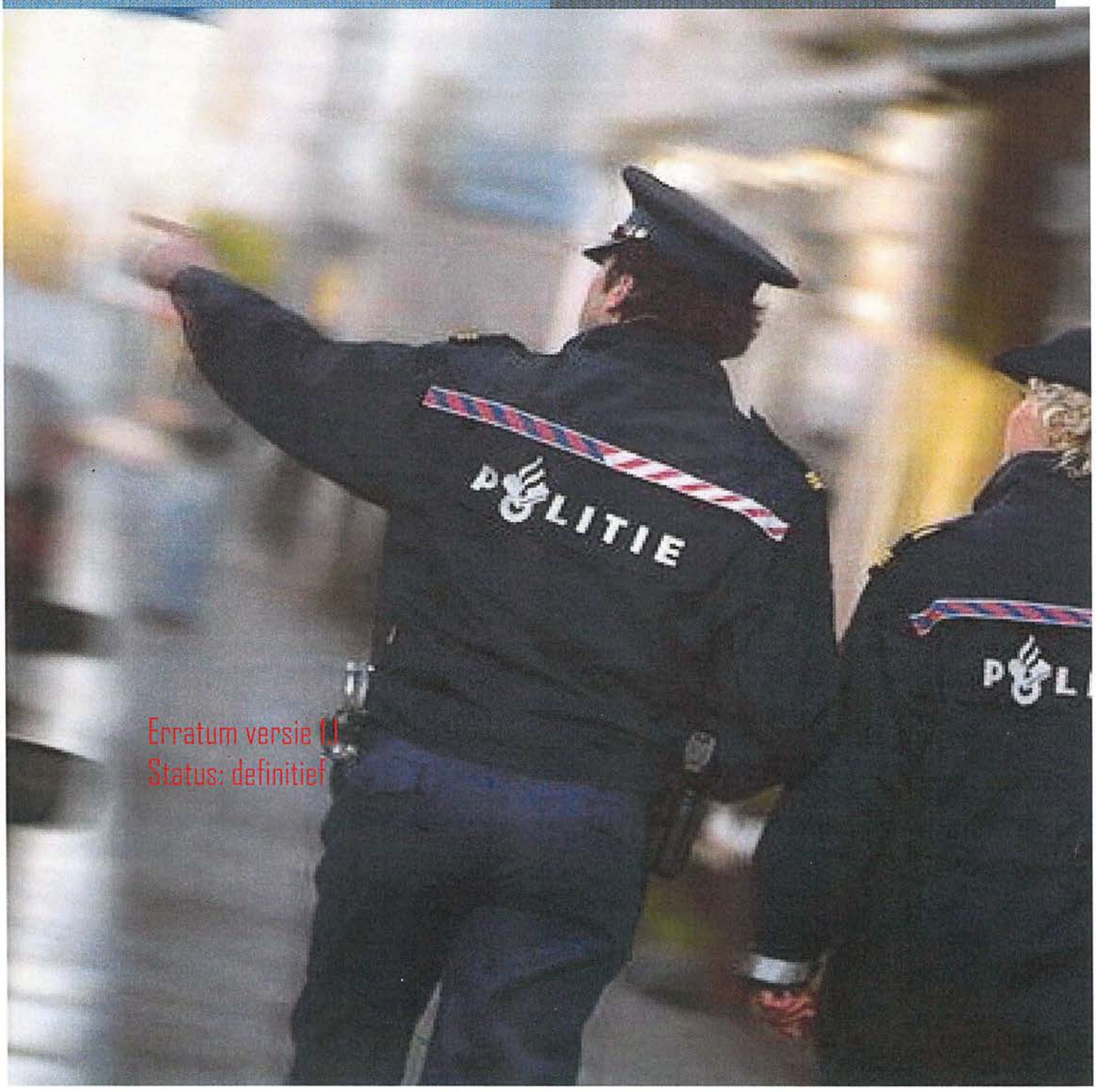
MAZARS

RAPPORT PRIVACY AUDIT WET POLITIEGEGEVENS POLITIE ZEELAND



Erratum versie 1.1
Status: definitief

Versiegeschiedenis

Versie	Versiedatum	Opgesteld door	Samenvatting van aanpassingen
1.0	20-06-11	[redacted]	Definitief en vastgesteld rapport
1.1	06-09-11		Erratum Correcties op tik- en stijlfouten door het gehele rapport. Inhoudelijke correcties in de bijlage I voor wat betreft de scores in de volgende paragrafen: 1.2.5 1.2.5.4: A verplaatst naar 1.2.5.1 1.3.8 1.3.8.3 en 1.3.8.4: V gecorrigeerd in D 1.4.2 1.4.2.4: A toegevoegd 1.4.3.1: D gewist 1.5.1 1.5.1.1: A toegevoegd 1.6.3 1.6.3.4: V gecorrigeerd in – 1.6.4 1.6.4.1: A toegevoegd 1.6.6 1.6.6.1 en 1.6.1.2: A toegevoegd 1.7.1 1.7.1.3: V gecorrigeerd in – 1.7.4 1.7.4.1: A toegevoegd 1.8.2 1.8.2.4 en 1.8.2.5: V gecorrigeerd in D. A toegevoegd 1.9.1 1.9.1.3: Toegevoegd – 1.10.1 1.10.1.3: Toegevoegd – Inhoudelijke correcties in de bijlage V v.w.b. de volgende toelichtingen en scores: 1.2.1 1.2.1.2: BV gecorrigeerd in BD 1.2.1.7: OV gecorrigeerd in OD 1.2.5 1.2.5.1: A toegevoegd 1.2.5.4: A gewist 1.3.1 1.3.1.4 t/m 1.3.1.8: A toegevoegd 1.3.2 1.3.2.6: OV gecorrigeerd in OD. BV gecorrigeerd in BD 1.3.4 1.3.4.2 t/m 1.3.4.8: A gewist 1.3.7 1.3.7.1 en 1.3.7.2: A toegevoegd 1.3.7.6 en 1.3.7.7: OV gecorrigeerd in OD 1.3.8 1.3.8.3 en 1.3.8.4: V gecorrigeerd in D 1.3.8.4: OD toegevoegd 1.4.2 1.4.2.2: BV gecorrigeerd in BD 1.4.2.3: - gecorrigeerd in OV/BV 1.4.2.4: OV gecorrigeerd in OD en A toegevoegd 1.4.2.5 en 1.4.2.6: OV gecorrigeerd in OD 1.4.3 1.4.3.1 en 1.4.3.2: A toegevoegd 1.6.3 1.6.3.3: V gecorrigeerd in – 1.6.4 1.6.4.1: A toegevoegd 1.6.5 1.6.5.1: - gecorrigeerd in V 1.6.6 1.6.6.1, 1.6.6.2 en 1.6.6.6: A toegevoegd 1.6.7 1.6.7.3, 1.6.7.4 en 1.6.7.5: A toegevoegd 1.7.1

			1.7.1.3: V gecorrigeerd in – 1.7.2 1.7.2.4, 1.7.2.5: OV gecorrigeerd in OD. BV gecorrigeerd in BD. V gecorrigeerd in D. A toegevoegd 1.7.2.6: OV gecorrigeerd in OD. V gecorrigeerd in D. BV gecorrigeerd in - .A toegevoegd. 1.8.1 1.8.1.3: V gecorrigeerd in – 1.9.1 1.9.1.3: A gecorrigeerd in – 1.10.1 1.10.1.3: A gecorrigeerd in – 1.11.1 1.11.1.3: A gecorrigeerd in – 1.11.6 1.11.6.1 en 1.11.6.2: D gewist 1.11.6.3: V gewist en A toegevoegd 1.11.6.4: D gewist 1.14.1 1.14.1.1: V toegevoegd

MAZARS

Inhoudsopgave

1 Aanleiding opdracht 9
2 Doel van de privacy audit WPG 9
3 Objecten van de privacy audit 9
4 Beperkingen toegang tot verwerkingen van politiegegevens 10
5 Gehanteerde normen 10
6 Aanpak en werkwijze 10
7 Beperkingen van het onderzoek 12
8 Verspreidingskring van het rapport 12
9 Oordeel 12
10 Verdere opbouw van het rapport 15
Bijlage I: Managementsamenvatting, normen en bevindingen 16
1.1 GO: Gebruikersorganisatie 18
1.1.1 Inrichting van de organisatie 18
1.2 Artikel 8 (dagelijkse politietaak) 21
1.2.1 Noodzakelijkheid, rechtmatigheid en doelbinding 21
1.2.2 Juistheid, volledigheid en beveiliging politiegegevens 22
1.2.3 Autorisaties 24
1.2.4 Geautomatiseerd vergelijken 25
1.2.5 In combinatie met elkaar verwerken 26
1.2.6 Bewaartermijnen en vernietiging 27
1.2.7 Ter beschikking stellen van politiegegevens (tbs) 28
1.2.8 Verstrekkingen 29
1.3 Artikel 9 (verwerking voor de rechtsorde in een bepaald geval) 32
1.3.1 Noodzakelijkheid, rechtmatigheid en doelbinding 32
1.3.2 Juistheid, volledigheid en beveiliging politiegegevens 33
1.3.3 Autorisaties 34
1.3.4 Geautomatiseerd vergelijken 36
1.3.5 In combinatie met elkaar verwerken 37
1.3.6 Bewaartermijnen en vernietiging 37
1.3.7 Ter beschikking stellen van politiegegevens 38
1.3.8 Verstrekkingen 39
1.4 Artikel 10,1A CIE (verkrijgen van inzicht in betrokkenheid personen) 41
1.4.1 Noodzakelijkheid, rechtmatigheid en doelbinding 41
1.4.2 Juistheid, volledigheid en beveiliging politiegegevens 42
1.4.3 Autorisaties (protocolplicht) 43
1.4.4 Geautomatiseerd vergelijken 44
1.4.5 In combinatie met elkaar verwerken 45
1.4.6 Bewaartermijnen en vernietiging 46
1.4.7 Ter beschikking stellen van politiegegevens 47
1.4.8 Verstrekkingen 47
1.5 Artikel 10,1B Themaverwerking (verkrijgen van inzicht in betrokkenheid personen) 49
1.5.1 Noodzakelijkheid, rechtmatigheid en doelbinding 49
1.5.2 Juistheid, volledigheid en beveiliging politiegegevens 50
1.5.3 Autorisaties (protocolplicht) 50
1.5.4 Geautomatiseerd vergelijken 51
1.5.5 In combinatie met elkaar verwerken 51
1.5.6 Bewaartermijnen en vernietiging 51

1.5.7 Ter beschikking stellen van politiegegevens ... 52
1.5.8 Verstrekkingen ... 52
1.6 Artikel 10,1C, RID (verkrijgen van inzicht in betrokkenheid personen) ... 53
1.6.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 53
1.6.2 Juistheid, volledigheid en beveiliging politiegegevens ... 54
1.6.3 Autorisaties (protocolplicht) ... 55
1.6.4 Geautomatiseerd vergelijken ... 55
1.6.5 In combinatie met elkaar verwerken ... 56
1.6.6 Bewaartermijnen en vernietiging ... 57
1.6.7 Ter beschikking stellen van politiegegevens ... 57
1.6.8 Verstrekkingen ... 58
1.7 Artikel 12 Informanten CIE ... 59
1.7.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 59
1.7.2 Juistheid, volledigheid en beveiliging politiegegevens ... 59
1.7.3 Autorisaties ... 60
1.7.4 Geautomatiseerd vergelijken ... 61
1.7.5 Bewaartermijnen en vernietiging ... 62
1.7.6 Ter beschikking stellen van politiegegevens ... 62
1.8 Artikel 12 Informanten RID ... 63
1.8.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 63
1.8.2 Juistheid, volledigheid en beveiliging politiegegevens ... 63
1.8.3 Autorisaties ... 64
1.8.4 Geautomatiseerd vergelijken ... 65
1.8.5 Bewaartermijnen en vernietiging ... 65
1.8.6 Ter beschikking stellen van politiegegevens ... 65
1.9 Artikel 13 (Landelijke registers) ... 67
1.9.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 67
1.9.2 Juistheid, volledigheid en beveiliging politiegegevens ... 67
1.9.3 Autorisaties ... 68
1.9.4 Bewaartermijnen en vernietiging ... 68
1.9.5 Ter beschikking stellen van politiegegevens ... 68
1.9.6 Verstrekkingen ... 68
1.10 Artikel 13 (VROS-taak) ... 69
1.10.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 69
1.10.2 Juistheid, volledigheid en beveiliging politiegegevens ... 69
1.10.3 Autorisaties ... 70
1.10.4 Bewaartermijnen en vernietiging ... 70
1.10.5 Ter beschikking stellen van politiegegevens ... 70
1.10.6 Verstrekkingen ... 71
1.11 Artikel 13 (Diensten Justitie) ... 72
1.11.1 Noodzakelijkheid, rechtmatigheid en doelbinding ... 72
1.11.2 Juistheid, volledigheid en beveiliging politiegegevens ... 72
1.11.3 Autorisaties ... 73
1.11.4 Bewaartermijnen en vernietiging ... 73
1.11.5 Ter beschikking stellen van politiegegevens ... 73
1.11.6 Verstrekkingen ... 74
1.12 Rechten van betrokken ... 75
1.12.1 Verzoek om kennisneming ... 75
1.12.2 Verzoek om verbetering, aanvulling, verwijdering of afscherming ... 75

1.12.3 Mededeling van verbetering, aanvulling, verwijdering of afscherming 76
1.12.4 Vergoeding van kosten 76
1.13 Audits 76
1.14 Privacyfunctionaris 77
1.15 Functionaris gegevensbescherming 78
Bijlage II: Basisbeveiliging Politie 80
2.1 Gebruikersorganisatie 80
2.1.1 Informatievoorzieningproces 80
2.1.2 Medewerkers 80
2.1.3 Middelen 81
2.1.4 Strategie & Beleid 82
2.1.5 Leiderschap 83
Bijlage III: Overzicht geraadpleegde documenten 84
Bijlage IV: Overzicht van de organisatie- en informatiestructuur van Politie Zeeland 88
Bijlage V: Transponeringstabel WPG / BPG 92
1.1 GO: Gebruikersorganisatie 92
1.1.1 Inrichting van de organisatie 92
1.2 Artikel 8 (verwerking voor de dagelijkse politietaak) 92
1.2.1 Noodzakelijkheid, rechtmatigheid en doelbinding 92
1.2.2 Juistheid, volledigheid en beveiliging politiegegevens 92
1.2.3 Autorisaties 92
1.2.4 Geautomatiseerd vergelijken 93
1.2.5 In combinatie met elkaar verwerken 93
1.2.6 Bewaartermijnen en vernietiging 93
1.2.7 Ter beschikking stellen van politiegegevens 93
1.2.8 Verstrekkingen 93
1.3 Artikel 9 (verwerking voor de rechtsorde in een bepaald geval) 93
1.3.1 Noodzakelijkheid, rechtmatigheid en doelbinding 93
1.3.2 Juistheid, volledigheid en beveiliging politiegegevens 94
1.3.3 Autorisaties 94
1.3.4 Geautomatiseerd vergelijken 94
1.3.5 In combinatie met elkaar verwerken 94
1.3.6 Bewaartermijnen en vernietiging 94
1.3.7 Ter beschikking stellen van politiegegevens 94
1.3.8 Verstrekkingen 95
1.4 Artikel 10,1A CIE (verkrijgen van inzicht in betrokkenheid personen) 95
1.4.1 Noodzakelijkheid, rechtmatigheid en doelbinding 95
1.4.2 Juistheid, volledigheid en beveiliging politiegegevens 95
1.4.3 Autorisaties 95
1.4.4 Geautomatiseerd vergelijken 95
1.4.5 In combinatie met elkaar verwerken 95
1.4.6 Bewaartermijnen en vernietiging 96
1.4.7 Ter beschikking stellen van politiegegevens 96
1.4.8 Verstrekkingen 96
1.5 Artikel 10,1B Themaverwerking (verkrijgen van inzicht in betrokkenheid personen) 96
1.5.1 Noodzakelijkheid, rechtmatigheid en doelbinding 96
1.5.2 Juistheid, volledigheid en beveiliging politiegegevens 96
1.5.3 Autorisaties 97
1.5.4 Geautomatiseerd vergelijken 97

1.5.5 In combinatie met elkaar verwerken 97
1.5.6 Bewaartermijnen en vernietiging 97
1.5.7 Ter beschikking stellen van politiegegevens 97
1.5.8 Verstrekkingen 97
1.6 Artikel 10,1C RID (verkrijgen van inzicht in betrokkenheid personen) 98
1.6.1 Noodzakelijkheid, rechtmatigheid en doelbinding 98
1.6.2 Juistheid, volledigheid en beveiliging politiegegevens 98
1.6.3 Autorisaties 98
1.6.4 Geautomatiseerd vergelijken 98
1.6.5 In combinatie met elkaar verwerken 98
1.6.6 Bewaartermijnen en vernietiging 98
1.6.7 Ter beschikking stellen van politiegegevens 99
1.6.8 Verstrekkingen 99
1.7 Artikel 12 Informanten CIE 99
1.7.1 Noodzakelijkheid, rechtmatigheid en doelbinding 99
1.7.2 Juistheid, volledigheid en beveiliging politiegegevens 99
1.7.3 Autorisaties 99
1.7.4 Geautomatiseerd vergelijken 100
1.7.5 Bewaartermijnen en vernietiging 100
1.7.6 Ter beschikking stellen van politiegegevens 100
1.8 Artikel 12 Informanten RID 100
1.8.1 Noodzakelijkheid, rechtmatigheid en doelbinding 100
1.8.2 Juistheid, volledigheid en beveiliging politiegegevens 100
1.8.3 Autorisaties 100
1.8.4 Geautomatiseerd vergelijken 100
1.8.5 Bewaartermijnen en vernietiging 101
1.8.6 Ter beschikking stellen van politiegegevens 101
1.9 Artikel 13 (landelijke registers) 101
1.9.1 Noodzakelijkheid, rechtmatigheid en doelbinding 101
1.9.2 Juistheid, volledigheid en beveiliging politiegegevens 101
1.9.3 Autorisaties 101
1.9.4 Bewaartermijnen en vernietiging 101
1.9.5 Ter beschikking stellen van politiegegevens 101
1.9.6 Verstrekkingen 102
1.10 Artikel 13 (VROS-taak) 102
1.10.1 Noodzakelijkheid, rechtmatigheid en doelbinding 102
1.10.2 Juistheid, volledigheid en beveiliging politiegegevens 102
1.10.3 Autorisaties 102
1.10.4 Bewaartermijnen en vernietiging 102
1.10.5 Ter beschikking stellen van politiegegevens 102
1.10.6 Verstrekkingen 102
1.11 Artikel 13 (diensten Justitie) 103
1.11.1 Noodzakelijkheid, rechtmatigheid en doelbinding 103
1.11.2 Juistheid, volledigheid en beveiliging politiegegevens 103
1.11.3 Autorisaties 103
1.11.4 Bewaartermijnen en vernietiging 103
1.11.5 Ter beschikking stellen van politiegegevens 103
1.11.6 Verstrekkingen 103
1.12 Rechten van betrokkenen 104

1.12.1. Verzoek om kennisneming 104
1.12.2. Verzoek om verbetering, aanvulling, verwijdering of afscherming 104
1.12.3. Mededeling van verbetering, aanvulling, verwijdering of afscherming 104
1.12.4. Vergoeding van kosten 104
1.13 Audits 104
1.14 Privacyfunctionaris 104
1.15 Functionaris gegevensbescherming 104

MAZARS

Aan de Korpschef van de politie Zeeland
Mevrouw A.M. Demmers-van der Geest
Postbus 5009
4330 KA Middelburg

Rotterdam, 20 juni 2011
MMC/HW/10648

Betreft: Uitvoeren opdracht privacy audit politiegegevens

Ingevolge uw opdracht, hebben wij de privacy audit uitgevoerd op de verwerking van politiegegevens door de medewerkers van politie Zeeland.

Met dit rapport brengen wij u verslag uit omtrent de uitkomsten van onze werkzaamheden.

1 Aanleiding opdracht

Op het verwerken van persoonsgegevens ten behoeve van de politietaak, als bedoeld in de Politiewet 1993, zijn regels bij of krachtens de Wet politiegegevens (WPG) van toepassing.

Artikel 33 van de WPG bevat de verplichting voor een verantwoordelijke om periodiek op het verwerken van politiegegevens een privacy audit te doen uitvoeren.

De wijze waarop de privacy audit moet worden uitgevoerd is nader geregeld in de ministeriële Regeling periodieke audit politiegegevens (RPAP) van 9 december 2008, nr. 5578598/08.

2 Doel van de privacy audit WPG

Het doel van de privacy audit was:

1. het op systematische wijze toetsen of aan de bepalingen van de Wet politiegegevens op adequate wijze uitvoering is gegeven;
2. het, in dat kader, beoordelen van de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien.

3 Objecten van de privacy audit

De privacy audit richtte zich op het stelsel van maatregelen en procedures waarmee de Korpschef, namens de korpsbeheerder, van de politie Zeeland beoogde te voldoen aan de beheersdoelstellingen die bij of krachtens de Wet politiegegevens voor de politie Zeeland gelden ten aanzien van de verwerkingen van politiegegevens:

1. met het oog op de uitvoering van de dagelijkse politietaak (artikel 8 WPG);
2. ten behoeve van onderzoeken met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9 WPG);
3. met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10, lid 1, onder a, b en c, WPG:), zijnde
    a. de verwerkingen door de Regionale Criminele Inlichtingen Eenheid (RCIE) (artikel 10, lid 1, onder a, WPG);
    b. de themaverwerking mensenhandel/mensensmokkel (artikel 10, lid 1, onder b, WPG);
    c. de verwerkingen door de Regionale Inlichtingen Dienst (RID) (artikel 10, lid 1, onder c, WPG);

MAZARS MANAGEMENT CONSULTANTS
Rivium Promenade 200 - Postbus 23123 - 3001 KC Rotterdam - mmc@mazars.nl
Tel: 010-2771500 - Fax: 010-4217915

Accountants - Belastingadviseurs - Organisatie-adviseurs
Mazars Paardekooper Hoffman N.V., statutair gevestigd te Rotterdam (KvK Rotterdam nr. 24389296).

4. met het oog op de controle op en het beheer van informantgegevens alsmede de beoordeling en verantwoording van het gebruik van informantgegevens (artikel 12 lid 1, WPG) door de CIE en de RID;
5. ten behoeve van de ondersteuning van de politietaak, zijnde verwerkingen voor zover zij relevant zijn voor:
    a. het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten (artikel 13, lid 1, onder a, WPG);
    b. het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte (artikel 13, lid 1, onder b, WPG);
    c. de identificatie van personen of zaken (artikel 13, lid 1 onder c, WPG);
    d. het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling danwel met het oog op een juiste bejegening van personen (artikel 13, lid 1 onder d, WPG);
    e. geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon, daarvoor ter beschikking gesteld en verder verwerkt (artikel 13, lid 3, WPG);
    f. het uitvoeren van taken ten dienste van de justitie (artikel 13, lid 1 onder e, WPG).

De privacy audit richtte zich tevens op het stelsel van maatregelen en procedures waarmee de politie Zeeland beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de WPG gelden ten aanzien van:

1. rechten van betrokkenen (artikel 25 t/m 31 WPG);
2. de privacy functionaris (PF) (artikel 34 WPG);
3. de functionaris gegevensbescherming (artikel 36 WPG).

4 Beperkingen toegang tot verwerkingen van politiegegevens

De Korpsbeheerder heeft op basis van zijn bevoegdheid ingevolge artikel 2, lid 4, RPAP aan alle interne auditors, met uitzondering van de projectleider interne audit de toegang geweigerd tot de volgende verwerkingen van politiegegevens:

- Het informantenregister CIE (artikel 12 WPG);
- Bruto verslagen CIE (artikel 12 WPG);
- Het informantenregister RID (artikel 12 WPG);
- De strafrechtelijke interne onderzoeken.

5 Gehanteerde normen

Het voor de privacy audit gehanteerde normenkader is vastgelegd in de navolgende documenten:

- Wet politiegegevens, de wet van 21 juli 2007, Staatsblad 300, houdende regels inzake de bescherming van politiegegevens;
- Besluit politiegegevens, besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens;
- Regeling periodieke audit politiegegevens, de Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegevens voorschriften;
- De Handreiking Normstelling Wet politiegegevens, vastgesteld door de Raad van Korpschefs, omstreeks november 2009;
- De Handreiking Auditing Wet politiegegevens, vastgesteld door de Raad van Korpschefs omstreeks november 2009.

6 Aanpak en werkwijze

Bij de aanpak en de uitvoering van de werkzaamheden is rekening gehouden met de richtlijnen voor het uitvoeren van EDP audits van de Nederlandse Orde van EDP Auditors (NOREA).

Mazars Management Consultants (MMC) is in juli 2010 gestart met de training interne auditor WPG voor het interne auditteam van de politie Zeeland. Het laatste onderdeel van het trainingsprogramma betrof het coachen van de interne auditors tijdens de uitvoering van de interne audit bij de politie Zeeland. De interne audit is uitgevoerd in de periode juli 2010 tot en met februari 2011.

Van de interne audit is een concept-rapport door de interne auditors opgesteld. De politie Zeeland heeft ervoor gekozen om redenen van inzichtelijkheid en compactheid niet de gehele format voor het Rapport privacy audit WPG van de Raad van Korpschefs te hanteren. In die format zijn namelijk alle beheerdoelstellingen met de daarmee corresponderende artikelen uit de WPG en het BPG vermeld. De politie Zeeland beschikt zelf over de Handreiking Normstelling WPG als referentiekader. Door de interne auditors zijn de bevindingen rechtstreeks onder de tabellen van de management samenvatting vermeld. De daarbij gehanteerde id.nrs en paragraaf aanduidingen corresponderen met de betreffende id.nrs en de paragraaf aanduidingen in de Handreiking Normstelling WPG. Voor de volledigheid van de beheersdoelstellingen en de hiermee corresponderende artikelen van de WPG en het BPG wordt kortheidshalve naar de Handreiking Normstelling WPG verwezen.

MMC heeft het concept rapport van de interne audit, alsmede het onderliggende interne auditdossier, in het kader van de training doorgenomen. Met de leden van het interne auditteam zijn gesprekken gevoerd over de gang van zaken tijdens de interne audit, de wijze waarop de evidence voor de concept rapportage tot stand is gekomen en de inzichten die de interne auditors tijdens de interne audit, maar ook tijdens hun reguliere werkzaamheden over de naleving van de WPG in de politiepraktijk hebben opgedaan. Tijdens die gesprekken zijn op onderdelen van het concept rapport rechtstreeks bevindingen en inzichten aan het rapport toegevoegd.

De coaching van MMC is overgegaan in het uitvoeren van de privacy audit. Aanvankelijk was het de bedoeling, dat MMC conform optie 3 van het Uitvoeringsvoorschrift WPG een op basis van een vastgesteld intern auditrapport en een door de korpschef opgemaakte bestuursverklaring een oordeel zou afgeven. Het concept rapport interne audit bevatte op onderdelen echter nog te weinig bevindingen om een eindoordeel op te kunnen baseren. In gezamenlijk overleg is omwille van de doorlooptijd en de beperkte budgettaire ruimte gekozen voor een praktische oplossing in de vorm van een doorstart die het midden vormt tussen optie 2 en optie 3 van het Uitvoeringsvoorschrift Privacy Audit WPG. De review op het concept interne audit rapport is door MMC uitgevoerd op de wijze zoals deze bij optie 3 is aangegeven. Bij de doorstart is overgeschakeld naar optie 2, maar dan met beperkte zekerheid, en met ondersteuning van de interne auditors. De format en onderdelen van de inhoud van het concept rapport zijn door MMC overgenomen in haar eigen rapport, waarbij de stijl van rapporteren van de interne auditors zo veel mogelijk is aangehouden.

Bij de doorstart naar optie 2 met beperkte zekerheid is zo veel mogelijk gesteund op de bevindingen in het concept rapport van de interne audit. Op onderdelen zijn de bevindingen in het concept rapport geverifieerd, geredigeerd, bijgesteld en aangevuld met bevindingen uit groepsinterviews met de teamchefs "blauw" en de teamchefs recherche. [redacted] MMC heeft een aantal deelwaarnemingen uitgevoerd op aanvullende documentatie, de mappenstructuur op de O-schijf, de I90 logging uit BVH, een overzicht verstrekkingen uit de module VST van BVO en het verstrekkingenoverzicht van het postregistratiesysteem Corsa. De resultaten van die deelwaarnemingen zijn aan het concept rapport toegevoegd.

MMC heeft tijdens de privacy audit ook in belangrijke mate gesteund op de inzichten van de interne auditors in de dagelijkse praktijk van de politie Zeeland. Die inzichten zijn eveneens rechtstreeks in het concept rapport verwerkt. Het concept rapport met de bevindingen van de privacy audit is tenslotte voor commentaar ter beschikking gesteld aan de korpsleiding.

De doorlooptijd van zowel de interne audit was langer dan aanvankelijk werd voorzien. Dit werd onder meer veroorzaakt doordat drie van de vier interne auditors naast hun werk als onderzoeker hun dagelijkse functionele werkzaamheden moesten uitvoeren (één man functies). Eén interne auditor is full-time vrijgemaakt voor 18 uren per week. Een andere beperking (in materie-deskundigheid) bij de interne auditors was dat medio 2010 de FG met FLO is vertrokken en de opvulling van de vacature eerst in maart 2011 plaatsvond. De doorlooptijd van de privacy audit was eveneens langer dan voorzien. Enerzijds, doordat er vanwege de lange doorlooptijd aanvullende interviews met het oog op de verificatie en validatie van de resultaten van de interne audit moesten worden gehouden. Anderzijds gaven bepaalde bevindingen in de interne audit aanleiding voor diepergaand onderzoek, mede ten aanzien van de wetsuitleg van de WPG naar de politiepraktijk. Diverse onderdelen van de WPG bleken voor meerderlei uitleg vatbaar. Vanwege samenloop met andere auditprojecten van MMC moesten planningen vanwege capaciteitsverdelingen worden bijgesteld. Niet onvermeld mag blijven, dat door de politie Zeeland veel capaciteit in de interne en de externe audit is gestoken.

Het eindrapport is tenslotte met inachtneming van het ontvangen commentaar vastgesteld.

7 Beperkingen van het onderzoek

Ons onderzoek was gericht op het geven van een oordeel met een beperkte mate van zekerheid over het stelsel van maatregelen en procedures met betrekking tot de aangegeven verwerkingen van politiegegevens en de overige in de WPG genoemde onderwerpen.

Incidentele inbreuken op het stelsel die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving behoeven daarom niet altijd te zijn geconstateerd.

Wij kunnen niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures.

De Korpsbeheerder, voor deze Korpschef van de politie Zeeland, heeft geen gebruik gemaakt van haar bevoegdheid ingevolge artikel 2, lid 4, RPAP om MMC de toegang te weigeren tot andere dan de met name genoemde verwerkingen van politiegegevens in par. 4. MMC heeft, gezien de doelstelling van het oordeel, het verschaffen van beperkte zekerheid en de deelname van de interne auditors aan haar auditteam, volstaan met het houden van interviews en het uitvoeren van deelwaarnemingen op de ontvangen documentatie.

8 Verspreidingskring van het rapport

Het auditrapport is vertrouwelijk en niet bestemd voor het maatschappelijk verkeer.
De specifieke doelgroep waarvoor het rapport is bestemd, bestaat uit:

- de korpsbeheerder van politie Zeeland;
- de korpsleiding en door hen geautoriseerde functionarissen van politie Zeeland;
- de Hoofdofficier van het parket Middelburg;
- de Voorzitter van het College bescherming persoonsgegevens.

Het rapport mag verder uitsluitend met toestemming van de Korpschef en na overleg met MMC aan derden ter beschikking worden gesteld.

9 Oordeel

Op grond van onze in dit rapport beschreven werkzaamheden is ons niets gebleken op basis waarvan wij zouden moeten concluderen, dat de opzet en het bestaan van de maatregelen en procedures die in de borging van de wettelijke eisen moeten voldoen ten aanzien van de bescherming van de verwerkingen van politiegegevens door de politie Zeeland voor wat betreft:

> de inrichting van de organisatie op de WPG, de verwerkingen artikel 8; 9; 10, lid 1, a (CIE); 10, lid 1, onder c (RID); 12 (CIE); 12 (RID) van de Wet politiegegevens, alsmede de onderwerpen rechten van betrokkenen, privacyfunctionaris en audits in de Wet politiegegevens,

naar de stand van medio mei 2011, niet in alle van materieel belang zijnde opzichten hebben voldaan aan de gestelde normen, zoals dit is gespecificeerd in de bijlage V (transponeringstabel) van dit rapport.

Dit met uitzondering van de deficiënties in de opzet en het bestaan van het stelsel van maatregelen en procedures, zoals dit is gespecificeerd in de bijlage V van dit rapport.

Op grond van ons onderzoek hebben wij ons geen oordeel kunnen vormen over de opzet en het bestaan op van de maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien ten aanzien van:

> de verwerkingen artikelen 10, lid 1, onder b; 13, lid 1 en lid 3, van de Wet politiegegevens, alsmede het onderwerp Functionaris gegevensbescherming vanwege het ontbreken van de benodigde capaciteit en tijd tijdens de interne audit en de privacy audit, mede veroorzaakt door de complexiteit in de toepassing van het normenkader in de Wet en het Besluit politiegegevens in de politiepraktijk.

Toelichting bij het oordeel
Ons onderzoek was gericht op het geven van een oordeel met een beperkte mate van zekerheid met betrekking tot het stelsel van maatregelen en procedures van de bescherming van de verwerking van politiegegevens door de politie Zeeland.

De procedures die zijn uitgevoerd voor het verzamelen van de assurance-informatie zijn beperkter dan bij een opdracht tot het verkrijgen van een redelijke mate van zekerheid. Ons oordeel is met name gebaseerd op de informatie verkregen uit het beoordelen van alle relevante documenten, waaronder documenten in het kader van de managementcontrolcyclus, procesbeschrijvingen, autorisatieoverzichten, de inrichting van de informatiestructuur, alsmede het houden van interviews met de korpschef, key-functionarissen op stafniveau, de privacyfunctionaris, de informatiebeveiligingsfunctionaris, de projectleider interne audit, teams die politiegegevens verwerken, de functioneel applicatiebeheerder en facilitair beheerders van gebouwen. Wij hebben geen deelwaarnemingen uitgevoerd op politiegegevens in informatiesystemen, databases, dossiers, journaals, loggingen of andere bestanden. In informatiesystemen geïmplementeerde autorisaties zijn door ons niet onderzocht. Het oordeel biedt om die reden een beperkte mate van zekerheid.

