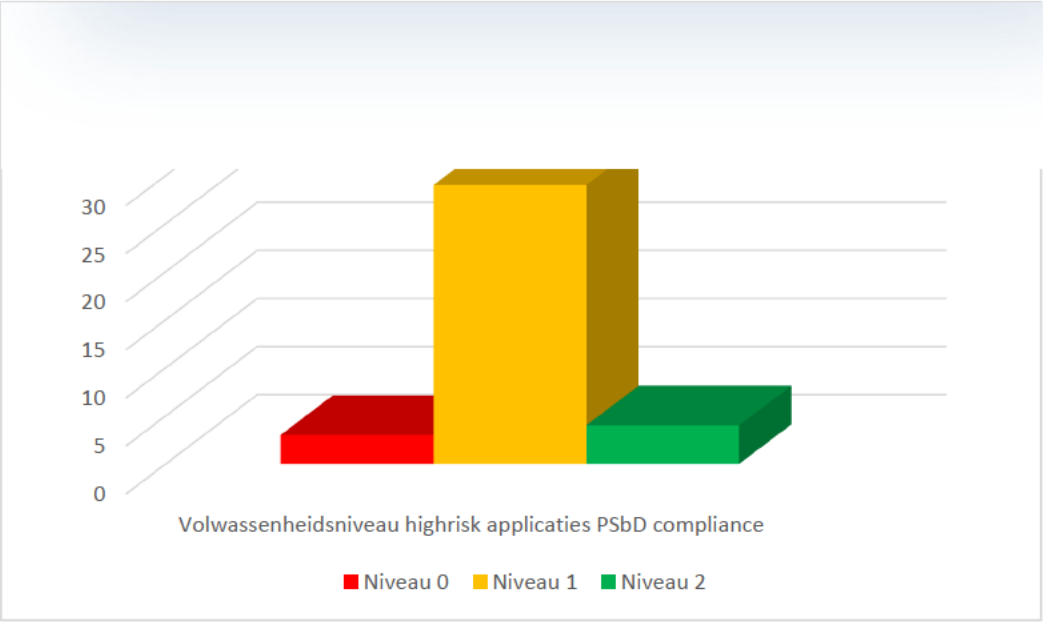
# Eindrapport
# 0-metingen PSbD




**Het proces en het resultaat**

Definitief

Versie 1.00

Versie datum 14 mei 2019

Rubricering: Intern

« waakzaam en dienstbaar »

# Documentinformatie

**Versiegeschiedenis**

| Versie | Versie datum | Samenvatting van de aanpassing |
|---|---|---|
| 0.1 | 09-01-2019 | Opzet algemeen rapport (indeling) |
| 0.2 | 30-01-2019 | Invulling aan de titels |
| 0.3 | 12-02-2019 | Vullen van proces |
| 0.4 | 22-02-2019 | Vullen van resultaten |
| 0.5 | 01-03-2019 | Vullen van de hoofdstukken conclusie, vervolgstappen en reflectie |
| 0.6 | 08-03-2019 | Eerste aanpassingen aan de van review |
| 0.7 | 15-03-2019 | Managementsamenvatting |
| 0.8 | 03-04-2019 | Bijlagen toevoegen |
| 0.9 | 17-04-2019 | Bijlage resultaten toegevoegd. |
| 0.91 | 01-05-2019 | Review wijzigingen doorgevoerd |
| 0.92 | 07-05-2019 | Review wijzigingen doorgevoerd |
| 0.93 | 10-05-2019 | Review wijzigingen doorgevoerd |
| 1.00 | 14-05-2019 | Opmaak aangepast en rapport definitief gemaakt |

**Review commentaar**

| Versie | Wanneer | Wie | Afdeling |
|---|---|---|---|
| 0.5 | 07-03-2019 | | Gegevensautoriteit |
| 0.91 | 29-04-2019 | | Gegevensautoriteit |
| 0.92 | 07-03-2019 | | Gegevensautoriteit |
| 0.93 | 10-05-2019 | | Gegevensautoriteit |
| 0.93 | 10-05-2019 | | Gegevensautoriteit |

# Inhoudsopgave

# Managementsamenvatting

De Auditdienst Rijk (ADR) heeft gerapporteerd (2015) dat er op het gebied van Privacy & Security verbeteringen nodig zijn in de informatievoorzieningen. Het verbeterprogramma Wpg en IB is gestart om te kijken hoe de Privacy & Security compliance het beste gerealiseerd kon worden. Hiervoor is gebruik gemaakt van een 0-meting om vanaf de start een beeld te kunnen krijgen van de volwassenheid van de informatievoorzieningen van politie op het gebied van Privacy & Security by Design (PSbD). Er is hierbij een keuze gemaakt uit twee methodes voor het uitvoeren van de 0-metingen. Een selectie maken van highrisk applicaties (snelle methode) of het selecteren op basis van verwerkingen (normal risk) die over applicaties heen gaan (juiste methode, maar complex). Er is gekozen voor de highrisk methode, waarbij highrisk o.a. staat voor de soort en de hoeveelheid informatie die via de applicatie loopt en niet de staat waarin de applicatie zich verkeert. Het voordeel van highrisk methode is dat er relatief snel resultaat behaald kan worden en er verantwoordelijken gericht aangesproken kunnen worden. De opzet van de 0-meting is gehaald uit de 12 principes van het uitvoeringskader PSbD, waarbij de wet (Wpg) en het politiebeleid centraal staan.

***Onderzoeksvraag: In hoeverre zijn de vastgestelde highrisk applicaties van de politie PSbD compliant?***

**Proces**

Er is veel aandacht gestopt in het proces om ervoor te zorgen dat er bij de 0-metingen betrokkenheid en transparantie is. De start van de 0-metingen is begonnen met het vooronderzoek (1) wat is vastgesteld door de stuurgroep Wpg & IB. Aan de portefeuillehouders van de highrisk applicaties is d.m.v. een eerste brief (2) aandacht gevraagd voor het uitvoeringskader PSbD en het toepassen daarvan. Na het sturen van de eerste brief zijn er presentaties (3) gegeven bij de portefeuilleteams van de verschillende eenheden. Naast de uitleg over PSbD is er per portefeuilleteam gevraagd of de applicaties die van tevoren geselecteerd waren overeenkwamen met de applicaties die zij zelf zien als potentiele highrisk applicaties binnen hun portefeuille. In een de tweede brief (4) aan de portefeuillehouders is opnieuw gevraagd om medewerking en om de highrisk applicaties die binnen de portefeuilleteams besproken zijn vast te stellen. Nadat de highriskapplicaties waren vastgesteld zijn de 0-meting sessies ingepland (5), waarbij in een sessie van 6-8 uur 90 criteria (verdeeld over twaalf principes) gebaseerd op het uitvoeringskader PSbD behandeld zijn.

***Uitvoeringskader PSbD v2.0***

1. Eenmalige vastlegging
2. PDCA- cyclus
3. Doelbinding
4. Verantwoording
5. Autorisatie
6. Metagegevens
7. Kwaliteitszorg
8. Bewaren en vernietigen
9. Informatiebeveiliging
10. Privacy by default
11. Toepassen standaarden
12. Verantwoordelijkheden belegd


De criteria bestaan uit gesloten vragen die met Ja/Nee/Deels/NVT beantwoord konden worden. Indien een criteria werd beantwoord met Nee of Deels was dit de basis voor een actiepunt in het rapport. Het rapport is zowel het verslag van de gegeven antwoorden tijdens de 0-meting als het advies gebaseerd op die antwoorden. Vervolgens is het rapport als concept naar de betrokkenen verstuurd (6), zodat deze de inhoud konden controleren/aanpassen. Bij de betrokkenen van de 0-meting is gevraagd om een schriftelijk akkoord te geven, zodat er wederzijds overeenstemming is over de inhoud (actiepunten) van het rapport waaraan voldaan moet worden. Als de betrokkenen een schriftelijk akkoord hebben gegeven, dan is het rapport definitief en kan het verstuurd worden naar de portefeuillehouders (7). Aan het eind van het jaar gaat er een evaluatie plaatsvinden (8) over de status van de actiepunten met de betrokkenen van de 0-meting.

| Proces | |
|---|---|
| 1. | Vooronderzoek |
| 2. | Brief 1: Uitleg Privacy & Security by Design (PSbD) compliance (november 2017) |
| 3. | Presentaties aan o.a. de portefeuilleteams met het verzoek de applicaties te bevestigen |
| 4. | Brief 2: Vaststellen van de highriskapplicaties (april 2018) |
| 5. | Uitvoeren van de 0-metingen PSbD |
| 6. | Concept rapport versturen naar betrokkenen |
| 7. | Brief 3: Definitief rapport versturen naar portefeuillehouders na wederzijds akkoord betrokkenen |
| 8. | Evaluatie actiepunten (eind 2019) |

### Conclusies

Op dit moment **voldoet 89%** (32/36) van de applicaties (nog) **niet** aan de minimale eisen op het gebied van Wpg. Dit is zorgelijk, maar het moet wel in perspectief gezien worden. Een applicatie scoort pas een voldoende (niveau 2) bij een 100% score op het gebied van de wet (Wpg), waarbij de norm om een voldoende te halen erg hoog is. Er zijn 10 applicaties die met een paar aanpassingen (max. 3 actiepunten) een voldoende kunnen scoren op het gebied van de wet (Wpg). Desondanks kan er worden vastgesteld dat PSbD niet voldoende geborgd is binnen de highrisk applicaties van de politie. Er is meer aandacht vereist om PSbD structureel binnen de organisatie in te bedden.
Een positieve concludering is dat de bewustwording omtrent privacy groot is. Het merendeel van de betrokkenen is meteen in beweging gekomen om aan de actiepunten te voldoen. Hieronder staan in het kort de belangrijkste positieve en negatieve conclusies die uit de 0-metingen gehaald kunnen worden.

| Positief | Negatief |
|---|---|
| Een beeld van de Wpg-compliance van highrisk-applicaties | Wpg compliance is onvoldoende bij merendeel highrisk-applicaties |
| Specifieke aandacht voor de problematiek van de applicaties | Borging PSbD niet geregeld |
| Bewustwording van privacy | Beleidskaders zijn vaak onbekend, onduidelijk en moeilijk te vinden |
| Evalueren adviespunten zorgt voor betrokkenheid | Privacy kennis bij de betrokkenen onvoldoende |
| Rapport een middel om verandering tot stand te brengen | Communicatie op het gebied van privacy verloopt moeizaam |
| | Artikel 13 protocollen niet geactualiseerd, wat kan leiden tot nieuwe actiepunten |

| Volwassenheidsniveau 0 | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid* |
| TRIS (v1) | 32% | 41% |
| AVR (v1) | 27% | 43% |
| Kantoorautomatisering (v1) | 25% | 58% |

| Volwassenheidsniveau 1 | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid* |
| BOSZ (v2) | 94% | 69% |
| HAVANK (v1) | 93% | 85% |
| Internet aangifte (v1) | 87% | 62% |
| PSH-VM (v1) | 81% | 49% |
| Raffinaderij (v2) | 76% | 72% |
| BVI-IB | 75% | 79% |
| Live Journaal Politie (v1) | 74% | 37% |
| SBV (v2) | 73% | 73% |
| SMC (v2) | 70% | 79% |
| Agora (v1) | 64% | 62% |
| LSV (v1) | 64% | 62% |
| VROS (v2) | 64% | 46% |
| I-Base (v2) | 61% | 77% |
| Hansken (v2) | 60% | 63% |
| Servicemodule (v1) | 58% | 60% |
| PSH-TM / Digibon (backoffice) (v2) | 57% | 55% |
| FCM (v1) | 55% | 59% |
| BVH (v2) | 53% | 57% |
| SUMMIT (v1) | 50% | 67% |
| ZUIS (v2) | 50% | 42% |
| Verificatiemodule (v2) | 50% | 33% |
| Mappen standaard (v2) | 46% | 70% |
| ANPR (v2) | 46% | 60% |
| BVI-BlueSpotMonitor (v2) | 46% | 58% |
| Amazone (v2) | 42% | 65% |
| DCS (v2) | 41% | 37% |
| PSH-V (v1) | 40% | 41% |
| Personenserver (v2) | 37% | 33% |

| Volwassenheidsniveau 2 | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid* |
| BVI-Blueview 4.0 (v1) | 100% | 90% |
| MEOS (v1) | 100% | 86% |
| BVID 2.0 (v1) | 100% | 85% |
| Orion (v2) | NVT | 87% |

### Vervolgstappen

Eind 2019 gaat er met alle betrokkenen van de highrisk applicaties contact worden opgenomen om doormiddel van de 'pas toe' of 'leg uit'-methode te bekijken in hoeverre de actiepunten zijn geadresseerd. Indien er onvoldoende vooruitgang is (zonder verklaring) gaat er vanuit de korpsleiding worden geëscaleerd. Dit moet gedaan worden via een afsprakenset vanuit de planning en control cyclus.

### Borgen

Om ervoor te zorgen dat de 0-meting PSbD geen eenmalige actie is moet de borging goed geregeld worden. De borging geschiedt op basis van de registerplicht. Iedere verwerking dient vastgelegd te worden in het zogenaamde verwerkingsregister. Daarbij gaat er een schema gemaakt worden, met welke privacyaspecten doorlopen moet worden zodat er bepaald wordt of er voldaan is aan de privacywetgeving (Wpg en AVG) en (politie)beleid (PSbD compliant). Om dit voor elkaar te krijgen is het van belang dat PSbD een vast onderdeel gaat worden in de organisatie. In het productiehuis en bij innovaties moeten er structureel medewerkers met een PSbD-rol aanwezig zijn die meehelpen, controleren en opleveren op basis van PSbD en vragen kunnen beantwoorden van collega's.

# Inleiding

## Aanleiding

Eind 2015 heeft de Auditdienst Rijk (ADR) gerapporteerd over een (extern) uitgevoerde privacy audit en dat heeft aangetoond dat er op het gebied van Privacy en Security verbeteringen nodig zijn. De informatieverwerkende applicaties van de politie voldoen op meerdere onderdelen nog niet aan de eisen van de Wpg. 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 is onderdeel van het verbeterprogramma Wpg en IB[2]. Het uitvoeringskader PSbD[3] staat aan de basis om 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 algemeen resultaat van 0-metingen die zijn uitgevoerd op potentiele highrisk applicaties[4]. Door het gebruik te maken van 0-metingen is vanaf de start een beeld gecreëerd van de volwassenheid van de highrisk applicaties van de politie op het gebied van PSbD. Waarbij highrisk staat voor de soort en de hoeveelheid informatie die via de applicatie loopt en niet de staat waarin de applicatie zich verkeert.
Hierbij wordt in gegaan worden op het proces van de 0-meting, maar ook op scores (per getoetste principe) die opgehaald zijn uit de 0-meting. Daarnaast wordt er aangegeven op welke punten van het Wpg & IB-verbeterprogramma de 0-meting invloed heeft.

## Doelstellingen

Het doel van het algemeen rapport, ten opzichte van de specifieke applicatie rapporten, is om het proces zoals deze is uitgevoerd te beschrijven en daarnaast de resultaten te bespreken inclusief de opvallende resultaten per principe. Op basis van deze resultaten wordt een duidelijk beeld geschetst hoe de highrisk applicaties van de politie ervoor staan op het gebied van Wpg-compliance en PSbD-compliance (Wpg-compliance + politiebeleid). Met de uitkomst van het onderzoek kan de volgende onderzoeksvraag worden beantwoord:

***In hoeverre zijn de vastgestelde highrisk applicaties van de politie PSbD compliant?***

Op basis van de uitkomst van de onderzoeksvraag is het doel om de vastgestelde highrisk applicaties van de politie PSbD compliant te krijgen. Hierbij gaat hulp gevraagd worden van de portefeuillehouders en indien noodzakelijk van de korpsleiding van de politie.

## Doelgroepen en gebruik

Initieel is de doelgroep voor dit document de stuurgroep Wpg & IB. Daarnaast geeft het de portefeuillehouders inzicht in de maatregelen die nodig zijn om de highrisk applicaties te laten voldoen aan PSbD. De specifieke rapporten van de 0-meting moeten ervoor zorgen dat de betreffende portefeuilleteams overleg voeren met hun portefeuillehouder om de maatregelen uit te voeren. Daarbij prioriteert de productowner de actiepunten om deze op de backlog te verwerken. Het document dient ook als start voor een verbeterde controle door PSbD ongeacht het soort verwerking (bestaande verwerkingen, vernieuwing/projecten of innovaties).

[1] Verbeterplan Wet Politiegegevens en Informatiebeveiliging
[2] Tranche 2018, Verbeterprogramma Wpg en IB
3 2018-04-26_Uitvoeringskader_Privacy en Security by Design_v2.0
[4] Vooronderzoek_PSbD_Highrisk_applicaties v1.1 def stuurgroep 20171025

# 1 Proces van de 0-meting

Een belangrijk onderdeel van de 0-meting is de keuze voor methode. In dit hoofdstuk staan de keuzes beschreven die gemaakt zijn vanuit het verbeterprogramma en structuur en de tijdslijn van de 0-metingen en wordt er uitgelegd hoe de tijdslijn loopt gedurende het proces.

## 1.1 Verbeterprogramma Wpg & IB

Zoals eerder beschreven is de 0-meting onderdeel van het Wpg & IB verbeterprogramma. De methode om van start te gaan stond nog niet vast. Het doel vanuit het verbeterprogramma was om op een efficiënte manier zo snel mogelijk resultaat te kunnen behalen binnen het verbeterprogramma. Uiteindelijk is een afweging gemaakt tussen de volgende 2 methoden.

*Normal risk methode*

De meest complete manier om in beeld te krijgen in hoeverre de Wpg op de verschillende onderdelen wordt nageleefd is om de verwerkingen in combinatie met werkprocessen in beeld te krijgen. Dit is echter de meest complexe methode aangezien bij veel verwerkingen overlap zitten tussen applicaties. Het is ook niet direct mogelijk om de verantwoordelijken en betrokkenen aan te wijzen die hier direct wat mee kunnen en moeten doen. Deze methode is dermate intensief, dat omwille van de voortgang in het kader van het verbeterprogramma gekozen is voor een snellere variant. In het hoofdstuk Vervolgstappen staat dit verder beschreven.

*Highrisk methode*

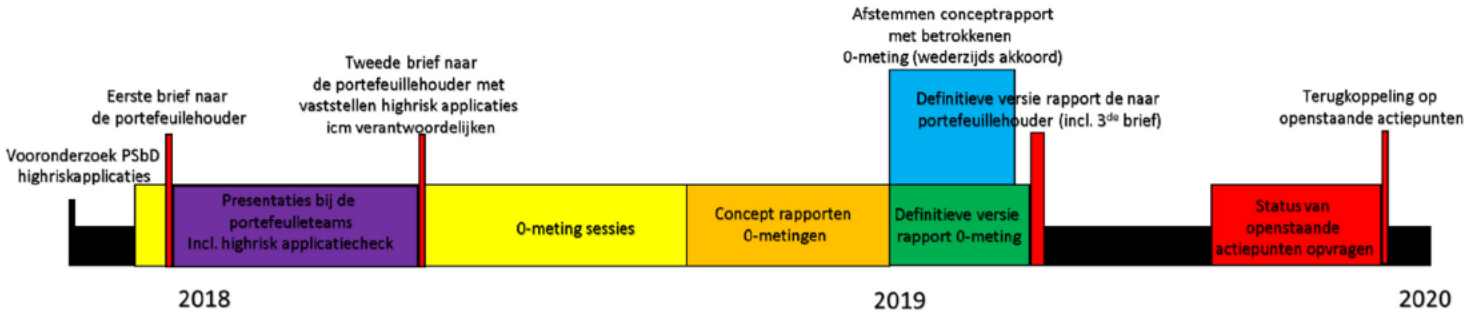
De snelste methode is de highrisk methode. Met highrisk wordt bedoelt *het soort informatie wat via de applicatie loopt* niet de staat waarin de applicatie zich verkeerd. Er wordt dus niet uitgaan van verwerkingen i.c.m. werkprocessen, maar van applicaties. Het voordeel hiervan is dat er relatief snel resultaat behaald kan worden. De scope kan beperkt worden tot de meest relevante applicaties, waardoor betrokkenen en verantwoordelijken makkelijker aan te wijzen zijn. Door een selectie te maken van potentiele highrisk applicaties kon de scope afgebakend worden in aansluiting op het verbeterprogramma Wpg & IB. Voor de 0-metingen is zodoende gebruik gemaakt van de highrisk methode.

## 1.2 Structuur

In deze paragraaf staat de structuur van de 0-metingen beschreven met daarin de tijdslijn waarin de onderdelen zijn uitgevoerd. Gedurende de gehele periode zijn haalbare proces verbeteringen direct toegepast. Een voorbeeld hiervan is de aanpassing van de 0-meting naar aanleiding van de nieuwe versie van het uitvoeringskader PSbD (v1.0 naar v2.0) vanwege de AVG en nieuwe richtlijnen van de Wpg.

| Proces 0-metingen | |
|---|---|
| 1. | Vooronderzoek |
| 2. | Brief 1: Uitleg Privacy & Security by Design (PSbD) compliance (november 2017) |
| 3. | Presentaties aan o.a. de portefeuilleteams met het verzoek de applicaties te bevestigen |
| 4. | Brief 2: Vaststellen van de highriskapplicaties (april 2018) |
| 5. | Uitvoeren van de 0-metingen PSbD |
| 6. | Concept rapport versturen naar betrokkenen |
| 7. | Brief 3: Definitief rapport versturen naar portefeuillehouders na wederzijds akkoord betrokkenen |
| 8. | Evaluatie actiepunten (eind 2019) |

*Tabel 1.2 Proces 0-metingen*




*Afbeelding 1.2a Het proces van het onderzoek*

### 1. Vooronderzoek

De structuur van de 0-metingen is gedurende de tijd bijgeschaafd, maar de basis is gelegd in het vooronderzoek[5]. Het vooronderzoek is vastgesteld door de stuurgroep Wpg & IB en is de start geweest van het onderzoeken naar de status van de highrisk applicaties op het gebied van PSbD.

