen zij een training. Afspraken over de compententies komen in het bedrijfsplan 2018 van zowel dienst IM als van dienst ICT.

- Opleiding voor dIMers en dICTers
    - Privacy en Security by Design (presentatie)
    - Specifieke PSbD opleidingen (per vakgroep)
    - Aanname 150 dIMer en 450 dICTers op te leiden en zal worden gedaan via het bedrijfsplan van IM en ICT

3. Beoordeel + impact analyse PSbD

De beoordeling van Wpg en IB compliance gebeurt op basis PSbD criteria. Initieel wordt er een 0-meting gedaan om te bepalen wat de huidige status is van de applicaties op het gebied van PSbD. Vervolgens kan er een impact analyse gemaakt worden met aanpassingen. Het opstellen van een Gegevenseffectenbeoordeling (GEB) Wpg is nodig per verwerkingsactiviteit. Het opstellen en aanpassen van een GEB Wpg wordt beschouwd als een functionele wijziging. De procesbeheerder voert deze uit.

- 0-meting applicaties op basis van PSbD criteria
- Impactanalyse van de noodzakelijke wijzigingen
- Opstellen van een GEB Wpg

4. Functionele wijziging via project of beheer

De 10% claim voor het compliant maken zit in de impactanalyse (7.3 daar waar nodig) en de functionele wijzigingen (7.4 daar waar nodig). Opdracht voor functionele wijzigingen is verstrekt:

- Als functionele wijziging via het beheerproces.
- Als (onderdeel van) projectopdracht.
- Op de backlog (in geval applicatie onder regime van [redacted] valt)

Besluiten over het al dan niet verstrekken van de opdracht tot wijzigen moeten terug te vinden zijn in de notulen van het portefeuilleteamoverleg (comply or explain).

5. Realiseer wijziging

In deze fase worden de wijzigingen ten behoeve van PSbD compliancy en/of GEB Wpg gerealiseerd en gecontroleerd op werking functionaliteit.

- Realiseren van wijzigingen tbv PSbD compliancy
- Realiseren van wijzigingen tbv GEB Wpg

6. Vrijgave advies/volwassenheid

Na de wijzigingen wordt opnieuw de volwassenheid vastgesteld op basis van de criteria. Het resultaat wordt verwerkt in [redacted] Vervolgens kan de Wpg en IB compliance als indicator op [redacted] komen.

- Volwassenheid opnieuw toetsen
- Volwassenheid verwerken/bijwerken in [redacted]
- Volwassenheid als indicator op het [redacted]

Bijlage 3: Afkortingen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BVH	Basisvoorziening Handhaving
[redacted]	[redacted]
[redacted]	[redacted]
dICT	Dienst ICT
dIM	Dienst Informatiemanagement
[redacted]	[redacted]
GEB	Gegevenseffectenbeoordeling
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
PSbD	Privacy & Security en Design
Wpg	Wet politiegegevens
IB	Informatiebeveiliging