Incidentele inbreuken op het stelsel die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van politiegegevens betrekking hebbende wet- en regelgeving behoeven daarom niet altijd te zijn geconstateerd.

Wij kunnen niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures.

Het interne auditteam van de politie Zeeland en de privacy auditor hebben met veel inzet, gedrevenheid en passie de interne audit en de privacy audit uitgevoerd. Vele malen zagen zij zich gesteld voor (tijdrovende) interpretatievraagstukken bij de vertaling van de WPG en het BPG naar de politiepraktijk. Zowel de memorie van toelichting WPG en de toelichting op het BPG bevatten op onderdelen geen concrete handvatten van de politiepraktijk.

Artikelen van het WPG en uitwerking daarvan in het BPG die betrekking hebben op onder meer autorisaties, ter beschikking stellen, geautomatiseerd vergelijken, in combinatie met elkaar verwerken, verwijderen, bewaren en vernietigen van politiegegevens zijn nauw aan elkaar verwant en beïnvloeden integraal iedere verwerking van persoonsgegevens. Een verwerking van persoonsgegevens kent op onderdelen een eigen regime (artikel 8, 9, 10, 12 en 13 verwerkingen). Tussen die verwerkingen van politiegegevens worden politiegegevens uitgewisseld.

Een afwijking van een norm in één van die verwerkings- of interactiefasen kan als het ware een kettingreactie veroorzaken in het rechtmatig verder verwerken van politiegegevens in de verwerkingsketen. Zowel op regionaal, interregionaal, landelijk als internationaal niveau. Het beoordelen van de bevindingen in die integrale ketenverwerking stelt de auditors voor dilemma's. Dient een deficiëntie (afwijking van de norm) in één van de normen in de ketenverwerking te leiden tot een deficiëntie ten aanzien van de andere normen? Wanneer is er sprake van een non-conformiteit? Dit zou er toe leiden dat het in strijd handelen met één van die normen de gehele keten negatief zal beïnvloeden.

Daarnaast waren op landelijk niveau (onder meer de Raad van Korpschefs, Rijksauditdienst en de Departementale Audit Dienst van het Ministerie van Veiligheid en Justitie) discussies gaande over de omvang en diepgang van de privacy audit, alsmede de status van zowel de interne auditor als de privacy auditor. Van de zijde van het College bescherming persoonsgegevens zijn tot dusver geen (bruikbare) inzichten of aanwijzingen met betrekking tot de omvang en diepgang van de privacy audit WPG openbaar gemaakt.

Vanwege beperkingen in de capaciteit en de doorlooptijd zijn niet alle normen van de WPG en het BPG op naleving in de praktijk tijdens de interne audit en de privacy audit onderzocht kunnen worden. In de bijlage I en V is dit op de betreffende onderdelen aangegeven. In de bijlage IV is bij het organisatieoverzicht van de politie Zeeland aangegeven welke bureaus niet in de privacy audit zijn betrokken. Vanwege de hierboven bedoelde interactie tussen de schakels in de verwerkingsketen, heeft MMC ervoor gekozen om zoveel mogelijk, per norm, per fase van een verwerking van politiegegevens en de bevindingen te beoordelen om hiermee recht te doen aan de inspanningen van de politie Zeeland om zich naar vermogen aan de WPG te houden. Ten aanzien van de verwerkingen van politiegegevens die niet of niet voldoende zijn onderzocht komt MMC tot een oordeelonthouding.

In de Handreiking Normstelling WPG is er van uitgegaan, dat de implementatie van de WPG een plaats zou krijgen in de bestaande procesbeschrijvingen van de politie, dan wel in een afzonderlijke procesbeschrijving of instructie (de zogenaamde opzet). Zonder toereikende opzet is de sturing van de WPG in de management control cyclus, alsmede het toetsen van de naleving van de WPG in de politiepraktijk, in redelijkheid niet of nauwelijks controleerbaar. Tijdens de interne audit is dit op onderdelen bewaarheid. Niettemin is aanvullend in de interne audit en tijdens de privacy audit het bestaan aan de hand van groepsinterviews met teamchefs en een aantal key-functionarissen verder onderzocht om zoveel mogelijk inzicht te verschaffen in de naleving van de WPG in de praktijk.

De bijlage I met de bevindingen bevat een eindbeoordeling van de bevindingen. Hier wordt geen onderscheid gemaakt tussen de opzet en het bestaan. Indien in de opzet of het bestaan een deficiënte voorkomt, wordt de eindscore een deficiëntie. In de bijlage V: Transponeringstabel wordt de eindbeoordeling eveneens weergegeven, maar is de uitsplitsing naar de opzet en het bestaan wel zo veel mogelijk inzichtelijk gemaakt.

Advies vervolgaudit WPG
Wij adviseren om zo spoedig mogelijk, doch uiterlijk binnen een jaar, de aanvullende privacy audit op de door u gerealiseerde aanbevelingen te laten uitvoeren.

10 Verdere opbouw van het rapport

Het rapport van bevindingen wordt verder als volgt opgebouwd:

Bijlage I: Een rapportage in tabelvorm, die uit drie onderdelen bestaan. Eerst worden kort en bondig relevante normen uit de WPG per verwerkingenregime met scores ten aanzien van de naleving vermeld:

- V: de norm wordt voldoende nageleefd;
- D: er sprake is van een deficiëntie van de norm in opzet en/of bestaan;
- N: er is sprake van een non-conformiteit;
- A: een aanbeveling die in de heraudit moet worden uitgevoerd.

Aansluitend volgen per id van een norm uit de Handreiking Normstelling de bevindingen. Tenslotte volgen aanbevelingen indien dit voor de naleving van een norm relevant is.

Bijlage II: De aan het Basis Beveiligingsniveau Nederlandse Politie ingevolge artikel 4, lid 3, WPG ontleende normen. Per norm worden de scores, de bevindingen, en eventuele aanbevelingen vermeld.

Bijlage III: Een overzicht van de relevante documenten.

Bijlage IV: Een overzicht van de organisatie- en informatiestructuur van politie Zeeland.

Bijlage V: Een transponeringstabel, waarbij de scores in de bijlage I vertaald zijn naar de betreffende normen in de WPG en het BPG, onder vermelding van de relevante artikelnummers. Tevens is naar vermogen een uitsplitsing gemaakt van de scores naar opzet en bestaan.

Vaststelling en ondertekening

Capelle a/d IJssel, 20 juni 2011

w.g.

[redacted]
Partner-aandeelhouder

w.g.

[redacted]
Director IT & Compliance
Privacy auditor WPG

Bijlage I: Managementsamenvatting, normen en bevindingen

Toelichting

Een hoofdstuk met bevindingen vangt aan met een managementsamenvatting in tabelvorm. Hierin zijn de beheersdoelstellingen per verwerking uit de Handreiking Normstelling WPG in één zin samengevat. De id nummers van de verkorte beheersdoelstellingen komen overeen met die met de volledige tekst van beheerdoelstellingen met vermelding van de relevante wetsartikelen van de WPG en het BPG in de Handreiking Normstelling WPG. Voor de letterlijke tekst van de beheersdoelstellingen wordt kortheidshalve naar deze Handreiking verwezen.

Rechts in een managementtabel wordt aangegeven hoe de onderzoeksbevindingen op de naleving van de normen hebben gescoord. De soorten en de betekenis van de scores zijn ontleend aan Contouren voor Compliance, de handreiking bij het Raamwerk Privacy Audit van het CBP. De scores fungeren tegelijk als conclusies. De bijlage V bevat een transponeringstabel, waarin de betreffende wetsartikelen uit de Handreiking Normstelling WPG met de scores uit de managementtabellen, maar uitgeplitst naar opzet en bestaan zijn opgenomen.

De managementsamenvatting biedt in deze vorm per verwerking van politiegegevens of ander onderzoeksobject een snel overzicht van waar het goed gaat en waar het beter kan.

Een tabel met de managementsamenvatting wordt gevolgd door een tabel met bevindingen. De id.nrs in de tabellen met bevindingen corresponderen met de id.nrs in de daarboven vermelde managementabellen.

Soms slaan bevindingen integraal terug op meerdere beheersdoelstellingen. In dat geval zijn meerdere id. nrs van beheersdoelstellingen bij een veld met bevindingen verantwoord. Het kan ook zijn dat een aanbeveling betrekking heeft op meerdere beheersdoelstellingen. In dat geval komen ook meerdere id.nrs van beheersdoelstellingen en daaraan gerelateerde bevindingen bij een veld voor een aanbeveling voor. Dit voorkomt onnodige herhalingen en komt de leesbaarheid van het rapport ten goede.

Toelichting scores

V: Voldoende. Indien geen wezenlijk verschil wordt vastgesteld, functioneert het (deel)object of de beheersmaatregel conform de beheersdoelstelling.

N: Non-conformiteit. Een structurele (stelselmatige) materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de op basis daarvan door het bevoegde gezag vastgestelde instructie of richtlijn waardoor de bescherming van de persoonsgegevens van één of meer betrokkenen in ernstige mate is of kan worden geschaad. Ingeval van een geconstateerde non-conformiteit kan geen goedkeurend oordeel worden gegeven.

D: Deficiëntie. Een structurele (stelselmatige) niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de op basis daarvan door het bevoegde gezag vastgestelde instructie of richtlijn waardoor de bescherming van de persoonsgegevens van één of meer betrokkenen niet in ernstige mate is of kan worden geschaad.

A: Aanbeveling. Ter verbetering van de bestaande situatie uit te voeren aanbeveling in samenhang met een geconstateerde deficiëntie of non-conformiteit.

- (liggend streepje). De norm is niet op de politie Zeeland van toepassing. De reden hiervan kan zijn dat een verwerkingsvorm niet wordt uitgevoerd of dat een bepaald onderwerp niet aan de orde is.

Een score **I** (incidentele niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de op basis daarvan door het bevoegde gezag vastgestelde instructie of richtlijn waardoor de bescherming van de persoonsgegevens van één of meer betrokkene(n) niet in ernstige mate is of kan worden geschaad) wordt niet in de tabel meegenomen. Als de omvang en de aard van incidenten op een bepaalde norm naar het oordeel van de auditor te groot wordt, zal dit tot een deficiëntie of een non-conformiteit kunnen leiden. Dit komt dan in de score D of N tot uiting.

Toelichting gebruikte afkortingen in de managementtabellen:

ID: Identificatievolgnummer van de vraag, die met het nummer van de beheersdoelstelling in de hierna volgende tabellen in het rapport en in de Handreiking Normstelling WPG corresponderen. Indien er in een managementtabel meerdere zelfde id nummers voorkomen, betekent dit dat er in de beheersdoelstelling ook meerdere onderdelen voorkomen.
CBP: College bescherming persoonsgegevens
PF: Privacyfunctionaris
Tbs: Ter beschikking stellen (het beschikbaar stellen van politiegegevens binnen het politiedomein)
Vst: Verstrekken (het beschikbaar stellen van politiegegevens buiten het politiedomein)
Icmev: In combinatie met elkaar vergelijken
Avps: Ambtenaren van politie
Vzv: Voor zover
OTAP: Aparte omgevingen voor het ontwikkelen, testen, accepteren en in productie nemen van applicaties
IBF: Informatiebeveiligingsfunctionaris
Board VIP: Formeel overleg plaatsvervangend korpschefs Zuid-6

BVH: Basis Voorziening Handhaving
BVO: Basis Voorziening Opsporing
BVCM: Basis Voorziening Capaciteits Management
HKS: Herkenningsdienstsysteem
HKD: Herkenningsdienst
LMF: Landelijk Meldings Formulier
BPS: Bedrijfsprocessensysteem
P.G: Procureur Generaal
RIO: Regionale Informatie Organisatie
Zuid6: De zuidelijke politiekorpsen Zeeland, Midden en West Brabant, Brabant-Noord, Brabant Zuid-Oost, Limburg-Zuid, Limburg-Noord
RIK: Regionaal Informatie Knooppunt
DIK: Districtelijk Informatie Knooppunt
TC: Teamchef
HCIE: Hoofd Criminele Inlichtingen Eenheid
BBNP: Basis Beveiliging Nederlandse Politie
MT: Management team
PID: Project Initiatie Document (m.b.t. de implementatie van de WPG)
PDC: Product Diensten Catalogus
FCM: Foto Confrontatie Module
DCS: Digitale Communicatie Sporen
IB: Integrale Bevraging
ABS: Autorisatie Beheer Server
TGO: Team Grootschalig Optreden

1.1 GO: Gebruikersorganisatie

1.1.1 Inrichting van de organisatie

ID	Beheersdoelstellingen	V	D	N	A
1	Organisatieplan met beschrijving van alle organisatieonderdelen		X		X
1	Een beschrijving van de organisatorische maatregelen die genomen zijn om de organisatie op de beheersdoelstellingen van de WPG in te richten		X		X
2	Overzicht per korpsonderdeel van alle specifieke verwerkingen / regimes /informatiesystemen /applicaties		X		X
3	Overzicht benoemde proceseigenaren voor verwerkingen van politiegegevens		X		X
4	Migratieplan Wpolg naar WPG, projectplannen, implementatieplannen, voortgangsrapportages		X		X
5	Documenten borging managementcyclus: korpsbeleids- en jaarplan, districts/divisiejaarplannen, maraps		X		X
6	Aanwijzing bevoegde functionarissen		X		X

ID	Bevindingen
1	De politie Zeeland beschikt over documenten waarin de organisatie en alle organisatieonderdelen zijn beschreven. In totaal gaat het om 31 documenten. De documenten zijn opgenomen in de bijlage 1 van dit auditrapport.
1	Een beschrijving van concrete organisatorische maatregelen van de organisatie op de beheersdoelstellingen van de WPG is aanwezig in de vorm van het PID en de andere documenten die onder de migratie naar de WPG (id.nr. 4) zijn verantwoord. Verder zijn samengevat de volgende maatregelen genomen. De korpsleiding van de politie Zeeland heeft bij gelegenheid van de in werking treding van de WPG opdracht gegeven tot een implementatietraject WPG. WPG-opleidingen en themadagen zijn geïnitieerd. Bevoegde functionarissen zijn opgeleid. Het belang van de WPG dringt steeds meer serieus tot de werkvloer door. De laatste twee jaar is het draagvlak voor de WPG binnen de organisatie toegenomen. Merkbaar is dat er gezamenlijk steeds meer op een goede manier over de WPG wordt gesproken. De nadruk ligt hierbij op de noodzaak voor het vastleggen van politiegegevens. Medewerkers gaan ook steeds meer informeren over of dit mag, alvorens zij politiegegevens verstrekken. Men realiseert zich de WPG steeds beter. Het belang van de WPG wordt op initiatief van de korpschef steeds meer bij het OM op de agenda gezet. Over de resultaten en de voortgang laat de korpsleiding zich op een praktische manier schriftelijk dan wel mondeling bij gelegenheid door de projectleider WPG informeren. Ter besluitvorming voorgelegde documenten in het MT worden geformaliseerd, zoals het PID, de procesbeschrijving verwerking van politiegegevens en de procesbeschrijving voor de RID. De voortgang van de implementatie van de WPG wordt in het MT besproken. Voor wat betreft de communicatie in de lijn, zijn de lijnen kort en vaak mondeling. Wat de sturing op de implementatie WPG betreft is hierdoor op korpsleidingniveau relatief weinig documentatie over beschikbaar. Wisseling van de wacht op het niveau van de korpsleiding en de projectleiding WPG zorgden voor complicerende factoren. Naast de reguliere werkzaamheden legde de reorganisatie van de politie Zeeland evenals veranderingen in de informatie-infrastructuur, zoals de implementatie van BVO, BVO, BVH en BVCM veel beslag op de politie Zeeland. Reeds onder het regime van de Wet politieregisters beschikte de politie Zeeland over een privacyfunctionaris, een informatiebeveiligingsfunctionaris, een functionaris gegevensbescherming en een medewerker privacyzaken, die zich met alle voorkomende privacy- en daarmee samenhangende informatiebeveiligingszaken bezig houden. Die adviserende en toezichthoudende functies zijn onder het regime van de WPG gecontinueerd. In het voorjaar 2010 heeft de korpsleiding besloten om conform de WPG ter voorbereiding op de (externe) privacy audit, de interne audit uit te laten voeren. Hiervoor is een team samengesteld bestaande uit een projectleider interne audit, een senior controller, de privacy functionaris, de informatiebeveiligingsfunctionaris en de medewerkster privacyzaken. In juli 2010 is de interne audit gestart. De korpsleiding investeert bewust in de in- en externe audit om helder te krijgen welke maatregelen nog zonodig moeten worden genomen om de naleving van de WPG bij de politie Zeeland te borgen. Een analyse van de in het korps aanwezig procesbeschrijvingen die in de opzet voor de borging van de WPG moet voorzien, leidde tot het inzicht dat een behoorlijk aantal van de bestaande procesbeschrijvingen (verder) aan de WPG moest worden aangepast dan wel op onderdelen op de managementcontrolcyclus in het korps moet worden toegespitst. De korpsleiding onderkent de noodzaak van goede procesbeschrijvingen en is zich bewust dat hier nog een inhaalslag moet worden geleverd. De korpschef is voorzitter van de Board VIP Zuid 6. In de Board komen informatiseringsaangelegenheden aan de orde, waaronder de WPG. Aangezien één van de zuidelijke politieregio's WPG-procesbeschrijvingen ontwikkelt, is bewust gekozen voor het overnemen van die procesbeschrijvingen zodra deze landelijk beschikbaar worden gesteld. Naar verwachting zal dit binnen korte tijd het geval zijn. In opdracht van de korpschef werd, in haar hoedanigheid van voorzitter van de board VIP in de zes zuidelijke regio's en in het kader van het implementatietraject WPG een business case WPG opgesteld. Doel daarvan is om de situatie op het gebied van de implementatie WPG in die zes korpsen te duiden, op basis waarvan een keuze mogelijk is tot het gezamenlijk verder optrekken, opdat de verdere implementatie sneller en efficiënter kan worden afgerond. Ingeval zich op het terrein van de WPG ontwikkelingen voordoen wordt dit in de beheersdriehoek besproken. De korpsleiding laat zich door de projectleider WPG op de hoogte houden en heeft het voornemen om aan de hand van de uitkomst van de externe audit waar nodig verdere stappen te ondernemen. Tenslotte worden de landelijke ontwikkelingen op het terrein van de WPG gevolgd. Ondersteuning op dit terrein gaat wellicht via het politiediensten centrum lopen. De implementatie van de WPG, waaronder de uitvoering van de externe privacy audit, wordt nu de laatste vier maanden door de Raad van Korpschefs opgepakt. In onderlinge coördinatie is men van plan om op dit terrein van elkaar te leren. Zo speelde de discussie over de interne en externe audit. Landelijke coördinatie is ook voorstelbaar op bijvoorbeeld de autorisatieserver.

ID	Bevindingen
2	Een overzicht per korpsonderdeel van alle specifieke verwerkingen / regimes /informatiesystemen / applicaties is voorhanden. Daarnaast is inzicht in de mappenstructuur op de kantoorautomatiseringsomgeving van de politie Zeeland en de daarbij behorende autorisatiestructuur van belang. De applicaties BVH en BVO minder (BVH) of in het geheel niet (BVO) zijn niet geschikt voor het opslaan van alle voorkomende vormen en formaten van politiegegevens, danwel om omvangrijke complexe onderzoeksdossiers aan te maken en te beheren. Hierdoor is het momenteel onvermijdelijk om naast de BVH en de BVO een andere opslagmogelijkheid aan de gebruikers aan te bieden in de vorm van de kantoorautomatiseringsomgeving. Hiertoe werd voorgeschreven dat, indien er naar de Microsoftomgeving uitgeweken moet worden, politiegegevens slechts op de zogenoemde O-schijf mogen worden verwerkt. De O-schijf is hiertoe onderverdeeld in hoofdmappen die gerelateerd zijn aan de verschillende verwerkingen van de WPG. In grote lijnen wordt de O-schijf voor de meest voorkomende verwerkingen als volgt gebruikt: • De artikel 8 omgeving is onderverdeeld in jaargangen waardoor de verwerkingstermijnen van een artikel 8 verwerking gehanteerd kunnen worden. De oudste informatie dateert uit het jaar 2005. Om, met inachtneming van de beperkingen van Microsoft toch zo veel mogelijk te voldoen aan de artikel 8 bepalingen, wordt er onderscheid gemaakt in autorisaties. Immers, Microsoft kent niet de mogelijkheid om de toegang te beperken op basis van hit/no-hit voor gegevens die ouder zijn dan één jaar. Momenteel zijn de jaargangmappen op de volgende wijze geautoriseerd. De recentere jaargangmappen, vanaf 2009, zijn breed geautoriseerd voor alle operationele gebruikers. De oudere jaargangmappen, dus 2008 en ouder, zijn slechts geautoriseerd voor medewerkers van de RIO en de privacyfunctionaris t.b.v. zijn toezichttaak. De ervaring leert dat het "dichtzetten" van mappen ouder dan één jaar in de praktijk onwerkbaar is omdat in vele gevallen alsnog of aanvullend aan een zaak gewerkt wordt. In de artikel 8 omgeving mag slechts informatie worden opgeslagen onder vermelding van het onderhavige BVH registratienummer in de naamgeving van de opgeslagen informatie. • De artikel 9 omgeving is onderverdeeld in 09-actueel, 09-ingezonden en 09-parkeer. Deze mappen zijn successievelijk onderverdeeld in onderzoeksmappen per aangemelde artikel 9 verwerking. Een onderzoeksmap is onderverdeeld in mappen voor het onderzoeksdossier en werkmappen voor respectievelijk de teamleden en ondersteunende organisatieonderdelen (observatieteam, forensische opsporing, digitale recherche, analisten, etc.). Hierop worden de daarbij behorende en onderling afwijkende autorisaties toegekend. Door deze structuur en autorisatietoekenning worden alle politiegegevens van alle deelnemende organisatieonderdelen, verwerkt t.b.v. de bewuste artikel 9 verwerking, in deze onderzoeksmap opgeslagen. Hierdoor ontbreekt de noodzaak voor de ondersteunende organisatieafdelingen om politiegegevens elders op te slaan waardoor het beheer en toezicht vereenvoudigd wordt. Tevens kan de bevoegd functionaris op deze wijze daadwerkelijk invulling geven aan zijn rol. o In de 09-actueel worden artikel 9 verwerkingen opgeslagen waaraan daadwerkelijk gewerkt wordt. o In de 09-ingezonden worden artikel 9 verwerkingen opgeslagen waarvan het procesdossier werd ingezonden naar het Openbaar Ministerie ter vervolging. De autorisatietoekenning op deze onderzoeksmappen wordt beperkt tot de medewerkers die toegang nog daadwerkelijk nodig hebben. (O.a. de bevoegd functionaris en medewerkers RIO). Periodiek wordt een lijst van ingezonden artikel 9 verwerkingen naar het plaatselijke parket verzonden met de vraag welke artikel 9 verwerkingen onderwijl in kracht van gewijsde zijn gegaan en/of ontneming van het wederrechtelijk verkregene heeft plaatsgevonden. Indien hiervan sprake is, is het doel van de artikel 9 verwerking behaald. Afhankelijk van de terugkoppeling door het OM is het mogelijk om de opgeslagen gegevens als volgt te verplaatsen: o Indien er sprake is van sepot of vrijspraak is het onderhavige delict niet opgelost. Indien opnieuw geprioriteerd, wordt de onderzoeksmap teruggeplaatst naar de 09-actueel om opnieuw opgepakt te worden. Indien niet geprioriteerd, wordt de onderzoeksmap verplaatst naar de 09-parkeer in afwachting van eventuele prioritering cq de verjaringstermijnen zoals genoemd in art. 70 van het Wetboek van Strafrecht. o Indien het procesdossier heeft geleid tot een veroordeling, wordt het hieraan ten grondslag liggende procesdossier als brondocument van het HKS antecedent verplaatst naar de artikel 13 omgeving, processen-verbaal en rapporten. o De overige "bruto" gegevens in de bewuste artikel 9 verwerking worden, indien niet langer noodzakelijk voor de politietaak, verplaatst naar de artikel 14 omgeving, zijnde verwijderde gegevens. De O-schijf is verder voorzien van een artikel 10, 11, 12, 13, 14 en 15 omgeving. Elk van deze mappen wordt geautoriseerd voor medewerkers welke deze nodig hebben voor hun, bij de aard verwerking passende, taak. Voor de gebruikers werd een handleiding voor de O-schijf opgesteld, te beschouwen als een werkinstructie, welke raadpleegbaar is op Intranet. De in Zeeland ontwikkelde mappenstructuur werd door de board-VIP van de Zuid-6 korpsen vastgesteld als zijnde de standaard voor de Zuid-6. Tevens werd door politie Zeeland, in samenwerking en afstemming met regio Brabant-Noord, een autorisatiematrix voor rolgebaseerde autorisatie op de 09-actueel opgesteld. Daarnaast werd op dezelfde wijze een autorisatiematrix voor beheerrollen op de gehele O-schijf opgesteld. Een soortgelijke afstemming en ontwikkeling voor de overige mappen/omgevingen op de O-schijf dienen nog nader ontwikkeld te worden. Bovenstaande werd en wordt in nauw overleg met de Windows-beheerders van de vtsPN VG-Zuid ontwikkeld en toegepast. Echter, door o.a. capaciteitsgebrek bij zowel de vtsPN VG-Zuid als bij de korpsen, is nog (mei 2011) niet alles gerealiseerd en geïmplementeerd. Actueel is gebleken dat vele korpsen uit den lande belangstelling hebben voor deze Zuid-6 ontwikkelingen en voornemens zijn om hierbij aan te sluiten.
3	Een overzicht met benoemde proceseigenaren die aan de operationele politietaken zijn gekoppeld is voorhanden. Hierin is echter nog geen expliciete relatie gelegd met de verwerkingen van politiegegevens in de zin van de WPG.
4	De politie Zeeland beschikt over documenten, waarin de migratie van de Wpolr naar de WPG planmatig is weergegeven. De bijlage III bevat een overzicht van die documenten. Dit zijn onder meer het regionale PID, een communicatieplan, een planningmatrix en een concept impactanalyse. Aangezien de migratie in samenwerking met de andere regiokorpsen van Zuid-6 is gestart, is ook de onderlinge taakverdeling tussen de deelnemers aangegeven. Concrete resultaten en/of voorgangsrapportages zijn echter niet aangetroffen.

ID	Bevindingen
5	Documenten ter borging van de reguliere korpsmanagementcyclus zoals het korpsbeleids- en jaarplan, districts/divisiejaarplannen, maraps over 2009 en 2010 zijn beschikbaar op Deltanet. In die documenten is echter over die jaren geen relatie gelegd met de implementatie en borging van de WPG. Recentelijk (januari 2011) is door de Korpsleiding een herverdeling gemaakt van portefeuilles waarin de WPG is opgenomen. Het voornemen is ook om in de genoemde documenten het sturen op de borging van de WPG mee te nemen.
6	De aanwijzing van de bevoegde functionarissen is formeel geregeld in het aanwijzingsbesluit Bevoegde functionaris. Individuele aanwijzingen van bevoegde functionarissen zijn ook voorhanden, maar het overzicht hieromtrent is niet meer actueel.

ID	Aanbevelingen
1	Ga door met het nemen van de nog benodigde maatregelen om de organisatie op de beheersdoelstellingen van de WPG in te richten.
2	• Haak aan bij het landelijk beleid om een doorstart te maken met de implementatie van de WPG; • Ontwerp de nog op te stellen documenten m.b.t. de WPG (procesbeschrijvingen / instructies eenduidig en herkenbaar en maak ze bekend op een aparte site op Deltanet; • Geef duidelijk de taken, rollen, functies en de daaraan verbonden verantwoordelijkheden aan in de proces- en procedurebeschrijvingen, protocollen, werkinstructies, handleidingen, aanwijzingen etc.; • Zet in de administratieve organisatie een stelsel van interne controle op, inclusief een rapportagestructuur (lijnverantwoordelijken controleren binnen hun domein het eigen proces); • Zet in de administratieve organisatie een stelsel van verbijzonderde interne controle (controle op stafniveau) op, inclusief een rapportagestructuur bijvoorbeeld door de FG; • Beding geregeld evaluaties in de AO. Monitor het proces voortdurend; • Voer een centrale regie en één methodiek bij de beschrijving van de processen.
3	Stel "een overzicht benoemde proceseigenaren voor verwerkingen van politiegegevens" op.
4	Stel een hernieuwd plan op voor de implementatie van de opzet en het bestaan van het stelsel van maatregelen en procedures om in de borging van de wettelijke eisen te voorzien.
5	Zie de aanbeveling bij ID 2, 3 en 4.
6	Update het overzicht van de bevoegde functionarissen i.v.m. functiewisselingen.

1.2 Artikel 8 (dagelijkse politietaak)

1.2.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen politiegegevens voor dagelijkse politietaak met concrete doelstellingen	X			
2	Politiegegevens verwerken tot aan periode van uiterlijk één jaar na datum eerste verwerking		X		X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens		X		X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen		X		X
6	Politiegegevens zijn voor doel van verwerking toereikend, terzake dienend en niet bovenmatig	X			
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet		X		X

ID	Bevindingen
1	Volgens de Procesbeschrijving verwerking van politiegegevens artikel 8/9 WPG, d.d. 3-8-2010, vastgesteld door de plaatsvervangend korpschef, (verder te noemen Procesbeschrijving verwerking politiegegevens) mogen politiegegevens ingevolge artikel 8 uitsluitend in BVH worden opgeslagen. Alleen in de gevallen dat dit systeem hiervoor niet toereikend is, mag gebruik worden gemaakt van de O-schijf van de kantoorautomatiseringsomgeving. Politiegegevens voor de dagelijkse politietaak worden in de praktijk voornamelijk in BVH en de kantoorautomatiseringsomgeving conform de procesbeschrijving verwerkt. In die zin zijn de verwerkingen in het kader van artikel 8 transparant. Daarnaast is een overzicht aanwezig met overige applicaties die op korpsniveau worden gebruikt en aan artikel 8 zijn gerelateerd. Uit het groepsinterview met de teamchefs van de districten komt naar voren, dat er naast BVH afzonderlijke verwerkingen in mappen worden bijgehouden zoals bijvoorbeeld overlast gevende autobestuurders. Verder wordt niet uitgesloten, dat zich deelbestanden met politiegegevens op USB-sticks en een stand-alone pc kunnen bevinden. Hier hebben zij niet of nauwelijks zicht op en dit geldt ook voor de sturing op dergelijke bestanden (zie in dat verband ook par. 1.2.2.3). Een enkele teamchef gaf aan, dat er voor het verwerken van politiegegevens de mappenstructuur op de O-schijf wordt gebruikt en dat medewerkers hier over zijn geïnstrueerd. Uit deelwaarnemingen op een beperkt aantal mappen uit de kantoorautomatiseringsomgeving blijkt, dat de mappen voornamelijk foto's en documenten als uittreksels uit de Kamer van Koophandel bevatten. Soms ook wel een verslag van een verhoor.
2	De procesbeschrijving verwerking van politiegegevens bevat een beknopte instructie voor het verwerken van artikel 8 politiegegevens gedurende een periode van één jaar na datum van eerste opname. De medewerkers in het korps zijn over de regels van het gebruik van artikel 8 gegevens op de hoogte gebracht door middel van voorlichtingsessies van de PF, documenten op het Intranet en via een WPG e-learning module. De applicatie BVH en de O-schijf van de kantoorautomatisering zijn echter niet voorzien van een functionaliteit waarmee de politiegegevens één jaar na datum van eerste verwerking voor de uitvoering van de dagelijkse politietaak worden afgeschermd. Dit leidt er in de praktijk toe dat er in de wijze van raadpleging geen onderscheid wordt gemaakt tussen de gegevens binnen en buiten de termijn van 1 jaar. Tijdens het groepsinterview bleek een meerderheid van de teamchefs deze bepaling niet te kennen.
3	Van gemeenschappelijke verwerkingen die schriftelijk aan het CBP moeten worden gemeld, is uit de interviews niet gebleken. Bij de PF en de IBF zijn deze soort van verwerkingen ook niet bekend.
4	Het verwerken van gevoelige gegevens is niet in een instructie of procesbeschrijving geregeld. Uit de interviews blijkt, dat het bewustzijn dat gevoelige gegevens slechts mogen worden verwerkt als dit in aanvulling op andere gegevens noodzakelijk is, aanwezig is.
5	Aan de rechtmatigheid van de verkrijging is geen aandacht besteed in de vorm van een procesbeschrijving of instructie. Gedurende de implementatie van de WPG is op het Deltanet wel aandacht aan dit onderwerp besteed. Uit de interviews komt naar voren, dat de rechtmatigheid van de verkrijging in de dagelijkse praktijk de aandacht heeft van de medewerkers zelf, de teamchefs, de kwaliteitsfunctionaris en/of de OvJ. De indruk tijdens de interviews was dat teamchefs en zijn medewerkers hier goed mee willen omgaan. In gevallen van twijfel is er ook intensief contact met de PF en de Infodesk. Als men voor de 8 verwerking informatie van het bedrijfsleven of een overheidsinstantie wil hebben, gebeurt dit langs de weg van de hiervoor in aanmerking komende BOB-middelen, zoals126 nd SV (vorderen van gegevens). Voor het verkrijgen van een machtiging van de OvJ zijn standaard formulieren beschikbaar. Uit het groepsinterview met de teamchefs kwam naar voren, dat rechtmatigheid met enige regelmaat ter sprake komt in briefings en werkoverleggen. Dit omdat onrechtmatigheid mogelijk consequenties voor de vervolging tot gevolg heeft. O.a. om medewerkers van de basispolitiezorg met deze aspecten kennis te laten maken wordt door hen voor een periode van drie maanden stage gelopen bij de recherche.
6	Aan het bewaken van de kwaliteit van politiegegevens wordt doorlopend aandacht besteed. Dit gebeurt in de vorm van instructies inzake het juist en nauwkeurig verwerken van politiegegevens. Voorbeelden hiervan zijn de gebruikershandleiding BVH; de BVH Gebruikersafspraken d.d. 28-9-2010; het Handboek BVH Hulpofficier van Justitie; BVH Handleiding HOvJ 2009; de BVH Lijst Maatschappelijke klassen; de Opdrachtverstrekking gegevensbeheerder politie Zeeland, versie 2.3 september 2009 voor BVH; het Schema mailverkeer True Blue (TB) na geconstateerde fout in BVH. Deze documenten zijn op het intranet te raadplegen. In de praktijk is iedere functionaris ook zelf verantwoordelijk voor de kwaliteit van de invoer en verdere verwerking van verzamelde politiegegevens. Dit is als zodanig verwoord in de procesbeschrijving verwerking van politiegegevens. Politie Zeeland heeft twee gegevensbeheerders die het monitoren van de kwaliteit van de invoer en verdere verwerking van politiegegevens als dagtaak hebben. Hiervoor wordt de geautomatiseerde tool True Blue gebruikt. Het gaat hier om zowel het geautomatiseerd als handmatig toepassen van de zogenaamde "kennisregels" conform de hiervoor gemaakte afspraken en speerpunten. Dit is een korpsaangelegenheid. Indien een rapporteur zich niet aan de afspraken houdt, gaat er automatisch een mail naar de rapporteur om zijn tekortkoming te herstellen. Indien de fout niet wordt hersteld, volgt een rappel. Indien niet adequaat wordt gereageerd, wordt een leidinggevende in kennis gesteld. Deze vorm van controle is in het leven geroepen als alternatief voor de steekproefcontroles van leidinggevenden. Gezien de functionaliteit van BVH en het volume van de invoer is een structurele controle op een andere manier niet doenlijk. Er wordt overigens in BVH zo min mogelijk gemuteerd vanwege de gebruiksonvriendelijkheid van de applicatie en de werkdruk van de politiemensen.