### 2. Brief 1: Uitleg PSbD compliance (november 2017)[6]

Vanwege het belang om te voldoen aan privacy wetgeving en beleid zijn er op verschillende momenten brieven gestuurd naar de portefeuillehouders. In de eerste brief is vooral aandacht gevraagd voor het uitvoeringskader PSbD en het toepassen daarvan. Hierin is aangegeven dat het belang van informatie groot is en dat het juist verwerken van informatie een belangrijk onderdeel is voor de legitimiteit en het vertrouwen in de politie. Met tot slot het verzoek tot medewerking.

*Eerste lijst highrisk applicaties*

Een aantal specialisten van de Directie IV heeft een voorselectie gemaakt van potentiele highriskapplicaties. Hierbij is geselecteerd op de volgende criteria[5]: labeling, verwijderen & vernietigen, logging, autoriseren, verstrekken, risico-opslag, aantal gebruikers en levenscyclus applicatie.

### 3. Presentaties

Na het sturen van de eerste brief zijn er presentaties gegeven aan de portefeuilleteams van de verschillende eenheden. Naast de uitleg over PSbD is er per portefeuilleteam gevraagd of de applicaties die van te voren geselecteerd waren overeenkwamen met de applicaties die zij zelf zouden kiezen binnen hun portefeuille. Op basis hiervan zijn de volgende applicaties toegevoegd aan de lijst (Raffinaderij, Hansken, I-Base en personenserver).
Om iedereen in positie te brengen zijn er ook presentaties gegeven bij het privacy platform (privacy functionarissen), portefeuilleondersteuners, architecten en ketenpartners.

### 4. Brief 2: Vaststellen van de highrisk applicaties (april 2018)[7]

In de tweede brief is er opnieuw aan de portefeuillehouder gevraagd om medewerking en om de highrisk applicaties die binnen de portefeuilleteams besproken zijn vast te stellen. Een belangrijk element in deze brief is dat de portefeuillehouders gekoppeld zijn aan de applicaties. Met andere woorden de verantwoordelijkheid van de portefeuillehouder zijn expliciet belegd. Hierbij is er aan de portefeuillehouders gelegenheid gegeven om nog te reageren op de brief. Op basis hiervan is de verantwoordelijkheid voor een aantal applicaties verschoven naar een andere portefeuillehouder. Daarna is de lijst met applicaties definitief vastgesteld en gebruikt voor de 0-metingen.

5 Vooronderzoek_PSbD_Highrisk_applicaties v1.1 def stuurgroep 20171025
6 Brief PSbD compliance portefeuillehouders.pdf
7 Brief PSbD highriskapplicaties portefeuillehouders 20180410 def v2.pdf

## 5. Uitvoeren van de 0-metingen

Aan de basis van de 0-meting staat het uitvoeringskader Privacy & Security by Design (PSbD). In het uitvoeringskader PSbD staan 12 principes vanuit de architectuur geformuleerd. Voor elk principe zijn criteria opgesteld die op de wet of (politie)beleid zijn gebaseerd. In totaal zijn dat 90 criteria die behandeld worden tijdens de 0-meting. Daarnaast heeft elke principe een eigen weging: **L**icht (2), **M**iddel (6) of **Z**waar (10). Op basis van die weging worden de punten die per criteria worden behaald vermenigvuldigd.

*Uitvoeringskader PSbD v2.0*

1. Eenmalige vastlegging (Z)
2. PDCA- cyclus (M)
3. Doelbinding (Z)
4. Verantwoording (Z)
5. Autorisatie (Z)
6. Metagegevens (Z)
7. Kwaliteitszorg (Z) (Geen wetscriteria)
8. Bewaren en vernietigen (Z)
9. Informatiebeveiliging (Z)
10. Privacy by default (Z)
11. Toepassen standaarden (L) (Geen wetscriteria)
12. Verantwoordelijkheden belegd (M) (Geen wetscriteria)


Afbeelding 1.2b: Uitvoeringskader PSbD

*Ja/Nee/Deels/NVT*

De toetsing van de criteria vond plaats aan de van gesloten vragen die met Ja/Nee/Deels/NVT beantwoord konden worden. Indien een vraag met 'Ja' of 'NVT' was beantwoordt dan werd het alleen als score, maar niet als actiepunt opgenomen. Bij alle vragen waarbij 'Nee' of 'Deels' werd ingevuld kwam automatisch een actiepunt uit de betreffende vraag. Als het antwoord 'Deels' is dan telt deze voor de helft mee in de score. Ondanks dat de vragen gesloten zijn is er bij elke vraag de ruimte genomen om specifieke toelichtingen te noteren die die waar inhoudelijk van toepassing zijn meegenomen in de beoordeling.

*0-meting sessie*

De duur van 0-meting is gemiddeld 6 tot 8 uur, waarbij bij enkele metingen bleek significant dat meer tijd nodig was en ervoor gekozen is om een extra sessie te houden. Elke sessie begon met een introductie van de applicatie. Hierin werd de applicatie (waar mogelijk) getoond en kon er op voorhand een beeld gevormd worden van de werking van de applicatie. Vervolgens werd er op basis van artikel 1 van de Wpg een invulling gegeven aan de verschillende soorten verwerkingen binnen de applicatie. Dit had vooral als doel om verder tijdens de 0-meting gerichtere vragen te kunnen stellen. Daarna werden één voor één de principes behandeld om tot slot te eindigen met een open vraag of er nog iets m.b.t. de applicatie gemeld moest worden wat relevant kon zijn voor het rapport.

- Introductie onderling
- Introductie applicatie
- Doornemen soorten verwerkingen
- Per principes de criteria doorlopen
- Afsluiten met een open vraag

*Transparant*

Om de meting zo transparant te laten verlopen zijn de antwoorden die ingevuld werden (waar mogelijk) direct op het scherm getoond. Indien dit niet mogelijk was dan werd bij elke vraag duidelijk gecommuniceerd of het antwoord een 'Ja', 'Deels', 'Nee' of 'NVT' is. Zodat de betrokkenen van de 0-meting precies konden weten welke actiepunten er in het rapport zouden verschijnen.

*Betrokkenen*

De betrokkenen zijn van te voren afgestemd met de senior Coördinerend Business Expert (sCBE). Vanuit het onderzoek werd verzocht om een bepaalde collega's aan te dragen met bepaalde expertisegebieden/functies (architect, functioneel beheerder, productowner, technisch beheerder, ontwikkelaar), maar de invulling van degene die bij de 0-meting aanwezig zijn overgelaten aan de sCBE. Die kon op basis van de criterialijst die voor de 0-meting was gestuurd een beeld vormen wie van zijn specialisten aanwezig diende te zijn. Tot slot adviseerden wij altijd dat er een privacy functionaris bij aanwezig moest zijn of in ieder geval op de hoogte diende te zijn. Ook hier hebben we een vrije invulling gegeven aan de sCBE.

| Highrisk applicatie | Versie | Verzamelen | Vastleggen | Ordenen | Bewaren | Bijwerken | Wijzigen | Opvragen | Raadplegen | Gebruiken | Vergelijken | Verstrekken | Samenbrengen | In verband brengen | Afscherming | Uitwissen | Vernietigen |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Agora | 1.0 | x | x | x | x | x | x | | x | x | | x | x | | x | x | x |
| Amazone | 2.0 | x | x | x | x | x | x | x | x | x | | x | x | | x | x | x |
| ANPR | 2.0 | x | x | x | x | x | x | x | x | x | x | x | | | x | x | x |
| AVR | 1.0 | | x | | x | | x | x | x | x | | x | x | x | x | x | x |
| BOSZ | 2.0 | x | x | x | x | x | x | x | x | x | | x | x | | x | x | x |
| BVH | 2.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | |
| BVI-BlueSpotMonitor | 2.0 | x | | x | x | | | x | x | x | | x | x | x | x | | |
| BVI-Blueview 4.0 | 1.0 | | x | x | x | | | x | x | x | x | x | x | x | x | x | x |
| BVID 2.0 | 1.0 | x | | | x | | | x | x | x | x | x | | x | x | x | x |
| BVI-IB | 1.0 | x | | x | | | | x | x | x | x | | x | | x | | |
| | | | | | | | | | | | | | | | | | |
| DCS | 2.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| FCM | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Hansken | 2.0 | x | x | x | x | x | x | x | x | x | x | x | x | | x | | x |
| HAVANK | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x |
| I-Base | 2.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Internet Aangifte | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x |
| Kantoorautomatisering | 2.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Live Journaal Politie | 1.0 | x | x | x | x | x | x | x | x | x | | x | x | | x | x | x |
| LSV | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Mappen standaard | 2.0 | x | x | x | x | x | x | x | x | x | | x | x | | x | x | x |
| MEOS | 1.0 | x | | x | | | | x | x | x | | x | x | x | x | | |
| Orion | 2.0 | | | | | | | x | x | x | | | | | | | |
| Personenserver | 2.0 | x | x | | | x | x | x | x | x | x | x | x | | x | | x |
| PSH-TM / Digibon | 2.0 | x | x | x | x | x | x | x | x | x | | x | x | x | x | x | x |
| PSH-V | 1.0 | x | x | x | x | x | x | x | x | x | | x | | | x | | x |
| PSH-VM | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | |
| Raffinaderij | 2.0 | x | | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| SBV | 2.0 | x | x | x | x | x | | x | x | x | | x | | | x | | x |
| Servicemodule | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x |
| SMC | 2.0 | x | x | x | | x | x | x | x | x | | x | | x | x | x | |
| SUMMIT | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| TRIS | 1.0 | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | |
| Verificatiemodule | 2.0 | | | | | | | x | x | x | x | | | | x | | x |
| VROS | 2.0 | x | | x | x | | | x | x | x | | x | x | x | x | x | x |
| ZUIS | 1.0 | x | x | x | x | x | x | x | x | x | | | x | x | x | | x |

*Tabel 1.2a Verschillende soorten verwerkingen binnen de highrisk applicaties*

| Highrisk applicaties | Versie | Artikel 8 | Artikel 9 | Artikel 10 | Artikel 12 | Artikel 13 | AVG |
|---|---|---|---|---|---|---|---|
| ANPR | 2.0 | x | x | x | | x | |
| BOSZ | 2.0 | x | x | x | | x | |
| BVH | 2.0 | x | x | x | | x | |
| BVI-Blueview 4.0 | 1.0 | x | x | x | | x | |
| I-Base | 2.0 | x | x | x | | x | |
| Live Journaal Politie | 1.0 | x | x | x | | x | |
| Mappen standaard | 2.0 | x | x | x | | x | |
| Raffinaderij | 2.0 | x | x | x | | x | |
| SUMMIT | 1.0 | x | x | x | | x | |
| Amazone | 2.0 | x | x | x | | | |
| DCS | 2.0 | x | x | x | | | |
| Kantoorautomatisering | 2.0 | x | x | x | | | |
| Verificatiemodule | 2.0 | x | x | x | x | | |
| | | | | | | | |
| BVID 2.0 | 1.0 | x | x | | | | |
| BVI-BlueSpotMonitor | 2.0 | x | | | | x | |
| BVI-IB | 1.0 | x | | | | x | |
| SMC | 2.0 | x | | | | x | |
| Agora | 1.0 | x | | | | | |
| Internet Aangifte | 1.0 | x | | | | | |
| MEOS | 1.0 | x | | | | | |
| PSH-TM / Digibon (backoffice) | 2.0 | x | | | | | |
| Servicemodule | 1.0 | x | | | | | |
| LSV | 1.0 | | x | | | x | |
| AVR | 1.0 | | x | | | | |
| Hansken | 2.0 | | x | | | | |
| FCM | 1.0 | | | | | x | |
| HAVANK | 1.0 | | | | | x | |
| SBV | 2.0 | | | | | x | |
| TRIS | 1.0 | | | | | x | |
| VROS | 2.0 | | | | | x | |
| Orion | 2.0 | | | | | | |
| Personenserver | 2.0 | | | | | | x |
| PSH-V | 1.0 | | | | | | x |
| PSH-VM | 1.0 | | | | | | x |
| ZUIS | 1.0 | | | | | | x |

*Tabel 1.2b Verwerkingsgrondslagen binnen de highrisk applicaties*

### 6. Conceptrapporten versturen naar betrokken

Het rapport is zowel het verslag van de gegeven antwoorden tijdens de 0-meting als het advies gebaseerd op die antwoorden. Daarnaast biedt het richtlijnen voor de teams om hun applicatie compliant te maken. Met een aandachtspunt als de vraag niet in de 0-meting voorkwam, maar het wel van een dusdanig belang was dat het werd beschreven. In het rapport is onderscheid gemaakt tussen actiepunten gebaseerd op de Wet politiegegevens (minimale vereiste) en actiepunten gebaseerd op het politiebeleid PSbD (maximale score).

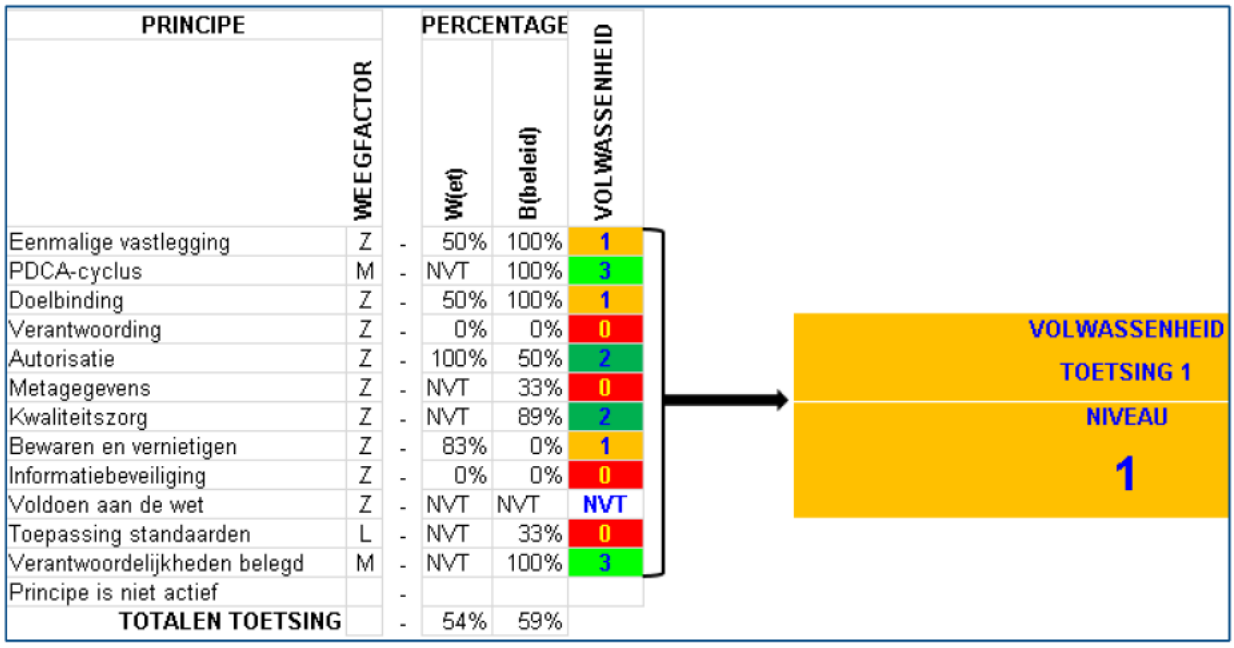
*Definitief*

Het definitief maken van een rapport is een schriftelijk (mail) akkoord dat de betrokkenen en de toetsers het eens zijn over de inhoud van het rapport. Met het wederzijds akkoord wordt het rapport definitief gemaakt en is het vrij voor interne weergave. Vervolgens is de portefeuillehouder, door middel van het definitieve rapport en bijbehorende brief, op zijn verantwoordelijkheden worden gewezen met als doel het opvolgen van de actiepunten.

*Volwassenheidsniveau*

In het rapport worden aan de hand van de gesloten vragen scores berekent die een direct beeld geven hoe de applicatie ervoor staat. De minimale score voor een voldoende is volwassenheidsniveau 2. Dat betekent dat er is voldaan aan de (privacy)wet en er alleen nog (politie)beleid actiepunten openstaan. De scores in niveaus worden in het rapport ook per principe getoond zodat duidelijk is op welk principe er goed en minder gescoord wordt (zie afbeelding hieronder).

- **Niveau 0:** Er is geen specifieke aandacht voor PSbD op basis van het (politie)beleid.
  - Wet: 0-35% en beleid: 0-100%
  - Wet: NVT en beleid: 0-35%
- **Niveau 1:** Er is wel specifieke aandacht op het gebied van PSbD, maar die is niet toereikend om te voldoen aan de wet (Wpg).
  - Wet 36%-99% en beleid 0-100%
  - Wet: NVT en beleid: 36%-50%
- **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
    - Wet: 100% en beleid: 0-99%
    - Wet: NVT en beleid: 51%-99%
- **Niveau 3:** De aandacht op het gebied van PSbD voldoet aan de wet en het vastgestelde (politie)beleid.
  - PSbD compliant
    - Wet: 100% en beleid: 100%
    - Wet: NVT en beleid: 100%
    - Wet: 100% en beleid: NVT



| PRINCIPE | WEEGFACTOR | | PERCENTAGE W(et) | PERCENTAGE B(beleid) | VOLWASSENHEID |
|---|---|---|---|---|---|
| Eenmalige vastlegging | Z | - | 50% | 100% | 1 |
| PDCA-cyclus | M | - | NVT | 100% | 3 |
| Doelbinding | Z | - | 50% | 100% | 1 |
| Verantwoording | Z | - | 0% | 0% | 0 |
| Autorisatie | Z | - | 100% | 50% | 2 |
| Metagegevens | Z | - | NVT | 33% | 0 |
| Kwaliteitszorg | Z | - | NVT | 89% | 2 |
| Bewaren en vernietigen | Z | - | 83% | 0% | 1 |
| Informatiebeveiliging | Z | - | 0% | 0% | 0 |
| Voldoen aan de wet | Z | - | NVT | NVT | NVT |
| Toepassing standaarden | L | - | NVT | 33% | 0 |
| Verantwoordelijkheden belegd | M | - | NVT | 100% | 3 |
| Principe is niet actief | | - | | | |
| TOTALEN TOETSING | | - | 54% | 59% | |



*Afbeelding 1.2c Een voorbeeld van de eindscore van een rapport met daarin de verschillende scores per principe*

### 7. Brief 3 Uitslag 0-meting specifieke applicatie in de vorm van een definitief rapport

Op het moment dat de portefeuillehouder de derde brief heeft ontvangen is dit het definitieve rapport waarin staat hoe de betreffende applicatie ervoor staat op het gebied van privacy compliance. Daarbij wordt de portefeuillehouder op zijn verantwoordelijkheid gewezen. Om te voldoen aan PSbD dient er te worden voldaan aan alle actiepunten. De verwachting is dat er gereageerd gaat worden volgens de 'pas toe of leg uit'-methode.

*Feedbackformulier*

Bij elk rapport is een feedbackformulier bijgeleverd met als doel om aan te geven wat er met een actiepunt is gedaan (pas toe of leg uit). Indien het actiepunt is opgelost kan er een backlognummer toegevoegd worden met een toelichting. Als het om bepaalde reden nog niet is gedaan of niet gaat gebeuren kan hier een verklaring worden gegeven.

### 8. Evaluatie (terugkoppeling actiepunten)

De laatste stap gaat aan het einde van 2019 plaatsvinden. Er gaat dan een controle plaatsvinden op de actiepunten volgens de 'pas toe' of 'leg uit'-methode. Indien er onvoldoende vooruitgang is (zonder verklaring) wordt er vanuit de korpsleiding worden geëscaleerd. Dit gaat gedaan worden via een afsprakenset vanuit de planning en control cyclus.

# 2 Resultaten applicaties

In dit hoofdstuk staan de afzonderlijke resultaten van de applicatie beschreven op basis van volwassenheidsniveau. Alle resultaten die in de onderstaande paragrafen zijn beschreven zijn definitief en dat betekent dat er wederzijds akkoord is over de inhoud van het rapport.

## 2.1 Volwassenheidsniveau 0

Op het moment van schrijven zijn er drie applicaties die het volwassenheidsniveau 0 hebben. Dat wil zeggen dat er geen specifieke aandacht is voor PSbD op basis van de wetgeving (Wpg) en het (politie)beleid. Uitleg over hoe de score tot stand is gekomen staat in de specifieke rapporten van de betreffende applicaties.

**Weging**

Uit de resultaten van deze 0-meting is op te maken dat de reden dat deze applicaties relatief laag scoren niet één oorzaak heeft. De weging van de scores kan er wel voor gezorgd hebben dat een applicatie lager scoort ondanks dat er beperkt een beperkt aantal actiepunten open staat. Een voorbeeld hiervan is Kantoorautomatisering, waarbij 24 van 26 wettelijke criteria niet van toepassing zijn, maar degene die van toepassing zijn werden niet gehaald. Het gevolg hiervan is dat de score[8] (%) van het principe automatisch sneller lager uitvalt. Datzelfde geldt ook voor de totale score. Echter dat heeft ook tot gevolg dat met paar aanpassingen de scores ook direct hoger uit zullen vallen. Voor TRIS en AVR heeft de weging niet direct invloed gehad op de lage score. De verklaring voor de lage score is benoemd in het specifieke rapport die TRIS en AVR heeft ontvangen. Hierbij is het van belang dat de verantwoordelijke portefeuilles voor deze applicaties snel maatregelen gaan nemen om in de toekomst te voldoen aan de privacy wetgeving en niet binnen afzienbare tijd tegen een privacy incident aan te lopen.

| **Volwassenheidsniveau 0** | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid*[9] |
| **TRIS (v1)** | 32% | 41% |
| **AVR (v1)** | 27% | 43% |
| **Kantoorautomatisering (v1)** | 25% | 58% |

*Tabel 2.1 Volwassenheidsniveau 0*

[8] Zie voor de berekening van de scores Bijlage 3: Resultaten
[9] De score op beleid telt alleen mee bij volwassenheidsniveau 2 of 3 (als de score op de wet 100% is).