ID	Bevindingen
6	Als bewerkerovereenkomsten is de SLA (Service Level Agreement) met de vtsPN 2009 overgelegd. Relevant is met name paragraaf 3.1. Op de SLA gestoelde producten zijn de PDC (Producten en Dienstencatalogus) en de DAP (Dossier Afspraken en Procedures). Het laatstgenoemde product wordt per politiekorps opgesteld. De vtsPN levert producten en diensten op het gebied van informatie- en communicatietechnologie (ICT) aan o.a. de politiekorpsen Limburg-Zuid, Limburg-Noord, Brabant Zuid-Oost, Brabant-Noord, Midden- en West Brabant en Zeeland. (Hierna te noemen de Zuid-6). Een groot deel van deze diensten heeft betrekking op de collectieve infrastructurele voorzieningen. Deze diensten worden in opdracht van de Zuid-6 uitgevoerd. De medewerkers van de Zuid-6 zijn in de dagelijkse praktijk de afnemers van deze dienstverlening. De dienstverlening collectieve infrastructurele voorzieningen is onderwerp van dit SLA. Aanvullend levert vtsPN producten en diensten in opdracht van individuele korpsen. Voor de collectieve infrastructurele voorzieningen is een Producten en Dienstencatalogus (PDC) vtsPN, VG -Zuid beschikbaar, waarin alle onderdelen van de dienstverlening binnen dit concept voor integrale dienstverlening zijn opgenomen. De PDC vormt de basis voor het afsluiten van dit SLA, het SLA kan niet los van de PDC gezien worden. Voor het geheel aan af te nemen diensten in het kader van dit SLA wordt uitgegaan van de dienstbeschrijvingen en gerelateerde voorwaarden in de catalogus. In het SLA wordt specifiek vermeld welke diensten met betrekking tot welke objecten worden afgenomen en de bijbehorende service levels. Tevens wordt in het SLA opgenomen of en zo ja welke toevoegingen gelden op de diensten als beschreven in de PDC. Uitgangspunt bij het SLA is dat er geen verbijzonderingen per korps gemaakt worden op de diensten en gerelateerde producten, serviceprofielen en service levels. In het SLA wordt beschreven welke objecten de korpsen bij vtsPN in beheer brengen en welke condities daarvoor gelden. Wat de uitvoering van het beheer en de ondersteuning van de gebruikers betreft, baseert vtsPN zich hierbij op de best practices van de ITIL beheermethodiek. De SLA 2009 is geldig vanaf 1 januari 2008 en wordt telkens met een jaar verlengd. De huidige SLA is nog van kracht en zal vervangen worden door een landelijke SLA.

ID	Aanbevelingen
3	Scherp de cleandesk policy op de politie bureaus van de "blauwe teams" aan.
4-5	Regel de toegang van de toezichthouders tot politiegegevens als bedoeld in artikel 4, lid 4 en 5, WPG in een procesbeschrijving.
6	Zorg dat een afschrift van een recente SLA met de vtsPN met bijlagen beschikbaar is.

1.2.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid		X		X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd		X		X
3	Specifieke autorisaties voor avps die onder het beheer van de verantwoordelijke vallen		X		X
4	Specifieke autorisaties in bijzondere gevallen voor niet avps die onder het beheer van de verantwoordelijke vallen		X		X
5	Specifieke autorisaties in bijzondere gevallen voor avps die onder het beheer van een andere verantwoordelijke vallen		X		X

ID	Bevindingen
1 2 3 4 5	De politie Zeeland beschikt over een Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. De autorisatieprocedure voorziet in de autorisatie voor intern of onder intern gezag werkend personeel, autorisatie van personeel dat in dienst is van een ander politiekorps en tenslotte autorisatie van overige medewerkers, kort gezegd de zogenaamde externen. De documenten zijn raadpleegbaar op het Intranet (Deltanet) en zijn voor iedere gebruiker toegankelijk. Daarnaast zijn momenteel nieuwe standaard autorisatieprofielen en autorisatiematrixen in (een vergevorderd) stadium van ontwikkeling. In die zin beschikt de politie Zeeland over een autorisatiebeheerssysteem, waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld, met het oog op het voldoen aan de eisen van zorgvuldigheid en evenredigheid. De procesbeschrijving en het autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties van het project Implementatie Wet politiegegevens. De procesbeschrijving is momenteel in bewerking bij de IBF. Verder handelt de politie Zeeland in voorkomende gevallen conform de "Interregionale regeling autoriseren". Bij besluit van het Korpsbeheerdersberaad is deze regeling sinds februari 2004 op de politiekorpsen van toepassing. De gang van zaken m.b.t. autorisaties in de praktijk is als volgt. De direct leidinggevende vraagt voor zijn medewerker een autorisatie aan waarbij hij gebruik maakt van het voorgeschreven formulier dat eenmaal ingevuld, verstuurd wordt vanuit de postbus van de leidinggevende naar de Postbus Privacy. Tot de laatste genoemde postbus hebben drie medewerkers toegang: de informatie beveiligingsfunctionaris, de privacyfunctionaris en de medewerkster van de administratieve ondersteuning. Na toetsing aan de hand van een aantal bekende criteria wordt de aanvraag door hen vanuit de postbus autorisaties doorgezet naar vtsPN. Alle formulieren worden opgeslagen binnen de daartoe ingerichte administratie in Zeeland. De opslag geschiedt zowel in hard copy als digitaal. Voor de digitale opslag is geen database beschikbaar, waardoor er geen actueel beeld is van lopende autorisaties en welke rechten daarbij horen. Op dat punt is de politie Zeeland afhankelijk van de vtsPN. Er bestaat wel een goed zicht op elke binnenkomende aanvraag doordat elke aanvraag digitaal wordt getekend en wordt opgeslagen door een klein aantal medewerkers. Alle aanpassingen worden geregistreerd en elke aanvraag is afgedekt door een leidinggevende waarmee tegelijk de verantwoordelijkheid is belegd.

ID	Bevindingen
	De noodzakelijkheid om eerder verleende autorisaties in te trekken is divers. Dit is onder meer het geval bij wijzigingen van functie of verplaatsingen, detacheringen en tijdelijke tewerkstellingen. Bij het beëindigen van het dienstverband door pensioen of overlijden dan wel om een andere reden geldt een mondelinge afspraak met de afdeling personeel en organisatie dat alle mutaties, die betrekking hebben op de gevallen van uitdiensttredingen, gemeld worden bij de administratieve ondersteuning middels een formulier. Naar aanleiding van dat formulier wordt aan de vtsPN opdracht gegeven om alle autorisaties van de betreffende medewerker in te trekken. Uit het groepsinterview met de teamchefs komt naar voren, dat de toekenning van autorisaties conform de autorisatieprocedure plaatsvindt. Het hierna tijdig intrekken van autorisaties kan echter worden verbeterd. Bij ontslag of vertrek van een medewerker wordt dit op aangeven van personeelszaken gedaan en dit is goed geregeld. Bij tijdelijke medewerkers ligt dit anders. Indien een medewerker een tijdelijke autorisatie behoeft, wordt dit op het aanvraagformulier aangegeven en gaat men er van uit dat de verleende autorisatie na verloop van die termijn wordt ingetrokken. Indien nodig worden in voorkomende gevallen ook "externe" politiemedewerkers geautoriseerd, zoals politiemensen uit MW-Brabant, die bijvoorbeeld in het kader van de samenwerking met Zeeuwse teams zijn geautoriseerd voor de Zeeuwse BVH. Ook vakantiekrachten die tijdelijk en beperkt worden geautoriseerd. Het op eigen initiatief intrekken van die autorisaties door teamchefs gebeurt echter incidenteel. Door de IBF wordt op het beheer van de autorisaties toegezien. Uit deelwaarnemingen van de IBF blijkt, dat de autorisaties in het informatiesysteem BVH redelijk goed worden beheerd (m.u.v. het deautoriseren). Indien de IBF constateert dan een autorisatie niet overeenkomt met een schriftelijk toegekende autorisatie dan wel ten onrechte actief is, wordt dit aan de betreffende teamchef gemeld. In die gevallen wordt door de teamchef actie ondernomen. Een aantal medewerkers van het Openbaar Ministerie heeft leesrechten op BVH. Dit is gerealiseerd op grond van artikel 16, lid 1, onder c, juncto artikel 23 WPG. Artikel 16 WPG regelt de verstrekking van politiegegevens aan leden van het openbaar ministerie voor zover zij deze behoeven in verband met hun gezag of zeggenschap over de politie of voor de uitvoering van andere hun bij of krachtens de wet opgedragen taken. De bedoelde politiegegevens kan het OM altijd aan de politie verzoeken. Art. 23 WPG regelt dat de rechtstreekse verstrekking van politiegegevens kan plaatsvinden voor zover noodzakelijk met het oog op strafvorderlijke beslissingen omtrent opsporing en vervolging en de hulp aan slachtoffers van strafbare feiten, alsmede bij amvb aan te wijzen beslissingen. De genoemde amvb is er (nog) niet. Voor wat betreft de mogelijkheid van het rechtstreekse verstrekken is BVH (nog) niet voldoende adequaat ingericht. De toegekende autorisatie impliceert, dat het OM rechtstreekse toegang heeft tot alle politiegegevens in BVH. Deze situatie is zo gegroeid omdat er een structureel tekort is aan capaciteit bij politiepersoneel om alle vragen te beantwoorden die het OM op grond van artikel 16 WPG stelt. Inmiddels wordt aan compenserende maatregelen gewerkt. Door het OM wordt een overzicht aangeleverd van een zo beperkt mogelijk aantal medewerkers aan wie ingevolge artikel 16 WPG politiegegevens kunnen worden verstrekt. Bekeken wordt hoe de toegang tot het BVH zo veel mogelijk op de genoemde taken van het OM kan worden toegespitst, bijvoorbeeld door medewerkers van de afdeling executie uitsluitend toegang te verlenen tot de arrestantenmodule van BVH. Iedere geautoriseerde wordt schriftelijk op de ingevolge artikel 7 WPG verplichte geheimhouding gewezen. Tenslotte dienen geautoriseerden een geheimhoudingsverklaring te ondertekenen. Uit de deelwaarnemingen bleek eerder dat een aantal leden van het Openbaar Ministerie waren geautoriseerd voor toegang tot de BVH terwijl zij daartoe geen rechten meer zouden moeten hebben vanwege wijziging van functie of het verlaten van de werkkring. Een en ander bleek niet doorgegeven te zijn door de applicatiebeheerder van het Openbaar Ministerie. De betreffende autorisaties zijn direct ingetrokken.

ID	Aanbevelingen
1-5	Scherp het beheer van de autorisaties aan. Maak voor het beheer van de autorisaties gebruik van één ABS voor Zuid 6. Laat zo spoedig mogelijk de betreffende documenten door de board VIP formaliseren (m.u.v. de standaardprofielen). Laat alle raadpleeghandelingen van de medewerkers van het OM loggen. Controleer de logging periodiek steekproefsgewijs. Stel instructies vast voor het raadplegen van BVH door het OM.

1.2.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Zonder beperking geautomatiseerd vergelijken met soortgelijke politiegegevens tot 1 jaar na datum eerste verwerking		X		X
1	Politiegegevens niet vergelijken met grote hoeveelheden gegevens uit openbare of andere externe bronnen		X		X
2	Eén jaar na datum eerste verwerking uitsluitend geautomatiseerd vergelijken met soortgelijke politiegegevens		X		X
2	Uitsluitend de gerelateerde gegevens verder verwerken voor de dagelijkse politietaak		X		X
3	De hierboven bedoelde politiegegevens zonodig tbs voor verdere verwerking op grond van de artikelen 9, 10 en 12		X		X

ID	Bevindingen
1 2 3	Voor het geautomatiseerd vergelijken van artikel 8 gegevens en de daarmee samenhangende voorschriften in de WPG is geen procesbeschrijving of instructie voor BVH en de kantoorautomatiseringsomgeving voorhanden. Althans niet specifiek voor de basispolitie medewerkers en de recherche. Wel is het geautomatiseerd vergelijken meegenomen in de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence • versie 1.2, van 30 maart 2010. Die procesbeschrijving is toegespitst op de werkzaamheden [redacted] en is aan de WPG aangepast. Politiegegevens onder het regime van artikel 8 WPG worden, zoals eerder is opgemerkt, hoofdzakelijk in BVH en in de kantoorautomatiseringomgeving verwerkt. Beide omgevingen beschikken niet over een voorziening waarmee wordt verzekerd dat politiegegevens met het oog op de uitvoering van de dagelijkse politietaak na 1 jaar van datum eerste verwerking uitsluitend geautomatiseerd (hit-no-hit) voor die taak kunnen worden vergeleken. In de praktijk kunnen de politiegegevens dan ook worden geraadpleegd op dezelfde wijze als binnen de termijn van maximaal 1 jaar na eerste opname. Uit de interviews blijkt dat er voor de toepassing van "geautomatiseerd vergelijken" in de praktijk interpretatieverschillen op landelijk niveau zijn, waarover tot dusver op regionaal en landelijk niveau geen consensus is bereikt. Dit ondanks de Handreikingen van het PIWPG die aan dit onderwerp aandacht besteden. In de betreffende Handreikingen wordt ook opgemerkt, dat de Memorie van Toelichting op de WPG op dit onderdeel niet duidelijk is. Een van de opvattingen is, dat geautomatiseerd vergelijken niet aan de orde is bij het gebruik van de hit-no-hit functie in BVH en ook niet bij het gebruik van de zoekfunctie in Word in de mappen op de kantoorautomatiseringsomgeving, omdat er sprake is van één artikel 8 verwerking. In die zin wordt er niet geautomatiseerd vergeleken met politiegegevens in andere artikel 8 verwerkingen. Hier is sprake van enkelvoudig vragen of verificatie: een naam of ander gegeven invoeren en kijken of dit gegeven in BVH of de mappen voorkomt, een vorm van verificatie. De andere opvatting is dat er in dit geval wel degelijk sprake is van geautomatiseerd vergelijken. M.b.v. de landelijke applicatie BlueView kunnen door de geautoriseerden [redacted] landelijk alle BVH's en, afhankelijk van de BlueView autorisatie, landelijk alle hiervoor in aanmerking komende BVO registraties [redacted] geautomatiseerd worden bevraagd. Over het hier al dan niet sprake zijn van geautomatiseerd vergelijken, is landelijk discussie gaande. Dit geldt ook voor de tool Integraal Bevragen, waarmee naar verluid op landelijk niveau BVH, HKS en FCM kunnen worden bevraagd. Landelijke applicaties als BlueView en Integraal Bevragen vallen buiten de scope van de privacy audit bij de politie Zeeland. Politiegegevens, ook uit de artikel 8 omgeving, worden ter beschikking gesteld ten behoeve van artikel 9 of artikel 10 verwerkingen. Uit de artikel 8 omgeving (voornamelijk opgeslagen uit de BVH) kunnen rechercheurs [redacted] eigenstandig de voor hun taak relevante informatie halen en verder verwerken in hun eigen registraties. Dit d.m.v. aan executief personeel toegekende BVH autorisaties en autorisaties op de artikel 8 omgeving van de O-schijf [redacted]

ID	Aanbevelingen
1 2 3	Bevorder op landelijk niveau een eenduidige interpretatie van het begrip automatisch vergelijken. Neem in een procesbeschrijving of instructie de volgende onderwerpen mee (artikel 8, lid 1, 2 en 4 WPG): • het geautomatiseerd vergelijken van politiegegevens met het oog op de uitvoering van de politietaak met soortgelijke politiegegevens tot aan de periode van één jaar na datum van eerste verwerking; • het verbod om politiegegevens met grote hoeveelheden gegevens uit openbare of andere externe bronnen te vergelijken; • het uitsluitend geautomatiseerd mogen vergelijken van politiegegevens voor de dagelijkse politietaak met andere soortgelijke politiegegevens na 1 jaar na datum eerste verwerking op basis van hit-no-hit; • het uitsluitend verder verwerken van de gerelateerde gegevens met het oog op de uitvoering van de dagelijkse politietaak; • het ter beschikking stellen van de hiervoor genoemde politiegegevens voor verdere verwerking op grond van de artikelen 9, 10 en 12.
2	Zorg voor een functionaliteit in de artikel 8 informatiesystemen, waarmee wordt verzekerd dat politiegegevens met het oog op de uitvoering van de dagelijkse politietaak na 1 jaar van datum eerste verwerking uitsluitend geautomatiseerd voor die taak kunnen worden vergeleken. Neem tussentijds adequate compenserende maatregelen om aan artikel 8, lid 1, 2 en 4 te kunnen voldoen.

1.2.5 In combinatie met elkaar verwerken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens na 1 jaar na datum eerste verwerking uitsluitend icmev voor vaststellen verbanden	-			X
1	Uitsluitend gerelateerde gegevens verder verwerken voor de dagelijkse politietaak	-			
2	De hierboven bedoelde politiegegevens zonodig tbs voor verdere verwerking op grond van de artikelen 9, 10 en 12	-			
3	Voldoen aan regels voor het schriftelijk vastleggen van de icmev van de gegevens	-			
4	Voor icmev uitsluitend avps Regionale Infodesk autoriseren	-			
5	De avps Regionale Infodesk voldoen aan de specifieke kennis- en vaardigheidseisen.	-			

ID	Bevindingen
1 2 3	Voor het uitsluitend in combinatie met elkaar verwerken van politiegegevens met het oog op de uitvoering van de politietaak met soortgelijke politiegegevens na 1 jaar na datum eerste verwerking is geen procesbeschrijving of instructie voor BVH en de kantoorautomatiseringsomgeving voorhanden. Althans niet specifiek voor de basispolitie medewerkers en de recherche. Wel is het geautomatiseerd vergelijken meegenomen in de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence • versie 1.2, van 30 maart 2010. Die procesbeschrijving is toegespitst op de werkzaamheden [redacted] en is aan de WPG aangepast.
4 5	Uit de interviews komt naar voren dat in combinatie met elkaar verwerken in relatie tot artikel 8 verwerkingen in BVH en de kantoorautomatiseringsomgeving niet aan de orde is. BVH en de kantoorautomatisering omgeving bevatten geen functionaliteit voor het in combinatie met elkaar verwerken van politiegegevens met soortgelijke gegevens en geen specifieke functionaliteit voor het vastleggen van de protocolgegevens. Tegen die achtergrond zijn de beide omgevingen ook niet uitgerust met een protocolvoorziening. Wel is op de O-schijf een zogenoemde artikel 11 map (geautomatiseerd vergelijken/in combinatie verwerken) gerealiseerd welke in voorkomende gevallen gebruikt zou kunnen worden voor dit soort handelingen. Punt van aandacht is wel dat de politie Zeeland binnenkort de tool Brains in gebruik neemt. De beoordeling van de functionaliteit en het mogelijke gebruik van Brains is niet meer in de onderhavige privacy audit meegenomen.

ID	Aanbevelingen
1	Bevorder op landelijk niveau een eenduidige interpretatie van het begrip in combinatie met elkaar verwerken. Laat een aanvullende privacy audit uitvoeren naar de functionaliteit en het gebruik van de tool Brains binnen politie Zeeland.

1.2.6 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Vernietigen indien niet langer noodzakelijk en uiterlijk vijf jaar na de datum van eerste verwerking verwijderen		X		X
2	Na verwijdering maximaal 5 jaar bewaren en gebruiken voor afhandeling klachten en verantwoording van verrichtingen		X		X
2	Verwijderde gegevens na afloop van de bewaartermijn vernietigen		X		X
3	Verwijderde gegevens tijdens bewaartermijn niet verstrekken aan personen / instanties in 16 t/m 20, 23, 24 WPG		X		X
4	In bijzondere gevallen tijdens de bewaartermijn in opdracht bevoegd gezag t.b.v. hernieuwde 9 of 10 verwerking		X		X
5	Voldoen aan de regels schriftelijke vastlegging hernieuwde verwerking en ter beschikking stelling verdere verwerking		X		X
6	Afzien van vernietiging ingeval waarde voor cultureel erfgoed of historisch onderzoek conform regels Archiefwet		X		X

ID	Bevindingen
1 2 3	In de procesbeschrijving Verwerking van politiegegevens, worden m.b.t. bewaartermijnen en vernietiging van de artikel 8 verwerking de taken, bevoegdheden en verantwoordelijkheden beschreven en belegd bij de betrokken functionarissen, i.c. de proceseigenaar en functioneel beheerders. In de procesbeschrijving wordt vermeld dat dit conform de procesbeschrijving "gegevensbeheer" dient te geschieden. Deze procesbeschrijving is echter (nog) niet beschikbaar. In geval van een veroordeling wordt door het Openbaar Ministerie niet teruggekoppeld dat een uitspraak in kracht van gewijsde is gegaan. De aanwijzing afloopberichten van het college van PG's dient nog te worden herzien en op dit punt te worden uitgebreid. Hierdoor ontbreekt het signaal om de daarvoor in aanmerking komende artikel 8 gegevens tijdig te verwijderen of aan te passen. Slechts indien het OM structureel de veroordelingen/sepots terugkoppelt aan de politie, is het voor de politie mogelijk om gegevensbeheer op dat onderdeel in te richten. Daarbij komt dat BVH technisch niet de mogelijkheid kent om verwijderde gegevens als zodanig te "labelen". De O-schijf van de kantoorautomatisering is wel zodanig ingericht dat verwijderde gegevens in een map artikel 14 verwerking kunnen worden opgeslagen en op basis van toegekende autorisaties slechts zeer beperkt (voor afhandelen klachten en verzoeken tot kennisneming) kunnen worden gebruikt. De BVH is sinds 10 november 2008 in gebruik. De wettelijke regels met betrekking tot de bewaartermijn van de verwijderde gegevens na 5 jaar na datum van eerste opname is nog niet aan de orde. BVH kent niet de mogelijkheid om geautomatiseerd gegevens ouder dan vijf jaar te verwijderen. Indien de verwerkingstermijn van vijf jaar zal worden bereikt dient dit verwijderen handmatig en per registratie te gebeuren. De voorganger van BVH, zijn het Bedrijven processen systeem (BPS) kende wel een automatische mogelijkheid tot schoning op basis van de leeftijd van de opgeslagen gegevens. Dit schonen betekent echter vernietigen en geen verwijderen zoals bedoeld in artikel 14 WPG. De genoemde schoning van gegevens ouder dan vijf jaar gaat nog steeds door, waardoor BPS steeds "leger" wordt. BPS is, m.u.v. functioneel beheer, slechts te raadplegen door geautoriseerde medewerkers. Afhankelijk van de mogelijkheden van de functionaliteit wordt de tussentijdse vernietiging, de bewaring, de afscherming en de vernietiging van politiegegevens incidenteel handmatig door de functioneel beheerder uitgevoerd.

ID	Bevindingen
4 5	De procesbeschrijving van de politie Zeeland voor de artikel 8 verwerking bevat nog geen specifieke instructie inzake: a. de bijzondere gevallen waarin het noodzakelijk is om tijdens de bewaartermijn voor een art. 9 of 10 doelstelling (de omschrijving van het bijzondere geval, de noodzaak en het specifieke doel van de verwerking), politiegegevens ter beschikking te stellen voor hernieuwde verwerking op grond van artikel 9 of 10; b. de opdracht die in die gevallen door het bevoegde gezag moet worden verstrekt (datum, naam en functie en voorwaarden); c. het schriftelijk vastleggen van de hernieuwde verwerking van politiegegevens op grond van artikel 9 of 10, bedoeld in artikel 14, derde lid (protocolplicht). Voor wat betreft BVH en de kantoorautomatiseringsomgeving zijn de mogelijkheden voor het ter beschikking stellen voor hernieuwde verwerking op grond van art. 9 of 10 nog niet aan de orde. BVH heeft zoals eerder opgemerkt, niet de mogelijkheid tot opslag en rubricering van (tussentijds) "verwijderde" gegevens. De gegevens worden sinds 2008 ingevoerd en hebben de termijn van 5 jaar na laatste datum van invoer nog niet bereikt. Politiegegevens in BPS worden na afloop van de 5 jaartermijn vernietigd. De in gebruik zijnde informatiesystemen bevatten geen functionaliteit voor het vastleggen van de protocolgegevens.
6	De BVH is sinds 10 november 2008 in gebruik. Archivering van digitale gegevens ingevolge de Archiefwet is thans nog niet aan de orde. Voor wat betreft het fysieke archief wordt gehandeld conform de Selectielijst voor archiefbescheiden van (regionale) politieorganisaties 2004. Deel 2 onder punt 3 van de selectielijst bevat een regeling voor archiefbescheiden m.b.t. de uitvoering van de politietaak. Deze lijst spreekt echter nog over de Wet politieregisters. Hiervoor werd door de betrokken teamchef op landelijke vergaderingen aandacht gevraagd, maar dit heeft nog niet geleid tot actualisering van genoemd document. Vervolgens heeft de teamchef, eind 2009, op eigen initiatief en op basis van zijn kennis en ervaring een concept "Toegankelijkheid en bewaartermijnen van politiegegevens op grond van de WPG" opgesteld. Aan de hand van dit document worden de archiefbescheiden door de politie Zeeland beheerd.

ID	Aanbevelingen
1-6	Voorzie de applicaties, waarin artikel 8 gegevens worden verwerkt, van functionaliteiten waarmee aan de naleving van artikel 14 WPG kan worden voldaan. Besteed in een procesbeschrijving aandacht aan de regels als bedoeld in artikel 14 WPG.

1.2.7 Ter beschikking stellen van politiegegevens (tbs)

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde avps indien nodig voor hun taakuitoefening		X		X
2	Artikel 8 verwerkingen tbs voor verdere verwerking op grond van de artikelen 9, 10 en 12		X		X
3	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 1, genoemde ondersteunende taken		X		X
4	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 2, genoemde ondersteunende taken		X		X
5	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 3, genoemde ondersteunende taken		X		X
6	Tbs van politiegegevens uitsluitend weigeren of beperken in de wettelijk toegestane gevallen		X		X
7	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld	X			

ID	Bevindingen
1 2 3 4 5 6	De politie Zeeland beschikt niet over een specifieke procesbeschrijving of instructie voor artikel 8 verwerkingen inzake de ter beschikking stelling van politiegegevens: a. aan geautoriseerde avps indien nodig voor hun taakuitoefening; b. voor verdere verwerking op grond van de artikelen 9, 10 en 12; c. voor de ondersteuning van de politietaak (artikel 13, lid 1, 2 en 3 verwerkingen) d. de gevallen waarin de ter beschikking stelling van politiegegevens kan worden geweigerd of aan beperkende voorwaarden kan worden onderworpen; De ter beschikking stelling vloeit echter ook voort uit de Autorisatieprocedure met de standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. Het feit dat medewerkers geautoriseerd zijn voor de gegevens/applicaties die noodzakelijk zijn voor hun taak, resulteert in een structurele vorm van ter beschikking stelling. Zo heeft een rechercheur werkzaam t.b.v. een artikel 9 verwerking d.m.v. zijn autorisaties toegang tot artikel 8 informatie in BVH. Relevante artikel 8 informatie is zodoende zonder tussenkomst van een natuurlijk persoon beschikbaar voor de onderhavige artikel 9 informatie. Hieronder volgen een aantal voorbeelden uit de praktijk. Iedere avp van één van de politiekorpsen van Zuid 6 is geautoriseerd voor het raadplegen van de BVH van de andere Zuid 6 politiekorpsen. Daarnaast wordt alle artikel 8 informatie op bovenomschreven wijze ter beschikking gesteld van artikel 9 onderzoeken. Ook medewerkers van de Infodesk en van het bureau Misdaadanalyse hebben hiervoor toegang tot de artikel 8 omgevingen. Ingeval politiegegevens in een artikel 8 onderzoek de aanleiding vormen voor het opstarten van een artikel 9 onderzoek, wordt zowel in BVO als in de mappenstructuur op de O-schijf een map onder het regime van artikel 9 aangemaakt. De politiegegevens uit de artikel 8 omgeving die voor dit onderzoek nodig zijn worden dan ter beschikking gesteld van het artikel 9 onderzoek. Politiegegevens uit de artikel 8 omgeving, zoals aangifte van vermiste paspoorten of rijbewijzen worden ter beschikking gesteld aan een artikel 13 verwerking, zoals NSIS. Politiegegevens inzake tegen verdachte opgemaakte processen-verbaal inzake misdrijven en opgemaakte processen-verbaal van misdrijven met een onbekende dader worden in het HKS opgenomen. De bedoelde aangiften worden dagelijks in de BVH door hiertoe geautoriseerde medewerkers en beheerders van de Infodesk (HKD) handmatig uit de BVH geselecteerd met behulp van een specifiek menu. De opgemaakte processen-verbaal tegen verdachten worden door de kwaliteitsfunctionarissen aan de Infodesk geleverd met behulp van het landelijk melding formulier

ID	Bevindingen
	(LMF) uit de zaakdossiers. Politiegegevens over afgenomen vingerafdrukken worden in het HKS opgenomen (onder vermelding van het BVH-p.v. nr.). De HKD bekijkt in die gevallen of de vingerafdrukken conform de wet- en regelgeving rechtmatig zijn afgenomen.
7	In de WPG training die voor medewerkers en leidinggevenden in het korps wordt verzorgd, wordt aandacht besteed aan de geheimhoudingsverplichting inzake het verwerken van politiegegevens. Bij indiensttreding leggen ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
1 2 3 4 5 6	Besteed in een procesbeschrijving aandacht aan de regels voor de ter beschikking stelling van politiegegevens (artikelen 6, 8, 13,15 WPG en daarmee corresponderende artikelen BPG): a. aan geautoriseerde avps indien nodig voor hun taakuitoefening; b. voor verdere verwerking op grond van de artikelen 9, 10 en 12; c. voor de ondersteuning van de politietaak (artikel 13, lid 1, 2 en 3 verwerkingen) d. de gevallen waarin de ter beschikking stelling van politiegegevens kan worden geweigerd of aan beperkende voorwaarden kan worden onderworpen. Bezie in landelijk verband de mogelijkheden voor aanpassingen van BVH om de diverse verplichtingen van de ter beschikking stelling waar nodig optimaal te faciliteren. Dit geldt ook voor de gevallen waarin de ter beschikking stelling van politiegegevens kan worden geweigerd of aan beperkende voorwaarden kan worden onderworpen.

1.2.8 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG		X		X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen		X		X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MID)		X		X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden		X		X

ID	Bevindingen
1 2 3	De politie Zeeland beschikt niet over procesbeschrijvingen of instructies inzake: a. de voorwaarden voor verstrekkingen ingevolge paragraaf 3 van de WPG toegespitst op de specifieke 8, 9, 10, 12 en 13 verwerkingen; b. de functionarissen die bevoegd zijn om bepaalde categorieën van politiegegevens te verstrekken; c. de functionarissen die in voorkomende gevallen moeten beslissen over een verzoek om bepaalde categorieën van politiegegevens; d. de gevallen waarin om advies of voor een beslissing contact moet worden opgenomen met de privacyfunctionaris en/of andere daartoe aangewezen (bevoegde) functionarissen; e. het ingeval van verstrekkingen op grond van de artikelen 19 en 20 schriftelijk wijzen van ontvangers op de geheimhoudingsverplichting ingevolge artikel 7; f. het vastleggen van de verstrekkingen en de uitzonderingen voor die verplichting. De politie Zeeland beschikt weliswaar over de procesbeschrijving Verwerking van politiegegevens, maar de hierboven vermelde onderwerpen zijn niet toereikend voor de praktijk uitgewerkt. De Handreiking Verstrekkingen met de verstrekkingentabellen en de Verstrekkingenwijzer WPG zijn wel op het intranet voor iedere relevante medewerker raadpleegbaar maar kunnen niet worden beschouwd als procesbeschrijvingen of instructies waar de Handreiking Normstelling op doelt. De praktijk is, dat schriftelijke verzoeken van verzekeraars, advocaten, instanties, etc. centraal worden afgehandeld door een medewerkster van de afdeling Integriteit & Veiligheid. In de incidentele gevallen als zo'n verzoek rechtstreeks aan een team wordt gericht, wordt meestentijds door de betrokken medewerker meteen contact opgenomen met de afdeling Integriteit & Veiligheid over de afhandeling van het verzoek. Afdeling Integriteit & Veiligheid adviseert dan om het verzoek ter afhandeling naar hen door te sturen. Langs die weg wordt in de afhandeling van informatieverzoeken in de praktijk voorzien. De privacyfunctionaris wordt frequent per mail of telefonisch door operationele medewerkers benaderd om m.b.t. een actuele casus te adviseren in het wel of niet mogen verstrekken van gegevens. Daarbij wijst de privacyfunctionaris structureel op de protocolplicht van een verstrekking in de vorm van het opmaken van een zogenoemde I90 in de BVH zoals vastgesteld door de korpsleiding. Relevante medewerkers (wijkagenten, infodesk en RIK/DIK medewerkers) zijn daarnaast in het bezit van de verstrekkingenwijzer WPG waarin verstrekkingen en daarmee verband houdende voorwaarden voor de politiepraktijk zijn opgenomen. De door de politie Zeeland met (keten)partners afgesloten convenanten werden op relevantie en actualiteit onderzocht. Geconstateerd werd dat convenanten niet centraal worden opgeslagen en dat een totaaloverzicht ontbreekt. Hierdoor is onduidelijk of alle convenanten zijn verkregen en beoordeeld. Ook is gebleken dat convenanten deels zijn verlopen, niet zijn geactualiseerd of zijn achterhaald door nieuwe wetgeving. In sommige gevallen is niet duidelijk of de politie nog handelt zoals vastgelegd in een convenant. Een aantal convenanten zijn, van politiezijde, ondertekend door functionarissen die hiertoe niet gemachtigd of gemandateerd zijn of waren. Vervolgens werden de aangetroffen convenanten onderscheiden in de volgende categorieën: 1. Convenanten die slechts inspanningsverplichtingen behelzen van de deelnemende partijen en waarbij geen sprake is van gegevensuitwisseling. Indien conform het convenant wordt gewerkt, zijn de bepalingen van de WPG niet van toepassing. 2. Convenanten die, naast inspanningsverplichtingen van de deelnemende partijen, gegevensuitwisseling beschrijven. Indien dit gegevensuitwisseling betreft welke mogelijk is op grond van het reguliere verstrekkingenregime van de WPG en het BPG is

ID	Bevindingen
	er geen sprake van een zogenoemde gegevensuitwisseling ten behoeve van een structureel samenwerkingsverband ingevolge artikel 20 WPG. Uiteraard zijn de overige bepalingen van de WPG van toepassing, bijvoorbeeld in de vorm van het schriftelijk vastleggen (protocolleren) van de verstrekking van politiegegevens buiten het politiedomein. Of aan deze protocolplicht werd en/of wordt voldaan is niet na te gaan. Dit onder andere omdat de convenanten meestentijds dateren van vóór 1 januari 2008, zijnde de datum van inwerkingtreding van de WPG. 3. Convenanten die, naast inspanningsverplichtingen van de deelnemende partijen, gegevensuitwisseling beschrijven, noodzakelijk ten behoeve van het onderhavige samenwerkingsverband met het oog op een zwaarwegend algemeen belang. Dit betreffen zogenoemde artikel 20 WPG convenanten. Met betrekking tot de categorie artikel 20 WPG convenanten is het volgende geconstateerd. In de voorhanden zijnde convenanten zouden twaalf convenanten onder de werking van artikel 20 WPG kunnen vallen, met dien verstande dat van vier convenanten duidelijk is dat er gegevens worden uitgewisseld en van acht convenanten het, niet bevestigde, vermoeden bestaat dat er in afwijking van het convenant, politiegegevens worden verstrekt aan deelnemende partijen. Omtrent het protocolleren van eventuele verstrekkingen werd geen duidelijkheid verkregen. De onderhavige 12 convenanten voldoen (nog) niet, of (nog) niet geheel aan de daaraan te stellen eisen. In Zeeland werd door de Korpschef op 4 mei 2010 een modelconvenant en bijbehorend besluit vastgesteld. De twaalf convenanten zijn (nog) niet conform ingericht en essentiële bepalingen ontbreken. De volgende documenten zijn recentelijk opgenomen in de AO en gepubliceerd op Deltanet: de Handleiding structureel samenwerkingsverband, het Modelconvenant en - besluit art 20 WPG en het document Samenwerking en incidentele verstrekking. Met ingang van medio 2010 worden (nieuwe) structurele samenwerkingsverbanden, vallende onder de bepalingen van art. 20 WPG, conform de genoemde handleiding en m.b.v. het modelconvenant en -besluit gerealiseerd en schriftelijk vastgelegd. Voorbeelden hiervan zijn ernstige woonoverlast Middelburg, project Houdgreep te Terneuzen, en verschillende vormen van buurtbemiddeling in enkele gemeenten. Uit de interviews met betrekking tot het onderwerp verstrekkingen van politiegegevens ingevolge par. 3 WPG met de afzonderlijke teamchefs kwam onder meer het volgende naar voren. BBRE. De teamchef gaf aan dat verstrekkingen plaatsvinden (bijv. aan de gemeente in het kader van sociale uitkeringen) maar dat deze niet op de voorgeschreven wijze worden vastgelegd in een I-90 verstrekkingenmutatie, maar middels een passage in een journaal. VP. Door de VP worden politiegegevens verstrekt. Weliswaar is de Verstrekkingenwijzer WPG niet bij hen bekend, maar er wordt in voorkomende gevallen wel goed beoordeeld wat wel en niet verstrekt mag worden. Een probleem met het bij de VP in gebruik zijnde systeem BVV (Basis Voorziening Vreemdelingen) is, dat hiertoe diverse instanties / afdelingen van het ministerie van Veiligheid en Justitie voor rechtstreekse toegang zijn geautoriseerd. Bevraging van politiegegevens door deze instanties worden niet automatisch gelogd. Hierdoor kan op geen enkele manier door de VP worden vastgesteld welke politiegegevens zijn bevraagd en worden gebruikt. De teamchef heeft voor deze omissie aandacht gevraagd maar hiervoor kan niet op korte termijn een adequate logfunctionaliteit worden ontwikkeld. Indien de VP een verzoek om een verstrekking krijgt, waarvan men de rechtmatigheid niet vertrouwt, wordt het verzoek altijd doorverwezen naar de Infodesk. RT-1. De teamchef geeft aan dat schriftelijke verstrekkingen bij de RT1 niet voorkomen. Alle schriftelijke verstrekkingen gaan via de OVJ. (standaard oplossing). Mondelinge verstrekkingen vinden wel plaats maar hier wordt geen I-90 van opgemaakt (geen schriftelijke vastlegging). Vastleggingen komen dan ook niet voor in de uitdraaien I-90. JP. De teamchef en een teamlid geven aan dat verstrekkingen in principe conform de Verstrekkingenwijzer plaatsvinden met dien verstande dat door tijdgebrek en de grote hoeveelheid verstrekkingen niet altijd de juiste procedure wordt gevolgd. Dit leidt tot veelvuldige verstrekkingen zonder de wettelijk voorgeschreven vastlegging. De PF heeft a.d.h.v. een per organisatie-eenheid uitgedraaide I90 lijst geconstateerd dat medewerkers van de jeugdpolitie zeer divers omgaan met het gebruik van de I-90. Een incidentele medewerker bleek een groot aantal I-90 aangemaakt te hebben, terwijl zijn collega's met dezelfde taak, geen enkele I-90 hadden gemaakt. Vervolgens heeft de PF zijn bevindingen kenbaar gemaakt aan de jeugdpolitiemedewerkers inclusief de teamchef. Naar aanleiding hiervan werd de PF uitgenodigd op een werkoverleg van de jeugdpolitie waar hij uitleg en aandacht heeft gevraagd voor de wettelijke bepalingen m.b.t. verstrekkingen. De teamchef en een teamlid gaven aan dat ze zich bewust zijn van deze omissie maar verklaren geen oplossing voor het tijdgebrek te hebben. Dit komt doordat er teveel werk met een hogere prioriteit is. Een belangrijk punt in dit kader is ook het ontbreken van een adequate functionaliteit voor de logging in de applicatie BVH. Ook het muteren via de I90 voorziening vraagt veel handmatig werk. De instructie hoe een I-90 aan te maken is opgenomen in de gebruikershandleiding BVH. Uit het groepsinterview met de teamchefs "blauw" kwam bij een meerderheid van hen naar voren, dat verstrekkingen in feite uit de opgemaakte mutaties blijken. Hierbij valt te denken aan de, bijvoorbeeld door wijkagenten en jeugdpolitiemedewerkers, opgemaakte mutaties waarin vermeld staat dat bepaalde instanties in kennis werden gesteld. Volgens een teamchef worden incidentele schriftelijke verstrekkingen (door bijvoorbeeld het wijksecretariaat) vastgelegd in het postregistratiesysteem. Of de, door de korpsleiding vastgestelde, I90 procedure in de BVH veel wordt gebruikt, is bij hen onbekend. De algemene indruk is dat verstrekkingen voornamelijk worden vastgelegd in de vorm van mutaties. Alle schriftelijke verzoeken om verstrekkingen van politiegegevens en de afhandeling hiervan wordt op centraal niveau door de afdeling Post- en archief zaken (PAZ) in het postregistratiesysteem Corsa, verantwoord met de zinsnede "verzoek inlichtingen uit politieregisters. Over de periode 1-1-2010 – 31-12-2010 zijn deelwaarnemingen uitgevoerd op alle inkomende verzoeken en de daarop volgende verstrekkingen. Voorbeelden van verstrekkingen zijn: • Verzekeringsmaatschappijen betreffende ongevallen en misdrijven ten behoeve van hun cliënten; • Gemeenten betreffende naturalisatieverzoeken door burgers; • Gemeenten betreffende decoratievoorstellen voor burgers; • Gemeenten in verband met de afgifte van Drank en Horecavergunningen; • Advocaten ten behoeve van civiele vorderingen van hun cliënten. Uit de deelwaarnemingen zijn geen indicaties naar voren gekomen voor het in strijd handelen met de bepalingen inzake de verstrekkingen in par. 3 WPG. Voor het vastleggen van verstrekkingen uit BVH kan de functionaliteit I90 worden benut. Zoals uit het voorgaande al blijkt, zijn alle medewerkers van de politie Zeeland hierop door de privacyfunctionaris geattendeerd. Uitgevoerde deelwaarnemingen op de I90 vastleggingen, over de periode van 1-8-2009 – 1-8-2010, leverden de volgende aantallen op. Team Goes en Team Schouwen

ID	Bevindingen
	Duiveland: 4; Team Hulst: 6; Team Terneuzen: 10; Team Reimerswaal: 1; Team Goes: 18; Team Middelburg 68; Team Sluis: 5; Team JP (6 á 7 wijkagenten): geen; medewerker Kabinetszaken: 220; Infodesk: 75; Jeugdpolitie 257 (8 medewerkers); Team RT 1: 2; Team RT: 2; BBRE: geen; Veiligheidshuis systeem 770; Op de code E62 voor bestuurlijke rapportages sinds het opstarten BVH: 3. Uit het interview met de JP kwam verder nog naar voren, dat door de aard van de werkzaamheden, o.a. de intensieve contacten van de jeugdpolitie met het Veiligheidshuis, er geregeld een situatie ontstaat dat politiegegevens mogelijk aan derden verstrekt worden, die vervolgens door deze ontvangers weer gebruikt wordt voor andere doeleinden. Bij de verstrekking wordt door de jeugdpolitie niet structureel aangegeven dat dit gebruik verboden is. Het risico is, dat de ontvangers later in strijd handelen met de geheimhoudingsplicht zoals verwoord in art. 7 WPG. Tijdens het groepsinterview met de teamchefs is gevraagd of de zogenoemde "Verstrekkingenwijzer" bekend is en gebruikt wordt. Een groot deel van de aanwezigen kent deze verstrekkingenwijzer. De verstrekkingenwijzer is deels in hard-copy op de bureaus aanwezig en anders digitaal raadpleegbaar op het Intranet. Volgens een teamchef zijn medewerkers bang om politiegegevens ongewild naar buiten te "lekken". Regelmatig wordt overlegd met brigadiers/teamchefs en/of PF of een verstrekking überhaupt wel mogelijk is. Op de vraag of men de verschillende mogelijkheden tot verstrekking van politiegegevens buiten het politiedomein kent, in de vorm van doorbreking van: • de geheimhoudingsplicht indien noodzakelijk voor de politietaak (art. 7 WPG); • een incidentele verstrekking in geval van een zwaarwegend algemeen belang (art. 19 WPG); • of een verstrekking in het kader van een structureel samenwerkingsverband (art. 20 WPG), is door de aanwezigen geantwoord dat de kennis over deze verstrekkingsmogelijkheden zeer beperkt is. De mogelijkheid van het onder mandateren van een art. 19 verstrekking tot op het niveau van bijvoorbeeld de wijkagent is niet toegepast in het korps. Na een uitleg over de strekking van deze artikelen voor de politiepraktijk, komen de aanwezigen tot de conclusie dat de bulk van verstrekkingen plaats vindt op grond van art. 7 WPG, omdat anders de reguliere artikel 2 Politiewet werkzaamheden binnen de basispolitiezorg niet kunnen worden uitgevoerd. Eventueel gebruik van art. 19 WPG wordt centraal door de afdeling privacy geregeld. In tegenstelling tot wat uit de eerder beschreven inventarisatie van de convenanten blijkt, is men v.w.b. de art. 20 WPG verstrekkingen bekend met de convenanten t.b.v. de hennep, huiselijk geweld, etc. Volgens de teamchefs staat dit op de rails en lijkt in dit op orde. Door de aandacht die tijdens de in- en externe audit aan dit onderwerp is besteed, is de ervaring van de PF, dat (schriftelijke) verzoeken om informatie in voorkomende gevallen bij hem worden gemeld, In die gevallen neemt de PF de behandeling van het verzoek over. Ook het aantal I-90 mutaties neemt toe. In het kader van de toekomstige samenvoeging van de korpsen Midden-West Brabant en Zeeland wordt reeds samengewerkt tussen respectievelijk de Unit Veiligheid & Integriteit en de afdeling Integriteit & Veiligheid. In april/mei 2011 werd geïnventariseerd waar de overeenkomsten en verschillen in taken en werkwijzen zitten. Deze inventarisatie heeft geleid tot concrete voorstellen om te komen tot eenduidige procedures. In de zeer nabije toekomst zullen o.a. procedures t.b.v. kennisnemingsverzoeken en verstrekkingen worden ontwikkeld.

ID	Aanbevelingen
1 2 3 4	Besteedt in een procesbeschrijving aandacht aan: a. de voorwaarden voor verstrekkingen ingevolge paragraaf 3 van de WPG toegespitst op de specifieke 8, 9, 10, 12 en 13 verwerkingen; b. de functionarissen die bevoegd zijn om bepaalde categorieën van politiegegevens te verstrekken; c. de functionarissen die in voorkomende gevallen moeten beslissen over een verzoek om bepaalde categorieën van politiegegevens; d. de gevallen waarin om advies of voor een beslissing contact moet worden opgenomen met de privacyfunctionaris en/of andere daartoe aangewezen (bevoegde) functionarissen; e. het ingeval van verstrekkingen op grond van de artikelen 19 en 20 schriftelijk wijzen van ontvangers op de geheimhoudingsverplichting ingevolge artikel 7; f. het vastleggen van de verstrekkingen en de uitzonderingen voor die verplichting. Geef daarbij ook duidelijk aan (criteria, voorbeelden) wat de verstrekkingsgronden in de praktijk kunnen zijn en in welke gevallen de protocolplicht van toepassing is. Regel waar dit mogelijk is en waar de praktijk toe noodzaakt, onder mandaat op grond van artikel 19 WPG. Wijs het korps op de regels voor de verstrekkingen en de protocolplicht. Sluit convenanten af onder supervisie van de WPG-procesverantwoordelijke functionaris, zodat de convenanten voldoen aan de eisen die daaraan gesteld zijn en bekend zijn bij alle betrokkenen. Draag zorg voor centrale opslag van de genoemde convenanten waarbij bovendien sprake moet zijn versiebeheer.

1.3 Artikel 9 (verwerking voor de rechtsorde in een bepaald geval)

1.3.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen politiegegevens voor onderzoeken rechtsorde in een bepaald geval met concrete	X			
2	Schriftelijke vastlegging en melding bij PF van doel onderzoek en deel politietaak binnen 1 week na aanvang	X			
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens		X		X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen.		X		X
6	Politiegegevens zijn toereikend, terzake dienend en niet bovenmatig		X		X
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet		X		X
8	Vermelding van de herkomst en de wijze van verkrijging van politiegegevens		X		X

ID	Bevindingen
1	Een overzicht met verwerkingen van politiegegevens voor onderzoeken met het oog op de handhaving van de rechtsorde in een bepaald geval, waarin de concrete doelstelling van de te auditen verwerking is opgenomen, wordt bijgehouden door 6 van de 12 onderzochte teams. 3 teams scoorden aan het begin van het onderzoek een onvoldoende resultaat en in de loop van het onderzoek zijn door hen verbetermaatregelen getroffen. Voor drie teams is dit onderwerp niet van toepassing. Ondanks het feit dat een artikel 9 verwerking voor zowel de recherche als de uniformdienst van toepassing kan zijn, leert de praktijk dat deze verwerking voornamelijk plaatsvindt bij de recherche. Een deel van de onderzochte teams zijn ondersteunend aan het rechercheproces en zijn niet belast met het eigenstandig voeren van een artikel 9 verwerking. Artikel 9 gegevens worden, naast de BVH (= Basis Voorziening Handhaving), ook opgeslagen in de BVO (=Basis Voorziening Opsporing) en een onderzoeksmap in Microsoft in de artikel 9 omgeving op de O-schijf. De verwerking in deze verschillende applicaties vindt zijn oorzaak in het feit dat de BVH niet geschikt blijkt te zijn om omvangrijke dossiers samen te stellen, het geen relationele database betreft, geen VROS meldingen genereert en ongeschikt is om een tapprocedure te verwerken. Daarbij komt dat BVH het onderscheid in artikel 8 en artikel 9 gegevens niet ondersteunt. In Zeeland werd hieromtrent bepaald dat ingeval van een artikel 9 verwerking, de bijbehorende BVH registratie op "besloten" wordt gezet. Dit lost echter de problematiek m.b.t. de verschillende verwerkingstermijnen van artikel 8 en artikel 9 verwerkingen niet op. BVO is wel een relationele database en geschikt om tapprocedures te verwerken, maar is niet voorzien van een tekstverwerkingsprogramma en dus ongeschikt om een omvangrijk dossier samen te stellen. Daartoe wordt uitgeweken naar de Microsoft applicatie. De verschillende applicaties zijn echter niet aan elkaar gekoppeld waardoor een groot deel van de gegevens telkenmale handmatig in de verschillende applicaties dient te worden ingevoerd. Een teamchef (bevoegd functionaris) vraagt een BVO registratie en bijbehorende onderzoeksmap op de O-schijf aan middels een tool in Microsoft Access. Deze tool is dusdanig dwingend ingericht dat een aanmelding artikel 9 verwerking inclusief doelomschrijving dient te worden aangemaakt. Tevens worden m.b.v. deze tool, door de betrokken teamchef, autorisaties in de aan te maken BVO registratie en onderzoeksmap op de O-schijf aangevraagd voor de onderhavige artikel 9 verwerking. Daarbij wordt rol / taak gebaseerd geautoriseerd. De O-schijf is ingedeeld naar de aard van de verwerkingen. In de artikel 9 omgeving van de O-schijf wordt per verwerking een onderzoeksmap aangemaakt. Deze onderzoeksmap is onderverdeeld in submappen. Een ondersteunend team maakt gebruik van de hen toegewezen submap t.b.v. hun bijdrage aan de onderhavige verwerking. De aanmelding van de artikel 9 verwerking en de aangevraagde autorisaties worden gemaild naar de Postbus autorisaties. Autorisaties worden op rechtmatigheid beoordeeld door de IBF en bij diens afwezigheid door de PF. Daar waar nodig vindt nader overleg plaats tussen de IBF / PF en de aanvragende teamchef en worden aanvragen gecorrigeerd/aangepast. De documenten worden door de afdeling Integriteit & Veiligheid uitgeprint en op naam van de artikel 9 verwerking opgeslagen in ordners. (=schriftelijke vastlegging conform art. 32/34, lid 2 WPG). Op de O-schijf is in de artikel 9 omgeving een submap beheer aangemaakt waarin, in de vorm van Microsoft Excelbestanden, overzichten van 9 verwerkingen worden bijgehouden. Het totaaloverzicht wordt bijgehouden door een infodeskmedewerker. De overige lijsten per team door de teamchefs. De taken, bevoegdheden en verantwoordelijkheden m.b.t. het aanvragen en de wijze van beheer worden summier verwoord in de Procesbeschrijving verwerking van politiegegevens.
2	De procesbeschrijving verwerking van politiegegevens geeft aan dat het onderzoek bij de PF moet worden gemeld en hoe men verder na de start van het onderzoek te werk moet gaan. Bij 5 teams is aanvankelijk geconstateerd dat dit proces nog niet geheel correct wordt uitgevoerd / toegepast / nageleefd. Afhankelijk van de interpretatie van de memorie van toelichting (wanneer is er concreet sprake van een 9 verwerking?) kan een verwerking aanvankelijk in artikel 8 worden opgestart en in de loop van het onderzoek overgaan naar een artikel 9 verwerking. De overgangsfase van artikel 8 naar artikel 9 tijdens een onderzoek, blijkt een grijs gebied te zijn, waarbij het moment van de overgang niet altijd exact is te bepalen en mede afhangt van het inzicht en de besluitvorming van de onderzoeksleider. Tot aan dat moment is niet uit te sluiten, dat er mogelijk onderzoeken lopen, die eigenlijk al de status van artikel 9 zouden moeten krijgen en dus al zouden moeten worden aangemeld. Aantallen of percentages van verwerkingen waarvoor dit geldt, zijn onbekend en zonder onevenredige inspanning, niet nader te bepalen. Door de eerder omschreven werkwijze (het aanvragen van autorisaties voor het aanmaken van een BVO-registratie) worden wel onderkende artikel 9 verwerkingen correct aangemeld. Door deze werkwijze is het pas, na aanmelding en autorisatietoekenning, mogelijk om artikel 9 gegevens op te slaan zoals is voorgeschreven. Voor "spoed"onderzoeken die buiten kantooruren worden opgestart, zijn op de O-schijf in de artikel 9 omgeving, twee mappen "leeg onderzoek" beschikbaar waarvoor alle rechercheurs zijn

ID	Bevindingen
	geautoriseerd. Z.s.m. na aanvang van het spoedonderzoek wordt het onderzoek alsnog aangemeld en de eerder omschreven werkwijze, inclusief autorisatietoekenning, gevolgd. De, in de map "leeg onderzoek", opgeslagen informatie wordt door functioneel beheer verplaatst naar de nieuw aangemaakte onderzoeksmap.
3	Van gemeenschappelijke verwerkingen die schriftelijk aan het CBP moeten worden gemeld, is uit de interviews niet gebleken. Bij de PF en de IBF zijn deze soort van verwerkingen ook niet bekend. Indien tijdens een onderzoek blijkt dat het "zwaartepunt" bij een ander korps ligt, danwel regio overstijgend is, wordt dit onderzoek volledig (inclusief de bijbehorende verantwoording) overgedragen aan dat betreffende korps danwel aan de Bovenregionale Recherche Zuid-Nederland (BRZN).
4	Het verwerken van gevoelige gegevens is niet in een instructie of procesbeschrijving geregeld. Uit de interviews blijkt, dat het bewustzijn dat gevoelige gegevens slechts mogen worden verwerkt als dit in aanvulling op andere gegevens onvermijdelijk is, aanwezig is en dat dit bij de meeste teams wel de aandacht heeft. De door de PF opgedane ervaring, verkregen tijdens het monitoren van het afhandelen van verzoeken tot kennisneming en vragen tot informatieverstrekking door externe partijen, leert dat medewerkers slechts gevoelige gegevens vermelden indien dit relevant is voor de politietaak.
5	Aan de rechtmatigheid van de verkrijging is geen aandacht besteed in de vorm van een procesbeschrijving of instructie. Gedurende de implementatie van de WPG is op het Deltanet wel aandacht aan dit onderwerp besteed. Uit een groepsinterview met de rechercheteamchefs werd, op de vraag of politiegegevens rechtmatig worden verkregen door alle teamchefs geantwoord dat hier zeer correct mee wordt omgegaan. Dit omdat onrechtmatig verkregen gegevens tot ongewenste consequenties in het vervolgingstraject kunnen leiden. Er wordt conform de wettelijke bepalingen (o.a. vorderen gegevens op grond van Strafvordering) gewerkt. Volgens een teamchef is het bijvoorbeeld zeer incidenteel voorgekomen dat camerabeelden worden verkregen zonder dat deze eerst worden gevorderd. Alsdan wordt altijd later nog een formele vordering bij de houder van de gegevens gedaan. Een ander voorbeeld was dat gegevens bij de Belastingdienst en financiële instellingen altijd worden gevorderd.
6	De procesbeschrijving Verwerking persoonsgegevens, vermeldt dat de ambtenaar van politie die gegevens heeft verzameld, zelfstandig verantwoordelijk is voor de vastlegging en de ordening van deze gegevens in de daarvoor ten dienste staande applicaties. Voor het uitvoeren van het gegevensbeheer wordt verwezen naar een procesbeschrijving gegevensbeheer. Die procesbeschrijving is er nog niet. Behalve de handleiding Proces Dossier Zeeland is er geen specifiekere procesbeschrijving of instructie inzake het toereikend, ter zake dienend en niet bovenmatig zijn van politiegegevens voorhanden. Uit de interviews blijkt wel, dat in de teams in de praktijk de hand aan deze kwaliteitseisen wordt gehouden. Dit gebeurt afhankelijk van de omvang van een onderzoek door de coördinator van het onderzoek, de dossiervormer of een ervaren rechercheur. Dossiervormers hebben in de regel een cursus dossiervorming gevolgd. De recherche beschikt over een Handleiding Proces Dossier Zeeland. Voor het deel van het onderzoek dat in BVH wordt verwerkt, gelden de kennisregels van TrueBlue. Zie in dat verband ook de bevindingen in par. 1.2.6.
7	Een procesbeschrijving, waarin het voor een ander doel verwerken van politiegegevens dan waarvoor ze zijn verkregen en voor zover de WPG daarin uitdrukkelijk voorziet, is in die zin niet voorhanden. Uit het groepsinterview met de teamchefs kwam naar voren, dat het gebruik voor andere doeleinden dan die voor de verkrijging eigenlijk erg weinig voorkomt. Hierbij kwam een aantal voorbeelden uit de praktijk naar voren. In geval van telecom gegevens, gebeurt dit altijd met kennis of instemming van de betrokken zaaks-OvJ, zelfs in de vorm van medeondertekening van het 126dd verbaal door de OvJ. Hiervan wordt melding gemaakt in het onderzoeksjournaal. Als er t.b.v. bestuurlijke handhaving politiegegevens worden gebruikt, wordt dit vastgelegd. Alle teamchefs zorgen er voor dat, door het aanmaken van een MRO mutatie in de BVO registratie, de gegevens ter beschikking worden gesteld aan een artikel 13 verwerking (VROS). Als er een politiegegeven aan een andere verwerking ter beschikking wordt gesteld, wordt hiervan altijd een zogenoemde VST mutatie in de BVO registratie aangemaakt. Door het Regionaal Recherche Team) wordt ook in het BVO journaal melding gemaakt van het ter beschikking stellen van gegevens aan andere verwerkingen. De RT teamchefs zeggen dat men geen gebruik maakt van een BVO journaal. Doordat CIE/RID/tactische rechercheurs tegelijkertijd geautoriseerd kunnen zijn voor meerdere artikel 9 verwerkingen is het mogelijk dat gegevens vanuit de ene artikel 9 voor een andere artikel 9 en/of artikel 10 verwerking worden gebruikt. Aangezien de rechercheurs, door landelijke ervaringen m.b.t. onrechtmatige verkrijging van onderzoeksgegevens, doordrongen zijn van het feit dat gegevens rechtmatig verkregen dienen te zijn, wordt hierbij de rol van de bevoegd functionarissen gerespecteerd.
8	Een procesbeschrijving inzake het vermelden van de herkomst en de wijze van verkrijging van politiegegevens is niet aanwezig. Tijdens het groepsinterview met de teamchefs is op de vraag of de herkomst en de wijze van verkrijging van politiegegevens wordt vermeld, geantwoord dat dit altijd wordt vastgelegd in de vorm van processen-verbaal van bevindingen en vorderingen ingevolge het Wetboek van Strafvordering. Het komt niet voor dat de bron/herkomst of wijze van verkrijging niet wordt vastgelegd.

ID	Aanbevelingen
4-8	Besteed aandacht aan de betreffende onderwerpen in een procesbeschrijving.

1.3.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig		X		X
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn		X		x
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies en onrechtmatige verwerking		X		X
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG		X		X
5	Toegang voor CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens		X		X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt		X		X

ID	Bevindingen
1	Zie de bevindingen bij par.1.3.1.6. Dit geldt ook voor het juist en nauwkeurig zijn van de politiegegevens. De applicatie BVO is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. Het juist en nauwkeurig verwerken van politiegegevens wordt weer negatief beïnvloed door het noodzakelijk gebruik van verschillende applicaties (BVH / BVO / Microsoft) zoals eerder verwoord. Hierdoor ontstaat de situatie dat eventueel beheer in

ID	Bevindingen
	deze verschillende applicaties telkenmale handmatig dient te worden uitgevoerd. Voor de O-schijf is dit, door de huidige structuur, mogelijk, maar de BVH en BVO kennen geen onderverdeling in aard verwerking zodat gegevens niet verplaatst kunnen worden naar bijvoorbeeld een artikel 13 (processen-verbaal en rapporten) en/of artikel 14 (verwijderde gegevens) omgeving. Uit het groepsinterview met de teamchefs van de recherche komt naar voren, dat er na Commissie Posthumus (Schiedammer Parkmoord) vereist wordt dat zo veel mogelijk gegevens worden verwerkt. Een gevolg is bijvoorbeeld dat de CIE alle gegevens, die ook maar enigszins betrekking kunnen hebben op een onderzoek, ter beschikking stelt. Ook niet relevante of ontlastende informatie voor een verdachte wordt in opdracht van de OvJ verwerkt. Alle teamchefs zijn ervan overtuigd dat rechercheurs doordrongen zijn van de kwaliteitseisen van de verwerkte informatie. In de werkoverleggen is kwaliteit een zwaarwegend aandachtspunt. Bij de RT's worden PV's via de teamchefs ingeleverd en beoordeeld door kwaliteitsfunctionarissen. Bij het RRT worden dossiers meegelezen door o.a. de tactisch coördinator en/of teamchef.
2	Zie de voorgaande bevindingen die ook ten aanzien van het verbeteren, vernietigen of aanvullen van onjuiste of onvolledig informatie gelden. De invoerende medewerkers (rechercheurs) zijn verantwoordelijk voor de juistheid en volledigheid van de ingevoerde gegevens. Inhoudelijk beheer van de opgeslagen gegevens vindt verder niet of nauwelijks plaats door de rechercheurs. Dit omdat hen hiertoe de tijd en capaciteit ontbreekt. In voorkomende gevallen wordt aanvullend gemuteerd door de rechercheurs. Structureel gegevensbeheer BVO is niet belegd en vindt niet (RT's), of slechts incidenteel (RRT), plaats. Bij het RRT bestaat dit beheer, bij gelegenheid, slechts uit het koppelen van objecten welke in de mutatietekst worden genoemd door administratief medewerkers/rechercheassistenten (BOA's). De bevraagde medewerkers zeggen allen dat deze situatie mede veroorzaakt wordt door een gebrek aan beheerscapaciteit en hoge werkdruk.
3	Zie de bevindingen bij par. 1.2.2.3. De landelijke regeling BBNP is bekend bij en van toepassing op Politie Zeeland. Daarnaast is een Procesbeschrijving inzake autorisaties (autorisatieprocedure) aanwezig. Deze is gepubliceerd op de Intranetsite (DELTANET). Uit het groepsinterview met de teamchefs van de recherche komt aanvullend naar voren, dat de fysieke toegang tot hun afdelingen goed geautoriseerd is. Zeker buiten kantooruren zijn deze afgesloten en slechts toegankelijk voor gerechtigden. Een teamchef gaf aan, dat hij onlangs de lijst van geautoriseerden met toegang tot zijn afdeling heeft geschoond. Een andere teamchef vraagt met enige regelmaat (om de 2, 3 weken) zo'n lijst op en schoont deze van tijdelijke krachten, zoals stagelopers etc. Weer een andere teamchef geeft aan dat hij wel aan cleandesk policy wil doen, maar dat hij dit niet kan omdat op zijn afdeling simpelweg kastruimte ontbreekt voor de opslag van fysieke dossiers waar de rechercheurs actueel aan werken. De teamchef heeft ruim 4 maanden geleden kastruimte gevraagd, maar dit is nog niet gerealiseerd.
4	Zie de bevindingen en aanbeveling over dit soortgelijke onderwerp bij par.1.2.2.4. Toegang t.b.v. toezicht wordt, afhankelijk van het onderzochte, op de volgende wijze verkregen: • in voorkomende gevallen wordt, afhankelijk van de applicatie, op grond van art. 4, lid 5, WPG toegang verkregen in de vorm van autorisaties voor de toezichthouder; • en/of de functioneel beheerder van de applicaties levert de benodigde informatie aan; • en/of in het bijzijn van een toezichthouder wordt door een geautoriseerde (operationeel gebruiker) inzage verleend in een applicatie.
5	Zie de bevindingen en aanbeveling over dit soortgelijke onderwerp bij par.1.2.2.5. M.b.t. toegang voor toezichthouders: zie hierboven onder punt 4. M.b.t. toegang voor medewerkers van de vtsPN welke technische werkzaamheden verrichten volgt dit uit de inspanningsverplichtingen vastgelegd in een SLA.
6	Door of namens de korpsbeheerders van Zuid 6, waaronder de politie Zeeland is een Service Level Agreement (SLA) gesloten voor alle bij de vtsPN in technisch beheer zijnde politiesystemen. In de SLA zijn ook de beveiligingsvoorwaarden opgenomen. Over de uitvoering van de SLA wordt periodiek in de vorm van een Service Level Report (SLR) door de vtsPN gerapporteerd. Daarnaast is er regulier overleg tussen de functioneel beheerders en de vtsPN over de uitvoering van de SLA. In die zin ziet de korpsbeheerder toe op de uitvoering van de SLA. In dat verband wordt verwezen naar het uitvoerige verslag bij artikel 8 in par. 1.2.2.6. Een SLR is niet tijdens de privacy audit overgelegd.

ID	Aanbevelingen
1-2	Zorg voor procesbeschrijvingen die betrekkening hebben op het gegevensbeheer van de artikel 9 verwerkingen. Scherp het gegevensbeheer voor die verwerkingen aan.
3	Zorg voor een adequate cleandeskpolicy op alle politiebureau's en vervul hiervoor waar nodig de randvoorwaarden.
4-5	Regel de toegang van de toezichthouders tot politiegegevens als bedoeld in artikel 4, lid 4 en 5, WPG in een procesbeschrijving.
6	Zorg dat een afschrift van een recente SLA met de vtsPN met bijlagen beschikbaar is.