## 2.2 Volwassenheidsniveau 1

Het merendeel van de highrisk applicaties valt onder het volwassenheidsniveau 1. Dat wil zeggen dat er specifieke aandacht is op het gebied van PSbD maar dat die niet toereikend is om te voldoen aan de wet (Wpg) op basis van het (politie)beleid. 78%(29/36) van de applicaties heeft wel maatregelen genomen, maar niet voldoende om te voldoen aan de privacy wetgeving. Dit moet wel in perspectief gezien worden. Er zijn 10 applicaties die met een paar aanpassingen (max 3 actiepunten) kunnen voldoen aan de wetgeving. Een voorbeeld hiervan is het uitvoeren van een informatiebeveiligingsrisicoanalyse. Bij veel applicaties is de bewustwording van de problematiek aanwezig, maar verwijzen ze vaak naar capaciteit en middelen (geld) om de problemen aan te pakken. De wettelijke criteria voor de audittrail (Verantwoording) en de verwerkingsgrondslag (Doelbinding) scoren over het algemeen goed.

| Volwassenheidsniveau 1 | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid*[10] |
| **BOSZ (v2)** | 94% | 69% |
| **HAVANK (v1)** | 93% | 85% |
| **Internet aangifte (v1)** | 87% | 62% |
| **PSH-VM (v1)** | 81% | 49% |
| **Raffinaderij (v2)** | 76% | 72% |
| **BVI-IB** | 75% | 79% |
| **Live Journaal Politie (v1)** | 74% | 37% |
| **SBV (v2)** | 73% | 73% |
| **SMC (v2)** | 70% | 79% |
| **Agora (v1)** | 64% | 62% |
| **LSV (v1)** | 64% | 62% |
| **VROS (v2)** | 64% | 46% |
| **I-Base (v2)** | 61% | 77% |
| **Hansken (v2)** | 60% | 63% |
| **Servicemodule (v1)** | 58% | 60% |
| **PSH-TM / Digibon (backoffice) (v2)** | 57% | 55% |
| **FCM (v1)** | 55% | 59% |
| **BVH (v2)** | 53% | 57% |
| **SUMMIT (v1)** | 50% | 67% |
| **ZUIS (v2)** | 50% | 42% |
| **Verificatiemodule (v2)** | 50% | 33% |
| **Mappen standaard (v2)** | 46% | 70% |
| **ANPR (v2)** | 46% | 60% |
| **BVI-BlueSpotMonitor (v2)** | 46% | 58% |
| **Amazone (v2)** | 42% | 65% |
| **DCS (v2)** | 41% | 37% |
| **PSH-V (v1)** | 40% | 41% |
| **Personenserver (v2)** | 37% | 33% |

*Tabel 2.2 Volwassenheidsniveau 1*

[10] De score op beleid telt alleen mee bij volwassenheidsniveau 2 of 3 (als de score op de wet 100% is).

## 2.3 Volwassenheidsniveau 2

Een klein aantal van de highrisk applicaties valt onder het volwassenheidsniveau 2. Dat wil zeggen dat er specifieke aandacht is op het gebied van PSbD en afdoende is om te voldoen aan de wet (Wpg), maar dat die niet toereikend is om aan alle eisen te van het (politie)beleid te voldoen. Dit is het niveau wat de politie minimaal moet behalen om Wpg compliant te zijn. Indien een applicatie op volwassenheidsniveau 2 zit dan scoort de applicatie ook hoger op het (politie)beleid aangezien die veelal een verband hebben (85% of hoger). Blueview 4.0 is de applicatie die gebouwd is op basis van de richtlijnen van het uitvoeringskader en scoort daarom heel hoog.

| **Volwassenheidsniveau 2** | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid* |
| **BVI-Blueview 4.0 (v1)** | **100%** | **90%** |
| **MEOS (v1)** | **100%** | **86%** |
| **BVID 2.0 (v1)** | **100%** | **85%** |
| **Orion (v2)** | **NVT** | **87%** |

*Tabel 2.3 Volwassenheidsniveau 2*

## 2.4 Volwassenheidsniveau 3

Niet één highrisk applicatie scoort vooralsnog het volwassenheidsniveau 3. Dat wil zeggen dat niet één applicatie zowel 100% voldoet aan de wet alsmede voor 100% voldoet aan het (politie)beleid. Dit is het niveau wat nagestreefd wordt, maar wat nu (nog) niet gehaald is. Indien hieraan wordt voldaan, dan wordt er gesproken van PSbD compliant.

| **Volwassenheidsniveau 3** | | |
|---|---|---|
| *Applicatie (versie PSbD)* | *Wet (Wpg)* | *Beleid* |
| - | - | - |

*Tabel 2.4 Volwassenheidsniveau 3*

# 3 Resultaten principes uitvoeringskader PSbD

In dit hoofdstuk worden de principes uit het uitvoeringskader PSbD besproken die gebruikt zijn tijdens de 0-meting. Per principe wordt er een toelichting gegeven worden op punten die zowel in positieve als in negatieve zin opgevallen zijn.

**De 12 principes uit het uitvoeringskader PSbD v2.0**

1. Eenmalige vastlegging (Z)
2. PDCA- cyclus (M)
3. Doelbinding (Z)
4. Verantwoording (Z)
5. Autorisatie (Z)
6. Metagegevens (Z)
7. Kwaliteitszorg (Z) (Geen wetscriteria)
8. Bewaren en vernietigen (Z)
9. Informatiebeveiliging (Z)
10. Privacy by default (Z)
11. Toepassen standaarden (L) (Geen wetscriteria)
12. Verantwoordelijkheden belegd (M) (Geen wetscriteria)

## 3.1 Eenmalige vastlegging

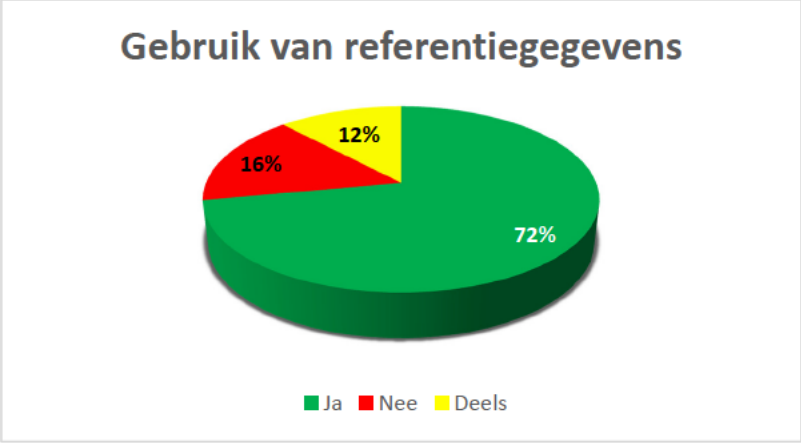
*"Gegevens worden eenmalig vastgelegd en meervoudig gebruikt"*

Naast dat het efficiënter en effectiever 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 moet er eerst gekeken 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 principe van eenmalige vastlegging is in de 0-meting lastig te beoordelen bij bestaande applicaties aangezien die vaak in een periode zijn gemaakt waarbij eenmalige vastlegging en meervoudig gebruik geen standaard waren. Desondanks is er per applicatie een duidelijk beeld geschetst hoe er met gegevens wordt omgegaan wordt. Een goed voorbeeld hiervan zijn de referentiegegevens.

### 3.1.1 Referentiegegevens

De referentiegegevens zijn in de basis bij de politie goed geregeld. De [redacted] heeft hier de controle over en het is duidelijk dat de betrokkenen hiervoor bij [redacted] kunnen aansluiten. Ongeveer 72% (18/25) van de highrisk applicaties die referentiegegevens gebruiken doen dit in samenspraak met de [redacted]. Desondanks zijn er situaties waarin het gebruik van referentiegegevens lastig is bijvoorbeeld in ketensamenwerkingsverbanden of internationale samenwerkingen. Een goed voorbeeld is het gebruik van de landentabel, waarbij de samenwerking verloopt via organisaties/landen die bijvoorbeeld een anderen landentabel hanteren dan de politie dat doet.




*Afbeelding 3.1.1.Gebruik van referentiegegevens*

### 3.1.2 Kernregisters

Een belangrijk onderwerp bij de 0-meting was het op de toekomstgerichte kernregisters. [redacted]. Er is bij de highrisk applicaties wel aangegeven dat er rekening moet worden gehouden met toekomstig gebruik van kernregisters (indien van toepassing). Tot het moment dat kernregisters echt gebruikt kunnen worden moet er gebruik worden gemaakt van de personenserver (en verificatiemodule). Aangezien de ontwikkeling van de [redacted] in stappen, gaat betekent dat de personenserver en verificatiemodule voorbereid moeten zijn voor langduriger gebruik. [redacted].

## 3.2 PDCA-cyclus

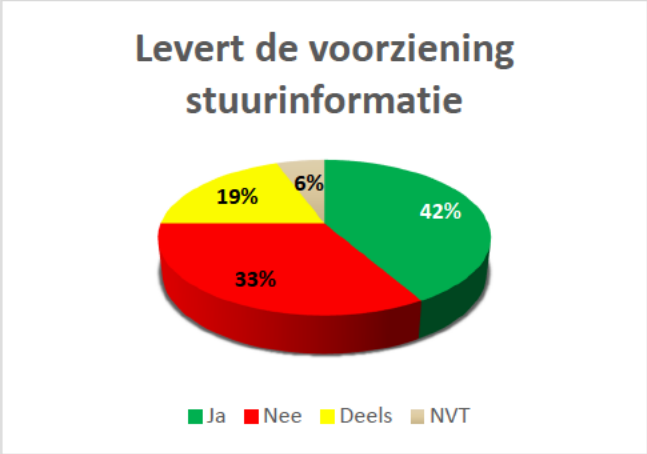
*"De werking van de informatievoorziening wordt bestuurd op basis van cyclische terugkoppeling"*

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.

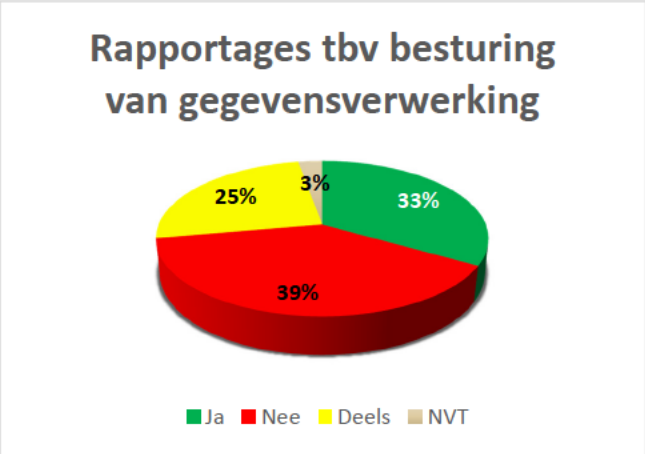
In diverse 0-metingen komt terug dat het proces bij de politie nooit direct een cyclische terugkoppeling heeft. Met andere woorden, het evalueren heeft binnen de politie nog onvoldoende aandacht. Dit komt ook terug uit de resultaten die beschreven zijn in dit hoofdstuk.

### 3.2.1 Stuurinformatie

Veel van de highrisk applicaties levert geen stuurinformatie aan, terwijl dit wel zou kunnen helpen ter verbetering van de applicatie. Er worden geen periodieke rapportages opgeleverd die ook worden bewaard. Veelal worden er op ad-hoc basis rapportages aangeleverd. Er wordt dan wel aangegeven dat het nut er wel is, maar dat er geen prioriteit is om hier actief wat aan te veranderen. Dit heeft in de 0-meting gezorgd voor veel actiepunten bij het principe PDCA-cyclus.




*Afbeelding 3.2.1a Levert de voorziening stuurinformatie*




*Afbeelding 3.2.1b. Rapportages tbv besturing van gegevensverwerking*

### 3.2.2 Beheer van gegevens, processen en software

Het beheer van de software binnen de politie voldoet aan de PDCA-cyclus. Echter bij processen en gegevens zijn er verbeteringen noodzakelijk. Processen worden wel verbeterd, maar niet geëvalueerd. Bij veel 0-metingen is aangegeven dat processen aangepast worden zonder op een later moment terug te kijken of een proces daadwerkelijk verbeterd is. De oorzaak voor het ontbreken van evaluatie is veelal werkdruk en geringe prioritering. De gehele levenscyclus van gegevens wordt ook niet 100% nageleefd aangezien het verwijderen en vernietigen (nog) geen standaard onderdeel is in de levenscyclus.

### 3.2.3 GEB

Aangezien de 0-metingen gebaseerd waren op bestaande applicaties ontbreekt de verplichting om een GEB uit te voeren op bestaande verwerkingen er vanuit de Wpg. Een GEB dient uitgevoerd te worden bij nieuwe verwerkingen die waarschijnlijk hoog risico voor betrokkenen opleveren. Om vast te stellen of aan de voorwaarden voor een GEB wordt voldaan, dient een quickscan uitgevoerd te worden. Bij veel applicaties werden er geen nieuwe verwerkingen ontwikkeld of hoorde dat niet meer bij de huidige applicatie, maar bij een nieuwe traject. Er is veelal bewustwording gecreëerd voor de verplichte uitvoer van een GEB bij een nieuwe verwerking met hoog risico.

### 3.2.4 Verwerkingsovereenkomst

Bij veel van de bestaande highrisk applicaties is een verwerkingsovereenkomst met een derde en/of externe partij niet van toepassing.

## 3.3 Doelbinding

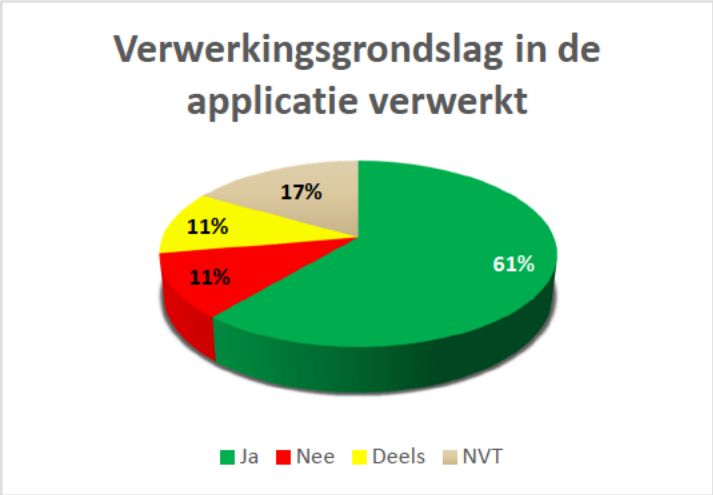
*"Persoonsgegevens worden alleen verwerkt als daar een gerechtvaardigd doel voor bestaat en ze worden niet verder verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel."*

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.

Tijdens de 0-metingen is duidelijk geworden dat er nog teveel gebruik wordt gemaakt van aannames uit bronsystemen. Vooral bij het gebruik van BVH kan dit ervoor zorgen dat in een later proces de rechtvaardigheid van een gegeven ter discussie kan komen te staan. Er moet gewerkt worden aan een juiste doelbinding van een gegeven op het moment dat het verwerkt wordt.

### 3.3.1 Verwerkingsgrondslag

Bij de meeste applicaties (58% 22/36) is doelbinding in de vorm van verwerkingsgrondslag duidelijk. De verwerkingsgrondslag is in de applicatie verwerkt. Dit is vooral herleidbaar als er binnen de applicatie gebruikt wordt gemaakt van één verwerkingsgrondslag. Daarnaast is de verwerkingsgrondslag uit [redacted] leidend [redacted]




*Afbeelding 3.3.1. Verwerkingsgrondslag in de applicatie verwerkt*

### 3.3.2 Artikel 13

In een deel van de applicaties uit deze 0-meting kunnen persoonsgegevens, die initieel zijn vastgelegd met Wpg verwerkingsgrondslag 8, 9 of 10, verder verwerkt worden onder Wpg artikel 13[11]. De verdere verwerking moet beschreven zijn in een protocol. Voor deze 0-meting zijn de protocollen voor HKS, Forensische Opsporing, FCM en VROS van toepassing. Het HKS protocol geldt voor de gegevens die vroeger in HKS stonden

[redacted]

De applicaties voor raadplegen en de applicaties voor analyse van gegevens volgen de verwerkingsgrondslag en de betreffende protocollen uit de registratieve applicaties. In onderstaande afbeelding worden de applicaties uit de 0-meting die artikel 13 verwerkingen kunnen bevatten getoond met daarbij de betreffende protocollen


*Afbeelding 3.3.2. Verdeling van applicaties binnen het artikel 13 protocol*

De volgende applicaties kennen geen artikel 13 verwerking: Agora, Amazone, AVR, BVID 2.0 [redacted], DCS, Hansken, Internet Aangifte, kantoorautomatisering, MEOS, Orion, Personenserver, PSH-TM / Digibon (backoffice), PSH-V, PSH-VM, Servicemodule, Verificatiemodule en ZUIS.

[11] Er wordt hierbij nog onderscheid gemaakt tussen algemene verdere verwerking (13 lid 1), verdere verwerking voor landelijk inzicht in specialistische onderwerpen(13 lid 2) en geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon (13 lid 3).

## 3.4 Verantwoording

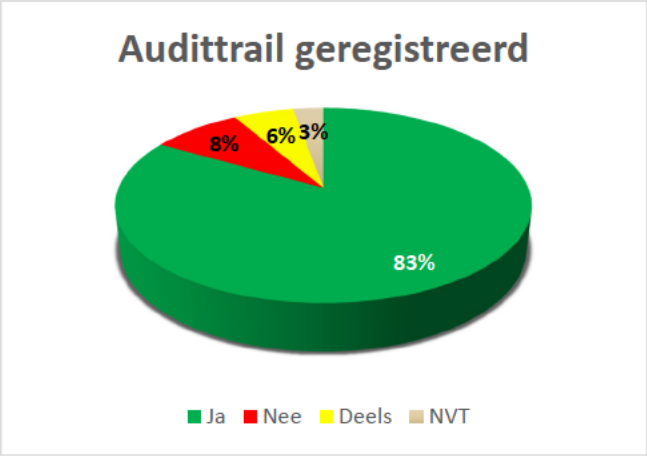
*"De politie moet verantwoording kunnen afleggen over zijn taakuitvoering en over de gegevensverwerking die daarbij plaatsvindt."*

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.

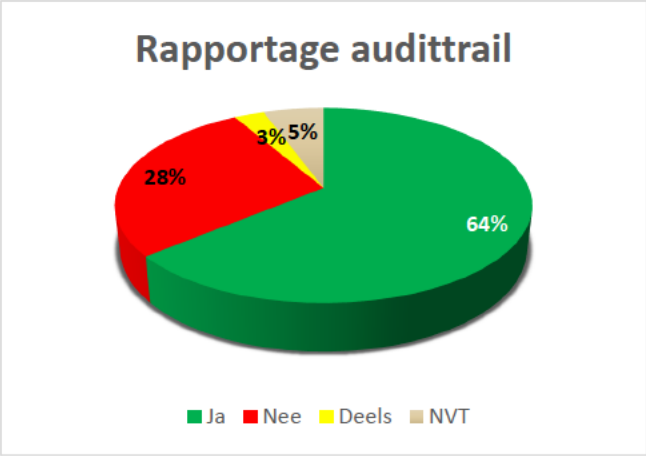
Bij het uitvoeren van de 0-metingen is duidelijk geworden dat de verantwoording een belangrijk onderdeel is in de gegevensverwerking van de politie, waarbij de beveiliging tegen manipulatie extra aandacht nodig heeft.

### 3.4.1 Audittrail

De verantwoording doormiddel van een audittrail is bij de meeste highrisk applicaties, binnen de politie, goed geborgd. Bij 83% (30/36) van de highrisk applicaties wordt een audittrail geregistreerd. Aangezien dit een wettelijke eis is wordt dit goed nageleefd. Daarnaast bleek dat bij 64% (23/36) van de highrisk applicaties er een mogelijkheid is om een rapport te maken van de audittrail. Hierbij zijn ook de mogelijkheden getolereerd waarbij er doormiddel van query de betreffende informatie getoond wordt.