1.3.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid		X		X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd		X		X
3	Specifieke autorisaties voor avps die onder het beheer van de verantwoordelijke vallen		X		X
4	Specifieke autorisaties in bijzondere gevallen voor niet avps die onder het beheer van de verantwoordelijke vallen		X		X
5	Specifieke autorisaties in bijzondere gevallen voor avps die onder het beheer van een andere verantwoordelijke vallen		X		X

ID	Bevindingen
1 2 3 4 5	De politie Zeeland beschikt over een Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. De autorisatieprocedure voorziet in de autorisatie voor intern of onder intern gezag werkend personeel, autorisatie van personeel dat in dienst is van een ander politiekorps en tenslotte autorisatie van overige medewerkers, kort gezegd de zogenaamde externen. De documenten zijn raadpleegbaar op het Intranet (Deltanet) en zijn voor iedere gebruiker toegankelijk. Daarnaast zijn momenteel nieuwe standaard autorisatieprofielen en autorisatiematrixen in (een vergevorderd) stadium van ontwikkeling. In die zin beschikt de politie Zeeland over een autorisatiebeheerssysteem, waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld, met het oog op het voldoen aan de eisen van zorgvuldigheid en evenredigheid. De procesbeschrijving en het

ID	Bevindingen
	autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties van het project Implementatie Wet politiegegevens. De procesbeschrijving is momenteel in bewerking bij de IBF. Verder handelt de politie Zeeland in voorkomende gevallen conform de "Interregionale regeling autoriseren". Bij besluit van het Korpsbeheerdersberaad is deze regeling sinds februari 2004 op de politiekorpsen van toepassing. Intrekking van autorisaties loopt naar behoren bij medewerkers die de dienst verlaten. Intrekking van autorisaties gebeurt zelden bij functiewisselingen bij intern personeel. De gang van zaken met betrekking tot de aanvraag en het verdere beheer van autorisaties voor artikel 9 verwerkingen in de praktijk is als volgt. De onderzoeksleider vraagt via Access een artikel 9 verwerking aan. De namen van de onderzoeken worden automatisch toegekend. Er wordt automatisch aangemaakt: 1. een aanmelding artikel 9 verwerking; 2. een aanvraag voor de autorisatie van een BVO registratie, en 3. een aanvraag voor toekenning van een onderzoeksnummer en aanmaak van een onderzoeksmap op de O-schijf in de Microsoft kantoorautomatiseringomgeving (KA). De onderzoeksleider doet een dergelijk verzoek: 1. naar aanleiding van een opdracht van de korpsleiding/hoofdofficier van justitie om een TGO op te starten; 2. een opdracht afkomstig vanuit een prio-overleg, en 3. een aanvraag op eigen initiatief naar aanleiding van bijvoorbeeld BOB-middelen in een relatief eenvoudige zaak cq. spoedzaak. (denk aan spoedtap i.v.m. woninginbraak, roofoverval etc.) In de eerste twee situaties is er een, weliswaar indirecte, opdracht van een hoger echelon. In de derde situatie is die opdracht er niet. De onderzoeksleider vraagt voor zich zelf een autorisatie aan voor zijn nieuwe onderzoek en vraagt tevens autorisaties aan voor zijn medewerkers. In de BVO zijn landelijk menu' s met onderling verschillende mogelijkheden vastgesteld. De onderzoeksleider heeft, d.m.v. zijn toegekende menu behorende bij het zijn van onderzoeksleider, de mogelijkheid om medewerkers aan zijn BVO registratie toe te voegen. Dit is echter slechts mogelijk voor medewerkers die reeds een BVO account hebben. Een BVO account wordt slecht toegekend indien een medewerker geïnstrueerd is m.b.t. de werking van deze applicatie. Omdat de te autoriseren medewerker naast de BVO toegang ook toegang dient te krijgen tot de bijbehorende onderzoeksmap op de O-schijf, wordt in de praktijk meestentijds toch de reguliere autorisatieprocedure gevolgd. Slechts in geval er noodzaak is, bijvoorbeeld het verwerken van een tap tijdens het weekend door een andere, maar niet onderzoeksgeautoriseerde medewerker, wordt van deze BVO mogelijkheid gebruik gemaakt in afwijking van de reguliere autorisatieprocedure. In de eerste twee situaties is er min of meer stilzwijgende toestemming van de divisiechef. Een autorisatie voor de applicatie BlueView geeft landelijk toegang tot inhoudelijke BVH informatie. M.b.t. BlueView is een landelijk autorisatiemodel vastgesteld. In Zeeland worden BlueView autorisaties conform dit model toegekend en zijn beperkt tot Infodesk- en CIE-medewerkers behorende tot de Regionale Informatie Organisatie (RIO). Niet uit te sluiten is dat door andere korpsen, in afwijking van het landelijk autorisatiemodel, BlueView autorisaties worden verleend aan bijvoorbeeld wijkagenten. Door deze vorm van autoriseren kan de korpschef van de politie Zeeland niet voldoen aan de bepalingen van artikel 6, lid 5, WPG. Er zijn deelwaarnemingen tijdens de interne audit op toegekende autorisaties in een brede context uitgevoerd. Hiervan is een rapport opgesteld. In de rapportage is verwoord hoe het onderzoek is uitgevoerd, hoe de steekproeven tot stand zijn gekomen en is het vervolg daarvan beschreven. In het onderhavige rapport zijn de bevindingen en conclusies zoveel mogelijk over de relevante paragrafen "Autorisaties" bij de betreffende verwerkingen verantwoord. Dit geldt ook voor de conclusies en aanbevelingen. Het was niet altijd mogelijk om de relevante teksten geheel op te knippen, waardoor net als hieronder, bevindingen voorkomen die op andere soorten verwerking betrekking hebben. De routering van autorisatieaanvragen is divers en de daarbij behorende toegang tot informatie en/of applicaties wordt niet eenduidig verleend. Functiescheiding wordt daarbij niet consequent toegepast. Tot een aantal applicaties wordt door een andere afdeling of individuele persoon toegang tot de informatie verleend of wordt de toegang ingetrokken. Voorbeelden daarvan zijn: BlueView (Landelijke Database), JD (Justitiële Documentatie), FCM, IB (Integrale Bevraging), RI-Online (Recherche Informatie), Reliant (Interceptie), DCS (Digitale Communicatie Sporen), VROS (Verwijsindex Recherche Objecten en Subjecten). Door de afdeling I & V wordt periodiek (meestentijds jaarlijks, maar deze termijn wordt in de nabije toekomst verkort) een lijst van aangemelde artikel 9 verwerkingen naar het Openbaar Ministerie, arrondissementsparket Middelburg, gestuurd met de vraag welke artikel 9 verwerkingen in kracht van gewijsde zijn gegaan en of ontneming van het wederrechtelijk verkregen voordeel heeft plaatsgevonden. Indien hiervan sprake is, is hiermee het doel van de onderhavige artikel 9 verwerking volledig behaald. Het behalen van het doel heeft voor een deel van de informatie (procesdossier waarop de veroordeling plaatsvond) tot gevolg dat deze een andere aard WPG verwerking veroorzaakt, namelijk overplaatsing naar de zogenoemde artikel 13 verwerking, zijnde processen-verbaal en rapporten. Niet langer voor de politietaak noodzakelijke gegevens dienen te worden verwijderd en overgebracht naar de artikel 14 omgeving. Bij deze verschillende vormen van verwerking behoort een ander autorisatieregime. Op de O-schijf is het verplaatsen en wijzigen van aard verwerking realiseerbaar en vindt deels ook plaats. In de andere gebruikte applicaties, zoals BVH en BVO is dit volstrekt onmogelijk. Uit het groepsinterview met de teamchefs van de recherche komt het volgende naar voren. Op de vraag omtrent de correctheid van toegekende autorisaties is door een teamchef geantwoord dat, i.v.m. spoedeisend karakter en het feit dat een autorisatie niet altijd snel gerealiseerd wordt (weekenden) soms wachtwoorden worden uitgewisseld t.b.v. toegang tot de tapmodule in BVO. Alle teamchefs vragen slechts autorisaties aan voor politieambtenaren die dit nodig hebben voor hun taak. Er wordt altijd gewerkt conform de autorisatieprocedure. Wel hebben de teamchefs, met hun menu registratiebeheerder, in hun BVO registratie de mogelijkheid om zelf medewerkers te autoriseren voor hun registratie. Dit gebeurt voornamelijk indien, i.v.m. de voortgang van een onderzoek (weekends, etc.) medewerkers toegang tot de tapmodule moeten hebben. Dit kan slechts voor medewerkers die al een BVO-account hebben. Teamchefs laten vertrekkende medewerkers de-autoriseren. Andere autorisaties, bijvoorbeeld omdat er niet meer aan een onderzoek wordt gewerkt, worden niet ingetrokken. Eén van de oorzaken is de drukte van de waan van de dag en mogelijk te weinig aandacht voor dit aspect. Bekend is ook dat bij niet gebruik van BVO het account na zes maanden wordt geblokkeerd. Intrekkingen van autorisaties loopt naar behoren bij medewerkers die de dienst verlaten. Intrekkingen van autorisaties gebeurt

ID	Bevindingen
	zelden bij functiewisselingen bij intern personeel.

ID	Aanbevelingen
1-5	Scherp het beheer van de autorisaties aan voor met name het deautoriseren van medewerkers die niet meer bij een onderzoek zijn betrokken. Maak voor het beheer van de autorisaties gebruik van één ABS (Autorisatie Beheer Server) voor Zuid 6.

1.3.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens met andere politiegegevens ogv art. 8 of 9 voor vast stellen verbanden tussen de gegevens	X			X
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	X			
2	Voor gv de avps autoriseren van de Regionale Infodesk	X			
2	Voor gv in voorkomende gevallen de avps bij de CIE, RID en Themaverwerking autoriseren	X			
3	Avps die gv beschikken over de wettelijk vereiste kennis en vaardigheden	X			
4	Indien bij gv gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	X			
5	Indien noodzakelijk voor goede gv worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	X			
6	Vzv noodzakelijk voor het onderzoek politiegegevens gv met andere gegevens dan politiegegevens	X			
7	Voldoen aan protocolplicht gv met andere gegevens	X			
8	Voldoen aan protocolplicht gv met andere gegevens tijdens de bewaartermijn van 5 jaar	X			

ID	Bevindingen
1	Een Procesbeschrijving inzake: a. het geautomatiseerd en vergelijken van politiegegevens met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens; b. het na instemming van de daartoe bevoegde functionaris, zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder verwerken van de gerelateerde gegevens, is aanwezig in de vorm van de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence. Uit het groepsinterview met de teamchefs recherche komt het volgende naar voren. Op de vraag of er door hun medewerkers geautomatiseerd wordt vergeleken, wordt geantwoord dat meestentijds informatie over een persoon wordt verkregen door bevraging door de Infodesk. Wel wordt door de rechercheurs in voorkomende gevallen gezocht in de BVO registraties waartoe men is geautoriseerd. Deze mogelijkheid zit "ingebakken" in de BVO applicatie. In de kantoorautomatiseringsomgeving (in Word) wordt door de Infodesk gezocht m.b.v. Zylab (mits geautoriseerd) en de standaard Word-zoekmogelijkheden. Men krijgt dan echter slechts de resultaten te zien waarvoor men is geautoriseerd. BlueView autorisaties zijn toegekend aan de Infodesk. In geval informatie vanuit het ene naar het andere onderzoek dient te worden gehaald, wordt altijd de rol van de betrokken bevoegd functionaris en in voorkomende gevallen artikel 126 dd Sv gerespecteerd. Indien een artikel 9 verwerking MRO (Melding Recherche Onderzoek) waardig is, dient in de bijbehorende BVO registratie een zogenoemde MRO mutatie aangemaakt te worden. Hieraan worden onderzoeksobjecten gekoppeld. Deze onderzoeksobjecten worden wekelijks landelijk in VROS vergeleken, waarna bij het aantreffen van een onderzoeksobject in een andere BVO registratie, een verwijzing plaatsvindt naar een contactpersoon van dat betreffende onderzoek. Inhoudelijke informatie wordt daarbij niet meegezonden. Het informatiesysteem BVO bevat een functionaliteit voor geautomatiseerd vergelijken (hit-no-hit)(=VROS). [redacted] M.b.v. deze autorisatie is op basis van hit/nog-hit te raadplegen of een persoon CIE subject is of gekoppeld is aan een MRO mutatie in een BVO registratie (landelijk). Is dit het geval dan worden door [redacted] de betrokken contactfunctionarissen met elkaar in contact gebracht. Hiermee wordt de rol van de bevoegd functionarissen gerespecteerd. Dit valt onder hun "makelfunctie".
2	Het verstrekken van autorisaties voor het geautomatiseerd vergelijken van politiegegevens aan uitsluitend de ambtenaren van de Regionale Infodesk wordt geregeld via de eerder in dit rapport vermelde autorisatieregelingen en vloeit voort uit het document Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence.
3	Functiebeschrijvingen voor de medewerkers van de Infodesk zijn aanwezig op Deltanet. Dit zijn onder meer gegevensbewerker A & B, analist A operationeel criminaliteitsanalist en analist A bij de misdaadanalyse. [redacted] De analisten zijn als volgt opgeleid voor hun taak: RINF opleiding, e-learning Blue View, BVO en Basisinternetrechercheur. Een nieuwe analist volgt de basis analisten opleiding (OCA) en wordt opgeleid voor de in gebruik zijnde applicaties, analist notebook, Excel en applicatiegerichte opleidingen. Alle analisten beschikken over gedegen kennis van de politieorganisatie en de politieprocessen. Verder zijn de analisten bekend gemaakt met de WPG.
4 5 6 7 8	De gegevensvergelijking, waaronder die met andere dan politiegegevens, het al dan niet zichtbaar maken van de verbanden bij de gegevensvergelijking en gerelateerde gegevens, het coderen van politiegegevens (11, lid 3, WPG), de besluitvorming over die processen en de protocolverplichting, komen aan de orde in het document Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence. Dat een bevoegde functionaris de ter beschikking stelling op basis van artikel 2:13 BPG wel kan weigeren of beperkende voorwaarden kan opleggen is ook aangegeven in het voornoemde procesmodel. BVO of andere applicaties beschikken voor wat betreft de artikel 9 verwerkingen niet over een functionaliteit die het proces van de gegevensvergelijking, het al dan niet zichtbaar maken van verbanden en overeenkomende gegevens, het coderen van de gegevens en de besluitvorming over die processen ondersteunen. De systemen zijn niet "WPG proof". Wat wel min of meer als compenserende maatregel mogelijk is, is dat via de verticale autorisatiemogelijkheden van BVO, informatie die vertrouwelijk is en niet mag worden geraadpleegd, conform het landelijk autorisatiemodel BVO op een dusdanig hoog autorisatieniveau

ID	Bevindingen
	weggeschreven kan worden, dat deze niet door analisten kan worden benaderd. Dit gebeurt ook in de praktijk. Gegevensvergelijking met andere dan politiegegevens als bedoeld in artikel 11, lid 5, WPG is via BVH en BVO niet mogelijk. Verbindingen met andere dan politiesystemen zijn niet toegestaan conform de richtlijnen van de vtsPN. De analistenapplicatie Brains wordt momenteel uitgerold en medewerkers worden hiertoe opgeleid. Afhankelijk van de aard en aantal van de ontsloten bronbestanden, biedt Brains wel de mogelijkheid tot een vorm van verwerking zoals omschreven in art. 11, lid 5, WPG. De momenteel ontsloten bronbestanden zijn qua aard en aantal nog beperkt. Naar de toepassing van Brains is, gezien het moment van de afronding van de privacy audit, geen onderzoek ingesteld. Het geautomatiseerd vergelijken wordt door de medewerkers geprotocolleerd in het Infodeskregistratiesysteem in BVO. Vastgelegd wordt het mut.nr, de gegevens van de informatieaanvrager, de reden van het verzoek en het doel van het gebruik. Op het moment dat de medewerker een artikel 9 hit heeft, is te zien, dat er informatie in het onderzoek aanwezig is. De medewerker kan niet zelf in de mutatie. Wel is te zien wie de teamleider (bevoegd functionaris) van het onderzoek is. Aan de verzoeker wordt dan de naam van de teamleider doorgegeven (zogenaamde "makelfunctie" van de infodesk). Ingeval de analist BlueView bevraagt, worden bij een hit de gerelateerde gegevens naar het Infodeskregistratiesysteem BVO gekopieerd. Ingeval de analisten voor een TGO analyseren, worden de resultaten van de analyse en de protocolgegevens in een aparte map in de omgeving van de TGO ondergebracht. Van artikel 9 verwerkingen die in de bewaartermijn verkeren, zijn de autorisaties voor toegang ingetrokken.

ID	Aanbevelingen
1	Breng het vraagstuk van het geautomatiseerd vergelijken op landelijk niveau onder de aandacht van de wetgever. Neem naar aanleiding van de uitkomst van deze actie waar nodig beheersmaatregelen.

1.3.5 In combinatie met elkaar verwerken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens icmev met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	-			X
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	-			
2	Voor icmev de avps autoriseren van de CIE	-			
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd CIE,RID of Themaverwerking	-			
3	Avps die icmev beschikken over de wettelijk vereiste kennis en vaardigheden	-			
4	Indien bij icmev gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	-			
5	Indien noodzakelijk voor goede icmev worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	-			
6	Voldoen aan protocolplicht icmev met andere gegevens	-			
7	Voldoen aan protocolplicht icmev met andere gegevens tijdens de bewaartermijn van 5 jaar	-			

ID	Bevindingen
17	Een Procesbeschrijving inzake de onderwerpen die te maken hebben met in combinatie met elkaar verwerken, is aanwezig in de vorm van de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence. Uit de interviews komt naar voren, dat de politie Zeeland politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 in niet combinatie met elkaar verwerkt teneinde vast te stellen of verbanden bestaan tussen de gegevens. De politie Zeeland beschikt niet over applicaties of tools die over een dergelijke functionaliteit beschikken. Daarnaast blijkt dat er op landelijk niveau geen consensus bestaat over de interpretatie van artikel 11, lid 4, WPG naar de dagelijkse politiepraktijk. Recentelijk is de tool Brains door de politie Zeeland aangeschaft. Naar de werking van deze tool is binnen het bestek van deze privacy audit geen onderzoek meer ingesteld.

ID	Aanbevelingen
1	Bevorder op landelijk niveau een eenduidige interpretatie van het begrip "in combinatie met elkaar verwerken". Laat met het oog op het in combinatie met elkaar verwerken een aanvullende privacy audit uitvoeren op het gebruik van Brains in de praktijk.

1.3.6 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Politie gegevens na verwijdering een half jaar verwerken voor mogelijk nieuw art. 9/10 onderzoek		X		X
2	Na verwijdering maximaal 5 jaar bewaren en gebruiken voor afhandeling klachten en verantwoording van verrichtingen		X		X
3	Verwijderde gegevens tijdens bewaartermijn niet verstrekken aan personen/ instanties in 16 t/m 20, 23 en 24 WPG		X		X
4	Uitsluitend in bijzondere gevallen tijdens bewaartermijn in opdracht bevoegd gezag tbv hernieuwde 9 of 10 verwerking		X		X
5	Voldoen aan de regels schriftelijke vastlegging vernieuwde verwerking en ter beschikking stelling verdere verwerking		X		X
6	Afzien van vernietiging ingeval waarde voor cultureel erfgoed of historisch onderzoek conform regels Archiefwet		X		X

ID	Bevindingen
1-6	De procesbeschrijving Verwerking van politiegegevens artikel 8/9 besteedt, zij het zeer summier, en op onderdelen onvolledig aandacht aan alle bepalingen met betrekking tot het onderwerp bewaren en vernietigen. BVH, BVO en de kantoorautomatiseringsomgeving bieden, voorzover het om de artikel 9 verwerkingen gaat, geen functionaliteiten voor het ondersteunen van dit proces. Afhankelijk van de mogelijkheden van de functionaliteit wordt de verwijdering automatisch of

ID	Bevindingen
	handmatig door de functioneel beheerder uitgevoerd. Handmatig verwijderen kan nog door Functioneel Beheer gecorrigeerd worden. Uit de groepsinterviews kwam naar voren, dat na de Commissie Posthumus alle informatie bewaard wordt en er tussentijds niets uit een lopende verwerking wordt verwijderd. De teamchefs weten slechts incidenteel wanneer een onderzoek is beëindigd doordat het in kracht van gewijsde is gegaan. Ook in deze incidentele gevallen wordt de zes maanden termijn, waarin men nog gegevens uit deze verwerking ter beschikking kan stellen aan onderdelen van de politietaak, niet benut. Fysieke dossiers (ordners op de rechercheafdeling) worden ook wel bewaard om er in voorkomende gevallen gegevens uit te gebruiken. Zoals uit het groepsinterview met de recherche teamchefs bleek, worden onder andere n.a.v. commissie Posthumus, tussentijds geen gegevens verwijderd uit een lopende artikel 9 verwerking. In geval van een veroordeling wordt door het Openbaar Ministerie niet teruggekoppeld dat het doel van de artikel 9 verwerking (waaronder vervolging en ontneming van het wederrechtelijk verkregene) werd behaald. Hierdoor ontbreekt het signaal om de daarvoor in aanmerking komende artikel 9 gegevens te verwijderen. De aanwijzing afloopberichten van het college van PG's dient te worden herzien en op dit punt te worden uitgebreid. Slechts indien het OM structureel de veroordelingen/sepots terugkoppelt aan de politie, is het voor de politie mogelijk om gegevensbeheer in te richten en te voorkomen dat artikel 9 gegevens onterecht als zodanig blijven aangemerkt en zo verder verwerkt worden. Daarbij komt dat BVH en de BVO technisch niet de mogelijkheid kennen om verwijderde gegevens als zodanig te "labelen". In BVO kan een zogenoemde eindmutatie worden aangemaakt waardoor de VROS matching van de in de registratie vermelde objecten zes maanden na de eindmutatie stopt. Daarnaast kunnen de "operationele" autorisaties worden ingetrokken, maar zoals eerder vermeld is het intrekken van autorisaties een verbeterpunt. De O-schijf is wel zodanig ingericht dat verwijderde gegevens in de artikel 14 verwerking worden opgeslagen en slechts zeer beperkt (voor afhandelen klachten en verzoeken tot kennisneming) worden geautoriseerd. Een informele oplossing is gevonden door het parket Middelburg jaarlijks een lijst met artikel 9 verwerkingen toe te sturen met de vraag welke artikel 9 verwerkingen in kracht van gewijsde zijn gegaan. Schriftelijke verzoeken van externe instanties worden centraal afgehandeld door de afdeling Integriteit & Veiligheid. Hierbij is de ervaring dat meestentijds om actuele politiegegevens wordt gevraagd. Slechts in uitzonderingsgevallen wordt verzocht om oudere gegevens. In dit soort gevallen wordt bezien of de gegevens de status van verwijderd ingevolge artikel 14 hebben, of zouden moeten hebben. Indien er sprake blijkt te zijn van verwijderde gegevens worden de politiegegevens niet verstrekt. Operationele teams zijn niet belast met afhandeling van dergelijke schriftelijke verzoeken. Tijdens de groepsinterviews met de teamchefs recherche is van hun zijde aangegeven, dat verstrekkingen ingevolge par. 3 WPG niet of nauwelijks voorkomen. Uit verkregen informatie van de teamchef Post & Archiefzaken, blijkt dat gehandeld wordt conform de Selectielijst voor archiefbescheiden van (regionale) politieorganisaties 2004. In deel 2 onder punt 3 is de selectielijst voor archiefbescheiden m.b.t. de uitvoering van de politietaak opgenomen. Echter deze selectielijst spreekt nog over de Wet politieregisters en is niet geactualiseerd. Door de betrokken teamchef werd hiervoor op landelijke vergaderingen aandacht gevraagd, maar dit heeft nog niet geleid tot aanpassing van bedoeld document. Vervolgens heeft hij, eind 2009, op eigen initiatief en met zijn kennis en ervaring een concept "Toegankelijkheid en bewaartermijnen van politiegegevens op grond van de WPG" opgesteld, a.d.h. waarvan de archiefbescheiden in Zeeland worden beheerd. Dit betreft de fysieke informatie en niet de digitale informatie.

ID	Aanbevelingen
1-6	Vul de bestaande procesbeschrijving verwerken van politiegegevens artikel 8/9 aan met de nog ontbrekende regels voor het verwijderen, bewaren en vernietigen van politiegegevens. Implementeer zo spoedig mogelijk voorzieningen in de informatiesystemen die de regels op genoemd terrein ondersteunen. Zorg voor voldoende capaciteit op het terrein van het gegevensbeheer en beleg de hierbij behorende taken, bevoegdheden en verantwoordelijkheden. Draag zorg dat aan de regels in de WPG in relatie tot de Archiefwet wordt voldaan.

1.3.7 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie indien nodig voor hun taakuitoefening		X		X
2	Politiegegevens tbs aan art. 8, 9, 10,12 na instemming bevoegde functionaris		X		X
3	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 1, genoemde ondersteunende taken		X		X
4	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 2, genoemde ondersteunende taken		X		X
5	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 3, genoemde ondersteunende taken	X			
6	Tbs van politiegegevens uitsluitend weigeren of beperken in de wettelijk toegestane gevallen		X		X
7	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld		X		X

ID	Bevindingen
1-7	Een Procesbeschrijving inzake het ter beschikking stellen van politiegegevens met relevante onderwerpen is niet aanwezig. BVO bevat functionaliteiten voor het ondersteunen van dit proces. Externen kunnen hierdoor, geautoriseerd, gebruik maken van het systeem. Zoals eerder verwoord worden artikel 9 gegevens voornamelijk opgeslagen in BVO registraties en de artikel 9 omgeving op de O-schijf. D.m.v. autorisaties op "superregistraties" hebben [redacted] toegang tot de gegevens. Indien zij daadwerkelijk gebruik gaan maken van artikel 9 gegevens wordt dit gevraagd aan de bevoegd functionaris van de onderhavige artikel 9 verwerking. M.a.w. de taak en bevoegdheid van de betrokken bevoegd functionaris wordt gerespecteerd. Dit betreft een vorm van ter beschikking stelling. Een bron van zorg is de applicatie BlueView Opsporing. Deze ontsluit landelijk de hiervoor in aanmerking komende artikel 9 registraties in de BVO t/m niveau 4. Ook dit betreft een vorm van ter beschikking stelling. Aangezien functioneel beheer BVO aan kan geven welke BVO registraties wel of niet dienen te worden ontsloten door BlueView Opsporing is dit mogelijk te beschouwen

ID	Bevindingen
	als een vorm van coderen. Hierdoor heeft iedere BlueView Opsporing geautoriseerde inhoudelijk toegang tot de daarvoor in aanmerking komende artikel 9 gegevens, maar vindt dit plaats buiten medeweten van de betrokken bevoegde functionaris. Daarbij is een complicerende factor dat de rechtmatigheid van toegekende BlueView Opsporing autorisaties niet is na te gaan, omdat deze autorisaties door alle regio's worden aangevraagd en door de landelijk functioneel beheerder BlueView worden gerealiseerd. De indruk bestaat dat het landelijke autorisatiemodel BlueView niet altijd door alle korpsen correct wordt toegepast. Toegekende autorisaties hebben echter wel een landelijke werking. E.e.a. is in strijd met artikel 6, lid 5, WPG. Naar aanleiding van een signaal hieromtrent door de PF aan de FG van de politie Zeeland, heeft deze in 2009 een nader onderzoek ingesteld. Hiertoe werd een bezoek gebracht aan de vtsPN en werden de landelijk verleende BlueView autorisaties opgevraagd. Het gevraagde overzicht werd echter niet verkregen. Door de FG werd hierover op 23 september 2009 aan de plv. Korpschef o.a. het volgende gerapporteerd: "De gemaakte landelijke autorisatie afspraken worden door korpsen vermoedelijk niet nagekomen. Korpsen autoriseren kennelijk ruimer dan is afgesproken. Hierdoor worden mogelijk politiegegevens verstrekt (opmerking privacyfunctionaris: moet zijn ter beschikking gesteld) in strijd met het regime van de WPG. Controle op de uitgifte van autorisaties door andere regio's blijkt onmogelijk. Hierdoor kan de korpsbeheerder niet aan zijn verantwoordelijkheid voor de gegevensverwerking voldoen." Deze rapportage heeft niet geleid tot landelijke aanpassingen. Of deze situatie nog steeds voortduurt, is verder niet onderzocht. Door het feit dat (CIE/RID/tactische rechercheurs) tegelijkertijd geautoriseerd kunnen zijn voor meerdere artikel 9 verwerkingen, is het mogelijk dat gegevens vanuit de ene artikel 9 voor een andere artikel 9 en/of artikel 10 verwerking worden gebruikt. Aangezien de rechercheurs, door landelijke ervaringen m.b.t. onrechtmatige verkrijging van onderzoeksgegevens, doordrongen zijn van het feit dat gegevens rechtmatig verkregen dienen te zijn, wordt hierbij de rol van de bevoegd functionarissen gerespecteerd. De BVO en de kantoorautomatiseringsomgeving zijn niet voorzien een functionaliteit, waarmee politiegegevens ter beschikking kunnen worden gesteld voor de genoemde landelijke artikel 13 verwerkingen. Een uitzondering is de MRO-functie in BVO waarmee politiegegevens aan het VROS ter beschikking worden gesteld. Dit proces is beschreven in de BVO en VROS-gebruikershandleiding. Met betrekking tot de weigeringsgronden voor het ter beschikking stellen van politiegegevens kan het volgende worden opgemerkt. Voor wat betreft de hier behandelde artikel 9 verwerkingen zijn slechts de uitzonderingsgronden zoals genoemd in art. 2:13, lid 1, onder b, c en f, van het BPG van toepassing. Deze uitzonderingsgronden zijn: • indien gevaar voor leven of gezondheid van betrokkene of derden is te duchten: dit wordt d.m.v. de actieve rol van de bevoegd functionaris bewaakt; • indien sprake is van een intern integriteitonderzoek: de uitzonderingsgrond wordt, d.m.v. het feit dat dit soort verwerkingen onder leiding van de teamchef Integriteit & Veiligheid in de kantoorautomatiseringsomgeving worden gevoerd, bewaakt. • indien sprake is van een door het college van PG's aangemerkt embargo-onderzoek: de uitzonderingsgrond is, door het feit dat er tot op heden geen onderzoek als embargo-onderzoek werd aangemerkt, niet van toepassing. Ten aanzien van de geheimhoudingsverplichting ingeval van ter beschikking stelling is het volgende van belang. Bij indiensttreding leggen alle ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
1-4 6-7	Zorg voor een procesbeschrijving waarin alle relevante onderwerpen met betrekking tot het terbeschikking stellen van politiegegevens worden geregeld. Zorg voor functionaliteiten in de automatiseringssystemen ten behoeve van de terbeschiking stelling van politiegegevens aan artikel 13 verwerkingen. Stel de problematiek van het landelijk autoriseren van BlueView in de Raad van Korpschefs aan de orde.

1.3.8 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG		X		X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen		X		X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MID)		X		X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden		X		X

ID	Bevindingen
1	Een Procesbeschrijving inzake de voorwaarden voor verstrekkingen ingevolge paragraaf 3 van de WPG toegespitst op de specifieke artikel 8, 9, 10, 12 en 13 verwerkingen is niet aanwezig. Wel is de Handreiking Verstrekkingen met de verstrekkingentabellen op het intranet voor iedere relevante medewerker raadpleegbaar. Voor samenwerkingsovereenkomsten wordt gehandeld conform de Handreiking Verstrekkingen en is een format vastgesteld door het KMT. In het kader van de toekomstige samenvoeging van de korpsen Midden-West Brabant en Zeeland wordt reeds samengewerkt tussen respectievelijk de Unit Veiligheid & Integriteit en de afdeling Integriteit & Veiligheid. In april/mei 2011 werd geïnventariseerd wat de overeenkomsten en verschillen in taken en werkwijzen zijn. Deze inventarisatie heeft geleid tot concrete voorstellen om te komen tot eenduidige procedures. In de zeer nabije toekomst zullen o.a. procedures t.b.v. kennisnemingsverzoeken en verstrekkingen worden ontwikkeld. Uit het groepsinterview met de recherche teamchefs komt naar voren, dat er door hen niet of nauwelijks verstrekkingen vanuit hun onderzoeken buiten het politiedomein worden gedaan. Incidentele verstrekkingen van politiegegevens buiten het politiedomein worden handmatig geprotocolleerd. Bij het RRT in de vorm van een melding in het BVO journaal, bij de RT's in de vorm van het

ID	Bevindingen
	doorlopend journaal op de kantoorautomatiseringsomgeving in Word. Politiegegevens worden aan het OM verstrekt in de vorm van processen-verbaal en mondelinge overleggen met een zaaksofficier. Van een overleg wordt in voorkomende gevallen verslag gedaan in het onderzoeksjournaal. Aan het OM wordt verstrekt in de vorm van PV's en journaals van onderzoeken. Dit wordt niet apart vastgelegd en hier geldt ook geen protocolplicht. Voor wat betreft convenanten kwam naar voren, dat het milieuteam conform het SOZ (Samenwerking Overeenkomst Zeeland) convenant werkt. Voor wat betreft de bepalingen omtrent de geheimhoudingsplicht, wordt dit verwoord in PV's van bevindingen en/of journaals. Zoals eerder is verwoord, worden artikel 9 verwerkingen voornamelijk verwerkt m.b.v. de applicatie BVO. Deze applicatie kent een landelijk vastgestelde lijst van verschillende mutatiesoorten. Deze lijst stamt van voor de inwerkingtreding van de WPG. Eén van deze mutatiesoorten is genaamd VST (=Verstrekking). Deze VST mutatiesoort wordt echter meestentijds voor het ter beschikking stellen van politiegegevens binnen het politiedomein gebruikt. De PF heeft al in 2009 bij het functioneel beheer BVO voorgesteld om een zogenoemde TER-mutatie (Ter beschikking stelling) te realiseren. Hierdoor zou in de BVO registratie onderscheid gemaakt kunnen worden in ter beschikking stellingen en verstrekkingen. Het voorstel is echter niet overgenomen. De applicatie BVO is hiermee niet voorzien van een mogelijkheid tot vastleggen vergelijkbaar met de maatschappelijke klasse I-90 in de BVH. Zoals onder het hoofdstuk Verstrekkingen in deze rapportage wordt verwoord, worden schriftelijke verzoeken van externe instanties centraal afgehandeld door de afdeling Integriteit & Veiligheid. De ervaring leert dat deze verzoeken tot op heden geen betrekking hadden op artikel 9 informatie.

ID	Aanbevelingen
1-4	Zorg voor een procesbeschrijving waarin par. 3 verstrekkingen WPG worden geregeld en besteed tevens aandacht aan welke verstrekkingen wel en niet moeten worden geprotocolleerd. Besteed daarbij aandacht aan het verschil tussen ter beschikking stellen en verstrekken. Implementeer zo spoedig mogelijk de functionaliteit voor het protocolleren van verstrekkingen voor de BVO indien deze door de vtsPN wordt uitgeleverd. Stimuleer als compenserende maatregel naast de vastlegging in mutaties en journaals het gebruik van de mut-VST in BVO.

1.4 Artikel 10,1A CIE (verkrijgen van inzicht in betrokkenheid personen)

1.4.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen politiegegevens voor verkrijgen inzicht in betrokkenheid personen bij bepaalde misdrijven	X			
2	Politiegegevens worden conform de wettelijk bepaalde categorieën van personen verwerkt	X			X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens	X			
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen	X			
6	Politiegegevens zijn toereikend, terzake dienend en niet bovenmatig	X			
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet	X			
8	Vermelding van de herkomst en de wijze van verkrijging van politiegegevens	X			

ID	Bevindingen
1	In het korps brede overzicht met verwerkingen van politiegegevens is het gericht verwerken van politiegegevens door de CIE met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde misdrijven opgenomen.
2	[redacted]
3	Bij de CIE is geen sprake van een gemeenschappelijke verwerking van politiegegevens.
4	[redacted] Uit de interviews blijkt dat gevoelige gegevens slechts worden verwerkt indien dit onvermijdelijk is.
5	[redacted] Uit de interviews blijkt, dat aan de rechtmatigheid van de verkrijging van informatie van informanten in de praktijk doorlopend en intensief aandacht wordt besteed [redacted]
6	[redacted] met betrekking tot het toereikend, ter zake dienend en niet bovenmatig zijn van politiegegevens. Uit de interviews blijkt, dat in de praktijk ook conform die instructies wordt gewerkt. Dit verwerkingsproces wordt nauwgezet door zowel de leidinggevenden als de CIE-OvJ gecontroleerd. Op de kwaliteit van de politiegegevens wordt doorlopend door hen gestuurd. Dit is bijvoorbeeld aan de orde bij het opmaken van de zogenaamde "brutoverslagen" en het vervolgens overbrengen van de "netto-informatie" naar de "nettoverslagen" in BVO.
7	[redacted] met betrekking tot de regel dat politiegegevens uitsluitend voor een ander doel worden verwerkt dan waarvoor zij zijn verkregen voor zover de WPG daar uitdrukkelijk in voorziet. De Teamchef en diens vervanger zien in de verwerkingspraktijk strikt op de naleving van deze verplichting toe. Zij zijn ook altijd nauw bij dergelijke verwerkingen betrokken.
8	[redacted] De BVO biedt ook de functionaliteit om kenmerken aan een mutatie te koppelen. Indien dit relevant en mogelijk is, wordt deze functie gebruikt. Als deze functionaliteit in een voorkomend geval te weinig mogelijkheden biedt, wordt een en ander verwoord in de vrije tekstvelden. [redacted]

ID	Bevindingen
	[redacted]

ID	Aanbevelingen
2	Breng de problematiek met betrekking tot de in afwijking van de wettelijke bepalingen opgenomen CIE-subjecten onder de aandacht van de wetgever tenende hier een oplossing voor te bewerkstelligen.

1.4.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig	X			
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn		X		X
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies en onrechtmatige verwerking	X			
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG		X		X
5	Toegang voor CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens		X		X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt		X		X

ID	Bevindingen
1	[redacted] Uit de
2	interviews blijkt, [redacted] De BVO is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. [redacted] • Iedere ingevoerde mutatie wordt doorgenomen en eventuele omissies worden gesignaleerd. [redacted] • De verwerkingstermijnen van de artikel 10 informatie conform de WPG worden handmatig op ad hoc basis gehanteerd daar waar mogelijk. Zodra een CIE-subject actuele aandacht krijgt wordt gekeken of de bijbehorende informatie geschoond dient te worden. (Zowel doel- als expiratiedatum). In de praktijk levert schonen, in de vorm van verwijderen, problemen op daar een landelijke schoningsmodule voor BVO nog niet beschikbaar is. Er zijn compenserende maatregelen getroffen in de vorm van gegevensbeheer bij nieuwe invoer van subjectinformatie. Hierdoor wordt eventueel onrechtmatige verwerking van verwijderde gegevens zoveel mogelijk voorkomen. • In geval van schonen betekent dit vernietigen maar niet verwijderen conform artikel 14. Er wordt niet bewaard omdat de techniek dit niet mogelijk maakt. Tot nu toe is het niet voorgekomen dat informatie ouder dan vijf jaar ter beschikking werd gesteld. Niet alleen omdat dit wettelijk niet mag, maar ook omdat er geen sprake meer is van actualiteit. In principe wordt informatie ouder dan twee jaar niet ter beschikking gesteld. Een uitzondering zou kunnen zijn het ter beschikking stellen t.b.v. een zogenoemde cold-case. Dit is in de praktijk echter nog niet voorgekomen. • de wettelijk voorgeschreven halfjaarlijkse controle vindt niet plaats omdat de techniek dit niet ondersteunt. Zoals eerder vermeld ontbreekt een landelijke schoningsmodule en handmatige schoning is ondoenlijk. [redacted] Gesteld kan worden, dat het gegevensbeheer zeer zorgvuldig wordt uitgevoerd. [redacted]
3	[redacted] De bestanden worden geactualiseerd a.d.h. van informanteninformatie. Voor CSV's bestanden wordt wekelijks een actueel bestand aangehouden. [redacted]
4	Een procesbeschrijving of een ander document dat de toegang tot de politiegegevens regelt ten behoeve van het in het kader van de WPG door of namens de korpsbeheerder of de korpschef uit te oefenen toezicht is niet in het korps voorhanden. Maar in dit geval vervult de CIE-OvJ juist een belangrijke toezichthoudende rol bij het toezicht op de verwerking van politiegegevens. Een en ander is formeel geregeld in de Instructie van de P.G's aan de CIE-OvJ en de Instructie van de P.G's aan de CIE OvJ inzake de verwerking van politiegegevens. In die zin wordt het toezicht op de verwerkingen van politiegegevens door de CIE in de dagelijkse praktijk adequaat uitgeoefend.
5	De politie Zeeland beschikt niet over een specifieke procesbeschrijving of ander relevant document waarin de toegang tot politiegegevens is geregeld voor degene die met de controle en het toezicht op de WPG zijn belast. Dit zijn de interne auditor, de auditor, de privacyfunctionaris, de functionaris gegevensbescherming en het CBP. Voor het CBP zal de toegang tot de verwerking van politiegegevens bij gelegenheid van hun eventuele onderzoek bij de politie Zeeland worden geregeld. Een en ander voor zover nodig ten behoeve van het in dat specifieke geval in te stellen onderzoek. [redacted]

ID	Bevindingen
	[redacted]
	De toegang tot politiegegevens voor de interne auditor, de privacyfunctionaris en de functionaris gegevensbescherming is niet apart geregeld, maar impliciet via de reguliere autorisatieprocedure. Deze functionarissen hebben toegang tot verwerkingen van politiegegevens voor zover dit voor hun taakoefening noodzakelijk is.
	[redacted]
	[redacted] Deze handelswijze wordt in de regel in de praktijk ook toegepast.
	Als de PF en de IBF namelijk hun taak willen uitoefenen, wenden zij zich tot de betreffende Teamchef, gegevensbeheerder of functioneel beheerder en verkrijgen langs die weg de benodigde informatie. Een bijkomend argument voor deze praktische oplossing is, dat de PF en de IBF niet alleen over toereikende kennis en ervaring met alle applicaties bij de politie Zeeland zouden moeten beschikken, maar deze ook doorlopend moeten onderhouden. Dit ligt volgens hen, gezien de complexiteit in de functionaliteiten van bepaalde applicaties in samenhang met het beperkte gebruik, waaronder de BVO, niet in de rede. De kanttekening die hierbij geplaatst kan worden, is wel, dat de functionarissen er op moeten vertrouwen dat zij langs die weg altijd alle informatie verkrijgen waarom zijn vragen.
	[redacted]
6	Door of namens de korpsbeheerders van Zuid 6, waaronder de politie Zeeland is een Service Level Agreement (SLA) gesloten voor alle bij de vtsPN in technisch beheer zijnde politiesystemen. In de SLA zijn ook de beveiligingsvoorwaarden opgenomen. Over de uitvoering van de SLA wordt periodiek in de vorm van een Service Level Report (SLR) door de vtsPN gerapporteerd. Daarnaast is er regulier overleg tussen de functioneel beheerders en de vtsPN over de uitvoering van de SLA. In die zin ziet de korpsbeheerder toe op de uitvoering van de SLA. Ook de BVO waarin de CIE haar artikel 10 gegevens verwerkt, valt onder deze SLA. [redacted]

ID	Aanbevelingen
1-2	Implementeer met het oog op de doelschoning en het overbrengen van geschoonde gegevens naar de bewaarfase zo spoedig mogelijk de schoningsmodule voor BVO indien deze beschikbaar komt.
4	Maak in een beleidsnotitie of instructie transparant op welke wijze de korpsbeheerder toegang heeft tot de politiegegevens van de CIE die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens de WPG bepaalde. Hierin kan ook worden geregeld aan wie en op welke wijze de korpsbeheerder diens bevoegdheden en verantwoordelijkheden mandateert.
5	Stel een procesbeschrijving vast inzake de toegang tot politiegegevens voor degene die met de controle en het toezicht op de WPG zijn belast, zijnde de interne auditor, de auditor, de privacyfunctionaris, het CBP en de functionaris gegevensbescherming, alsmede degenen die in opdracht van de verantwoordelijke technische werkzaamheden verrichten.
6	Zorg voor een adequate regeling voor het toekennen en beheren van de rechten van de technisch beheerders op de CIE-omgeving in de SLA met de vtsPN. Besteed daarbij ook aandacht aan het toezicht op het beheer van die rechten.

1.4.3 Autorisaties (protocolplicht)

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid	X			X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd	X			X
3	Voldoen aan specifieke regels voor het autoriseren van avps bij de CIE, medewerkers Infodesk en misdaadanalisten	X			
4	Aanwijzing categorieën van ambtenaren voor de autorisaties in overeenstemming met de OvJ		X		X
5	Voldoen aan specifieke regels voor kennis en vaardigheden voor avps die de politiegegevens verwerken	X			

ID	Bevindingen
1 2	De politie Zeeland beschikt over een Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. De documenten zijn raadpleegbaar op het DELTANET, dat voor iedere gebruiker toegankelijk is. [redacted]

ID	Bevindingen
	[redacted] [redacted] De autorisaties op de zwacri (10 omgeving) in de BVO en kantoorautomatisering zijn voor het overige juist, tijdig, correct, etc. [redacted] Toegang/autorisatie van medewerkers van andere politieregio's (landelijk) is technisch niet mogelijk. [redacted]
3	[redacted] De Teamchef CIE of diens plaatsvervanger besluiten in de praktijk altijd zelf over iedere autorisatie op de CIE-omgeving.
4	[redacted]
5	[redacted] De overige functionarissen bij de CIE (niet zijnde runners) zijn intern / extern opgeleid / geïnstrueerd. Kort na inwerkingtreding van de WPG zijn CIE-medewerkers naar cursussen (e-learning) geweest. Toen de implementatie WPG in Zeeland werd opgepakt was de CIE al bezig om de WPG te implementeren. In december 2007 was reeds een praktisch overzicht overgang Wpolr naar WPG bij de CIE aanwezig. Hier werd aandacht aan besteed in een werkoverleg. De teamchef is van mening dat zijn medewerkers voldoende WPG geschoold en bewust zijn. Nieuwe medewerkers volgen de WPG e-learning [redacted] CIE-medewerkers moeten een BVO opleiding volgen. [redacted]

ID	Aanbevelingen
1-2-4	Bewerkstellig een landelijke regeling om grip te krijgen op de autorisaties van functioneel en technisch beheerders op de artikel 10 verwerking. Betrek hier het openbaar ministerie bij, gezien hun verantwoordelijkheid bij de aanwijzing van de categorieën van ambtenaren die voor de artikel 10 verwerking worden geautoriseerd.

1.4.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens gv met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			X
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	X			
2	Voor gv de avps autoriseren van de CIE	X			
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd CIE	X			
3	Avps die gv beschikken over de wettelijk vereiste kennis en vaardigheden	X			
4	Indien bij gv gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	X			
5	Indien noodzakelijk voor goede gv worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	X			
6	Vzv noodzakelijk voor het onderzoek politiegegevens gv met andere gegevens dan politiegegevens	X			
7	Voldoen aan protocolplicht gv met andere gegevens	X			
8	Voldoen aan protocolplicht gv met andere gegevens tijdens de bewaartermijn van 5 jaar	X			

ID	Bevindingen
1-8	Een procesbeschrijving inzake geautomatiseerd vergelijken is aanwezig in de vorm van de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence. [redacted] CIE medewerkers [redacted] hebben een zogenoemde superregistratie in de BVO. Dit betekent concreet dat men in de Zuid-6 (dus niet landelijk) de andere artikel 10 verwerkingen inhoudelijk kan raadplegen. Indien runners een Zeeuws onderzoek (= artikel 9 verwerking) bijlopen, dan wordt door de onderhavige bevoegd functionaris van deze artikel 9 verwerking een autorisatie voor hen aangevraagd. Op dit punt zijn zij te vergelijken met een gewoon teamlid. Sinds kort maakt de CIE gebruik van de mogelijkheid om BlueView geautoriseerd te worden. (Zie landelijk autorisatiemodel m.b.t. BlueView). Hiermee hebben zij de mogelijkheid om landelijk zowel BVH (waarin voornamelijk artikel 8 en deels artikel 9 gegevens worden opgeslagen) als de door BlueView ontsloten BVO artikel 9 registraties inhoudelijk te raadplegen. Echter, lang niet alle artikel 9 registraties worden ontsloten door BlueView. Ook hierover zijn landelijk afspraken gemaakt. M.b.v. bovengenoemde mogelijkheden worden subjecten bevraagd. Indien deze eenvoudige handeling valt onder de reikwijdte van een art. 11, lid 2, WPG verwerking, dan is onduidelijk of men voldoet aan de bepalingen van art. 6:4 BPG. Deze casus is zowel tussen de interne auditor als de externe auditor een bron van discussie geweest ten aanzien van de vraag of hier wel of niet sprake is van geautomatiseerd vergelijken. Ook op landelijk niveau is hierover nog steeds discussie gaande, waarover tot dusver nog geen consensus is bereikt. Immers *"Indien politiegegevens geautomatiseerd worden vergeleken met andere gegevens of in combinatie met elkaar worden verwerkt, als bedoeld in artikel 11, eerste, tweede, vierde en vijfde lid van de wet, worden van die verwerking de volgende gegevens vastgelegd:* ***a.** de gegevens die voor de rechtstreekse raadpleging zijn gebruikt;* ***b.** de identiteit of het kenmerk van de politieambtenaar die de rechtstreekse raadpleging heeft uitgevoerd;* ***c.** de gegevens op grond waarvan kan worden nagegaan welke gegevens ter beschikking zijn gesteld voor verdere verwerking voor een doel, als bedoeld in artikel 9 of 10 van de wet."* Wat zowel BVO als BlueView doen, is het loggen van handelingen in deze applicaties. Mogelijk dat deze logging zover gaat dat hiermee aan de verplichtingen, zoals onder a, b en c genoemd, wordt voldaan. Dit is niet verder onderzocht. Maar uit gesprekken met de functioneel beheerder BVO komt naar voren, dat de BVO logging (bijna) onleesbaar is. De logging in BlueView is dusdanig omvangrijk, dat de vergelijking "met een speld in een hooiberg zoeken" opgaat. In de praktijk is (kan) de controle of het toezicht op logging in dat geval dan ook niet of nauwelijks aanwezig (worden uitgevoerd). [redacted] [redacted] [redacted] [redacted] De bestanden worden geactualiseerd a.d.h. van informanteninformatie. Voor CSV's bestanden wordt wekelijks een actueel bestand aangehouden. Oudere bestanden blijven bewaard [redacted]

ID	Aanbevelingen
1	Breng het vraagstuk van het geautomatiseerd vergelijken op landelijk niveau onder de aandacht van de wetgever. Neem naar aanleiding van de uitkomst van deze actie waar nodig beheersmaatregelen.

1.4.5 In combinatie met elkaar verwerken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens icmev met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	-			
2	Voor icmev de avps autoriseren van de CIE	-			
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd CIE	-			
3	Avps die icmev beschikken over de wettelijk vereiste kennis en vaardigheden	-			
4	Indien bij icmev gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	-			

ID	Beheersdoelstellingen				
5	Indien noodzakelijk voor goede icmev worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	-			
6	Voldoen aan protocolplicht icmev met andere gegevens	-			
7	Voldoen aan protocolplicht icmev met andere gegevens tijdens de bewaartermijn van 5 jaar	-			

ID	Bevindingen
1-7	[redacted] Uit de intensieve interviews die over dit onderwerp met de teamchef CIE [redacted] zijn gehouden, zijn geen indicaties naar voren gekomen, dat er bij CIE tot dusver sprake is van in combinatie met elkaar verwerken. De systemen en de tools die de CIE ter beschikking heeft voorzien niet in deze vorm van verwerking.

ID	Aanbevelingen
1	Geen.

1.4.6 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Politie gegevens elk half jaar op noodzaak controleren en uiterlijk 5 jaar na datum laatste verwerking verwijderen		X		
2	Na verwijdering maximaal 5 jaar bewaren en gebruiken voor afhandeling klachten en verantwoording van verrichtingen		X		
3	Verwijderde gegevens tijdens bewaartermijn niet verstrekken aan personen/instanties in 16 t/m 20, 23 en 24 WPG	X			
4	Uitsluitend in bijzondere gevallen tijdens bewaartermijn in opdracht bevoegd gezag tbv hernieuwde 9 of 10 verwerking	X			
5	Voldoen aan de regels schriftelijke vastlegging hernieuwde verwerking en ter beschikking stelling verdere verwerking	X			
6	Afzien van vernietiging ingeval waarde voor cultureel erfgoed of historisch onderzoek conform regels Archiefwet		X		X

ID	Bevindingen
1-6	[redacted] Gegevens worden maximaal 5 jaar na de laatste verwerking bewaard, daarna worden ze verwijderd. Dit wordt maandelijks gecontroleerd. Voor gegevens die tussen de 5 en 10 jaar oud zijn, wordt voor 'hergebruik' toestemming gevraagd aan de OvJ (artikel 14, lid 3, WPG). Dit wordt geprotocolleerd. Degenen die toegang hebben tot deze gegevens, zijn van deze werkwijze op de hoogte en zijn of worden opgeleid in de WPG. De teamchef CIE is alert op de naleving van dit voorschrift. De CIE-OvJ houdt daadwerkelijk toezicht op de uitvoering van de bedoelde verwerkingsprocessen. Echter, ook kwam naar voren, dat er in de afgelopen periode tijdelijk bij de CIE een achterstand is ontstaan in de handmatige schoning na de bewaartermijn. Wegens het ontbreken van een technische voorziening in BVO is tot en met juni 2008 de schoning handmatig en consistent uitgevoerd. Sinds die periode gebeurt dit meer op ad-hoc basis waarbij de gegevens worden vernietigd. Inmiddels is het applicatie technisch schonen in de functionele eisen voor BVO opgenomen en zal dit in de eerstvolgende release mogelijk zijn. Het verstrekken tijdens de bewaartermijn aan de in par. 3 WPG genoemde personen of instanties, alsmede hernieuwd gebruik tijdens de bewaartermijn is nog niet voorgekomen. [redacted] De te beantwoorden vraag is nu wie de "beheerder" wordt of moet zijn van deze verwijderde CIE informatie. Het beheer beleggen bij de CIE betekent dat een CIE medewerker, in strijd met artikel 14 WPG, onvermijdelijk een soort van "operationele" toegang tot verwijderde gegevens verkrijgt. Hiervoor zullen compenserende maatregelen moeten worden genomen. Tot op heden is er niets ter archivering aangeboden buiten de eigen CIE opslagstructuur. [redacted]. Aangezien op dit moment de techniek niet voldoet aan de criteria die gesteld worden in de WPG, zoals verwijderen van gegevens uit artikel 10 WPG naar artikel 14 WPG wordt er slechts sporadisch geschoond. Deze schoning houdt in dat de gegevens al geruime tijd, doch geen 5 jaar, voldoen aan het criterium dat zij verwijderd hadden moeten zijn en dat uit de gegevens blijkt dat er van een Zeeuws karakter (woonachtig in Zeeland of actief in Zeeland) geen sprake is. Bij een dergelijke schoning worden de gegevens niet verwijderd maar vernietigd. Bij de schoning wordt gekeken naar waarde voor cultureel erfgoed of historisch onderzoek. Deze situatie heeft zich nog niet voorgedaan.

ID	Aanbevelingen
1	Continueer de compenserende maatregelen voor politiegegevens in de bewaarfase.
2	Implementeer zo spoedig mogelijk de voorziening voor het geautomatiseerd schonen indien deze door de vtsPN wordt uitgeleverd.
6	Zorg voor een voorziening om aan de Archiefwet te voldoen.

1.4.7 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie indien nodig voor hun taakuitoefening	X			
2	Politiegegevens tbs aan art. 8, 9, 10,12 na instemming bevoegde functionaris	X			
3	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 1, genoemde ondersteunende taken	X			
4	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 2, genoemde ondersteunende taken	X			
5	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 3, genoemde ondersteunende taken	X			
6	Tbs van politiegegevens uitsluitend weigeren of beperken in de wettelijk toegestane gevallen	X			
7	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld	X			

ID	Bevindingen
1-7	Het onderwerp terbeschikking stelling van politiegegevens is geregeld in het Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. [redacted] Dit onderwerp is ook nauw verweven met de regelingen in par. 1.4.3 (autorisaties). [redacted] Binnen de Zuid-6 operationele teams is sprake van lezen en labelen bij ter beschikking stelling van politiegegevens door de CIE-en. Ter beschikking stelling vindt ook plaats via het geïmplementeerde landelijke autorisatiemodel BVO, [redacted]. De definitieve ter beschikking stelling aan bijvoorbeeld een rechercheteam vindt plaats in de vorm van een proces-verbaal. Een ter beschikking stelling vindt altijd plaats met instemming van de teamchef CIE of diens vervanger. [redacted] [redacted] Ter beschikking stellingen (binnen het politiedomein) anders dan langs geautomatiseerde weg worden structureel vastgelegd in de BVO registratie. De CIE-OvJ krijgt structureel kopieën van alle PV's van ter beschikkingstellingen. Van ieder p.v. wordt ook een mut VST in BVO aangemaakt. Aan de CIE-en onderling wordt CIE-informatie ter beschikking gesteld door middel van de zogenaamde 4x4's. In relatie tot de weigeringsgronden genoemd in artikel 2:13, lid 1, onder a en b, BPG worden betreffende gegevens binnen de CIE verwerkingen gecodeerd met de coderingen: • 11: operationeel te gebruiken; • 01: alleen te gebruiken in overleg met afzender; • 00: informatie met zware beperkingen voor gebruik; • 200: kan niet operationeel gebruikt worden, verhoogd afbreukrisico; • 300:kan niet operationeel gebruikt worden, bron beschermingsbelangen; Er wordt nauwgezet gewerkt met deze coderingen. In principe wordt alleen 01 en 11 informatie ter beschikking gesteld buiten de CIE-structuur. Tot op heden is er geen CIE informatie verstrekt op grond van artikel 19 WPG en artikel 20 WPG. [redacted]

ID	Aanbevelingen
1-7	Geen.

1.4.8 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG	X			
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen	X			
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MID)	X			
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden	X			

ID	Bevindingen
1-4	Er worden slechts incidenteel CIE gegevens buiten het politiedomein verstrekt. Voorbeelden hiervan zijn verstrekkingen t.b.v. naleving van de BIBOB wetgeving. Deze verstrekkingen vinden plaats in de vorm van een proces-verbaal met instemming van de CIE-OvJ. Ook deze verstrekkingen worden structureel vastgelegd in de BVO registratie. De teamchef RID heeft op grond van een convenant inzage in de CIE verwerking t.b.v. zijn AIVD taak. (Betreft convenant m.b.t. autorisaties RID voor CIE-info van het college van PG's, gememoreerd in een brief van de Raad van KC's d.d. 10-02-2011, kenmerk 201110598).

ID	Aanbevelingen
1-4	Geen.

1.5 Artikel 10,1B Themaverwerking (verkrijgen van inzicht in betrokkenheid personen)

1.5.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen politiegegevens voor verkrijgen inzicht in betrokkenheid van personen bij themamisdrijven				X
2	Politiegegevens worden conform de wettelijk bepaalde categorieën van personen verwerkt				X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden				X
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens				X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen				X
6	Politiegegevens zijn, toereikend, terzake dienend en niet bovenmatig				X
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet				X
8	De herkomst en de wijze van verkrijging van politiegegevens wordt vermeld				X

ID	Bevindingen
1	Tijdens de interne audit maar ook tijdens de privacy audit is geruime tijd aandacht besteed aan de vraag of er bij de Vreemdelingenpolitie sprake is van een verwerking als bedoeld in artikel 10, lid 1, onder b, WPG, de zogenaamde themaverwerking op het terrein van mensensmokkel / mensenhandel. Uiteindelijk is voorzichtig de conclusie getrokken, dat er bij de VP sprake zou kunnen zijn van een verwerking als bedoeld in voornoemd artikel voor zover het betreft mensenhandel als bedoeld in art. 273f WvSr en mensensmokkel als bedoeld in art. 197a WvSr. Door capaciteits- en tijdgebrek zijn een aantal onderwerpen bij de VP niet toereikend in de interne audit en de externe audit onderzocht. Om die reden wordt in deze paragraaf en de hierna volgende paragrafen waar dit relevant is volstaan met de weergave van de bevindingen en de aanbevelingen. Informatie wordt ingevoerd in een systeem dat verplicht is. Een en ander is voorgeschreven door de PG. Uit het interview met de Vreemdelingenpolitie (VP) kwam naar voren, dat het systeem BVV en PSHV niet aansluiten op de bestaande, specialistische werkzaamheden / registraties / vastleggingen van VP. Ook om aan landelijke verplichtingen te voldoen, wordt gebruik gemaakt van andere systemen die door de VP worden gevoed en die elders worden beheerd.
2	Een procesbeschrijving inzake de verwerking van de politiegegevens van de wettelijk bepaalde categorieën van personen en de samenhang met de wettelijke aangewezen misdrijven is niet aanwezig. Het gaat bij de VP over mensenhandel als bedoeld in art. 273f WvSr en mensensmokkel als bedoeld in art. 197a WvSr. Een en ander volstrekt zich conform de richtlijnen. Controle op dit op onderwerp is er niet.
3	De gemeenschappelijke verwerking, is door de verantwoordelijke schriftelijk aan het College Bescherming Persoonsgegevens gemeld (protocolplicht). Dat zou dan gebeurd moeten zijn door de PG maar dat is bij de teamchef van de VP niet bekend.
4	Een procesbeschrijving inzake het verwerken van gevoelige gegevens is niet aanwezig. Verwerken van gevoelige gegevens komt voor. Bijvoorbeeld bij prostitutiecontroles en worden als zodanig geregistreerd, maar slechts in aanvulling op andere politiegegevens indien dit onvermijdelijk is. In andere gevallen komt dit niet voor. Bij de VP komen regelmatig situaties voor waarbij de ketenpartners informatie willen die de VP, conform het gestelde in de WPG, niet kan / mag verstrekken. (bijv. bij prostitutiecontroles).
5	Een procesbeschrijving inzake de rechtmatigheid van de verkrijging is niet aanwezig. Onrechtmatige verkrijging komt bij de VP voor, naar men vermoed op de volgende terreinen. Men maakt gebruik van de BVV (Basis Voorziening Vreemdelingen) en de PSHV (Politie Suite Handhaving Vreemdelingen). Tussen de genoemde systemen waar de PV gebruik van maakt en de BVH en BVO vindt informatie uitwisseling/verstrekking/terbeschikking stelling van informatie plaats. De rechtmatigheid/onrechtmatigheid vergt veel zorgvuldigheid. Een protocol is er niet. Zoals eerder opgemerkt, een procesbeschrijving is er evenmin. Bij de VP is bekend, dat er bij dergelijke acties zaken verkeerd lopen. Het onderwerp rechtmatige verkrijging kwam tijdens de interviews bij de Vreemdelingenpolitie (VP) uitgebreid aan de orde. Zo valt de prostitutiecontrole onder het mandaat van de Burgemeester. Controles worden uitgevoerd op basis van de gemeentelijke vergunningencontroles. Bij dergelijke controles komt het voor dat er ook informatie over mensenhandel aan het licht komt. Bijvoorbeeld, als prostituees veel verplaatst worden van het ene naar het andere werkadres, is dit een signaal dat er sprake kan zijn van mensenhandel / mensensmokkel. Dit soort signalen staan in de desbetreffende aanwijzing van het college van PG's. Dergelijke signaal informatie is niet te scheiden van de reguliere controle informatie. In feite vindt er controle plaats met 2 doelen die met elkaar samenhangen en niet van elkaar zijn te scheiden. Vragen die in dat verband rijzen zijn hoe dan wel signaal informatie gegenereerd kan worden als er geen informatie over de identiteit van alle gecontroleerde prostituees opgeslagen zou mogen worden. Hier treedt een spanningsveld op tussen de privacy van personen die een vrij beroep uitoefenen en de politietaak in het kader van het voorkomen en bestrijden van de ernstige delicten. De VP worstelt met dit vraagstuk, is zich goed van dit spanningsveld bewust en gaat hier zo zorgvuldig mogelijk mee om. In bestuurlijke rapportages wordt met dit spanningsveld rekening gehouden. Tegen de achtergrond van de complexiteit van dit vraagstuk en de gewichtige belangen van de slachtoffers van mensenhandel en mensensmokkel, zijn uit de beoordeling van de handelswijze van VP, op voorhand geen indicaties naar voren gekomen dat hiermee in strijd met de betreffende richtlijn van de PG's zou worden gehandeld.
6	Een procesbeschrijving inzake het toereikend, terzake dienend en niet bovenmatig zijn van politiegegevens is niet aanwezig. De teamchef let hier bij gelegenheid op. Alleen relevante zaken worden verwerkt.
7	Een procesbeschrijving inzake het voor een ander doel verwerken van politiegegevens dan waarvoor ze zijn verkregen is niet aanwezig. De teamchef geeft aan dat dit niet voorkomt binnen zijn afdeling.
8	Een procesbeschrijving inzake het vermelden van de herkomst en de wijze van verkrijging van politiegegevens is niet aanwezig. Het informatiesysteem bevat geen velden waarin de herkomst en de wijze van verkrijging kan worden vastgelegd. Volgens de teamchef VP wordt de applicatie BVO gebruikt voor opslag van deze politiegegevens. Door zijn medewerkers worden in de BVO mutaties vermeld waar en op welke wijze politiegegevens zijn verkregen. Dit is een vereiste omdat, bijvoorbeeld indien een proces-verbaal wordt opgemaakt, de rechtmatigheid moet blijken.

ID	Aanbevelingen
1-8	Voorzie in de benodigde proces-beschrijvingen en laat op alle onderwerpen een aanvullende privacy audit uitvoeren.

1.5.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig				X
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn				X
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies en onrechtmatige verwerking				X
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG				X
5	Toegang voor CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens				X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt				X

ID	Bevindingen
1	Een procesbeschrijving inzake het juist en nauwkeurig verwerken van politiegegevens is niet aanwezig. De applicatie is niet voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. Hierop wordt de teamchef en een aantal andere medewerkers binnen de afdeling toegezien. Geheel sluitend is dat echter niet. Indien fouten en dergelijke worden geconstateerd, worden deze gecorrigeerd.
2	Een procesbeschrijving inzake het verbeteren, vernietigen of aanvullen van gegevens indien deze onjuist of onvolledig blijken te zijn, is niet aanwezig. In de alledaagse praktijk komt dit zelden voor. Er zijn wel degelijk controlemomenten door de TC of andere medewerkers binnen de afdeling. Bovendien weten alle medewerkers dat zij accuraat moeten werken aangezien daar veel van kan afhangen. Als een onvolkomenheid blijkt, wordt deze verbeterd en/of rechtgezet.
3	De maatregelen/procedures/afspraken zijn vastgelegd. De ruimte waar VP werkt maakt onderdeel uit van het politiebureau te Goes. Dat bureau kent een 24-uurs bezetting. Een clean-desk policy is er niet. In de dienstauto's gebruikt men geen C2000 en voor de rest geen verbindingsmiddelen behalve de standaard diensttelefoon voor een aantal medewerkers. Voor de afdeling VP wordt op de J schijf informatie weggeschreven, niet zijnde politiegegevens. Er zijn ook andere informatiedragers. Er wordt gebruik gemaakt van een stand-alone PC met 17 gebruikers [redacted]. Hierop draait mail-fit en web-fit dat door de vtsPN wordt ondersteund. De leverancier 'Bull' doet het onderhoud aan de PC en beschikt hiertoe over een autorisatie vekregen van de DNRI. De toegang wordt middels een password verkregen. Het vervoer van informatie op andere gegevensdragers komt voor. Bijvoorbeeld USB-sticks. De oude informatie die erop staat wordt consequent verwijderd. De teamchef ziet hierop toe.
4	Een procesbeschrijving inzake de toegang tot de politiegegevens ten behoeve van het toezicht door de verantwoordelijke op de naleving van het bij of krachtens de WPG bepaalde is niet aanwezig bij de teamchef VP
5	Procesbeschrijving inzake de toegang tot politiegegevens voor degene die met de controle en het toezicht op de WPG zijn belast, zijnde de interne auditor, de auditor, de privacyfunctionaris, het CBP en de functionaris gegevensbescherming, alsmede degenen die in opdracht van de verantwoordelijke technische werkzaamheden verrichten is niet aanwezig.
6	Bewerkerovereenkomsten zijn niet aanwezig cq. niet gemaakt. Ten aanzien van dit onderdeel bestaat onduidelijkheid.

ID	Aanbevelingen
1-6	Voorzie in de benodigde proces-beschrijvingen en laat op alle onderwerpen een aanvullende privacy audit uitvoeren.

1.5.3 Autorisaties (protocolplicht)

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid				X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd				X
3	Voldoen aan specifieke regels voor het autoriseren van avps bij de Themaverwerking				X
4	Aanwijzing van de categorieën van ambtenaren voor de autorisaties in overeenstemming met de OvJ				X
5	Voldoen aan specifieke regels voor kennis en vaardigheden voor avps die de politiegegevens verwerken				X

ID	Bevindingen	V	D	N	A
1 2 3 4	De politie Zeeland beschikt over een Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. De autorisatieprocedure voorziet in de autorisatie voor intern of onder intern gezag werkend personeel, autorisatie van personeel dat in dienst is van een ander politiekorps en tenslotte autorisatie van overige medewerkers, kort gezegd de zogenaamde externen. De documenten zijn raadpleegbaar op het Intranet (Deltanet) en zijn voor iedere gebruiker toegankelijk. Daarnaast zijn momenteel nieuwe standaard autorisatieprofielen en autorisatiematrixen in (een vergevorderd) stadium van ontwikkeling. In die zin beschikt de politie Zeeland over een autorisatiebeheerssysteem, waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld, met het oog op het voldoen aan de eisen van zorgvuldigheid en evenredigheid. De procesbeschrijving en het autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties van het project Implementatie Wet politiegegevens. De procesbeschrijving is momenteel in bewerking bij de IBF. Er zijn binnen VP een aantal applicaties die niet geautoriseerd worden door de PF/IBF. Autorisaties in het informatiesysteem komen niet allemaal overeen met de toegekende autorisaties. Er is sprake van vervuiling. Bovendien vraagt de teamchef soms autorisaties aan, anders dan via de hierboven genoemde procedure. Hij doet de aanvraag bijvoorbeeld bij de DNRI voor de hiervoor genoemde systemen (foto's en vingerafdrukken). Een en ander gaat dan buiten om PF/IBF en Functioneel Beheer om. Bewerkerovereenkomsten zijn, zoals dat al eerder is vermeld, niet aanwezig cq. niet gemaakt.				X

ID	Bevindingen	V	D	N	A
5	Een proces- of functiebeschrijving inzake de kennis en vaardigheden waarover de genoemde ambtenaren die de politiegegevens verwerken moeten beschikken, is niet aanwezig.				X

ID	Aanbevelingen
1-5	Voorzie in de benodigde proces-beschrijvingen en laat op alle onderwerpen een aanvullende privacy audit uitvoeren.