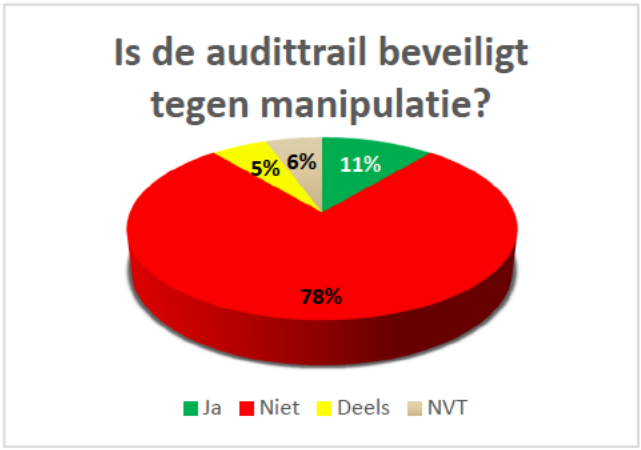



*Afbeelding 3.4.1a.Audittrail geregistreerd*




*Afbeelding 3.4.1b. Rapportage audittrial*

### 3.4.2 Manipulatie van de audittrail




*Afbeelding 3.4.2.Is de audittrail beveiligt tegen manipulatie*

## 3.5 Autorisatie

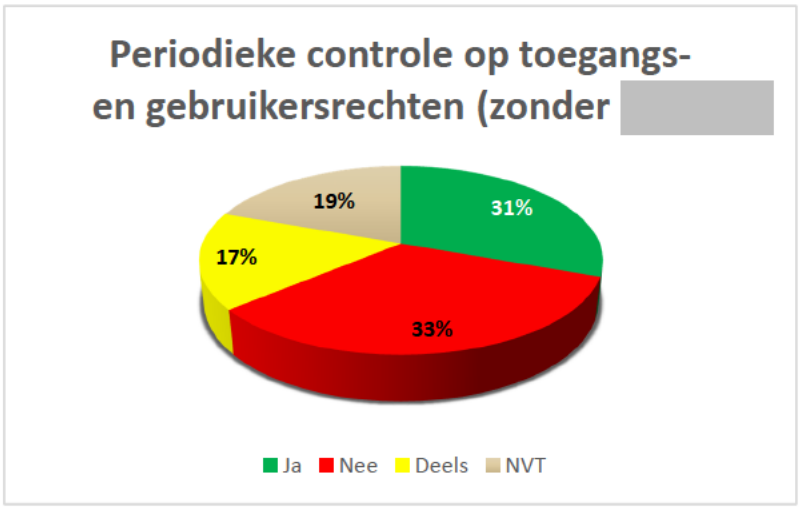
*“Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van noodzaak voor de uitvoering van de hen opgedragen werkzaamheden”*

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.

Tijdens de 0-metingen van de highrisk applicaties is naar voren gekomen dat autorisatie hoog op de prioriteiten lijst staat om in de komende tijd te ontwikkelen.

### 3.5.3 Periodieke controle op toegangs- en gebruikersrechten

Slechts bij 44% (11/36) van de highrisk applicaties wordt er een periodieke controle gedaan op toegangs- en gebruikersrechten. Normaal gesproken is dit geen probleem mits de highrisk applicatie gebruik maakt van




*Afbeelding 3.5.3.Periodieke controle op toegangs- en gebruikersrechten (zonder*

## 3.6 Metagegevens

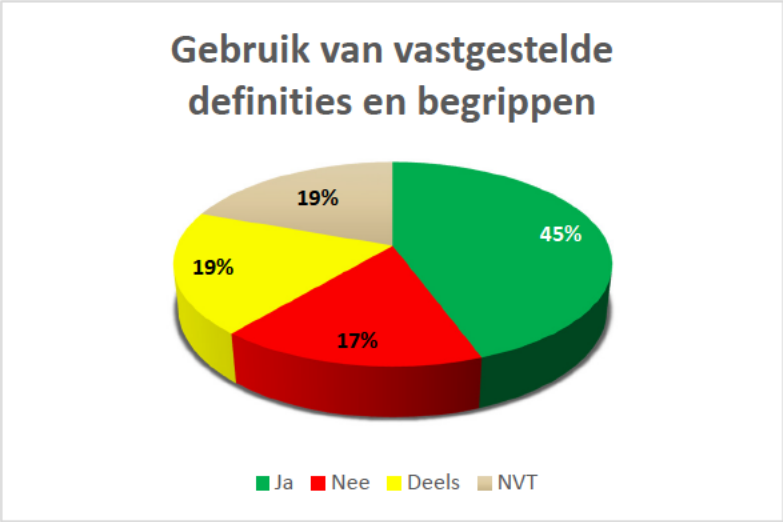
*"Gegevens worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de juistheid en de rechtmatigheid van de gegevensverwerking te waarborgen"*

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.

Tijdens de 0-metingen is naar voren gekomen dat het bewust gebruiken van metagegevens nog niet een standaard is.

### 3.6.1 Vastgestelde definities voor bedrijfsbegrippen

De meeste van de highrisk applicaties bestaan al langer dan 5 jaar waardoor het gebruik van metagegevens nog niet is verwerkt. Echter het vaststellen van definities en bedrijfsbegrippen is iets wat met enige regelmaat bijgehouden moet worden om de kwaliteit van de juistheid en rechtmatigheid te kunnen waarborgen. In 45% (16/36) van de gevallen is dit duidelijk vastgelegd en aangetoond. In 36% (13/36) van de highrisk applicaties het gebruik van definities en begrippen niet of deels vastgelegd.




*Afbeelding 3.6.1 Gebruik van vastgestelde definities en begrippen*

### 3.6.2 Toepassingsprofiel metagegevens politie

Het Toepassingsprofiel Metagegevens Rijk (TMR) was bij vrijwel alle betrokkenen van de 0-metingen onbekend. Ook het Toepassingsprofiel Metagegevens Politie (TMP), wat tijdens de 0-metingen nog in ontwikkeling was, is bij de meesten onbekend. Het gaat vooral voor het uitdragen van het TMP van belang zijn om duidelijk communiceren wat er van hen verwacht gaat worden. Daarnaast moet de doelgroep van het TMP duidelijk gemaakt moeten worden. Tijdens de 0-metingen was het TMP nog niet klaar en hebben wij verwezen naar het TMR. De toepasbaarheid was veelal onduidelijk en moet in het beleid verder uitgewerkt worden.

## 3.7 Kwaliteitszorg

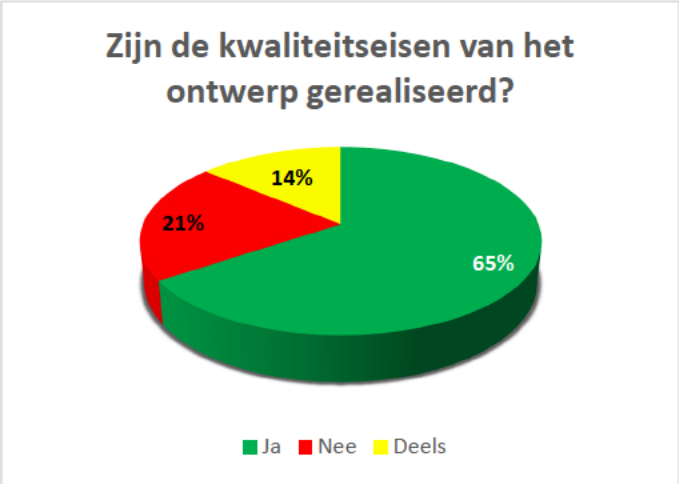
*"De informatievoorziening waarborgt de kwaliteit van de gegevensverwerking"*

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.

In de sessies van de 0-metingen is naar voren gekomen dat het duidelijk is hoe de kwaliteit verbeterd moet worden, maar dat er nog onvoldoende gerapporteerd wordt op de vereiste verbeteringen.

### 3.7.1 Kwaliteit van gegevens

Tijdens de 0-metingen werd duidelijk dat bij de highrisk applicaties de kwaliteit van gegevens voorop staat. In de statistieken staat dat 65% (19/29) van de kwaliteitseisen van het ontwerp zijn gerealiseerd. Bij de overige 33% (10/29) staan de kwaliteitseisen op de backlog om, waar mogelijk, zo snel mogelijk te realiseren.



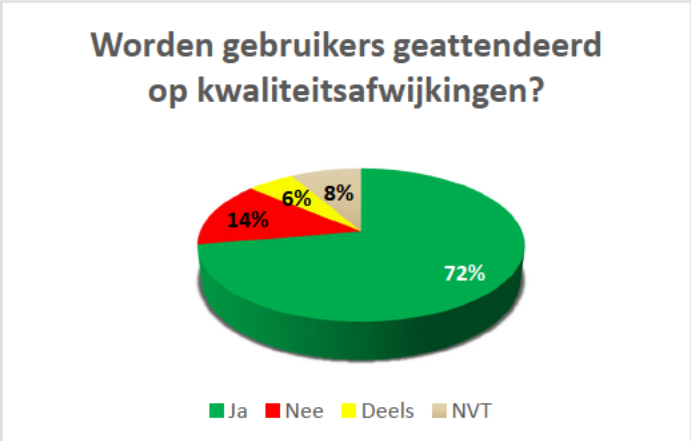

*Afbeelding 3.7.1 Kwaliteit van gegevens*

### 3.7.2 Bedrijfsregels formuleren

Voor het opstellen van bedrijfsregels is het van belang dat de bedrijfsbegrippen vaststaan en dat de business experts en IV-experts een gemeenschappelijke taal spreken. Tijdens de 0-metingen kwam naar voren dat het vooral eenvoudige bedrijfsregels die in de highrisk applicaties verwerkt zijn. Bijvoorbeeld dat er maar één keer aangifte mag worden gedaan van hetzelfde incident. Of regels die nageleefd moeten worden om NAW-gegevens in te voeren (postcode in 1111AA ipv 1111 AA). Wanneer het complexer wordt doordat er bijvoorbeeld een ketenpartners bij betrokken is, dan wordt het lastiger om de bedrijfsregels toe te passen. Deze worden daardoor minder snel gehanteerd.

### 3.7.3 Kwaliteitsafwijkingen

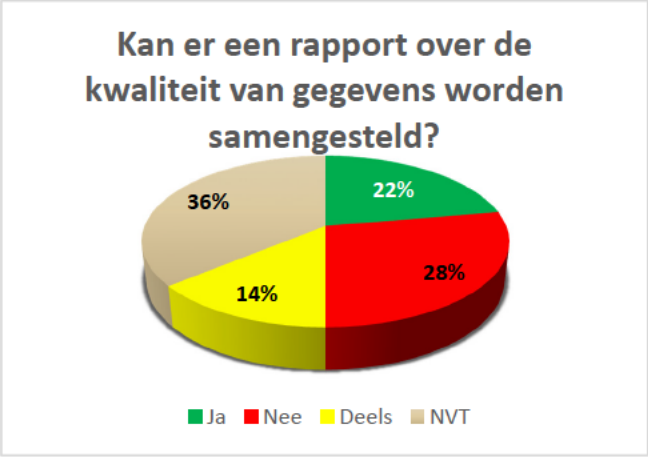
Een gebruiker wordt binnen de highrisk applicatie vaak geattendeerd (72% 26/36) op kwaliteitsafwijkingen. Bijvoorbeeld als niet alle velden ingevuld zijn, waardoor de gebruiker niet verder kan. Of bij een zoekopdracht dat duidelijk is dat er geen verbinding is met de server, waardoor er geen resultaten worden getoond.



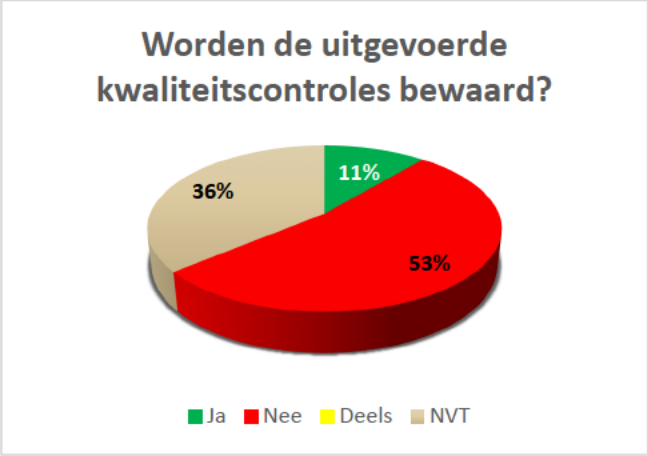

*Afbeelding 3.7.3.Worden gebruikers geattendeerd op kwaliteitsafwijkingen*

### 3.7.4 Rapport over de kwaliteit van gegevens

Een onderbelicht aspect is het rapporteren over de kwaliteit van gegevens. Er kan bijvoorbeeld gekeken worden naar de kwaliteit van invoer en op basis daarvan bijsturen. Een consequentie is wel dat er periodiek rapporten gemaakt worden over de kwaliteit van gegevens. Uit de 0-metingen blijkt dat dit niet vaak is gebeurd, omdat de prioriteit i.v.m. capaciteit aan andere functionaliteiten heen is gegaan. Het meest opvallende resultaat is dat als er een kwaliteitscontrole is gedaan dat deze niet bewaard wordt.




*Afbeelding 3.7.4a.Kan er een rapport over de kwaliteit van gegevens worden samengesteld?*




*Afbeelding 3.7.4b Worden de uitgevoerde kwaliteitscontroles bewaard?*

## 3.8 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.

Tijdens de 0-metingen is er extra aandacht gegeven aan de manier waarop gegevens worden verwijderd en/of vernietigd (Wpg-verbetermaatregelen 6.1, 6.2, 6.3 en 6.4).

### 3.8.1 Verschil tussen verwijderen en vernietigen

Bij de 0-meting is na voren gekomen dat het verschil tussen verwijderen en vernietigen niet altijd duidelijk is. Onder **verwijderen** wordt verstaan het buiten de operationele verwerking plaatsen van politiegegevens[12]. Het gaat om een gebruiksbeperking; de gegevens zijn wel beschikbaar, maar niet meer voor de dagelijkse taak. De meest duidelijke manier hierin is het poortwachter construct. Verwijderde gegevens kunnen nog wel beschikbaar gesteld worden, maar alleen als een poortwachter heeft beoordeeld of aan de specifieke voorwaarden is voldaan. Onder **vernietigen** wordt verstaan het onherstelbaar verwijderen van politiegegevens.

De helft van de onderzochte applicaties geven aan dat er zowel verwijderd als vernietigd kan worden. Echter bij het verwijderen en vernietigen verwijzen er veel automatisch naar de bronsystemen (BVH en Summit). Als daar een verzoek tot verwijdering of vernietiging komt, dan wordt dit gevolgd. Het automatisch verwijderen bij BVH op grond van artikel 8 (Wpg) gebeurt nu wel. Echter het vernietigen is technisch als verwerking wel mogelijk, maar wordt op dit moment niet gedaan binnen BVH en Summit.

| Applicatie | Versie[13] | Verwijderen | Vernietigen | Applicatie | Versie | Verwijderen | Vernietigen |
|---|---|---|---|---|---|---|---|
| Agora | 1.0 | X | X | PSH-VM | 1.0 | X | |
| AVR | 1.0 | X | X | BVH | 2.0 | X | |
| BVI-Blueview 4.0 | 1.0 | X | X | SMC | 2.0 | X | |
| BVID 2.0 | 1.0 | X | X | HAVANK | 1.0 | | X |
| FCM | 1.0 | X | X | Internet aangifte | 1.0 | | X |
| LJP | 1.0 | X | X | PSH-V | 1.0 | | X |
| LSV | 1.0 | X | X | Servicemodule | 1.0 | | X |
| Summ-IT | 1.0 | X | X | ZUIS | 1.0 | | X |
| Amazone | 2.0 | X | X | Hansken | 2.0 | | X |
| ANPR | 2.0 | X | X | Personenserver | 2.0 | | X |
| BOSZ | 2.0 | X | X | SBV | 2.0 | | X |
| DCS | 2.0 | X | X | Verificatiemodule | 1.0 | | X |
| I-Base | 2.0 | X | X | | | | |
| Kantoorautomatisering | 2.0 | X | X | BVI-IB | 1.0 | | |
| Mappen standaard | 2.0 | X | X | MEOS | 1.0 | | |
| PSH-TM / Digibon | 2.0 | X | X | TRIS | 1.0 | | |
| Raffinaderij | 2.0 | X | X | BlueSpotMonitor | 2.0 | | |
| VROS | 2.0 | X | X | Orion | 2.0 | | |

*Tabel 3.8.1.Highrisk applicaties en de toepassing van verwijderen en vernietigen*

[12] Persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak
[13] Op welke versie van het uitvoeringskader PSbD de meting is gebaseerd

### 3.8.2 Vernietigen in relatie tot een back-up

Tijdens de 0-metingen is naar voren gekomen dat bij het vernietigen van politiegegevens geen rekening wordt gehouden met een back-up. Wanneer nadat politiegegevens zijn 'vernietigd' er een back-up teruggeplaatst wordt, dan zijn de (verwijderde) politiegegevens weer beschikbaar. Er moet dus bij het vernietigen rekening worden gehouden met de retentietijd[14] van een back-up. De retentietijd moet worden opgeteld bij het moment dat een politiegegeven vernietigd wordt. Als er in die retentietijd geen back-up is teruggezet, dan is het politiegegeven vernietigd. Indien er wel een back-up is teruggezet, dan moet er een (automatische) procedure zijn dat eerst de 'vernietigde gegevens' in die periode weggehaald worden voordat de gegevens wordt vrijgegeven.

### 3.8.3 Generieke selectielijst (artikel 14) & DUTO

Zowel de generieke selectielijst als de DUTO (Duurzame Toegankelijkheid Overheidsinformatie) waren veelal onbekend bij de betrokkenen van de 0-metingen. Tijdens de 0-metingen is hier direct op ingehaakt door DIV (Documentaire Informatie Voorziening) te raadplegen en te vragen of de betrokkenen van de applicaties contact konden opnemen met DIV om een duidelijkere uitleg te kunnen krijgen waaraan voldaan moet worden. Om desondanks een duidelijk antwoord te krijgen op de vraag of de highriskapplicatie zou voldoen aan de generieke selectielijst hebben we artikel 14 (bewaartermijnen) van de Wpg als leidraad genomen in plaats van een harde eis.

[14] De hoeveelheid dagen dat het mogelijk is om met een backup terug te gaan in de tijd

## 3.9 Informatiebeveiliging

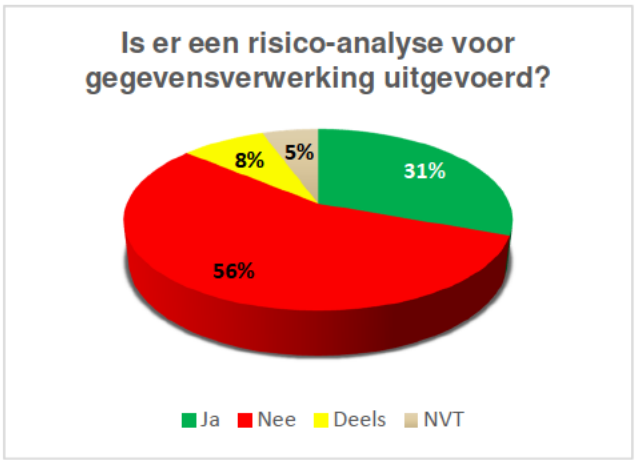
"*De informatievoorziening wordt beveiligd met een adequaat stelsel van maatregelen op basis van risicobeheersing*"

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

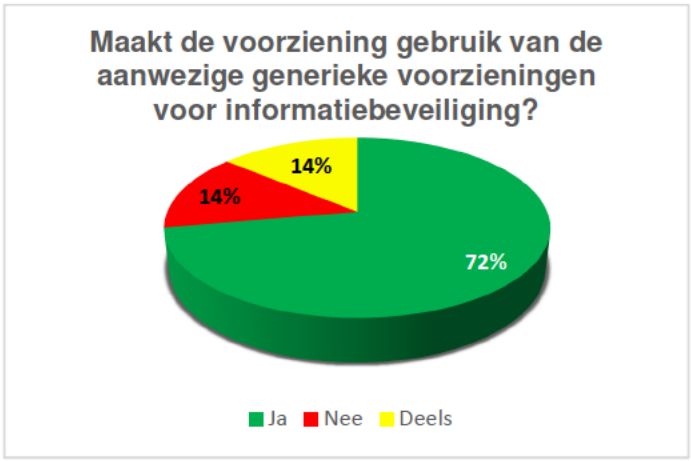
Wat tijdens de 0-metingen zichtbaar werd is, dat bij de betrokkenen niet bewust aandacht is voor informatiebeveiliging binnen de applicatie. Daarbij moet wel worden meegenomen dat de norm op informatiebeveiliging bij de politie erg hoog is. Het gaat dit niet om de informatiebeveiliging naar buiten toe, maar om de informatiebeveiliging die specifiek gericht is op de highrisk applicaties zelf en het maken van een risicoanalyse.

### 3.9.1 Risicoanalyse

Uit de resultaten, van de applicaties die een volwassenheidsniveau 1 scoren, is op te maken dat er bij 56% (20/36) geen risicoanalyse voor gegevensverwerking is uitgevoerd of enige vorm van risicoanalyse op gebied van informatiebeveiliging. Hierbij is uitgegaan van een risicoanalyse die binnen de afgelopen 5 jaar is uitgevoerd. Zoals eerder genoemd staat deze informatiebeveiliging los van de generieke voorzieningen die worden aangeboden t.b.v. informatiebeveiliging. In 72% (26/36) van de applicaties maakt gebruik van de aanwezige generieke informatiebeveiliging.



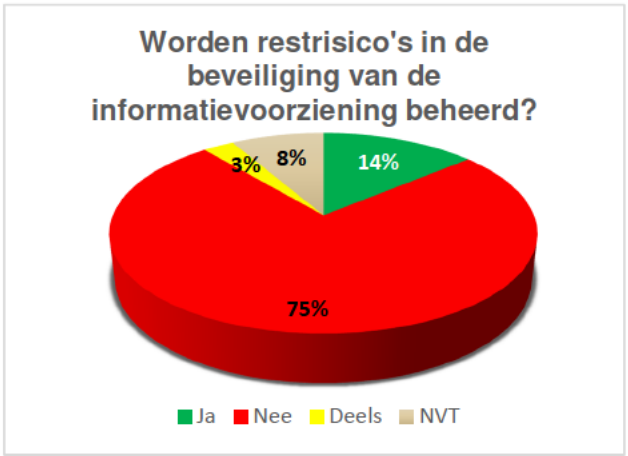

*Afbeelding 3.9.1a. Is er een risico-analyse voor gegevens verwerking uitgevoerd?*




*Afbeelding 3.9.1b.Maakt de voorziening gebruik van de aanwezige generieke voorzieningen voor informatiebeveiliging?*

### 3.9.2 Restrisico's

Wat misschien nog wel belangrijker is om in beeld te hebben zijn de restrisico's binnen de applicatie. Risico waarvan bekend is dat ze er zijn, maar waar bewust voor gekozen is om daar op een bepaald moment in de tijd niets mee te doen. Bij 75% (27/36) van de highrisk applicaties worden de restrisico's binnen de applicatie niet periodiek bijgehouden.