1.5.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens gv met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens				X
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek				X
2	Voor gv de avps autoriseren van de eenheid Themaverwerking				X
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd eenheid Themaverwerking				X
3	Avps die gv beschikken over de wettelijk vereiste kennis en vaardigheden				X
4	Indien bij gv gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt				X
5	Indien noodzakelijk voor goede gv worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd				X
6	Vzv noodzakelijk voor het onderzoek politiegegevens gv met andere gegevens dan politiegegevens				X
7	Voldoen aan protocolplicht gv met andere gegevens				X
8	Voldoen aan protocolplicht gv met andere gegevens tijdens de bewaartermijn van 5 jaar				X

ID	Bevindingen
1	Het onderwerp geautomatiseerd vergelijken is niet getoetst om reden dat het volgens de teamchef VP bij hen niet zou voorkomen.

ID	Aanbevelingen
1	Laat een aanvullende privacy audit uitvoeren bij de Vreemdelingenpolitie met betrekking tot het onderwerp geautomatiseerd vergelijken.

1.5.5 In combinatie met elkaar verwerken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens icmev met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens				
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek				
2	Voor icmev de avps autoriseren van de hoofd eenheid Themaverwerking				
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd eenheid Themaverwerking				
3	Avps die icmev beschikken over de wettelijk vereiste kennis en vaardigheden				
4	Indien bij icmev gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt				
5	Indien noodzakelijk voor goede icmev worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd				
6	Voldoen aan protocolplicht icmev met andere gegevens				
7	Voldoen aan protocolplicht icmev met andere gegevens tijdens de bewaartermijn van 5 jaar				

ID	Bevindingen
1	Het onderwerp in combinatie verwerken is niet getoetst om reden dat het volgens de teamchef VP bij hen niet zou voorkomen.

ID	Aanbevelingen
1	Geen.

1.5.6 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Politie gegevens elk half jaar op noodzaak controleren en uiterlijk 5 jaar na datum laatste verwerking verwijderen				X
2	Na verwijdering maximaal 5 jaar bewaren en gebruiken voor afhandeling klachten en verantwoording van verrichtingen				X
2	Verwijderde gegevens na afloop bewaartermijn vernietigen				X
3	Verwijderde gegevens tijdens bewaartermijn niet verstrekken aan personen/instanties in 16 t/m 20, 23 en 24 WPG				X
4	Uitsluitend in bijzondere gevallen tijdens bewaartermijn in opdracht bevoegd gezag tbv hernieuwde 9 of 10 verwerking				X
5	Voldoen aan de regels schriftelijke vastlegging hernieuwde verwerking en ter beschikking stelling verdere verwerking				X
6	Afzien van vernietiging ingeval waarde voor cultureel erfgoed of historisch onderzoek conform regels Archiefwet				X

ID	Bevindingen
1-5	Deze onderwerpen zijn niet getoetst omdat ze niet van toepassing zouden zijn volgens de TC Vreemdelingen Politie.
6	V.w.b. het "papieren" archief: uit verkregen informatie van de teamchef Post & Archiefzaken, blijkt dat gehandeld wordt conform de

ID	Bevindingen
	Selectielijst voor archiefbescheiden van (regionale) politieorganisaties 2004. In deel 2 onder punt 3 is de selectielijst voor archiefbescheiden m.b.t. de uitvoering van de politietaak opgenomen. Echter deze selectielijst spreekt nog over de Wet politieregisters en is niet geactualiseerd. Door de betrokken teamchef werd hiervoor op een landelijke vergaderingen aandacht gevraagd, maar dit heeft nog niet geleid tot aanpassing van bedoeld document. Vervolgens heeft hij, eind 2009, op eigen initiatief en met zijn kennis en ervaring een concept "Toegankelijkheid en bewaartermijnen van politiegegevens op grond van de WPG" opgesteld, a.d.h. waarvan de archiefbescheiden in Zeeland worden beheerd.

ID	Aanbevelingen
1-6	Laat met betrekking tot alle onderwerpen een aanvullende privacy audit uitvoeren bij de Vreemdelingenpolitie.

1.5.7 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie indien nodig voor hun taakuitoefening				X
2	Politiegegevens tbs aan art. 8, 9, 10,12 na instemming bevoegde functionaris				X
3	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 1, genoemde ondersteunende taken				X
4	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 2, genoemde ondersteunende taken				X
5	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 3, genoemde ondersteunende taken				X
6	Tbs van politiegegevens uitsluitend weigeren of beperken in de wettelijk toegestane gevallen				X
7	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld				X

ID	Bevindingen
1	Een procesbeschrijving inzake het ter beschikking stellen van politiegegevens door de verantwoordelijke aan personen die door hemzelf dan wel door een andere verantwoordelijke zijn geautoriseerd voor de verwerking van politiegegevens is niet aanwezig. De VP voedt landelijke systemen. Hierin worden gegevens opgeslagen die ingevoerd worden door VP. De server draait bij onder andere de DNRI en daar wordt ook het beheer gedaan. Alleen de opgeleide medewerkers kunnen de tool bevragen. VP voedt alleen het systeem.
2-7	Niet getoetst.

ID	Aanbevelingen
1-7	Laat met betrekking tot alle onderwerpen een aanvullende privacy audit uitvoeren bij de Vreemdelingenpolitie.

1.5.8 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG				X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen				X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MIVD)				X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden				X

ID	Bevindingen
1-4	Deze onderwerpen zijn niet getoetst.

ID	Aanbevelingen
1-4	Laat met betrekking tot alle onderwerpen een aanvullende privacy audit uitvoeren bij de Vreemdelingenpolitie.

1.6 Artikel 10,1C, RID (verkrijgen van inzicht in betrokkenheid personen)

1.6.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht met verwerkingen voor het inzicht in de betrokkenheid van personen bij bepaalde openbare orde misdrijven	X			
2	Politiegegevens worden conform de wettelijk bepaalde categorieën van personen verwerkt	X			
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens	X			
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen	X			
6	Politiegegevens zijn toereikend, terzake dienend en niet bovenmatig	X			
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet	X			
8	De herkomst en de wijze van verkrijging van politiegegevens wordt vermeld	X			

ID	Bevindingen
1	Een overzicht of een lijst met bewerkingen van lopende onderzoeken inzake artikel 10 is aanwezig. Alle zaken die de openbare orde betreffen worden opgenomen/verwerkt in de BVO in een afzonderlijke omgeving. Het gaat hier vaak over groepen van personen. Een persoon die in het kader van één van de openbare orde thema's in beeld komt, kan aan de hand van een startmutatie in de BVO worden geregistreerd, waarbij relaties met contacten worden gelegd. Er wordt zo een beeld van die persoon en zijn contacten gecreëerd. Dat wordt door de RID zorgvuldig gedaan en er wordt bewust mee omgegaan. De noodzakelijkheid en de doelbinding is er altijd en de overwegingen liggen vast bij mogelijke verstoringen van de openbare orde. De feiten en omstandigheden waarom de groep of het individu in beeld worden gebracht, worden goed omschreven. De BVH wordt voornamelijk als informatiebron gebruikt. In principe wordt alle openbare orde informatie opgeslagen/verwerkt in de BVO en alle zaken aangaande de informanten op een afzonderlijk systeem RIDS. Zie verderop voor nadere uitleg/beschrijving daarvan.
2	Een procesbeschrijving inzake de verwerking van de politiegegevens van de wettelijk bepaalde categorieën van personen is aanwezig bij de RID. De wettelijk bepaalde categorieën worden door het bevoegd gezag vastgelegd in het Inlichtingen behoefteplan en vanaf 2011 in de Intelligence agenda die goedgekeurd wordt door de burgemeesters en de korpsleiding van de politie Zeeland. De teamchef RID gaf aan dat naar aanleiding van de eerder gehouden interne WPG audit, het handboek RID op 26 april 2011 door de Korpsleiding is geaccordeerd. Ook eventueel toekomstige wijzigingen zullen op deze wijze worden geformaliseerd. Door de landelijke Expertgroep Openbare Orde wordt de Ministeriële regeling "Handleiding Informatie Inwinning Openbare Orde" van 11 mei 2000 geactualiseerd. De inwerkingtreding van de nieuwe Politiewet en de WPG kunnen nog aanleiding zijn tot detailwijzigingen. Voor wat betreft de opname criteria van artikel 10 WPG heeft de chef RID de volgende toelichtingen gegeven. Artikel 10 heeft het over de ernstige verstoring van de openbare orde. De memorie van toelichting geeft een uitgebreidere definitie van dat begrip en vult als het ware de kaders meer in voor wat betreft het begrip schending. Dat kan dus ook in proactieve zin gebeuren. De start van een onderzoek is niet echt een overweging. De argumentatie daarvoor is dat de start in feite reeds genoemd wordt in het Inlichtingen Behoefte Plan. Daarin staan de punten die meegenomen worden door de RID. Een en ander is in overleg met 13 burgemeesters en de korpsleiding van de regiopolitie Zeeland. Daarin staat dus al de reden dat naar die taken gekeken wordt. Vanaf 2011 wordt een en ander ingevuld in de regionale Intelligence agenda en wordt het inlichtingen behoefte plan niet meer ingevuld, maar wordt in de BVO een startmutatie gemaakt op de relevante onderwerpen. De RID heeft twee taken, namelijk de AIVD taak en de Openbare Orde taak onder gezag van de burgemeester. De informatie-inwinning is gebaseerd op artikel 2 Politiewet 1993. De burgemeester heeft op grond van artikel 12 van de Gemeentewet 1993 het gezag over de politie als die in een gemeente optreedt ter handhaving van de openbare orde. De burgemeester kan de betrokken ambtenaren de nodige aanwijzingen geven. De burgemeester is op grond van artikel 172 van de Gemeentewet belast met de handhaving van de openbare orde. Hij is bevoegd overtredingen van wettelijke voorschriften te beletten of te beëindigen en bedient zich daarbij van de onder zijn gezag staande politie. De burgemeester is bevoegd bij verstoring van de openbare orde of bij ernstige vrees voor het ontstaan daarvan, de bevelen te geven die noodzakelijk te achten zijn voor de handhaving van de openbare orde. Ook hier zit een discrepantie in de omschrijving van de ernst van de verstoring t.o.v. de WPG. Jaarlijks adviseert de teamchef RID de korpsleiding in de vorm van een inlichtingenbehoefte plan, openbare orde gerelateerd, welke items aandacht behoeven. Zoals hierboven ook aan de orde kwam, maakt dit plan sinds dit jaar deel uit van de regionale intelligence agenda en is voorgelegd aan het regionaal college. Na instemming van het regionaal college werkt de RID proactief o.a. ter verkrijging van een goede informatiepositie, aan de aandachtbehoevende items. M.b.t. de verwerkte politiegegevens en categorieën van personen merkte de teamchef, in aanvulling op het voorgaande, op dat er een discrepantie zit tussen de wetstekst van artikel 10, lid 1, onder c, WPG en de bijbehorende Memorie van toelichting. In de wetstekst wordt gesteld dat de openbare orde ernstig geschonden wordt. In de memorie van toelichting van artikel 10 WPG wordt gesproken over de proactieve functie van deze gegevensverwerking t.b.v. een goede informatiepositie ter voorkoming van ernstige schendingen van de openbare orde. Daarnaast wordt in artikel 172 van de Gemeentewet gesproken over verstoring van de openbare orde (dus niet: ernstige) of bij ernstige vrees voor het ontstaan daarvan. De RID'en verwerken informatie in verband met het voorkomen van ernstige schendingen van de openbare orde. Het doel van de werkzaamheden is het voorkomen van openbare ordeverstoringen door het verzamelen van inlichtingen teneinde het bevoegd gezag te kunnen adviseren. De teamchef geeft een concreet voorbeeld van een plaatsgevonden demonstratie waarbij absoluut geen sprake was van schending van de openbare orde, maar waarvan de verkregen gegevens wel degelijk van belang kunnen zijn om toekomstige openbare orde schendingen te duiden.
3	Een gemeenschappelijke verwerking is niet aan de orde. Wel worden in voorkomende gevallen "externe" RID functionarissen ingezet, maar deze werken dan onder verantwoording van de Korpsbeheerder Zeeland. De door hen verwerkte gegevens worden

ID	Bevindingen
	opgeslagen in de applicaties waarvoor de Korpsbeheerder Zeeland verantwoordelijke is.
4	Procesbeschrijving inzake het verwerken van gevoelige gegevens is aanwezig bij de RID in de vorm van het proceshandboek en de werkinstructie 'verzamelen informatie' en 'ethische code RID'. De richtlijnen in de procesbeschrijvingen staan op het intranet van de RID en zijn bekend bij de medewerkers. Er is bij voortduring aandacht voor de bepalingen in artikel 5 van de WPG. Bij twijfel neemt men contact op met de PF. Degene die in eerste instantie de gevoelige gegevens verwerkt, kijkt bij het verwerken van de informatie al naar de onvermijdelijkheid. Dat wordt vervolgens nog een keer door de bewerker en daarna nog een keer door de chef gedaan die al dan niet toestemming geeft voor opname, danwel opdracht geeft tot verwijdering van de gevoelige gegevens. De teamchef maakt telkens de afweging of een en ander in overeenstemming is met de Wpg. Verwerken van gevoelige gegevens (behoudens het ras-gegeven ter identificatie) komt in principe niet voor aangezien er geen reden voor te bedenken is. Een gevoelig gegeven met de onvermijdelijkheid wordt in een mutatie vermeld, nooit in een aparte registratie.
5	Rechtmatigheid van de verkrijging komt aan de orde in het Handboek RID tabblad 2.5.2, waarin onder meer is opgenomen dat de informant, zonder toestemming van het bevoegd gezag geen strafbare feiten mag plegen. Alle verkregen gegevens worden door de teamchef getoetst op rechtmatigheid. In werkoverleg wordt aandacht aan dit onderwerp besteed. Steeds worden de vragen gesteld aangaande de rechtmatigheid van: 'Kan het', 'Mag het' en 'Is het noodzakelijk'. De teamchef gaat uit van zelfredzaamheid van de teamleden, het onderwerp komt ook met regelmaat aan de orde in de briefings, en er vindt af en toe extra controle door de teamchef plaats. Soms wordt de informatie afkomstig van een informant zelfstandig gebruikt, maar doorgaans wordt de informatie eerst veredeld voordat er iets mee gedaan wordt.
6	Het toereikend, terzake dienend en niet bovenmatig zijn van politiegegevens komt aan de orde in Handboek RID tabblad 0.0, 2.7 en 2.5.1 (ethische code RID). Alleen relevante zaken worden verwerkt, conform de werkinstructies. Er vindt steeds een afweging plaats. Het doel waarvoor en waarom de gegevens vastgelegd moeten worden, moet steeds duidelijk zijn. Het doel is om in de eerste regel van de mutatie de doelbinding en noodzakelijkheid te vermelden. Die regel komt terug bij opmaak van elke mutatie. Wanneer er gesproken wordt over een brondocument wordt ermee bedoeld het hoofddocument als start waaronder alle mutaties gehangen worden. Voor alle personen is zodoende een startdocument aanwezig met de reden waarom die persoon vermeld wordt in het systeem, ook met het oog op de bewaartermijnen.
7	Het voor een ander doel verwerken als de WPG daar uitdrukkelijk in voorziet komt aan de orde in Handboek RID tabblad 2.6.1.
8	Het vermelden van de herkomst en wijze van verkrijging komt aan de orde in Handboek RID tabblad 0.0, 2.7 en 2.5.1 (ethische code RID). Hierin is ook de controle door de teamchef benoemd. Voorhanden is ook de procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence, voor de RID. Alle bronnen liggen vast. Enerzijds zijn dat de informanten met de daaruit voortvloeiende rapporten die een afzonderlijk traject hebben (RIDS) en vervolgens de bronvermelding binnen de BVO. De bron waaruit de informatie is ontsproten is herleidbaar en ligt vast. Er vindt steeds een controleslag plaats aan de hand van de gegevens en er wordt nagevraagd bij andere bronnen. De controle is vooral gericht en georganiseerd aan de voorkant. Hierop wordt door de teamchef toegezien.

ID	Aanbevelingen
	Geen.

1.6.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig	X			
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn	X			
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies en onrechtmatige verwerking	X			
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG		X		X
5	Toegang voor CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens		X		X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt	-			

ID	Bevindingen
1	In Handboek RID, tabblad 2.1 (proceshandboek RID BVO) wordt in meerdere processtappen gewezen op de juiste en complete invoer van gegevens. Alle medewerkers zijn doordrongen van kwaliteitsbesef. Er zijn werkafspraken in de vorm van het Handboek RID/instructies in de vorm van BVO mutaties. Voordat politiegegevens worden ingevoerd worden deze gecontroleerd aan de hand van andere bestanden zoals GBA en RDW. De applicatie BVO is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. De applicatie is voorzien van bedoelde functionaliteit. Functionarissen die politiegegevens verwerken m.b.v. BVO zijn hiervoor opgeleid. Het systeem sluit niet aan op de bestaande, specialistische werkzaamheden / registraties / vastleggingen van de RID. Ook om aan landelijke verplichtingen te voldoen, wordt gebruik gemaakt van andere systemen die door de RID worden gevoed en die elders worden beheerd.
2	Het verbeteren, vernietigen of aangevullen van politiegegevens komt aan de orde in Handboek RID, tapbladen 2.6.1 en 2.7. In de alledaagse praktijk komt dit zelden voor. Er zijn meerdere controlemomenten. Bovendien weten alle medewerkers dat zij accuraat moeten werken aangezien daar veel van kan afhangen. Als een onvolkomenheid blijkt, wordt deze verbeterd en/of rechtgezet. Bij nieuwe informatie vindt eerst een check plaats. Dan volgt nog veredeling. Dan controle van de veredeling en dan pas de invoer in het systeem. Deze zaken worden door de medewerkers zelf uitgevoerd. Dit is een doorlopend proces en is geheel aan de voorkant van de processen georganiseerd. [redacted] Zoals eerder verwoord wordt de kwaliteit zo goed als mogelijk geborgd door een gegevenscontrole bij invoer in de systemen.
3	[redacted]

IV

V

ID	Bevindingen
	De maatregelen/procedures/afspraken zijn vastgelegd. De ruimte waar RID werkt maakt onderdeel uit van het politiebureau te Middelburg. In de dienstauto's gebruikt men soms C2000 met een afgesloten bank, voor de rest geen verbindingsmiddelen behalve de diensttelefoon voor een aantal medewerkers. Men werkt op een gesloten netwerk zoals hiervoor omschreven. Daartoe hebben de medewerkers van de RID toegang middels een user-id en een wachtwoord. Na kantoortijden wordt de harddisk opgeborgen in de kluis. [redacted]
4	Een procesbeschrijving inzake de toegang tot de politiegegevens ten behoeve van het toezicht door de verantwoordelijke op de naleving van het bij of krachtens de WPG bepaalde is niet aanwezig. De toezichthouder is deels afhankelijk van wat de teamchef RID hem verstrekt.
5	Een procesbeschrijving inzake de toegang tot politiegegevens voor degene die met de controle en het toezicht op de WPG zijn belast, zijnde de interne auditor, de auditor, de privacyfunctionaris, het CBP en de functionaris gegevensbescherming, alsmede degenen die in opdracht van de verantwoordelijke technische werkzaamheden verrichten is niet aanwezig bij Politie Zeeland. De toezichthouders zijn deels afhankelijk van wat de teamchef RID hen verstrekt.
6	Een Bewerkerovereenkomst is niet relevant voor de RID.

ID	Aanbevelingen
4-5	Regel de toegang van de toezichthouders tot politiegegevens als bedoeld in artikel 4, lid 4 en 5, WPG in een procesbeschrijving.

1.6.3 Autorisaties (protocolplicht)

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid	X			
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd	X			
3	Voldoen aan specifieke regels voor het autoriseren van avps bij de RID, medewerkers Infodesk en misdaadanalisten	X			
4	Aanwijzing categorieën van ambtenaren voor de autorisaties in overeenstemming met de OvJ	-			
5	Voldoen aan specifieke regels voor kennis en vaardigheden voor avps die de politiegegevens verwerken	X			

ID	Bevindingen
1	De politie Zeeland beschikt over een Besluit Autorisatieprocedure met standaard autorisatieformulieren, alsmede een document Autorisatiebeleid Zuid-Nederland met bijlage Procesbeschrijving en autorisatieprofielen. De documenten zijn raadpleegbaar op het DELTANET, dat voor iedere gebruiker toegankelijk is. Binnen de door de informatiebeveiligingsfunctionaris uitgevoerde steekproef werden bij de RID geen onregelmatigheden geconstateerd. [redacted]
2	De autorisatieprocedure zoals vastgesteld in Zeeland wordt gehanteerd, maar door het geringe verloop in de weinige RID functionarissen levert autorisatieverlening en - intrekking geen problemen op. De toegekende actuele autorisaties zijn legitiem.
3	Autorisatie komt ook aan de orde in Handboek RID, tabblad 2.1 (autorisatie medewerkers in RID registraties). Alle medewerkers binnen de RID hebben een relatief uitgebreid pakket aan autorisaties voor veel systemen en applicaties. Autorisaties worden aangevraagd via een formulier en worden ook ingetrokken. Die acties worden alle gedaan door de teamchef. Het personeelsverloop binnen de afdeling is niet groot en daarom komt intrekken van autorisaties dan ook niet zo vaak voor. Er wordt nauwgezet op toegezien door de teamchef dat autorisaties worden ingetrokken.
4	Dit onderwerp is niet van toepassing ingevolge art. 2:6 BPG.
5	[redacted]

ID	Aanbevelingen
	Geen.

1.6.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens gv met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			X
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	X			
2	Voor gv de avps autoriseren van de RID	X			
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd RID	X			
3	Avps die gv beschikken over de wettelijk vereiste kennis en vaardigheden	X			
4	Indien bij gv gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	X			
5	Indien noodzakelijk voor goede gv worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	X			
6	Vzv noodzakelijk voor het onderzoek politiegegevens gv met andere gegevens dan politiegegevens	X			
7	Voldoen aan protocolplicht gv met andere gegevens	X			
8	Voldoen aan protocolplicht gv met andere gegevens tijdens de bewaartermijn van 5 jaar	X			

ID	Bevindingen
1-8	Geautomatiseerd vergelijken is verwoord in Handboek RID, tapbladen 0.0 (Procesmodel en - beschrijving veiligheidsinformatie genereren) en 2.1 (Proceshandboek BVO, RID) en de landelijke procesbeschrijving Update procesmodel en -beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence, voor de RID. D.m.v. de BVO superregistratie hebben RID medewerkers de mogelijkheid om alle inhoudelijke informatie (m.u.v. bepaalde CIE gegevens) van andere BVO registraties in de gehele Zuid-6 te bezien. Deze mogelijkheid heeft de BVO applicatie, gecombineerd met de toegekende BVO superregistratie, in zich. Permanent is de noodzaak hiertoe aanwezig om een goede informatiepositie op te bouwen. In de BVO registraties worden artikel 9 en artikel 10 gegevens opgeslagen. Aangezien artikel 8 gegevens voornamelijk m.b.v. de BVH applicatie worden verwerkt en niet gekoppeld is aan de BVO en/of BVO superregistratie, heeft 1 RID medewerkster (bewerkster) een BlueView autorisatie. Hiermee heeft zij de mogelijkheid om RID objecten en subjecten landelijk te bevragen in de BVH. Indien daadwerkelijk overeenkomende gegevens in een BVO registratie worden aangetroffen, wordt contact gezocht met de betrokken bevoegde functionaris om diens toestemming te vragen voor het ter beschikking stellen van diens informatie aan de RID taak. Handelingen in BVO worden structureel in de applicatie gelogd. Informatie verkregen m.b.v. BlueView betreft artikel 8 informatie waarvoor geen toestemming van een bevoegd functionaris noodzakelijk is. Handelingen in Blueview worden structureel in de applicatie gelogd. De bewaartermijn van alle loggingen is onbekend. Zie voor wat betreft deze loggingen de bevindingen bij de CIE in par. 1.5.4. Bovenstaande handelingen worden echter niet geprotocolleerd op de manier waarop het BPG op doelt. Een uitzondering hierop zijn de gevallen waarin gerelateerde gegevens werden aangetroffen en verkregen. De herkomst en wijze van verkrijging van de gerelateerde gegevens worden dan wel vermeld. [redacted] Bij afwezigheid van RID bewerkster worden bovenstaande handelingen verricht door een medewerker Infodesk. Er is een analist vrijgemaakt die de RID parttime ondersteunt. Dit is onvoldoende, omdat de capaciteit ontbreekt om op alle onderwerpen analyses uit te voeren. Alle medewerkers van de RID en de medewerkers die ten behoeve van de RID bevragings- en analysewerkzaamheden verrichten beschikken over de benodigde opleidingen en ervaring. In dat verband wordt ook verwezen naar par. 1.6.3.5 en par. 1.5.4. [redacted] Altijd wordt bij gebruik van informatie vooraf de toestemming van een betrokken bevoegde functionaris gevraagd. In die zin zijn er geen indicaties dat er bij de politie Zeeland niet zorgvuldig zou worden gehandeld.

ID	Aanbevelingen
1-8	Breng het vraagstuk van het geautomatiseerd vergelijken op landelijk niveau onder de aandacht van de wetgever. Neem naar aanleiding van de uitkomst van deze actie waar nodig beheersmaatregelen.

1.6.5 In combinatie met elkaar verwerken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens icmev met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			
1	Gerelateerde gegevens na instemming bevoegde functionaris verder verwerken voor dat onderzoek	-			
2	Voor icmev de avps autoriseren van de RID	-			
2	In voorkomende gevallen tevens avps Regionale Infodesk autoriseren i.o.m. hoofd RID	-			
3	Avps die icmev beschikken over de wettelijk vereiste kennis en vaardigheden	-			
4	Indien bij icmev gegevens overeenkomen worden de verbanden op de voorgeschreven wijze zichtbaar gemaakt	-			
5	Indien noodzakelijk voor goede icmev worden politiegegevens door leider onderzoek of plaatsvervanger gecodeerd	-			
6	Voldoen aan protocolplicht icmev met andere gegevens	-			
7	Voldoen aan protocolplicht icmev met andere gegevens tijdens de bewaartermijn van 5 jaar	-			

ID	Bevindingen
1-7	In combinatie met elkaar verwerken komt ondermeer aan de orde in de landelijke procesbeschrijving Update procesmodel en - beschrijving 'Veiligheidsinformatie genereren', Programma Intelligence, voor de RID, die in het Handboek RID is opgenomen. Zie verder de bevindingen in de hiervoorgaande paragraaf geautomatiseerd vergelijken. In combinatie verwerken is bij de RID Zeeland niet aan de orde.

ID	Aanbevelingen
1	Geen.

1.6.6 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Politie gegevens elk half jaar op noodzaak controleren en uiterlijk 5 jaar na datum laatste verwerking verwijderen		X		X
2	Na verwijdering maximaal 5 jaar bewaren en gebruiken voor afhandeling klachten en verantwoording van verrichtingen		X		X
2	Verwijderde gegevens na afloop van de bewaartermijn vernietigen	X			
3	Verwijderde gegevens tijdens bewaartermijn niet verstrekken aan personen/ instanties in 16 t/m 20, 23 en 24 WPG	X			
4	Uitsluitend in bijzondere gevallen tijdens bewaartermijn in opdracht bevoegd gezag tbv hernieuwde 9 of 10 verwerking	X			
5	Voldoen aan de regels schriftelijke vastlegging vernieuwde verwerking en ter beschikking stelling verdere verwerking	X			
6	Afzien van vernietiging ingeval waarde voor cultureel erfgoed of historisch onderzoek conform regels Archiefwet		X		X

ID	Bevindingen
1-2	Verwijderen, bewaartermijnen en vernietiging van politiegegevens komen aan de orde in Handboek RID, tabblad 2.7.8 (Verwijderen, vernietigen gegevens). Afhankelijk van de mogelijkheden van de functionaliteit wordt de verwijdering automatisch of handmatig door de functioneel beheerder BVO uitgevoerd in opdracht van de teamchef RID. Het informatiesysteem BVO bevat echter geen adequate functionaliteiten voor het ondersteunen van dit proces. [redacted] Ondanks het feit dat de halfjaarlijkse controle i.v.m. het ontberen van een gegevensbeheerder niet structureel plaatsvindt, wordt dit gecompenseerd doordat bij aanvullende invoer van subjectgegevens, bezien wordt of de reeds aanwezige informatie al verwijderd had moeten zijn.
3	Het verbod om verwijderde gegevens niet aan de personen en instanties genoemd in artikelen 16 t/m 20, 23 en 24 WPG te verstrekken is niet aanwezig. Het wettelijk verstrekkingregime wordt gevolgd. Verstrekking in de genoemde gevallen is in de praktijk nog niet voorgekomen.
4-5	De regels voor het ter beschikking stellen tijdens de bewaartermijn komt aan de orde in Handboek RID, tabblad 2.7.8 (Verwijderen, vernietigen gegevens). Ter beschikking stelling in dat kader is in de praktijk nog niet voorgekomen.
6	Een procesbeschrijving inzake de toepasselijkheid van de archiefwet is niet geregeld in het handboek RID. Bij gelegenheid wordt het wettelijke regime gevolgd. Uit verkregen informatie van de teamchef RID blijkt dat verwijderde artikel 10 lid 1, onder c, gegevens, vallend onder de werking van een artikel 14 WPG verwerking, fysiek niet worden gearchiveerd bij Post & Archiefzaken van politie Zeeland. Volgens de teamchef RID beschikt zijn afdeling wel over artikel 14 gegevens, maar worden deze gegevens niet bij PAZ gearchiveerd. Dit omdat de vernietigingstermijn nog niet is bereikt en daarnaast omdat deze Post & Archiefmedewerkers dan toegang zouden krijgen tot RID gegevens. De te beantwoorden vraag is nu wie de "beheerder" wordt of moet zijn van deze verwijderde RID informatie. Het beheer beleggen bij de RID betekent dat een RID medewerker, in strijd met artikel 14 WPG onvermijdelijk een soort van "operationele" toegang tot verwijderde gegevens verkrijgt. Hiervoor zullen compenserende maatregelen moeten worden genomen.

ID	Aanbevelingen
1	Continueer de compenserende maatregelen voor politiegegevens in de bewaarfase.
2	Implementeer zo spoedig mogelijk de voorziening voor het geautomatiseerd schonen indien deze door de vtsPN wordt uitgeleverd.
6	Zorg voor een voorziening om aan de Archiefwet te voldoen.

1.6.7 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie indien nodig voor hun taakuitoefening	X			
2	Politiegegevens tbs aan art. 8, 9, 10,12 na instemming bevoegde functionaris	X			
3	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 1, genoemde ondersteunende taken		X		X
4	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 2, genoemde ondersteunende taken		X		X
5	Tbs van politiegegevens ten behoeve van de in artikel 13, lid 3, genoemde ondersteunende taken		X		X
6	Tbs van politiegegevens uitsluitend weigeren of beperken in de wettelijk toegestane gevallen	X			
7	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld	X			

ID	Bevindingen
1-7	Ter beschikking stelling van politiegegevens komt aan de orde in Handboek RID, tabblad 2.8 en 2.8.2 (verstrekken en ter beschikking stellen informatie.) Door RID worden regelmatig politiegegevens terbeschikking gesteld aan onder andere RID-en in den lande (ongeveer 60 à 70 maal per jaar). Openbare orde informatie wordt ook d.m.v. een verstrekkingenrapport openbare orde of proces-verbaal ter beschikking gesteld aan de politietaak via de Regionale Informatie Organisatie (RIO) en/of korpsleiding. Ook wordt via de RIK/DIK openbare orde informatie verder verwerkt als een artikel 13 verwerking (IPOL). De teamchef RID wordt in het ter beschikking stellen altijd als bevoegd functionaris betrokken. Alle ter beschikking stellingen zijn geprotocolleerd in de vorm van een verstrekkingenrapport. In enkele gevallen komt het voor dat van zogenaamde "strafrechtelijke bijvangst", niet de core-business van de RID, door het hoofd van de RID een proces-verbaal wordt opgemaakt dat in overleg met het OM ter beschikking wordt gesteld, aan een rechercheonderdeel binnen de politie, of aan het OM zelf. Meestal betreft het dan de informatie aan de (RCIE) officier van justitie met wie overleg plaatsvindt. Het komt niet voor dat aan artikel 13, lid 1, verwerkingen (HKS/FCM) politiegegevens ter beschikking worden gesteld. Incidenteel is het voorgekomen dat aan een artikel 13, lid 2, verwerking is ter beschikking gesteld. De RID krijgt momenteel geen MRO en

ID	Bevindingen
	VROS hits op basis van hit-no-hit. De applicatie (BVO) is voorzien van een functionaliteit, waarmee politiegegevens ter beschikking kunnen worden gesteld aan de genoemde verwerkingen. De RID denkt momenteel na over het eventuele ter beschikking stellen van politiegegevens aan de VROS verwerking. Procesbeschrijvingen aangaande ter beschikking stelling aan de artikel 13 verwerkingen zijn niet aanwezig in het Handboek RID. Aan de wettelijke beperkingen en weigeringsgronden is aandacht besteed in Handboek RID, tabblad 2.8.1. De daarin vermelde evaluatiecodes zijn van invloed op het wel of niet ter beschikking stellen. Voor wat betreft de geheimhoudingsverplichting leggen ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
3-5	Neem een procesbeschrijving op in het Handboek RID voor het ter beschikking stellen aan artikel 13 verwerkingen.