*Afbeelding 3.9.2 Worden restrisico's in de beveiliging van de informatievoorziening beheerd?*

## 3.10 Privacy by Default / Voldoen aan de wet

"*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 minst inbreuk makende stand te zetten.

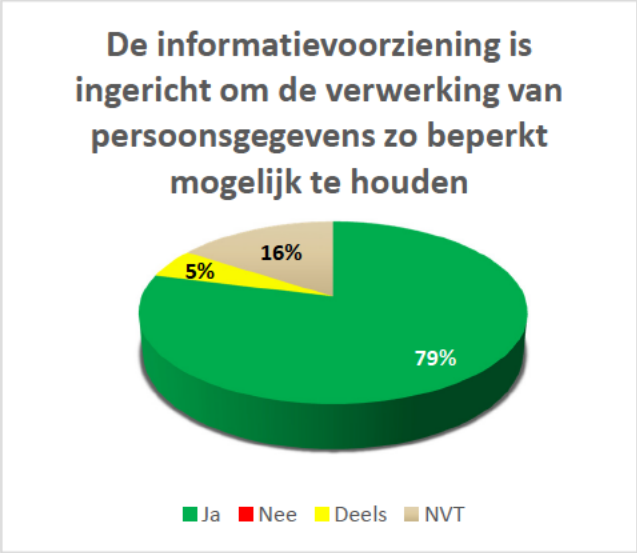
Alle vragen omtrent 'Voldoen aan de wet' zijn op "niet van toepassing" gezet aangezien die in versie 2 van het uitvoeringskader vervangen is voor het principe 'Privacy by default'. Het onderdeel 'Voldoen aan de wet' was al verdeeld over de andere principes. Het meten van de vragen omtrent 'Privacy by default' was lastig aangezien al snel duidelijk werd dat de privacy-kennis niet overal op een gelijk niveau is. Om een goed beeld te krijgen van de manier van verwerking van persoonsgegevens is een diepgaander onderzoek nodig.

### 3.10.1 Verwerking van persoonsgegevens zo beperkt mogelijk houden

Bij de 0-metingen is vooral aangegeven dat binnen de applicaties er alles aangedaan wordt om gegevens af te schermen voor gebruikers die er geen toegang toe hebben (autorisatie). Echter een belangrijke vraag die daaruit voortvloeit, is of er alleen gegevens getoond worden die noodzakelijk zijn voor het doel van de verwerking.

- Hoeveelheid verzamelde gegevens
- De mate waarin deze worden verwerkt
- De termijn waarvoor deze worden opgeslagen
- De toegankelijkheid

Ondanks de positieve score van 79% (15/21), wat aangeeft dat de informatievoorziening daadwerkelijk is ingericht om de verwerking van persoonsgegevens zo beperkt mogelijk te houden, is dit een onderdeel wat vele manieren van doorvragen vereist op de uitvoerende (executieve) partij. Hier moet bij nieuwe ontwikkelingen/vernieuwingen op een andere manier aandacht voor gevraagd moeten worden.




*Afbeelding 3.10.1 De informatievoorziening is ingericht om de verwerking van persoonsgegevens zo beperkt mogelijk te houden*

## 3.11 Toepassen standaarden

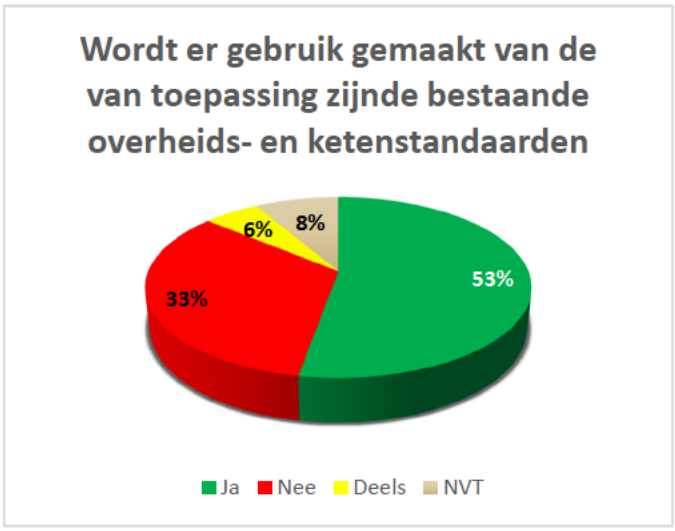
"*Bij de gegevensverwerking wordt gebruik gemaakt van bestaande overheids- en ketenstandaarden*"

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 moeten er afspraken gemaakt worden over koppelvlakken bij gegevensuitwisseling tussen externe partijen.

Het toepassen van standaarden is tijdens de 0-meting ruim aangehaald. Veel van de highrisk applicaties hadden niet direct een overheids- en ketenstandaard, maar maakte wel degelijk gebruik van standaarden. Dit is in het onderzoek meegenomen.

### 3.11.1 Overheids- en ketenstandaarden

Meer dan de helft van de highrisk applicaties maakt gebruik van overheids- en ketenstandaarden. De 33% (12/36) waarbij nee of deels werd aangegeven was het vooral een onbekende zoektocht of hier afspraken over gemaakt zijn. Als het onduidelijk is hebben wij dit beoordeeld als een actiepunt dat onderzocht dient te worden.




*Afbeelding 3.11.1 Wordt er gebruik gemaakt van de van toepassing zijnde bestaande overheids- en ketenstandaarden*

## 3.12 Verantwoordlijkheden belegd

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

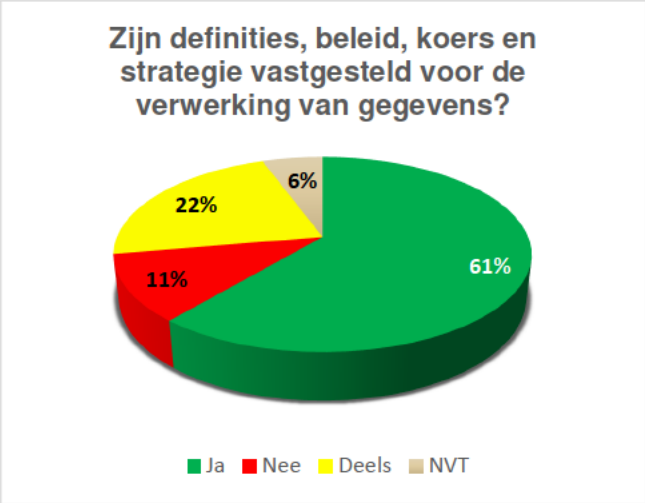
Het is van belang dat de verantwoordelijkheden voor gegevensverwerking belegd zijn om de rechtmatigheid en de kwaliteit van de gegevensverwerking te kunnen waarborgen.

Niet alleen tijdens de 0-metingen, maar ook achteraf blijkt dat het binnen de politie lastig is vast te stellen wie voor welke afzonderlijke verwerkingen verantwoordelijk is. Dit was dan ook de reden om in het kader van de 0-metingen te kiezen voor het beleggen van verantwoordelijkheid op basis van applicaties (zie paragraaf 1.2 Structuur)

### 3.12.1 Definities, beleid, koers en strategie

Tijdens de 0-metingen kwam na voren dat het beantwoorden van vragen over beleid, koers en strategie toch lastig is vanuit de hiërarchische structuur van de organisatie.


*Afbeelding 3.12.1a. Is de beleidsverantwoordelijke voor de gegevens die verwerkt worden met de informatievoorziening bekend?*




*Afbeelding 3.12.1b. Zijn definities, beleid, koers en strategie vastgesteld voor de verwerking van gegevens?*

# 4 Aandachtspunten

Met het uitvoeren van de 0-metingen zijn er actiepunten onder de aandacht gekomen die niet binnen de 0-meting vielen, maar toch vermeldenswaardig zijn. In dit hoofdstuk staan de belangrijkste aandachtspunten beschreven die tijdens 0-meting-sessies naar voren zijn gekomen, maar niet gekoppeld waren aan een vraag uit de 0-meting.

## 4.1 Doelbinding

Ondanks dat de vragen over doelbinding over het algemeen positief ingevuld zijn moet het strakker in de gaten gehouden worden. Bij verschillende applicaties is doelbinding onderwerp van gesprek, waarbij verbeteringen noodzakelijk zijn. Hieronder twee voorbeelden die direct opgepakt moeten worden.

**Agora**

- *Zorg dat het mogelijk is om de doelbinding van de verwerkte gegevens (binnen de pagina's) te controleren, ondanks de procedurele afspraken (art 8) die zijn voorgelegd aan de beheerders van Agora pagina's.*

**Internetaangifte**

- *(**Wet**): Op dit moment worden IP-adressen van burgers 30 dagen opgeslagen. De vraag is of er een doel is gesteld om de IP-adressen van de burgers op te slaan. Indien er geen doel is dan mogen de IP-adressen niet worden opgeslagen en dient dat worden stopgezet.*

## 4.2 Registratiesysteem

Hieronder een aantal voorbeelden van actiepunten m.b.t. het gebruik van een registratiesysteem.

**Agora**

- *Agora is niet bedoeld als registratiesysteem en er wordt daardoor niet of beperkt gecontroleerd of gegevens al bestaan. Dat is verklaarbaar, maar het proces wat wel en niet kan met Agora mbt politiegegevens moet actiever in de gaten worden gehouden (hiervoor zijn meer middelen nodig).*

**iBase**

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

**Live Journaal Politie**

- *Tijdens de gesprekken is naar voren gekomen dat in sommige gevallen LJP gebruikt wordt als bron-systeem (eerste en soms enige registratiesysteem). Dit zou te allen tijde voorkomen dienen te worden.*

## 4.3 Gegevens buiten het systeem

Om controle te houden op de rechtmatigheid en juistheid van gegevens is het van belang dat gegevens niet onnodig buiten de betreffende applicatie gezet worden. Hieronder zijn drie voorbeelden genoemd van situaties die spoedige aanpassing verlangen. Daarnaast tijdens de 0-meting is ook gebleken dat

**AVR**

- *Tijdens de 0-meting is aangegeven dat veel verhoren op USB-stick of DVD gezet zijn. Door het plaatsen van gegevens buiten het systeem is het niet mogelijk om de zorgvuldigheid en rechtmatigheid te waarborgen. Zorg dat er een manier komt zodat een verhoor niet meer buiten het systeem beschikbaar hoeft te zijn.*

**BlueSpotMonitor**

- *Onderzoek of het exporteren van gegevens naar Excel altijd een doel heeft en borg zo nodig de maatregelen. Als de analyse ook binnen de BSM uitgevoerd kan worden dan is een export van persoonsgegevens een onnodig risico op privacy schendingen.*

**Servicemodule**

- *Tijdens de 0-meting is aangegeven dat een terugbelbericht en/of reguliere meldingen via de email verzonden wordt aan de desbetreffende politiemedewerker. Hier staan persoonsgegevens in die niet via de mail verstuurd zouden mogen worden. Er werd al aangegeven dat dit opgelost kan worden door in de mail alleen een hyperlink mee te geven met een verwijzing naar de applicatie. Zorg dat gegevens altijd binnen de voorziening blijft.*

## 4.4 Kennis en kunde

Tijdens de 0-metingen is er veel gesproken over de kennis op het gebied van privacy. Binnen de politie wordt er hard gewerkt om dit op niveau te krijgen. Echter uit de 0-metingen bleek ook [redacted] Hieronder staan een aantal voorbeelden genoemd.

**DCS**

- *Er is een te brede gebruikersgroep binnen DCS wat een risico kan zijn voor onjuist gebruik. Zorg voor een specifieke opleiding*

**LJP**

- *Ontwikkeling van LJP zou niet onder één persoon moeten vallen*

**Mappenstandaard**

- *Er is beperkte kennis bij blauw over het gebruik van de mappen. Hierdoor is er een groot risico dat Mappenstandaard verkeerd gebruikt gaat worden.*

**VROS**

- *Voor VROS is er geen technische kennis aanwezig, waardoor bij een kleine storing het systeem (onnodig) lang niet beschikbaar is. Zorg dat er gekeken wordt naar de mogelijkheden om dit te verbeteren.*

**ZUIS**

- *Het is het zorgelijk dat het beheer van ZUIS (qua kennis) vooral in handen is van één persoon* [redacted]

# 5 Conclusies

De 0-metingen zijn uitgevoerd om antwoord te kunnen geven op de onderzoeksvraag: '***In hoeverre zijn de vastgestelde highrisk applicaties van de politie PSbD compliant?***' Er kan geconcludeerd worden dat de highrisk applicaties van de politie onvoldoende PSbD compliant zijn. Toch kan er aan de hand van de 0-metingen niet alleen negatieve conclusies gevormd worden. Hieronder is er een verdeling gemaakt tussen positieve en negatieve conclusies.

## 5.1 Negatief

De 0-meting heeft voor veel applicaties een negatieve uitkomst en dat is terug te zien uit de gemiddelden van alle 0-metingen. Bij bijna de helft (46% wet en 45% beleid) van de criteria zijn actiepunten nodig om verbetering aan te brengen.

### 5.1.1 Wpg compliance is onvoldoende

Uit de 0-metingen is gebleken dat er teveel applicaties zijn die niet voldoen aan de Wpg-compliance. Het is duidelijk dat 89% (32 van de 36 applicaties) van de highrisk applicaties niet volledig voldoet aan de wet, waarvan 3 applicaties (8%) ver onder de grens scoren (volwassenheidsniveau 0). Het is zorgelijk maar moet wel in perspectief gezien worden. Van de 32 applicaties zijn er 10 applicaties (31%) die met een paar aanpassingen (max. 3 aanpassingen) direct kunnen voldoen aan de wetgeving (Wpg).

### 5.1.2 Borging PSbD niet geregeld

Bij veel betrokkenen van de 0-meting is de privacy kennis nog laag. Na een uitleg door middel van praktijkvoorbeelden wordt vaak wel ingezien dat er verbeteringen nodig zijn.

### 5.1.3 Beleidskaders zijn vaak onbekend,

Het meest opvallende punt uit de 0-metingen is dat het beleid vaak onbekend is.

### 5.1.4 Onvoldoende communicatie

Als de privacy kennis niet hoog is dan wordt er verwacht dat de kennis indien nodig opgehaald moet worden bij de experts op het gebied van privacy. [redacted]. Er moet op basis van de rol (functie) duidelijk moeten zijn wat er wordt verwacht op het gebied van PSbD.

### 5.1.5 Artikel 13

Uit de 0-meting blijkt dat de artikel 13 protocollen geactualiseerd moeten worden. Dat heeft geleid tot aandachtspunten in de rapporten. Een aandachtspunt heeft geen invloed op de score. Voor alle protocollen geldt dat het actualiseren van dat protocol er toe gaat leiden dat er nieuwe actiepunten en lagere scores komen.

Het HKS protocol is gericht op de vervallen applicatie HKS en is tevens zo gedateerd dat het niet reëel is om te toetsen of aan het protocol wordt voldaan. Hierdoor zijn de betreffende criteria als “Niet van toepassing” beoordeeld. De verouderde protocollen voor FO, FCM en VROS zijn wel meegenomen in de meting.

## 5.2 Positief

Naast de negatieve punten die genoemd zijn heeft de 0-meting ook voor positieve punten gezorgd. Een 100% score halen is niet eenvoudig, maar na de 0-meting is wel duidelijk geworden dat er gedrevenheid zit om de genoemde actiepunten op te lossen te verklaren. Ondanks de negatieve hoofdconclusie is er veel gedrevenheid om aan de eisen te kunnen voldoen. Hieronder staan de positieve conclusies van 0-meting omschreven.

### 5.2.1 Privacy in beeld

Meten is weten. Door de 0-meting uit te voeren is er een goed beeld van de actuele status van de betreffende highrisk applicaties. Ongeacht het resultaat is in het overzicht duidelijk te zien hoe de highrisk applicaties er in het geheel voor staan, maar ook afzonderlijk. Waarbij per principe is te zien wat goed scoort en wat minder goed scoort, zodat ook meteen duidelijk is bij welke principes aandacht nodig is. Het onderscheid tussen wetgeving en beleid zorgt voor een gerichte prioritering.

### 5.2.2 Specifieke aandacht voor de applicaties

Naast de 0-meting (90 criteria) is er gelegenheid om aandachtspunten te benoemen die niet direct gerelateerd kunnen worden op de 0-meting, maar wel belangrijk zijn om te benoemen. Het zijn punten die vaak wel in beeld waren, maar niet voldoende aandacht kregen. Door het rapport van de 0-meting bij de portefeuillehouder neer te leggen zijn de aandachtspunten (opnieuw) aangekaart. Een voorbeeld hiervan is . Aandachtspunten die buiten de 0-meting zijn waargenomen, maar wat wel een reactie vereist om dit te verbeteren.

### 5.2.3 Bewustwording

. De kennis die is opgedaan bij de 0-meting zorgt voor een betere aansluiting op de (toekomstige) opleidingen die gaan over privacy.

### 5.2.4 Evaluatie

Er zijn door de 0-meting twee manieren van evaluatie. De eerste is door de betrokkenen zelf door in het rapport opnieuw naar de adviespunten te kijken . De tweede manier is de evaluatie aan het einde van het jaar waarin om duidelijkheid wordt gevraagd, op de openstaande actiepunten, ’.

### 5.2.5 Rapport een middel tot beweging

# 6 Vervolgstappen

Welke vervolgstappen moeten er genomen worden om de beschreven actiepunten te verbeteren en ervoor zorgen dat de highrisk applicaties PSbD compliant zijn. In dit hoofdstuk staan de vervolgstappen beschreven waar als eerste naar gekeken moet worden.

## 6.1 Bewustwording en expertise

Zoals eerder genoemd tijdens de conclusie zijn de eerste stappen gezet op gebied van bewustwording van privacy.

## 6.2 Evalueren status actiepunten (Q4 2019)

Aan het einde van het jaar (Q4 2019) gaat er een evaluatie plaatsvinden op de actiepunten die bij de highrisk applicaties open staan.

### 6.2.1 Afspraak maken

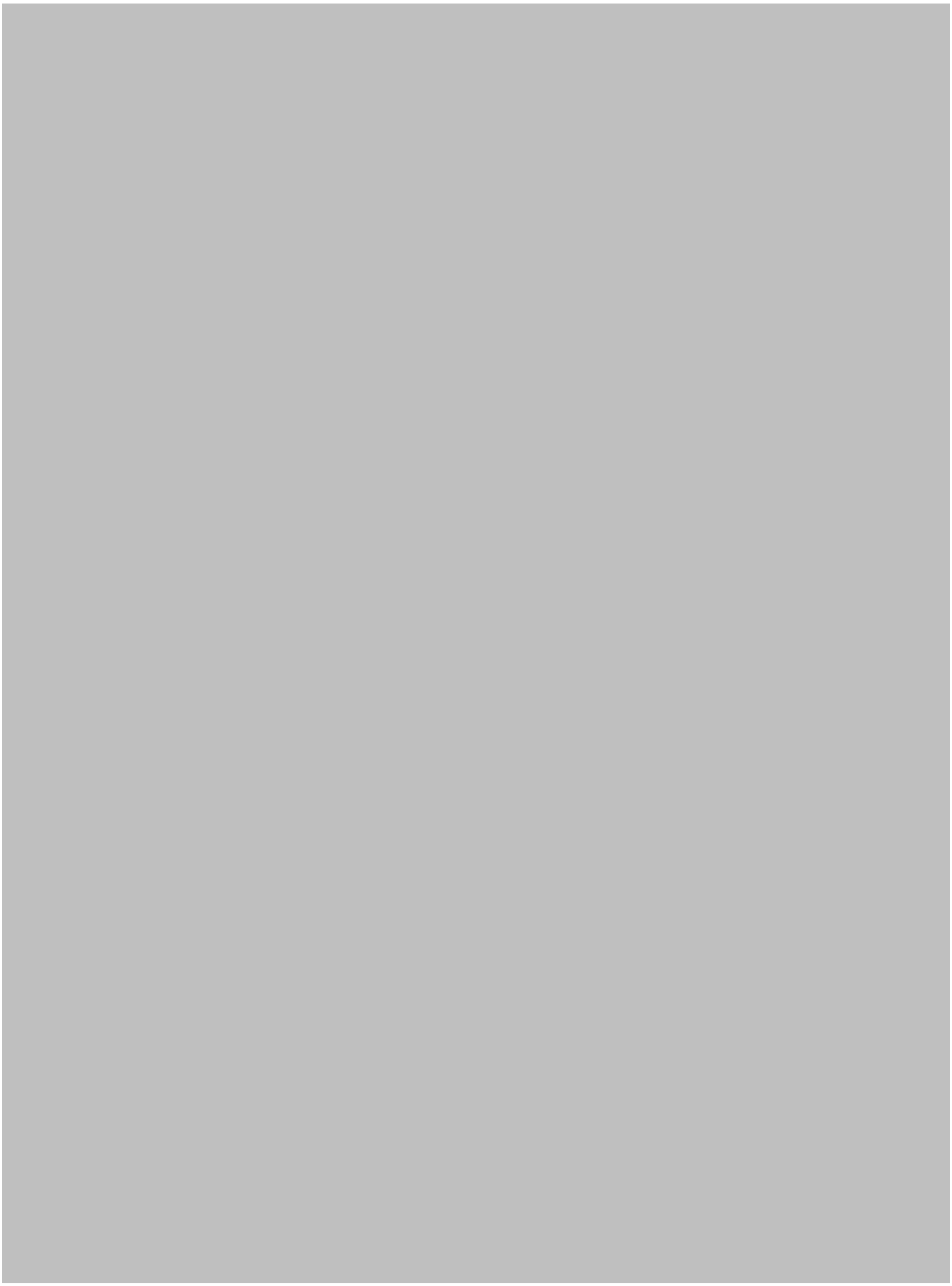
### 6.2.2 Escaleren

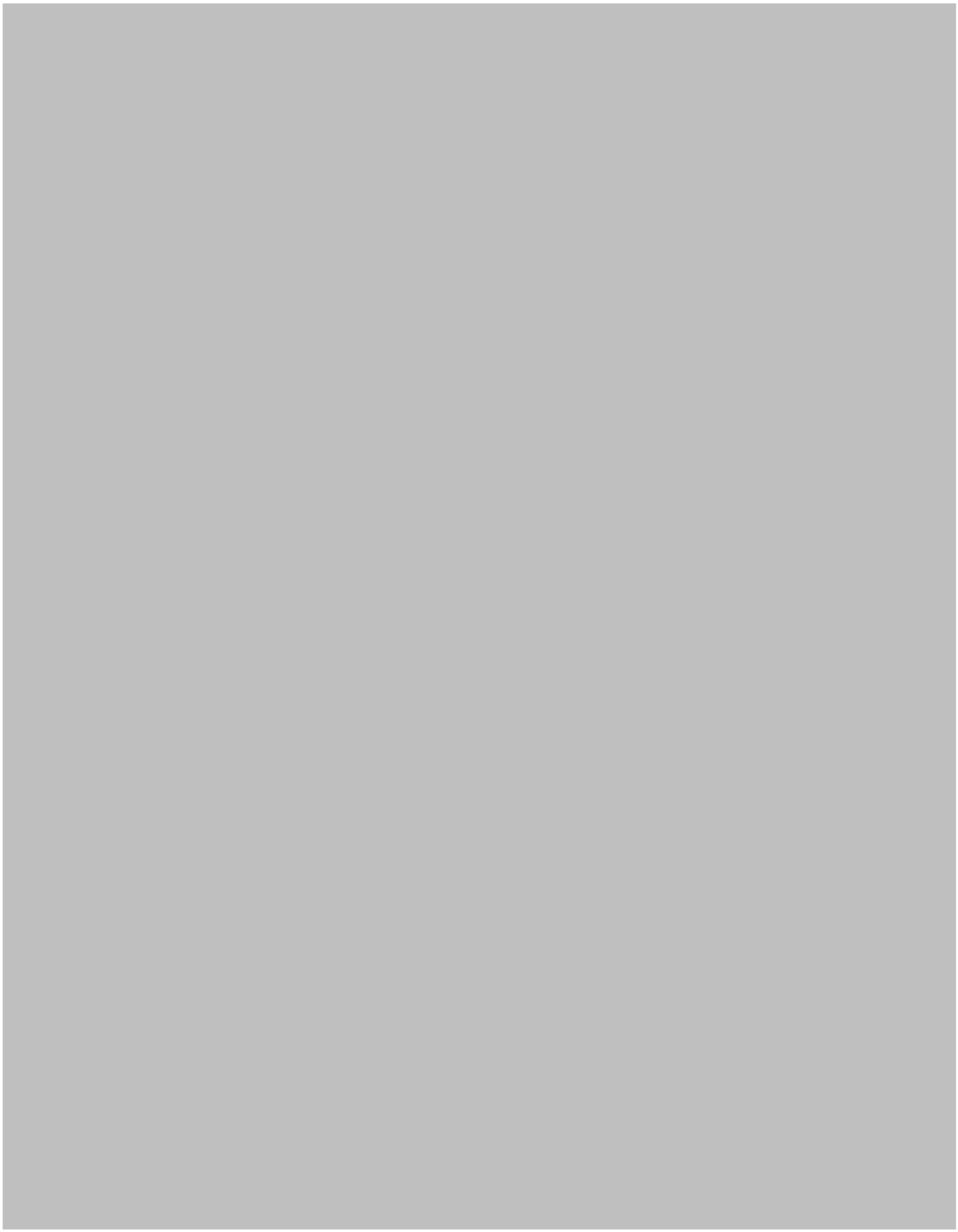
### 6.2.3 Terugkoppeling naar de stuurgroep

## 6.3 Borging in de organisatie

## 6.4 Borging doormiddel van PSbD-rol

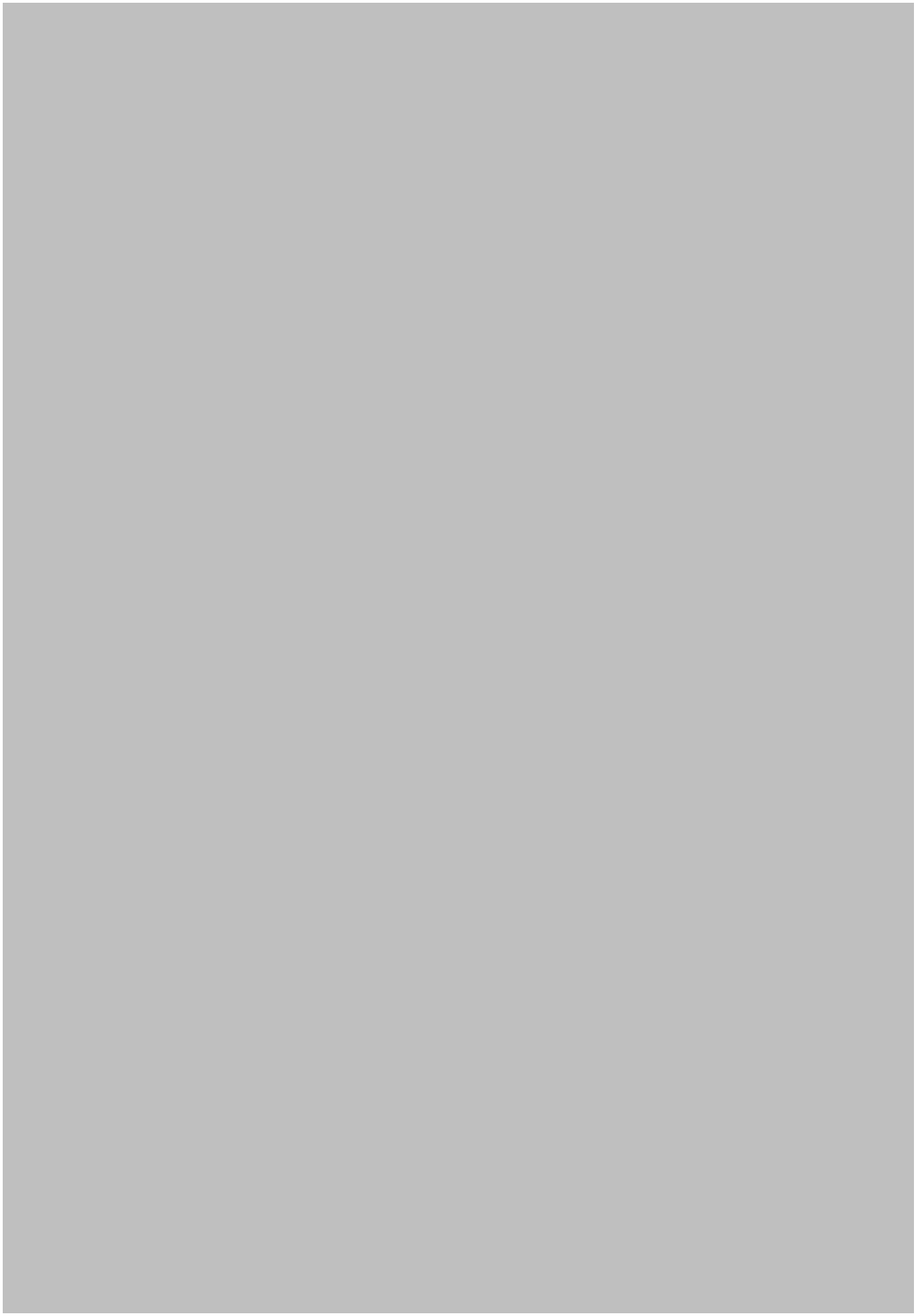
# Bijlage 1: Reflectie





# Bijlage 2: Maatregelen Wpg & IB-verbeterprogramma

De uitvoer van de 0-metingen is zoals eerder aangegeven een onderdeel van het Wpg & IB-verbeterprogramma. In dit hoofdstuk staan de verbetermaatregelen die een directe verbinding hadden met de 0-metingen en het resultaat op de betreffende maatregel.

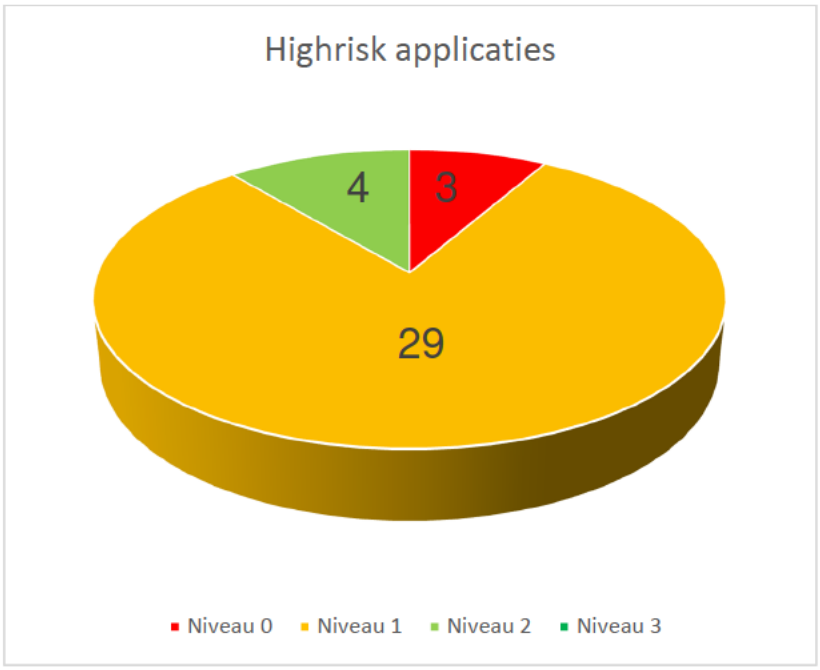


# Bijlage 3: Resultaten

Om een transparant beeld te geven hoe het rapport mede is opgesteld staan in dit hoofdstuk de scores en berekeningen per principe en per applicatie beschreven.

Van alle potentiele highrisk applicaties scoren:

- 3 applicaties (8%) niveau 0
- 29 applicaties (81%) niveau 1
- 4 applicaties (11%) niveau 2
- 0 applicaties (0%) niveau 3




*Afbeelding bijlage 3a: Volwassenheidsniveau highrisk applicaties*

## Score volwassenheidsniveau

In de tabel hieronder staan alle highrisk applicaties met het volwassenheidsniveau wat in totaal en per principe is behaald.

| Volwassenheids-niveau | Versie | Totaal | Eenmalige vastlegging (Z) | PDCA-cyclus (M) | Doelbinding (Z) | Verantwoording (Z) | Autorisatie (Z) | Metagegevens (Z) | Kwaliteitszorg (Z) | Bewaren en vernietigen (Z) | Informatiebeveiliging (Z) | Voldoen aan de (V1.0) wet (Z) | Privacy by default (v2.0) (Z) | Toepassen standaarden (L) | Verantwoordelijkheden belegd (Z) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Agora | 1.0 | 1 | 3 | 1 | 3 | 2 | 0 | 2 | 1 | 0 | 2 | NVT | - | 3 | 2 |
| 2. Amazone | 2.0 | 1 | 2 | 2 | 0 | 1 | 1 | 1 | 3 | 0 | 0 | - | 3 | 3 | 2 |
| 3. ANPR | 2.0 | 1 | 1 | 0 | 0 | 2 | 1 | 1 | 2 | 3 | 0 | - | 2 | 3 | 2 |
| 4. AVR | 1.0 | 0 | 0 | 1 | 2 | 2 | 0 | 1 | 2 | 0 | 2 | NVT | - | 0 | 1 |
| 5. BOSZ | 2.0 | 1 | 3 | 2 | 3 | 2 | 1 | 2 | 2 | 3 | 3 | - | 3 | 2 | 2 |
| 6. BVH | 2.0 | 1 | 1 | 2 | 0 | 2 | 1 | 1 | 2 | 0 | 3 | - | 2 | 2 | 2 |
| 7. BVI-BlueSpotMonitor | 2.0 | 1 | 3 | 3 | 0 | 1 | 1 | 2 | 3 | 3 | 0 | - | 1 | 0 | 2 |
| 8. BVI-Blueview 4.0 | 1.0 | 2 | NVT | 1 | 3 | 3 | 3 | 2 | 2 | 3 | 3 | NVT | - | 3 | 3 |
| 9. BVID 2.0 | 1.0 | 2 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | NVT | 2 | NVT | - | 3 | 3 |
| 10. BVI-IB | 1.0 | 1 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | NVT | 0 | NVT | - | 3 | 3 |
| 12. DCS | 2.0 | 1 | 0 | 0 | 1 | 1 | 1 | 2 | 1 | 0 | 0 | - | 3 | 0 | 2 |
| 13. FCM | 1.0 | 1 | 1 | 3 | 1 | 0 | 2 | 0 | 2 | 2 | 0 | NVT | - | 0 | 3 |
| 14. Hansken | 2.0 | 1 | NVT | 0 | 3 | 2 | 0 | 2 | 3 | 3 | 0 | - | 3 | 3 | 3 |
| 15. HAVANK | 1.0 | 1 | 3 | 2 | 3 | 2 | 2 | 2 | 3 | 3 | 1 | NVT | - | 3 | 3 |
| 16. I-Base | 2.0 | 1 | 3 | 0 | 3 | 2 | 1 | 3 | 3 | 0 | 0 | - | 3 | NVT | 3 |
| 17. Internet Aangifte | 1.0 | 1 | 3 | 2 | 3 | 0 | 2 | 0 | 2 | 2 | 1 | NVT | - | 3 | 3 |
| 18. Kantoorautomatisering | 2.0 | 0 | NVT | 0 | 3 | 0 | NVT | NVT | NVT | NVT | 3 | - | NVT | NVT | 2 |
| 19. Live Journaal Politie | 1.0 | 1 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 0 | NVT | - | 0 | 2 |
| 20. LSV | 1.0 | 1 | 2 | 1 | 3 | 2 | 2 | 2 | 2 | 0 | 0 | NVT | - | 0 | 3 |
| 21. Mappen standaard | 2.0 | 1 | 3 | 1 | 3 | 2 | 0 | 3 | 3 | 0 | 0 | - | 3 | 0 | 3 |
| 22. MEOS | 1.0 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | NVT | 3 | NVT | - | 3 | 3 |
| 23. Orion | 2.0 | 2 | NVT | 2 | NVT | NVT | NVT | NVT | NVT | NVT | 3 | - | NVT | 2 | 3 |
| 24. Personenserver | 2.0 | 1 | 3 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | - | 2 | 3 | 0 |
| 25. Digibon/PDB | 2.0 | 1 | 2 | 2 | 3 | 2 | 0 | 0 | 2 | 0 | 2 | - | 2 | 3 | 3 |
| 26. PSH-V | 1.0 | 1 | 1 | 0 | 0 | 2 | 2 | 2 | 1 | 0 | 0 | NVT | - | 2 | 2 |
| 27. PSH-VM | 1.0 | 1 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | NVT | - | 0 | 2 |
| 28. Raffinaderij | 2.0 | 1 | 2 | 2 | 1 | 2 | 2 | 2 | 3 | 0 | 2 | - | 2 | NVT | 2 |
| 29. SBV | 2.0 | 1 | NVT | 2 | 3 | 2 | 1 | 3 | 3 | 3 | 0 | - | 3 | 3 | 3 |
| 30. Servicemodule | 1.0 | 1 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 0 | NVT | - | 0 | 2 |
| 31. SMC | 2.0 | 1 | 3 | 3 | 3 | 2 | 1 | 2 | 3 | NVT | 0 | - | 3 | 3 | 3 |
| 32. SUMMIT | 1.0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 0 | NVT | - | 0 | 2 |
| 33. TRIS | 1.0 | 0 | 0 | 2 | 1 | 2 | 1 | 0 | 2 | 0 | 0 | NVT | - | 2 | 3 |
| 34. Verificatiemodule | 2.0 | 1 | 0 | 0 | 1 | 2 | 0 | 0 | 3 | 3 | 0 | 2 | - | 2 | 1 |
| 35. VROS | 2.0 | 1 | NVT | 0 | 3 | 2 | 0 | 2 | 1 | 3 | 0 | - | 3 | 3 | 2 |
| 36. ZUIS | 1.0 | 1 | 0 | 2 | 1 | 2 | 1 | 0 | 1 | 2 | 0 | NVT | - | 2 | 2 |

*Tabel bijlage 3b: Score volwassenheidsniveau's highrisk applicaties*

## Score wettelijke criteria

In de tabel hieronder staan alle highrisk applicaties met de score (%) die totaal en per principe behaald is op wettelijke criteria.

| Wet* | Versie | Totaal | Eenmalige vastlegging (Z) | PDCA-cyclus (M) | Doelbinding (Z) | Verantwoording (Z) | Autorisatie (Z) | Metagegevens (Z) | Bewaren en vernietigen (Z) | Informatiebeveiliging (Z) | Voldoen aan de (V1.0) wet (Z) | Privacy by default (V2.0) (Z) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Agora | 1.0 | 64% | 100% | NVT | 100% | 100% | 0% | 100% | 0% | 100% | NVT | - |
| 2. Amazone | 2.0 | 42% | 100% | NVT | 0% | 75% | 83% | 50% | 17% | 0% | - | 100% |
| 3. ANPR | 2.0 | 46% | 50% | NVT | 0% | 100% | 50% | 50% | 100% | 0% | - | 100% |
| 4. AVR | 1.0 | 27% | 0% | NVT | NVT | 100% | 0% | NVT | 0% | 100% | NVT | - |
| 5. BOSZ | 2.0 | 94% | NVT | NVT | NVT | 100% | 75% | NVT | 100% | 100% | - | 100% |
| 6. BVH | 2.0 | 53% | 75% | NVT | 0% | 100% | 75% | 50% | 20% | 100% | - | 100% |
| 7. BVI-BlueSpotMonitor | 2.0 | 46% | NVT | NVT | 33% | 50% | 50% | NVT | 100% | 0% | - | 50% |
| 8. BVI-Blueview 4.0 | 1.0 | 100% | NVT | NVT | 100% | 100% | 100% | 100% | 100% | 100% | NVT | - |
| 9. BVID 2.0 | 1.0 | 100% | 100% | NVT | 100% | 100% | 100% | NVT | NVT | 100% | NVT | - |
| 10. BVI-IB | 1.0 | 75% | 100% | NVT | 100% | 100% | 100% | NVT | NVT | 0% | NVT | - |
| 12. DCS | 2.0 | 41% | NVT | NVT | 50% | 75% | 67% | 100% | 0% | 0% | - | 100% |
| 13. FCM | 1.0 | 55% | 50% | NVT | 50% | 0% | 100% | NVT | 100% | 0% | NVT | - |
| 14. Hansken | 2.0 | 60% | NVT | 25% | 100% | 100% | 33% | NVT | 100% | 0% | - | 100% |
| 15. HAVANK | 1.0 | 93% | 100% | NVT | 100% | 100% | 100% | NVT | 100% | 50% | NVT | - |
| 16. I-Base | 2.0 | 61% | 100% | NVT | 100% | 100% | 50% | NVT | 25% | 0% | - | NVT |
| 17. Internet Aangifte | 1.0 | 87% | 100% | 100% | 100% | 0% | 100% | NVT | 100% | 75% | NVT | - |
| 18. Kantoorautomatisering | 2.0 | 25% | NVT | NVT | NVT | 25% | NVT | NVT | NVT | NVT | - | NVT |
| 19. Live Journaal Politie | 1.0 | 74% | 33% | NVT | 100% | 100% | 100% | 100% | 90% | 0% | NVT | - |
| 20. LSV | 1.0 | 64% | 100% | NVT | 100% | 100% | 100% | NVT | 33% | 0% | NVT | - |
| 21. Mappen standaard | 2.0 | 46% | NVT | NVT | 100% | 100% | 33% | NVT | 30% | 0% | - | 100% |
| 22. MEOS | 1.0 | 100% | 100% | NVT | 100% | 100% | NVT | NVT | NVT | 100% | NVT | - |
| 23. Orion | 2.0 | NVT | NVT | NVT | NVT | NVT | NVT | NVT | NVT | NVT | - | NVT |
| 24. Personenserver | 2.0 | 37% | 100% | 0% | 25% | 100% | 0% | NVT | 17% | 0% | - | 100% |
| 25. Digibon/PDB | 2.0 | 57% | 100% | NVT | 100% | 100% | 25% | 0% | 20% | 100% | - | 100% |
| 26. PSH-V | 1.0 | 40% | 67% | 0% | 0% | 100% | 100% | NVT | 0% | 0% | NVT | - |
| 27. PSH-VM | 1.0 | 81% | 100% | 0% | 100% | 100% | 100% | NVT | 100% | 0% | NVT | - |
| 28. Raffinaderij | 2.0 | 76% | NVT | 100% | 83% | 100% | 100% | 100% | 13% | 100% | - | 100% |
| 29. SBV | 2.0 | 73% | NVT | NVT | 100% | 100% | 50% | 100% | 100% | 0% | - | 100% |
| 30. Servicemodule | 1.0 | 58% | NVT | NVT | 100% | 100% | 100% | NVT | 50% | 0% | NVT | - |
| 31. SMC | 2.0 | 70% | NVT | NVT | 100% | 100% | 67% | 100% | NVT | 0% | - | 100% |
| 32. SUMMIT | 1.0 | 50% | 17% | NVT | 75% | 100% | 100% | NVT | 40% | 0% | NVT | - |
| 33. TRIS | 1.0 | 32% | 17% | NVT | 67% | 100% | 50% | NVT | 0% | 0% | NVT | - |
| 34. Verificatiemodule | 2.0 | 50% | 0% | NVT | 50% | 100% | 33% | NVT | 100% | 0% | - | 100% |
| 35. VROS | 2.0 | 64% | NVT | NVT | 100% | 100% | 0% | 100% | 100% | 0% | - | 100% |
| 36. ZUIS | 1.0 | 50% | 0% | NVT | 50% | 100% | 75% | NVT | 100% | 0% | NVT | - |

*Tabel bijlage 3c: Score wettelijke criteria highrisk applicaties*

*De principes 'Kwaliteitszorg', 'Toepassen standaarden' en 'Verantwoordelijkheden belegd' bevatten geen wetscriteria en staan daardoor niet vermeld in de tabel.

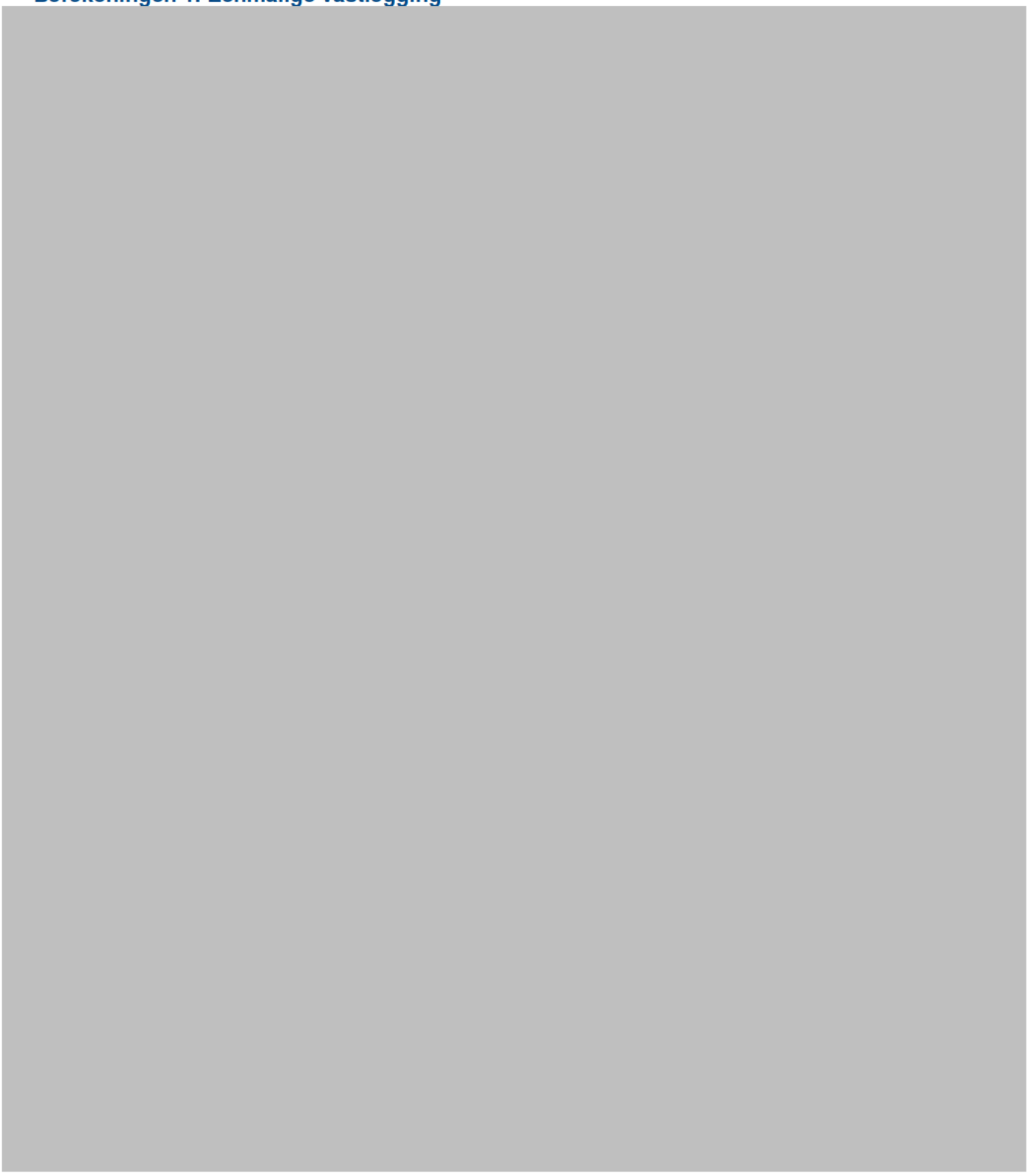
## Score beleidscriteria

In de tabel hieronder staan alle highrisk applicaties met de score (%) die totaal en per principe behaald is op beleidscriteria.

| Beleid | Versie | Totaal | Eenmalige vastlegging (Z) | PDCA-cyclus (M) | Doelbinding (Z) | Verantwoording (Z) | Autorisatie (Z) | Metagegevens (Z) | Kwaliteitszorg (Z) | Bewaren en vernietigen (Z) | Informatiebeveiliging (Z) | Voldoen aan de (V1.0) wet (Z) | Privacy by default (V2.0) (Z) | Toepassen standaarden (L) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Agora | 1.0 | 62% | 100% | 38% | 100% | 25% | 70% | 67% | 40% | 0% | 80% | NVT | - | 100% |
| 2. Amazone | 2.0 | 65% | 83% | 63% | 33% | 0% | 70% | 50% | 100% | 0% | 33% | - | 100% | 100% |
| 3. ANPR | 2.0 | 60% | 100% | 13% | 17% | 0% | 75% | 75% | 56% | 100% | 60% | - | 50% | 100% |
| 4. AVR | 1.0 | 43% | 50% | 38% | 50% | 0% | 40% | 43% | 56% | 0% | 50% | NVT | - | 0% |
| 5. BOSZ | 2.0 | 70% | 100% | 88% | 100% | 0% | 50% | 75% | 56% | NVT | 100% | - | NVT | 50% |
| 6. BVH | 2.0 | 58% | 100% | 88% | 0% | 0% | 50% | 50% | 56% | 38% | 100% | - | 67% | 50% |
| 7. BVI-BlueSpotMonitor | 2.0 | 58% | 100% | 100% | NVT | 0% | 63% | 60% | 100% | NVT | 20% | - | 33% | 0% |
| 8. BVI-Blueview 4.0 | 1.0 | 90% | NVT | 40% | 100% | 100% | 100% | 88% | 88% | 100% | 100% | NVT | - | 100% |
| 9. BVID 2.0 | 1.0 | 85% | 100% | 67% | 100% | 100% | 58% | 86% | 100% | NVT | 83% | NVT | - | 100% |
| 10. BVI-IB | 1.0 | 79% | 100% | 100% | 100% | 50% | 100% | 83% | 100% | NVT | 20% | NVT | - | 100% |
| 12. DCS | 2.0 | 39% | 33% | 33% | 33% | 0% | 60% | 33% | 44% | 0% | 20% | - | 100% | 0% |
| 13. FCM | 1.0 | 59% | 100% | 100% | 100% | 0% | 50% | 33% | 89% | 0% | 0% | NVT | - | 33% |
| 14. Hansken | 2.0 | 63% | NVT | 75% | NVT | 0% | 38% | 50% | 100% | NVT | 20% | - | 100% | 100% |
| 15. HAVANK | 1.0 | 85% | 100% | 88% | 100% | 50% | 67% | 86% | 100% | 100% | 50% | NVT | - | 100% |
| 16. I-Base | 2.0 | 77% | 100% | 25% | 100% | 0% | 100% | 100% | 100% | NVT | 20% | - | 100% | NVT |
| 17. Internet Aangifte | 1.0 | 62% | 100% | 60% | 100% | 0% | 25% | 29% | 72% | 50% | 80% | NVT | - | 100% |
| 18. Kantoorautomatisering | 2.0 | 58% | NVT | 0% | 100% | 0% | NVT | NVT | NVT | NVT | 100% | - | NVT | NVT |
| 19. Live Journaal Politie | 1.0 | 37% | 25% | 88% | 20% | 0% | 17% | 38% | 33% | 75% | 40% | NVT | - | 0% |
| 20. LSV | 1.0 | 62% | 33% | 38% | 100% | 50% | 80% | 50% | 83% | 75% | 10% | NVT | - | 0% |
| 21. Mappen standaard | 2.0 | 70% | 100% | 38% | NVT | 0% | 50% | 100% | 100% | 0% | 20% | - | 100% | 33% |
| 22. MEOS | 1.0 | 86% | 100% | 75% | 100% | NVT | 75% | 100% | 69% | NVT | 100% | NVT | - | 100% |
| 23. Orion | 2.0 | 87% | NVT | 75% | NVT | NVT | NVT | NVT | NVT | NVT | 100% | - | NVT | 50% |
| 24. Personenserver | 2.0 | 33% | 100% | 25% | 0% | 0% | 0% | 0% | 19% | NVT | 30% | - | 50% | 100% |
| 25. Digibon/PDB | 2.0 | 55% | 83% | 63% | 100% | 0% | 75% | 25% | 56% | 0% | 70% | - | 50% | 100% |
| 26. PSH-V | 1.0 | 41% | 50% | 30% | 50% | 0% | 20% | 56% | 44% | 0% | 20% | NVT | - | 83% |
| 27. PSH-VM | 1.0 | 49% | 70% | 90% | 50% | 0% | 40% | 31% | 61% | 75% | 20% | NVT | - | 0% |
| 28. Raffinaderij | 2.0 | 72% | 50% | 75% | 100% | 0% | 60% | 80% | 100% | NVT | 60% | - | 67% | NVT |
| 29. SBV | 2.0 | 73% | NVT | 50% | 100% | 0% | 75% | 100% | 100% | 100% | 20% | - | 100% | 100% |
| 30. Servicemodule | 1.0 | 60% | 100% | 75% | 50% | 0% | 60% | 58% | 92% | 0% | 25% | NVT | - | 17% |
| 31. SMC | 2.0 | 79% | 100% | 100% | 100% | 0% | 75% | 75% | 100% | NVT | 20% | - | 100% | 100% |
| 32. SUMMIT | 1.0 | 67% | 75% | 88% | 86% | 75% | 83% | 56% | 78% | 13% | 40% | NVT | - | 0% |
| 33. TRIS | 1.0 | 41% | 63% | 50% | 100% | 0% | 33% | 19% | 50% | 0% | 0% | NVT | - | 50% |
| 34. Verificatiemodule | 2.0 | 33% | NVT | 13% | 0% | 0% | 10% | 17% | 100% | NVT | 20% | - | 75% | 50% |
| 35. VROS | 2.0 | 46% | NVT | 25% | 100% | 0% | 60% | 40% | 40% | NVT | 10% | - | 100% | 100% |
| 36. ZUIS | 1.0 | 42% | 67% | 75% | 0% | 50% | 50% | 0% | 44% | 50% | 0% | NVT | - | 50% |

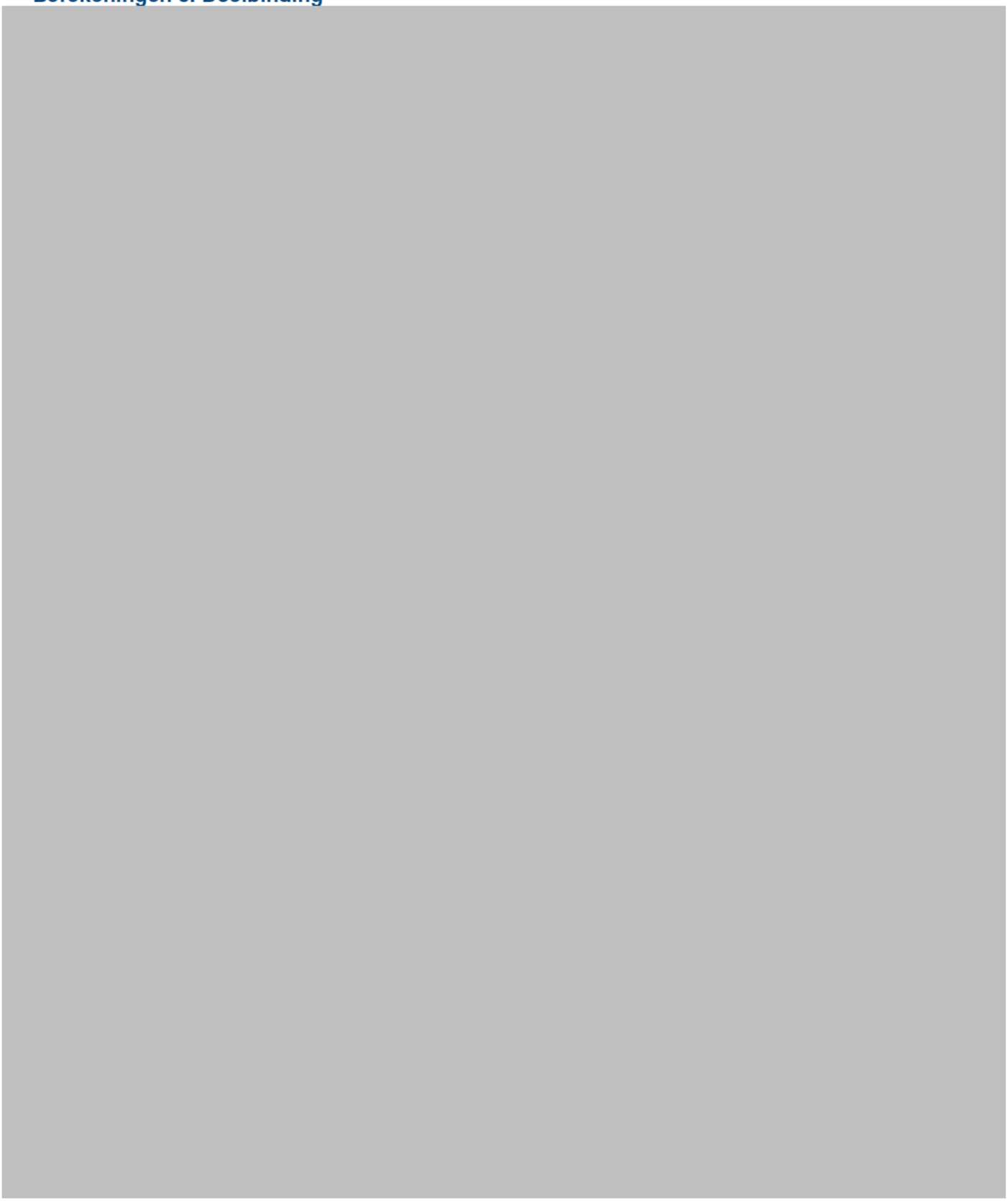
*Tabel bijlage 3d: Score beleidscriteria highrisk applicaties*

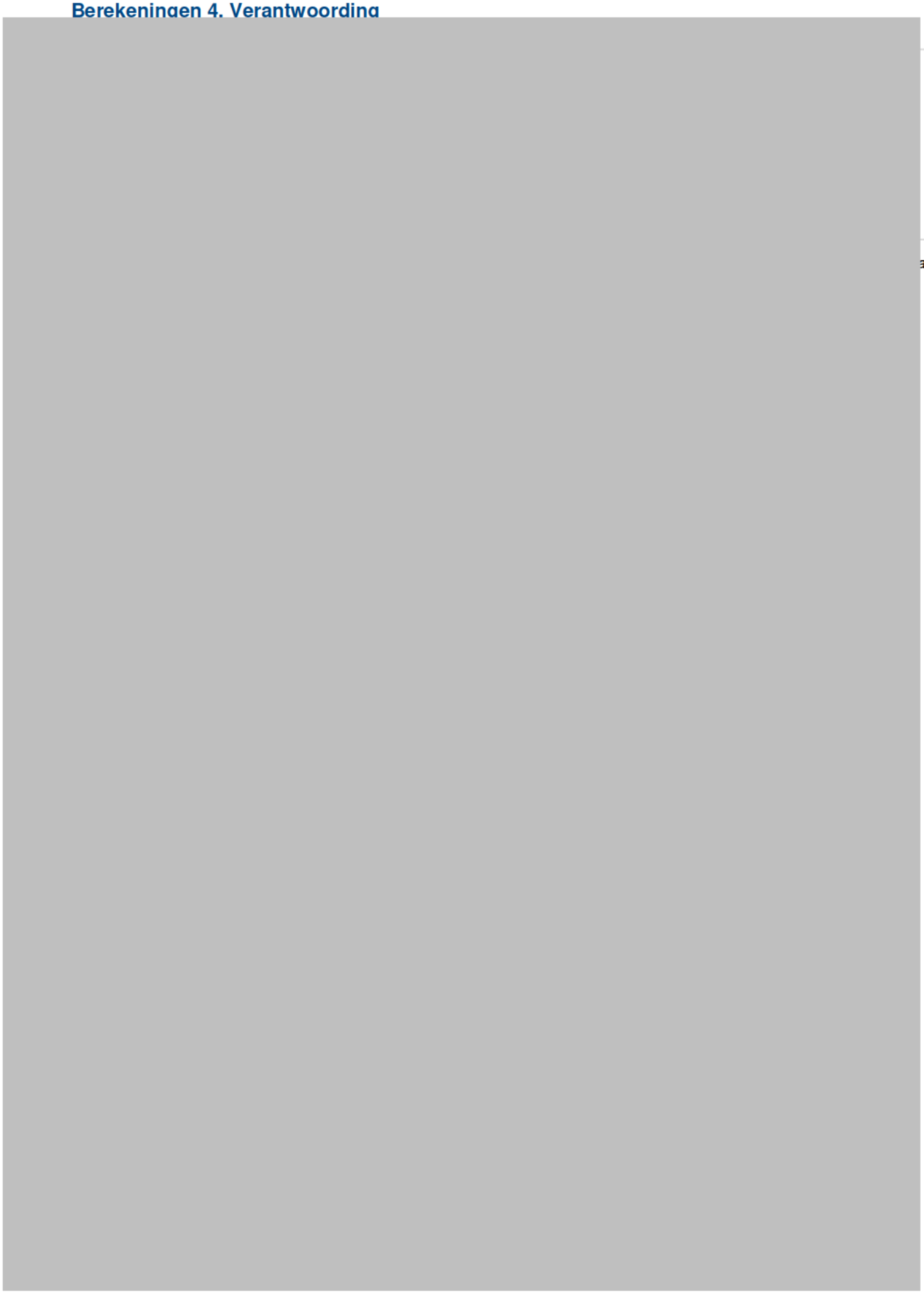
## Berekeningen 1. Eenmalige vastlegging

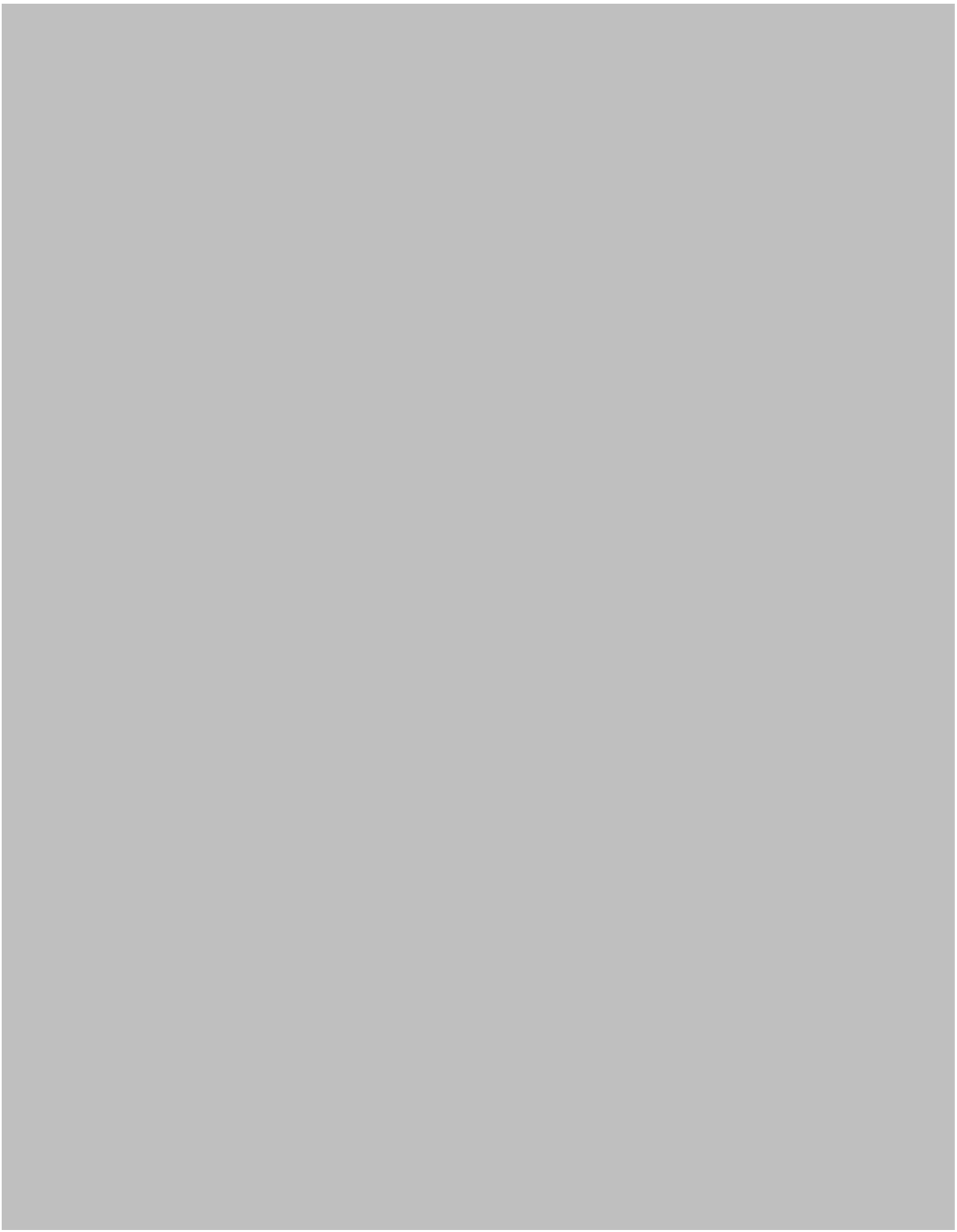


## Berekeningen 2. PDCA-cyclus

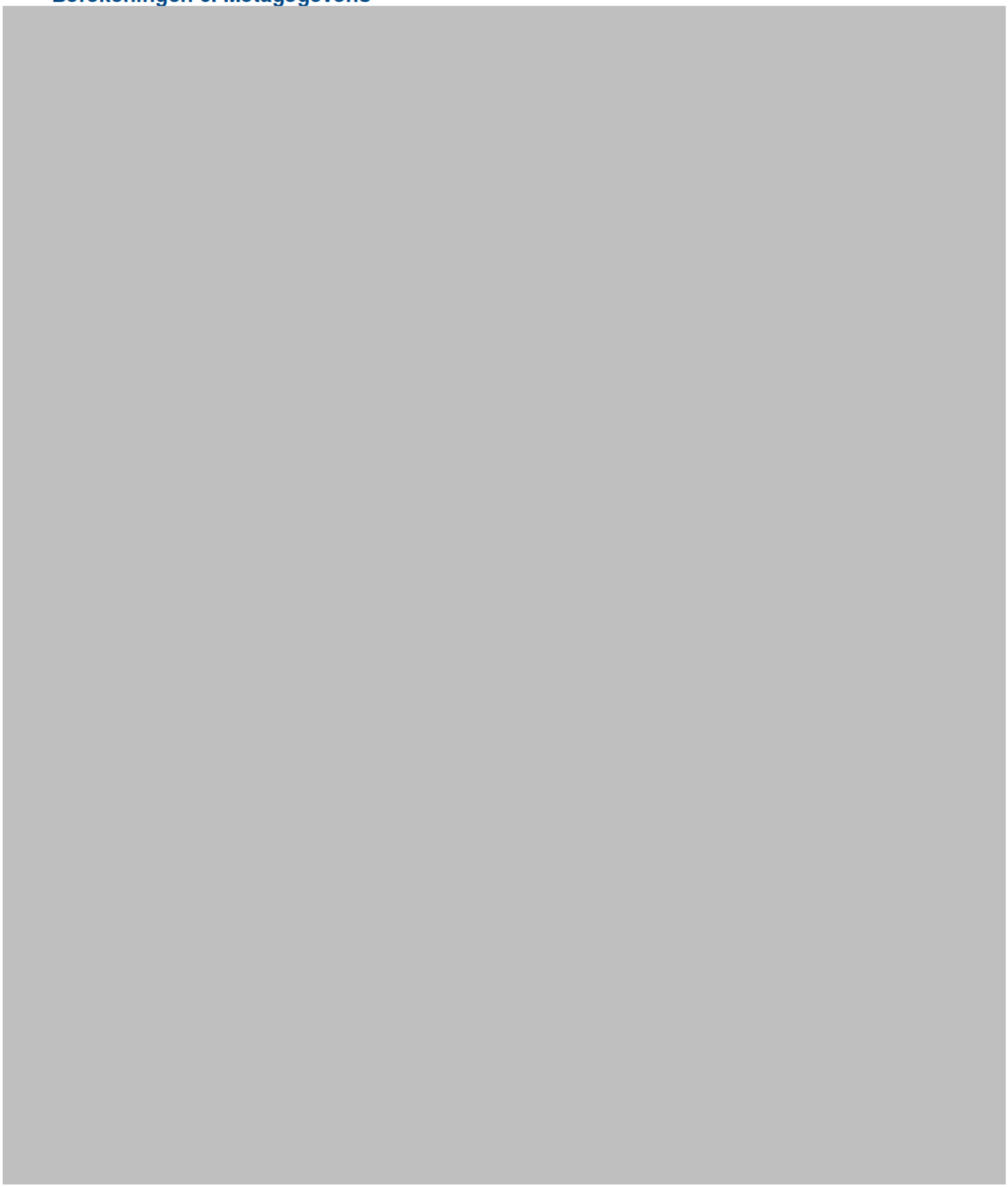
## Berekeningen 3. Doelbinding



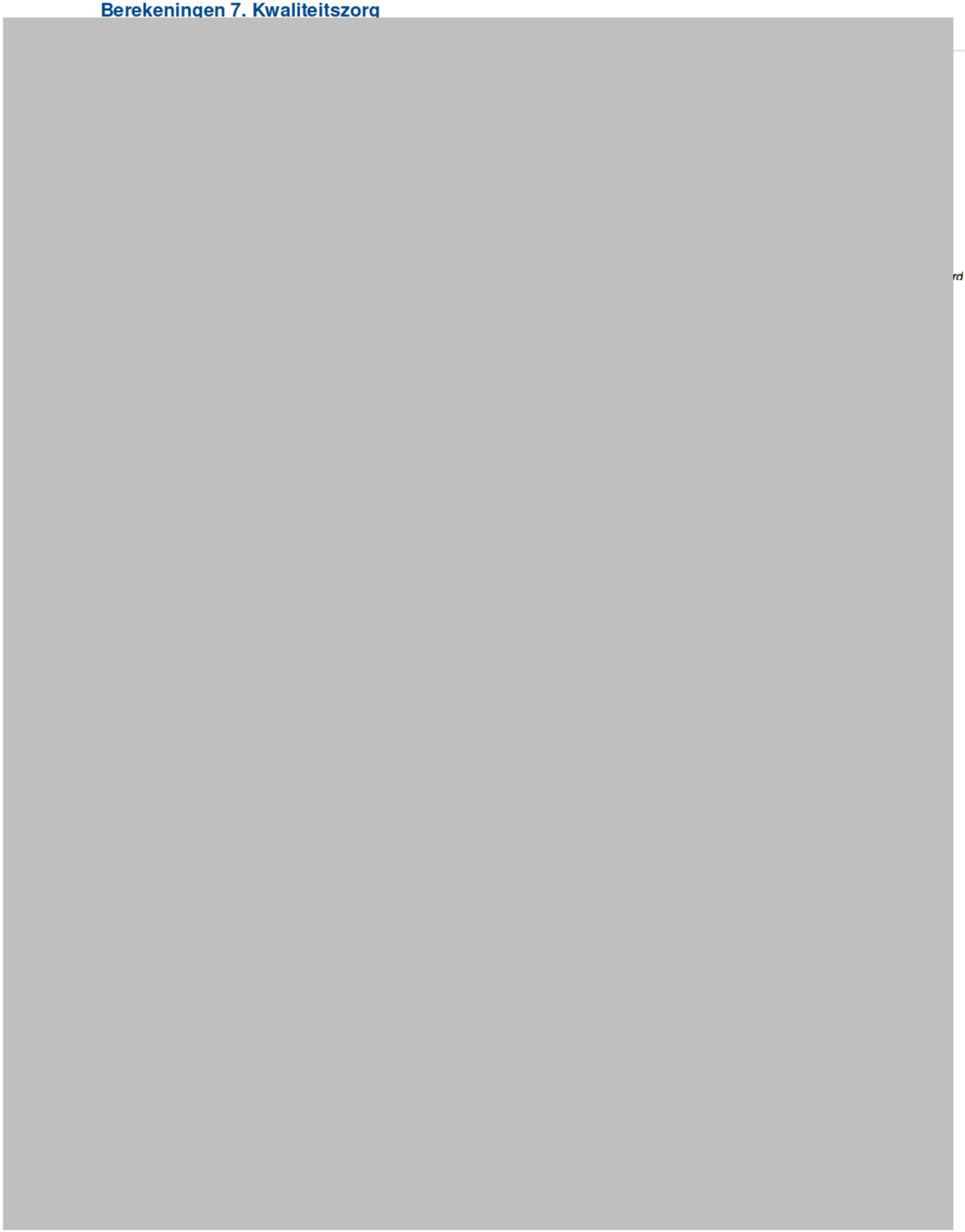




## Berekeningen 6. Metagegevens



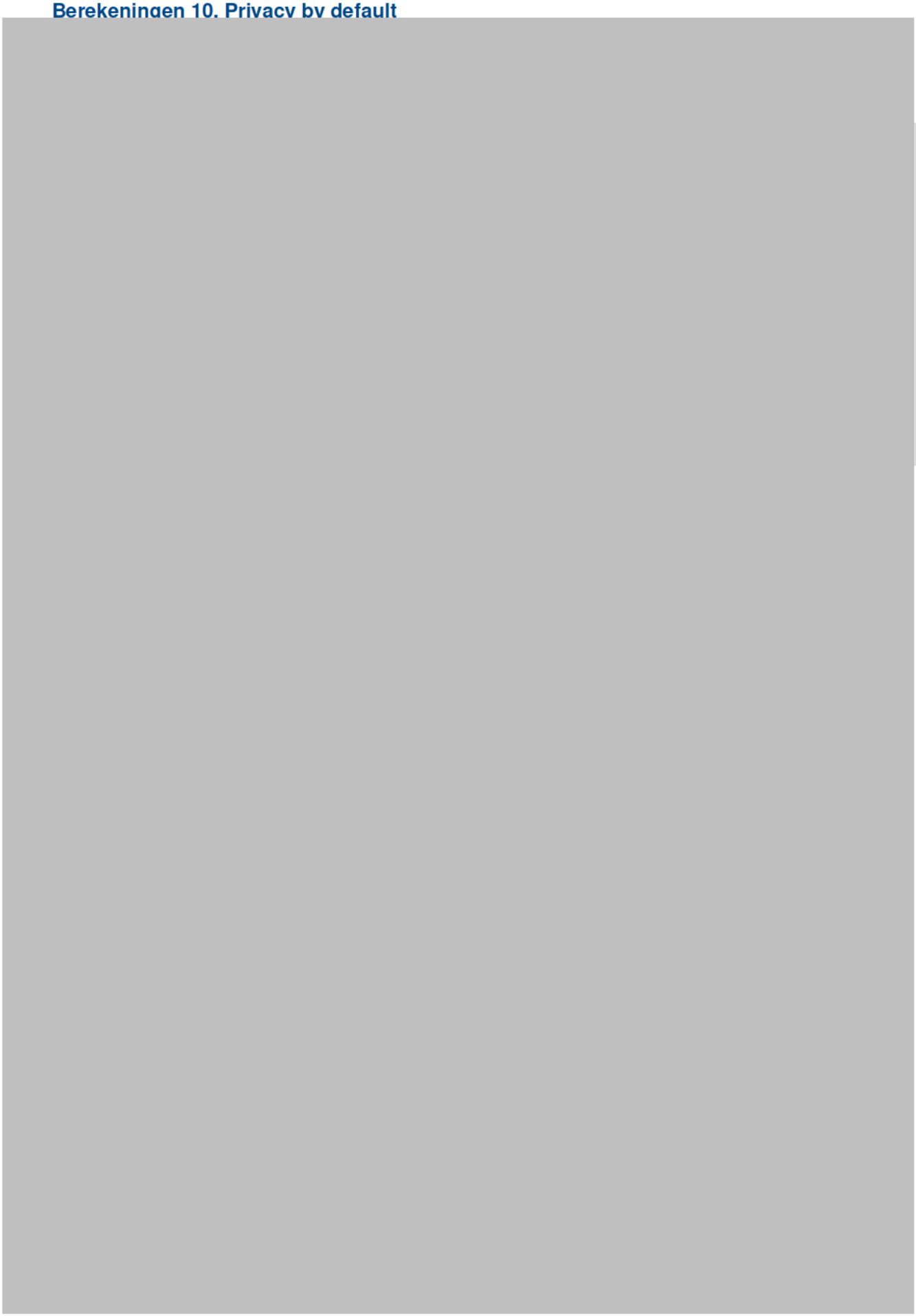
## Berekeningen 7. Kwaliteitszorg



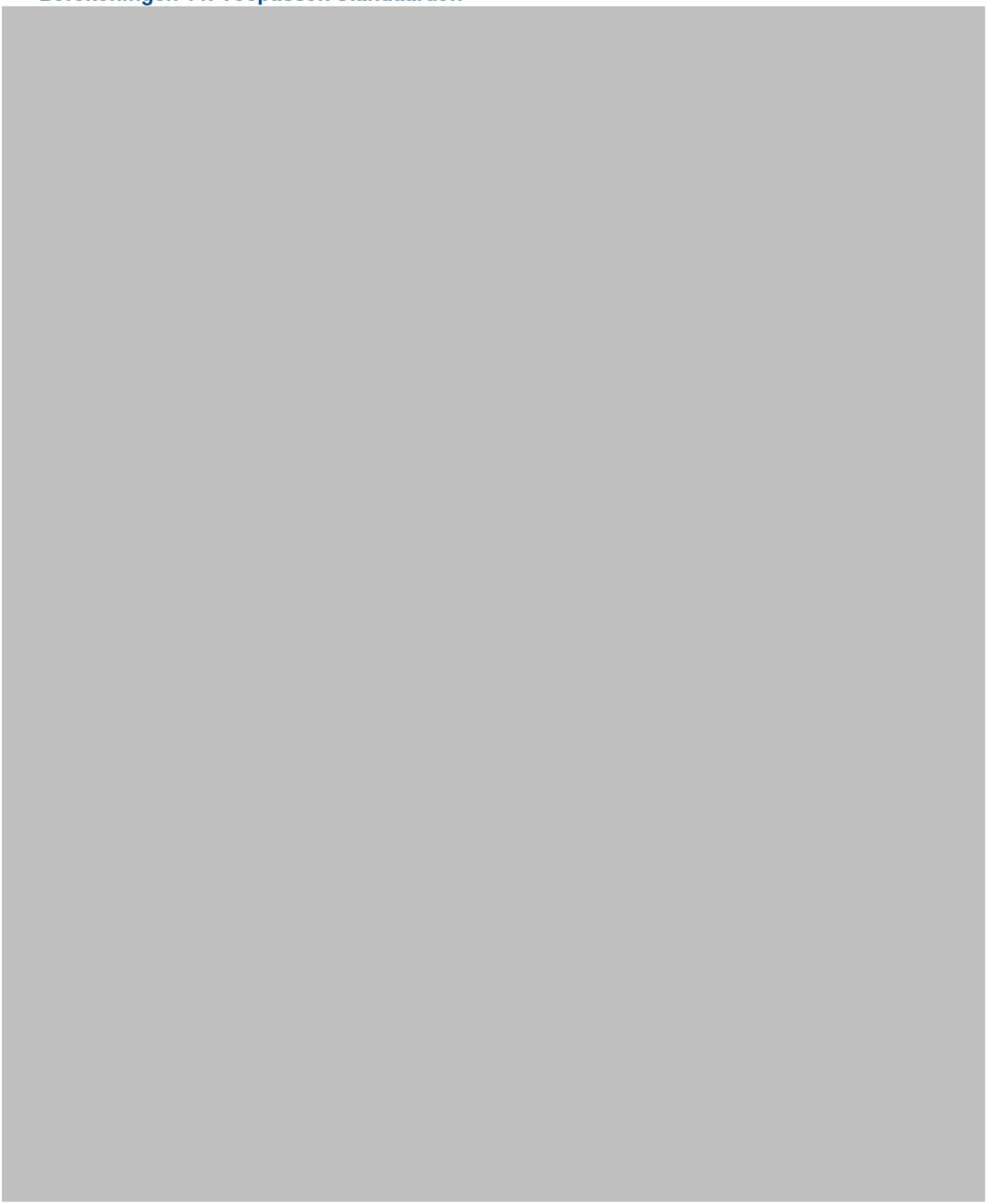
## Berekeningen 9. Informatiebeveiliging

?

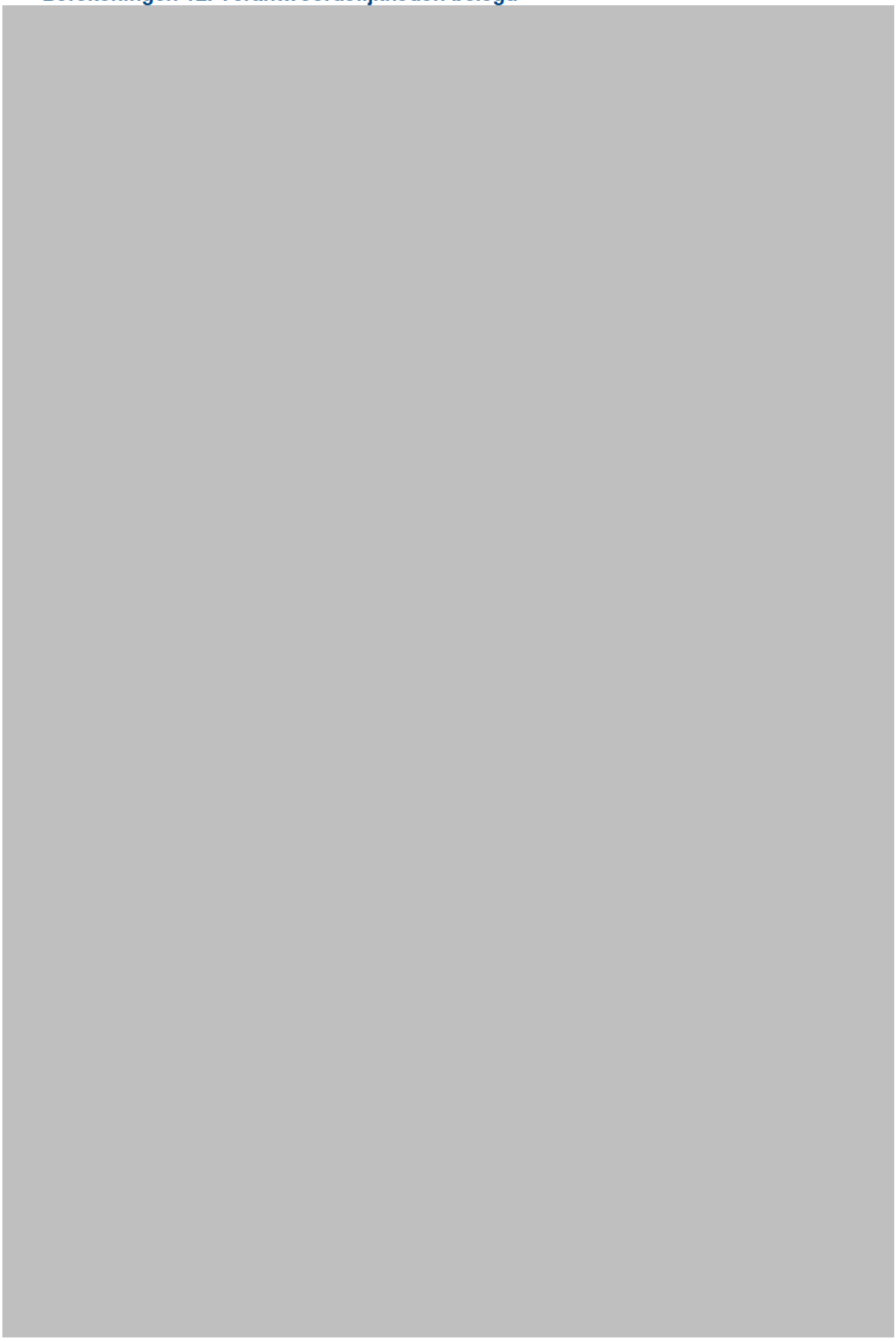
## Berekeningen 10. Privacy by default



## Berekeningen 11. Toepassen standaarden



## Berekeningen 12. Verantwoordelijkheden belegd



# Bijlage 4: Afkortingen

| Afkorting | Betekenis afkorting |
|---|---|
| ADR | Auditdienst Rijk |
| ANPR | Automatic NumberPlate Recognition |
| AVG | Algemene Verordening Gegevensbescherming |
| AVR | Auditieve/Audiovisuele verhoorregistratie |
| BOSZ | Betere Opsporing door Sturing op Zaken |
| BVH | Basisvoorzieining handhaving |
| BVI-IB | Basisvoorziening informatie – Integrale bevraging |
| BVID | Basisvoorziening Identiteitsvaststelling |
| DCS | Digitale communicatiesporen |
| DevOps | DevelopmentOperations |
| DIV | Documentaire InformatieVoorzieining |
| DUTO | Duurzame toegankelijkheid Overheidsinformatie |
| FCM | Foto Confrontatie Module |
| GA | Gegevensautoriteit |
| GEB | Gegevenseffectbeschermingbeoordeling |
| IB | Informatiebeveiliging |
| IV | Informatievoorziening |
| KMT | Korpsmanagement team |
| LJP | Live Journaal Politie |
| LSV | Landelijk Sporenvolgsysteem |
| MEOS | Mobiel Effectiever Op Straat |
| NAW | Naam Adres Woonplaats |
| OM | Openbaar Ministerie |
| NVT | Niet van toepassing |
| PDB | Politie Digibon Backoffice |
| PDCA-cyclus | Plan-Do-Check-Act-cyclus |
| PSbD | Privacy & Security by Design |
| PSH-V | Politiesuite Handhaving – Vreemdelingen |
| PSH-VM | Politiesuite Handhaving – Vergunningsmodule |
| SBV | Sirene Berichtenverkeer |
| SMC | Signalering Muteer Client |
| TMP | Toepassingsprofiel Metagegevens Politie |
| TMR | Toepassingsprofiel Metagegevens Rijk |
| TRIS | Technische Recherche Informatiesysteem |
| VROS | Verwijsindex Rechercheonderzoeken en -Subjecten |
| Wpg | Wet politiegegevens |
| ZUIS | Zeescheepvaart Uitbreidbaar Informatiesysteem |