1.6.8 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG	X			
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen	X			
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MIVD)	X			
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden	X			

ID	Bevindingen
1-4	Verstrekkingen komen aan de orde in het handboek RID, tabblad 5.0 waarin ook wordt verwezen naar de verstrekkingenwijzer. De verstrekkingenwijzer is bij de medewerkers van de RID bekend. Er wordt goed gekeken/gewogen wat wel en niet verstrekt mag/kan worden. Eventueel is er overleg met de PF-er. Er wordt altijd een rapport verstrekkingen opgemaakt. Volgens de teamchef worden politiegegevens aan de AIVD verstrekt op grond van art. 62 WIV. [redacted] Uit de openbare orde registratie (art. 10 lid 1 onder c WPG) worden, m.u.v. verstrekkingen aan burgemeester, geen verstrekkingen gedaan. Dit betekent dat er geen politiegegevens buiten het politiedomein worden gebracht. Conform art. 4:3 lid 1, onder i, BPG worden politiegegevens uit de openbare orde registratie verstrekt t.b.v. Koninklijke onderscheidingen. Deze verstrekkingen worden vastgelegd in Corsa. Tot op heden is er geen RID informatie verstrekt op grond van artikel 19 WPG en artikel 20 WPG. Voor eventuele verstrekkingen in de toekomst op grond van artikel 4:5 BPG zal in het Handboek RID Zeeland een passage worden opgenomen om geheimhouding te waarborgen (opnemen van zinsnede m.b.t. geheimhouding in het RID Proces Verbaal.

ID	Aanbevelingen
	Geen.

1.7 Artikel 12 Informanten CIE

1.7.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht met verwerkingen van politiegegevens met het oog op het verwerken van informantgegevens	X			
2	Politiegegevens worden conform de wettelijk bepaalde categorieën van personen verwerkt	X			
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens	X			
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen	X			
6	Politiegegevens zijn toereikend, ter zake dienend en niet bovenmatig	X			
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet	X			
8	De herkomst en de wijze van verkrijging van politiegegevens wordt vermeld	X			

ID	Bevindingen
1	Overzicht met verwerkingen van politiegegevens met het oog op het verwerken van informantgegevens is aanwezig bij de CIE.
2	[redacted]. De CIE verwerkt politie gegevens conform de wettelijke bepaalde categorieën van personen.
3	Niet van toepassing bij CIE.
4	[redacted] Uit de interviews blijkt dat de controle op de onvermijdelijkheid van gevoelige gegevens conform artikel 5 WPG wordt uitgevoerd [redacted]
5	[redacted] Uit de interviews blijkt, dat aan de rechtmatigheid van de verkrijging van informatie van informanten in de praktijk doorlopend en intensief aandacht wordt besteed [redacted]
6	[redacted] verwerkingsproces wordt nauwgezet door zowel de leidinggevenden als de CIE-OvJ gecontroleerd. Door hen wordt doorlopend op de kwaliteit van de politiegegevens gestuurd. Dit is bijvoorbeeld aan de orde bij het opmaken van de zogenaamde "bruto-verslagen" en het vervolgens overbrengen van de "netto-informatie" naar de "netto-verslagen" in BVO.
7	[redacted] Uit de interviews blijkt dat de teamchef en diens vervanger strikt op de naleving van deze verplichting toezien. [redacted]
8	[redacted] De BVO bevat ter ondersteuning van dit verwerkingsproces specifieke velden. De BVO biedt ook de functionaliteit om kenmerken aan een mutatie te koppelen. Indien dit relevant en mogelijk is, wordt deze functie gebruikt. Als deze functionaliteit in een voorkomend geval te weinig mogelijkheden biedt, wordt een en ander verwoord in de vrije tekstvelden.

ID	Aanbevelingen
	Geen.

1.7.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig	X			
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn	X			
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies of onrechtmatige verwerking	X			
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG		X		X
5	Toegang voor het CBP, de (interne) auditor, de auditor, de privacyfunctionaris en technische medewerkers		X		X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt		X		X

ID	Bevindingen
1	[redacted] .De applicatie is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. De CIE leiding ziet er op toe dat de runners met het juiste referentiemateriaal en conform de beleidsafspraken informanten runnen. [redacted]

ID	Bevindingen
	[redacted]
2	[redacted]
3	[redacted] M.i.v. 1 januari 2011 werkt CIE Zeeland v.w.b. de opslag van bruto informatie in een landelijke, eenduidige rode BVO omgeving. [redacted] Het beheer ervan is uitbesteed. De teamchef heeft momenteel geen SLA en/of bewerkerovereenkomst o.i.d. maar kan deze wel verkrijgen. [redacted] implementatie landelijk is afgerond en alle regio's zijn overgestapt naar deze omgeving, zal hier een audit op worden uitgevoerd. Er is vertrouwen dat v.w.b. de bruto informatie de toegang/beveiliging, etc. landelijk goed geregeld is. [redacted] Voor de persoonsidentificerende gegevens wordt gebruik gemaakt van een zgn. kluisapplicatie, [redacted]
4	[redacted] Toezichthouders hebben geen toegang tot bruto informatie. Het argument is het afschermen van de identiteit van de informant. Formeel is dit niet geregeld, maar de teamchef CIE heeft hier geen problemen mee. Wel heeft de teamchef CIE problemen met eventuele toegang van toezichthouders tot de brutogespreksverslagen in de rode BVO omgeving. Dit omdat toezichthouders niet tot de CIE-eenheid behoren en de CIE status niet hebben. Bronbescherming is het argument voor terughoudendheid op dit gebied. Verder is de CIE zo transparant mogelijk. Een ander argument is dat men inhoudelijk kennis moet hebben van de CIE-werkwijze om het toezicht juist uit te kunnen oefenen. [redacted] De controle op de artikel 12 informatie (informantenbestand) wordt tweemaal per jaar uitgevoerd door de CIE-OvJ.
5	Toegang in de vorm van autorisaties voor toezichthouders is niet gerealiseerd. De toezichthouder (PF) is afhankelijk van de informatie aangeleverd door de teamchef CIE. Teamchef CIE constateert dat de in de SLA gemaakte afspraken door vtsPN niet altijd worden opgevolgd. Het is in het verleden voorgekomen dat de vtsPN medewerkers stuurt t.b.v. systeemonderhoud zonder dat deze aan de screeningseisen voldoen. Dit is inmiddels besproken met belanghebbenden en komt sindsdien niet meer voor.
6	Met uitzondering van de relatief nieuwe ontwikkeling van centrale opslag in de BVO-rood omgeving, zoals eerder verwoord, maakt de CIE geen gebruik van bewerkers. Een bewerkerovereenkomst voor BVO-Rood is niet onderzocht.

ID	Aanbevelingen
4-5	Regel de toegang van de toezichthouders tot politiegegevens als bedoeld in artikel 4, lid 4 en 5, WPG in een procesbeschrijving.
6	Laat naar een aanvullende privacy audit uitvoeren naar de bewerkerovereenkomst / SLA voor BVO-Rood.

1.7.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid	X			
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd	X			
3	Voldoen aan specifieke regels autoriseren van avps bij de CIE voor het verwerken van informantgegevens	X			
4	Uitsluitend het hoofd CIE of RID of plaatsvervangers autoriseren voor verwerken identificerende gegevens informant	X			
5	Aanwijzing van de categorieën van ambtenaren voor de autorisaties in overeenstemming met de OvJ	X			
6	Voldoen aan specifieke regels voor kennis en vaardigheden voor avps die de politiegegevens verwerken	X			

ID	Bevindingen
1	[redacted] Een autorisatiebeheerssysteem waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld is aanwezig. Procesbeschrijving en het autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties. De procesbeschrijving is in bewerking bij de IBF.
2	Een Procesbeschrijving inzake door de verantwoordelijke te autoriseren ambtenaren van politie is aanwezig. Uit de interviews blijkt dat de gespreksverslagen in BVO-Bruto worden verwerkt. BVO-bruto staat in een Hoog Beveiligd Rekencentrum (BVO-rood). Alleen de daarvoor geautoriseerden kunnen verzoeken indienen tot autorisatie van bepaalde gebruikers. Alleen het hoofd CIE kan medewerkers voor de artikel 12 verwerkingen autoriseren. [redacted]

ID	Bevindingen
3	De CIE volgt artikel 6 van de WPG en heeft buiten de hierboven genoemde procesbeschrijving geen aanvullende regelgeving in de vorm van specifieke procesbeschrijvingen. Alle CIE-medewerkers zijn geautoriseerd voor toegang tot artikel 12 informatie in de BVO-rood. [redacted] De deelwaarneming bestond uit het observeren van de volledige inlogprocedure en onderzoeken van de autorisatieformulieren. De deelwaarneming gaf geen aanleiding tot op of aanmerkingen.
4	De CIE volgt artikel 6 van de WPG en heeft geen aanvullende regelgeving in de vorm van procesbeschrijvingen. De applicatie kent momenteel niet de mogelijkheid om onderscheid te maken in autorisatieniveau 's en / of menu 's. [redacted]
5	De CIE-OvJ kent de categorieën van ambtenaren die geautoriseerd zijn.
6	De runners hebben de verplichte CIE cursus gevolgd en zijn hierdoor gecertificeerd. Er is sprake van een leer- en ontwikkeltraject voor nieuwe medewerkers. De overige functionarissen (niet zijnde runners) zijn intern / extern opgeleid / geïnstrueerd.

ID	Aanbevelingen
	Geen.

1.7.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens gv met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			X
1	Gerelateerde gegevens verder verwerken voor dat onderzoek	X			
2	Voor gv de avps autoriseren van de CIE	X			
3	Avps en art. 141 opsporingsambtenaren dienen te beschikken over de wettelijk vereiste kennis en vaardigheden	X			

ID	Bevindingen
1-3	[redacted]

ID	Aanbevelingen
1	Bewerkstellig een landelijk eenduidige interpretatie van de reikwijdte van het begrip "geautomatiseerd vergelijken" en stel indien noodzakelijk, aan de hand hiervan een aanvullende procedurebeschrijving op.

1.7.5 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Informantgegevens elk half jaar op noodzaak controleren en uiterlijk 10 jaar na datum laatste verwerking vernietigen	X			

ID	Bevindingen
1	[redacted]

ID	Aanbevelingen
	Geen.

1.7.6 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs gedurende max. 4 mnd. na datum eerste verwerking voor verdere verwerking ogv art. 8, 9 of 10	X			
2	Voldoen aan de uitzonderingsregels op de tbs	X			
3	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld	X			

ID	Bevindingen
1	[redacted] De vertaling van bruto naar netto gegevens duurt bij CIE Zeeland veel korter dan de wettelijke viermaanden termijn. [redacted] De teamchef CIE en/of coördinator controleert in alle gevallen de bruto verslagen voordat deze netto worden gemaakt. [redacted] Hierdoor wordt voorkomen dat de netto-verslagen op meerdere wijze interpretabel zijn. [redacted] Zwacri informatie, operationele informatie uit teams, de intelligence-agenda, de opsporingsbrief van het OM, de actualiteit en maatschappelijke impact zijn van invloed op het gebruikte referentiemateriaal.
2	[redacted]. Hier wordt de hand aan gehouden.
3	[redacted] In het opleidingsprogramma van de CIE wordt aandacht besteed aan de geheimhoudingsverplichting inzake het verwerken van politiegegevens. Bij indiensttreding leggen ambtenaren van de politie Zeeland en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren van de politie Zeeland en andere personen in hun werkomgeving wordt door leidinggevenden ook aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
	Geen.

1.8 Artikel 12 Informanten RID

1.8.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht met verwerkingen van politiegegevens met het oog op het verwerken van informantgegevens	X			
2	Politiegegevens worden conform de wettelijk bepaalde categorieën van personen verwerkt	X			
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens	X			
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen	X			
6	Politiegegevens zijn toereikend, ter zake dienend en niet bovenmatig	X			
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet	X			
8	De herkomst en de wijze van verkrijging van politiegegevens wordt vermeld	X			

ID	Bevindingen
1	Een overzicht met verwerkingen van politiegegevens met het oog op het verwerken van informantgegevens is bij de RID aanwezig. [redacted] Dit bevindt zich op een RID intern afgeschermd netwerk.
2	Dit onderwerp is verwoord in Handboek RID 2011, onder tabblad 5.0. Hierin wordt verwezen naar de omschrijving zoals vermeld in art. 12 WPG en de memorie van toelichting. Het Handboek RID is op 26 april 2011 geaccordeerd door de plaatsvervangend Korpschef, De teamchef RID stelt jaarlijks een inlichtingenbehoefte plan (jaarwerkplan) op waarin hij m.b.v. zijn vakkennis, lokale bekendheid en voorspelbare items, de aandachtsgebieden voor de openbare orde taak van de RID beschrijft. Dit jaarwerkplan wordt via de korpsleiding (KMT) ter instemming voorgelegd aan het Regionaal College. Na verkregen instemming/toestemming van het Regionaal College worden de RID runners geïnstrueerd om openbare orde informatie gerelateerd aan de bedoelde aandachtsgebieden te verkrijgen.
3	Gemeenschappelijke verwerkingen zijn niet van toepassing op de RID.
4	Gevoelige politiegegevens worden, conform artikel 5 WPG, slechts in aanvulling op andere politiegegevens verwerkt indien dit onvermijdelijk is. De onvermijdelijkheid wordt beargumenteerd vastgelegd bij de betreffende gevoelige gegevens. In de BVO "beheerbak" RID wordt in een werkinstructie voor de medewerkers verwoord dat de onvermijdelijkheid telkenmale beargumenteerd dient te worden bij de vastlegging. De werkinstructie wordt opgenomen in het Handboek RID 2011. De teamchef RID heeft m.b.t. het bovenstaande op eigen initiatief meerdere malen advies ingewonnen bij de PF voordat tot opslag van gevoelige gegevens werd overgegaan.
5	Rechtmatigheid komt aan de orde in het Handboek RID, tabblad 2.5.2, waarin is opgenomen dat de informant, zonder toestemming van het bevoegd gezag geen strafbare feiten mag plegen. Alle verkregen gegevens worden door de teamchef getoetst op rechtmatigheid. Voordat de RID een informant gaat runnen, vindt met de beoogd informant een intake gesprek plaats waarin de do's en dont's voor de informant ter sprake komen. De runners vragen de informanten naar de herkomst van de door hem/haar aangeleverde gegevens. Het komt is nog niet voorgekomen dat een informant onrechtmatig verkregen (verduisterde/gestolen) gegevens heeft aangeboden.
6	Dit onderwerp is verwoord in Handboek RID, tabblad 2.6.1. De RID bewerker controleert de door de runners ingevoerde gegevens (bruto gespreksverslagen), vult deze aan en corrigeert deze, waar nodig. Vervolgens worden de ingevoerde gegevens door de teamchef bekeken en waar nodig door hem of door een ander gecorrigeerd. De chef RID leest alle bruto gespreksverslagen en ondertekent een print van de bruto en de vanuit het bruto verslag gemaakte netto verslagen, waarna dit document in de fysieke map van de informant die de informatie heeft aangeleverd, wordt opgeslagen.
7	Dit onderwerp is verwoord in Handboek RID tabblad 2.6.1.
8	Dit onderwerp is verwoord in Handboek RID tabblad 0.0, 2.7 en 2.5.1 (ethische code RID). Uit het interview blijkt, dat de herkomst en wijze van verkrijging ook altijd conform de instructies wordt vastgelegd. De BVO bevat ter ondersteuning van dit verwerkingsproces specifieke velden. De BVO biedt ook de functionaliteit om kenmerken aan een mutatie te koppelen. Indien dit relevant en mogelijk is, wordt deze functie gebruikt. Als deze functionaliteit in een voorkomend geval te weinig mogelijkheden biedt, wordt een en ander verwoord in de vrije tekstvelden.

ID	Aanbevelingen
	Geen.

1.8.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig	X			
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn	X			
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies of onrechtmatige verwerking	X			
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG		X		X
5	Toegang voor het CBP, de (interne) auditor, de auditor, de privacyfunctionaris en technische medewerkers		X		X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt	X			

ID	Bevindingen
1	Dit onderwerp is verwoord in Handboek RID, tabblad 2.1 (proceshandboek RID BVO) waarin in meerdere processtappen wordt gewezen op de juiste en complete invoer van gegevens. De RIDS applicatie is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen.

ID	Bevindingen
	In de artikel 12 verwerking wordt gewerkt met zogenoemde VPP (=Voorziening Product en Processen) formulieren waarin stapsgewijs gegevens dienen te worden ingevoerd t.b.v. de juistheid en nauwkeurigheid. De BVO-Rood omgeving, die gebruikt wordt voor de opslag van de bruto-gespreksverslagen, is voorzien van een vastgestelde format. Hiermee wordt de juistheid en nauwkeurigheid bevorderd. Bij de invoer van gegevens worden deze, daar waar mogelijk, geverifieerd door de runner, hetgeen gecontroleerd wordt door de bewerker.
2	Dit onderwerp is verwoord in Handboek RID, tabblad 2.5.12. (vernietiging informantengegevens). De artikel 12 verwerking, zijnde het informantenbestand, wordt conform het Handboek RID beheerd. Bij het aantreden van de huidige RID teamchef, zijn in de loop der tijd alle toenmalige gesprekcontacten omgezet in de formele status van informant. [redacted] Zoals eerder verwoord wordt de kwaliteit zo goed als mogelijk geborgd door een gegevenscontrole bij invoer in de systemen.
3	[redacted] De daadwerkelijke toegang tot de politiegegevens opgeslagen in de applicaties zijn middels autorisaties en conform de BBNP bepalingen beveiligd. Bruto gespreksverslagen van informanten worden opgeslagen in de BVO-Rood en zijn slechts geautoriseerd voor RID medewerkers. De maatregelen/procedures/afspraken zijn vastgelegd. De ruimte waar RID werkt maakt onderdeel uit van het politiebureau te Middelburg. In de dienstauto's gebruikt men soms C2000 met een afgesloten bank, voor de rest geen verbindingsmiddelen behalve de diensttelefoon voor een aantal medewerkers. Men werkt op een gesloten netwerk zoals hiervoor omschreven. Daartoe hebben de medewerkers van de RID toegang middels een user-id en een wachtwoord. Na kantoortijden wordt de harddisk opgeborgen in de kluis. [redacted]
4	Dit onderwerp is niet in een procesbeschrijving geregeld.
5	De toegang wordt als volgt gerealiseerd. De toezichthouder (o.a. PF) is afhankelijk van de informatie verkregen van de teamchef RID, danwel in het bijzijn van de teamchef RID wordt inzage gegeven voor de toezichthouder. In het verleden had een toezichthouder, de FG, autorisatie voor de RID verwerking Openbare Orde. De toezichthouders zoals nu in de WPG genoemd, zijnde het CBP, de PF en de FG hebben momenteel geen toegang, in de vorm van autorisaties, tot de openbare orde verwerkingen van de RID.
6	Dit onderwerp is niet van toepassing.

ID	Aanbevelingen
4-5	Regel de toegang van de toezichthouders tot politiegegevens als bedoeld in artikel 4, lid 4 en 5, WPG in een procesbeschrijving.

1.8.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid	X			
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd	X			
3	Voldoen aan specifieke regels autoriseren van avps bij de CIE of RID voor het verwerken van informantgegevens	X			
4	Uitsluitend het hoofd RID of plaatsvervangers autoriseren voor verwerken identificerende gegevens informant	X			
5	Aanwijzing van de categorieën van ambtenaren voor de autorisaties in overeenstemming met de OvJ	-			
6	Voldoen aan specifieke regels voor kennis en vaardigheden voor avps die de politiegegevens verwerken	X			

ID	Bevindingen
1	Een procesbeschrijving inzake autorisaties is aanwezig op het DELTANET. Er is een autorisatiebeheerssysteem waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld. Procesbeschrijving en het autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties. De procesbeschrijving is in bewerking bij Politie Zeeland (informatie beveiligingsfunctionaris). In de door de informatiebeveiligingsfunctionaris uitgevoerde steekproef werden bij de RID geen onregelmatigheden geconstateerd.
2	Een procesbeschrijving inzake door de verantwoordelijke te autoriseren ambtenaren van politie is aanwezig. De autorisatieprocedure zoals vastgesteld in Zeeland wordt gehanteerd. Door het geringe verloop in het beperkt aantal RID functionarissen levert autorisatieverlening en -intrekking geen problemen op. De bestaande autorisaties zijn actueel en legitiem.
3	De RID volgt artikel 6 van de WPG. Binnen de BVO van de RID wordt conform het proceshandboek BVO RID gewerkt met de autorisaties die daarin zijn opgenomen.
4	De RID volgt artikel 6 van de WPG. Binnen de BVO van de RID wordt conform het proceshandboek BVO RID gewerkt met de autorisaties die daarin zijn opgenomen.
5	Dit onderwerp is niet van toepassing op de RID.
6	[redacted]

ID	Aanbevelingen
	Geen.

1.8.4 Geautomatiseerd vergelijken

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens gv met andere politiegegevens ogv art. 8, 9, 10 voor vast stellen verbanden tussen de gegevens	X			
1	Gerelateerde gegevens verder verwerken voor dat onderzoek	X			
2	Voor gv de avps autoriseren van de CIE of RID	X			
3	Avps en art. 141opsporingsambtenaren die gv beschikken over de wettelijk vereiste kennis en vaardigheden	X			

ID	Bevindingen
12	Dit onderwerp is verwoord in Handboek RID, tapbladen 0.0 (Procesmodel en - beschrijving veiligheidsinformatie genereren) en 2.1 (Proceshandboek BVO, RID). D.m.v. de BVO superregistratie hebben RID medewerkers de mogelijkheid om alle inhoudelijke informatie (m.u.v. bepaalde CIE gegevens) van andere BVO registraties in de gehele Zuid-6 te bezien. Deze mogelijkheid heeft de BVO applicatie, gecombineerd met de toegekende BVO superregistratie, in zich. De noodzaak tot deze handeling is structureel aanwezig om een goede informatiepositie op te bouwen. In de BVO registraties worden artikel 9 en artikel 10 gegevens opgeslagen. Aangezien artikel 8 gegevens voornamelijk m.b.v. de BVH applicatie worden verwerkt en niet gekoppeld zijn aan de BVO en/of BVO superregistratie, [redacted] Indien daadwerkelijk overeenkomende gegevens in een BVO registratie worden aangetroffen, wordt contact gezocht met de betrokken bevoegd functionaris om diens toestemming te vragen voor het ter beschikking stellen van diens informatie aan de RID taak. Handelingen in BVO worden structureel in de applicatie gelogd. Informatie verkregen m.b.v. BlueView betreft artikel 8 informatie waarvoor geen toestemming van een bevoegd functionaris noodzakelijk is. Handelingen in BlueView worden structureel in de applicatie gelogd. Bovenstaande handelingen worden echter niet geprotocolleerd. Een uitzondering hierop zijn de gevallen waarin gerelateerde gegevens werden aangetroffen en verkregen. De herkomst en wijze van verkrijging van de gerelateerde gegevens worden vermeld. Er is een analist vrijgemaakt die de RID parttime ondersteunt. Dit is onvoldoende, omdat de capaciteit ontbreekt om op alle onderwerpen analyses uit te voeren. [redacted] Zoals bij de artikel 10 verwerkingen aan de orde kwam, beschikken de betreffende medewerkers over de vereiste kennis en vaardigheden.

ID	Aanbevelingen
	Geen.

1.8.5 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Informantgegevens elk half jaar op noodzaak controleren en uiterlijk 10 jaar na datum laatste verwerking vernietigen	X			

ID	Bevindingen
1	Een procesbeschrijving inzake het controleren vernietigen van politiegegevens die zijn verwerkt voor de controle op en het beheer van een informant gegevens is vastgelegd in Handboek RID Zeeland, document 2.5.12. De teamchef heeft op eigen initiatief aan functioneel beheer BVO gevraagd om een lijst van subjecten in de RID BVO-registratie aan te leveren aan de hand waarvan geschoond kan worden daar waar mogelijk en noodzakelijk. De teamchef merkt op dat er nog geen sprake is van vernietiging van verwijderde gegevens, simpelweg omdat er bij de aanvang van zijn taak (2005) formeel geen sprake was van RID informanten, maar dat deze personen als gesprekscontacten werden geregistreerd. Inmiddels zijn alle informanten zoals is afgesproken aangemeld bij de NCIE als RID informant.

ID	Aanbevelingen
	Geen.

1.8.6 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs gedurende max. 4 mnd na datum eerste verwerking voor verdere verwerking ogv art. 8, 9 of 10	X			
2	Voldoen aan de uitzonderingsregels op de tbs	X			
3	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld	X			

ID	Bevindingen
1	Dit onderwerp is verwoord in Handboek RID, tabblad 2.8 en 2.8.2 (verstrekken en ter beschikking stellen informatie). De bruto informantengegevens (gespreksverslagen, artikel 12 WPG) worden zeer ruim binnen de maximale termijn van vier maanden omgezet naar nettogegevens (artikel 10). Meestentijds is dit uiterlijk binnen een week gerealiseerd. Overige, voor de algehele politietaak relevante informatie, in de vorm van"bijvangst", wordt verwerkt en daar waar mogelijk aan andere verwerkingen ter beschikking gesteld. Hierbij wordt "strafrechtelijke bijvangst" op grond van de landelijke "Handleiding Informatie Inwinning Openbare Orde", na afstemming met de CIE-OvJ, in de vorm van een proces-verbaal ter beschikking gesteld aan een tactisch team. Met de CIE-OvJ wordt afgestemd aangezien er geen RID-OvJ is. De RID werkt immers niet onder gezag van het Openbaar Ministerie maar onder gezag van de burgemeester, daar waar het gaat over de openbare orde. De teamchef stelt elk jaar een jaarverslag van de RID openbare orde activiteiten op hetgeen aan de burgemeesters wordt verstrekt.
2	Art. 2:13.1, onder a, BPG wordt gehanteerd in de vorm van de gebruikelijke coderingen.

ID	Bevindingen
3	Bij indiensttreding leggen ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
1	Geen.

1.9 Artikel 13 (Landelijke registers)

1.9.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht landelijke verwerkingen ter ondersteuning van de politietaak met hun specifieke doelstellingen				X
2	Schriftelijke vastlegging van wettelijk bepaalde gegevens en het voldoen aan de termijn voor de ter inzage legging				X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens				X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen				X
6	Politiegegevens zijn, toereikend, terzake dienend en niet bovenmatig				X
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet				X

ID	Bevindingen
1	Gedurende de looptijd van het landelijk project implementatie WPG (PIWPG) werd verzuimd om voor artikel 13 WPG verwerkingen, welke in elke politieregio voorkomen zoals HKS, FCM, HAVANK, PV's en rapporten, een eenduidige schriftelijke vastlegging conform artikel 13, lid 4, op te stellen. Dit werd mede veroorzaakt door het feit dat, ondanks inspanningen van het PIWPG om een totaaloverzicht te verkrijgen van alle verwerkingen die mogelijk in aanmerking komen voor een artikel. 13 regime, hiervan geen totaaloverzicht verkregen kon worden. Het opstellen van landelijke formats zou ten goede gekomen zijn aan de eenduidigheid bij de Nederlandse politie alsmede het voorkomen van het per regio opstellen van een schriftelijke vastlegging van overeenkomende soorten artikel 13 verwerkingen, met het risico van onderlinge verschillen. Landelijke formats hadden regiospecifiek gemaakt kunnen worden en ter inzage kunnen worden gelegd. Ook de nazorgfase van het PIWPG heeft geen eenduidige schriftelijke vastleggingen opgeleverd. Uiteindelijk heeft een initiatief van de verschillende privacyoverleggen, ingedeeld naar verzorgingsgebieden van de vtsPN, een beperkt aantal concepten van veel voorkomende artikel 13 verwerkingen opgeleverd. De hierna volgende onderwerpen zijn in de interne audit en de externe audit niet toereikend onderzocht. In de aanbevelingen komt om die reden tot uiting dat een aanvullende privacy audit zal moeten worden uitgevoerd. Een "Overzicht met verwerkingen van politiegegevens, waarin de verwerkingen ter ondersteuning van de politietaak met hun specifiek doelstellingen zijn opgenomen" is recentelijk bij de privacyfunctionaris aanwezig. Dit zijn de verwerkingen HKS, HAVANK, PV's en rapporten en) die onderkend zijn als artikel 13, lid 1, verwerking. FCM, infodesk/ makelfunctie infodesk, moeten nog ter inzage worden gelegd.
2	Een procesbeschrijving, waarin taken, bevoegdheden en verantwoordelijkheden t.b.v. het opstellen van schriftelijke vastleggingen worden belegd, is niet aanwezig.
3	Dit onderwerp is niet van toepassing.
4-7	Deze onderwerpen zijn niet onderzocht.

ID	Aanbevelingen
1-2	Completeer het overzicht van artikel 13 verwerkingen en leg de betreffende gegevens ter inzage.
4-7	Laat voor deze onderwerpen een aanvullende privacy audit uit voeren.

1.9.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig				X
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn				X
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies of onrechtmatige verwerking				X
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG				X
5	Toegang voor het CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens				X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt				X

ID	Bevindingen
1-2	HKS gegevens van politie Zeeland worden beheerd conform het landelijke afsprakenboek. FCM gegevens van politie Zeeland worden beheerd conform het landelijk model Beheerreglement FCM. Het beheer van eventuele andere artikel 13 verwerkingen in andere applicaties is onbekend. HKS en FCM medewerkers vallen formatief onder de RIO.
3	Dit onderwerp is niet onderzocht.
4	Een "Procesbeschrijving inzake de toegang tot de politiegegevens ten behoeve van het toezicht door de verantwoordelijke op de naleving van het bij of krachtens de Wpg bepaalde" is niet aanwezig. Er is geen toegang in de vorm van een autorisatie. Aangezien nog niet in alle gevallen duidelijk is wanneer sprake is van een 13 verwerking en de wel onderkende 13 verwerkingen in diverse applicaties worden opgeslagen, wordt in de praktijk toegang verkregen m.m.v. gebruikers/functioneel beheerders.
5-6	Deze onderwerpen zijn niet onderzocht.

ID	Aanbevelingen
1-6	Laat naar deze onderwerpen een vervolg privacy audit uitvoeren.

1.9.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid				X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd				X
3	Voldoen aan specifieke autorisatieregels voor avps die onder het beheer van de verantwoordelijke vallen				X
4	Specifieke autorisatieregels in bijzondere gevallen voor niet avps die onder het beheer van de verantwoordelijke vallen				X
5	Specifieke autorisatieregels in bijzondere gevallen voor avps die onder beheer van een andere verantwoordelijke vallen				X

ID	Bevindingen
1-5	Een procesbeschrijving inzake autorisaties is op het DELTANET aanwezig. Een autorisatiebeheerssysteem waarin specifieke rechten aan specifieke functies/rollen en specifieke taken zijn gekoppeld is aanwezig. De procesbeschrijving en het autorisatiebeheersysteem volgen de algemene uitgangspunten en regels in de Handreiking Autorisaties. De procesbeschrijving is in bewerking bij de Politie Zeeland (informatie beveiligingsfunctionaris). De autorisaties zijn v.w.b HKS gecheckt en op orde. Bij de andere artikel 13 verwerkingen is dit niet onderzocht. Een punt van aandacht is dat bij de afdeling Integriteit & Veiligheid (I & V) geen compleet overzicht is van alle autorisatieaanvragen. Daardoor ontstaat een incompleet beeld en de onbekende autorisatietoekenning valt dientengevolge buiten de toetsing door de medewerkers van deze afdeling. Toegang tot applicaties zoals VROS, RI- Online, FCM, Bom Data Systeem, worden gerealiseerd door andere medewerkers van politie Zeeland in afwijking van de reguliere autorisatieprocedure. Deze vorm van autoriseren is echter een landelijk fenomeen en vindt zijn oorzaak in de landelijke applicatieafspraken en werkwijzen.

ID	Aanbevelingen
1	Laat naar deze onderwerpen een aanvullende privacy audit uitvoeren.

1.9.4 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Tevoren schriftelijk vastleggen van termijn/gevallen voor beëindiging verwerking en de frequentie van de controle hierop				X

ID	Bevindingen
1	De schoning van het HKS had een achterstand van 4 jaar en zou op korte termijn worden ingelopen. Normaliter wordt er iedere maand geschoond. Dit onderwerp is verder niet onderzocht.

ID	Aanbevelingen
1	Laat naar deze onderwerpen een aanvullende privacy audit uitvoeren.

1.9.5 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie personen indien nodig voor hun taakuitoefening				X
2	Gegevens landelijk raadpleegbaar stellen / tbs aan door verantwoordelijken geautoriseerde personen tbv politietaak				X
3	Voldoen aan de uitzonderingsregels op de tbs				X
4	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld				X

ID	Bevindingen
1-4	Deze onderwerpen zijn niet onderzocht.

ID	Aanbevelingen
1-4	Laat naar deze onderwerpen een aanvullende privacy audit uitvoeren.

1.9.6 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG				X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen				X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MID)				X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden				X

ID	Bevindingen
1-4	Deze onderwerpen zijn niet onderzocht.

ID	Aanbevelingen
1-4	Laat naar deze onderwerpen een aanvullende privacy audit uitvoeren.

1.10 Artikel 13 (VROS-taak)

1.10.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen ondersteuning politietaak voor geautomatiseerde vergelijking meldingen jegens één persoon				X
2	Schriftelijke vastlegging van wettelijke genoemde gegevens en het voldoen aan de termijn voor de ter inzage legging				X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden	-			
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens				X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen				X
6	Politiegegevens zijn toereikend, terzake dienend en niet bovenmatig				X
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet				X

ID	Bevindingen
1	VROS = Verwijzing Recherche Onderzoeken en subjecten. Uit zowel de interne audit als de privacy audit is vanwege de beperkingen in de capaciteit en tijd niet duidelijk geworden of de politie Zeeland zelfstandig over een VROS-verwerking beschikt of dat er sprake is van een landelijke verwerking waarvoor de korpsbeheerder van de KLPD als verantwoordelijke moet worden aangemerkt. Op landelijk niveau is deze discussie voor zover bekend nog niet uitgekristalliseerd. In deze paragraaf en de navolgende paragrafen wordt volstaan met het vermelden van een beperkt aantal bevindingen uit de interne en de privacy audit. De onderwerpen zijn allen niet toereikend onderzocht. In de aanbevelingen komt om die reden tot uiting dat hier een aanvullende privacy audit zal moeten worden uitgevoerd. [redacted] Hij heeft in een eerder stadium het VROS beheerhandboek aan het auditteam ter beschikking gesteld. Dit betreft een versie uit 2002 waarop feitelijk geen wijzigingen meer zijn toegepast. VROS meldingen kunnen slechts worden gerealiseerd indien, in geval een onderzoek MRO waardig (MRO=melding Recherche Onderzoek) blijkt te zijn en in de bijbehorende BVO registratie een zogenoemde MRO mutatie wordt aangemaakt. Aan deze MRO mutatie worden subjecten en objecten gekoppeld welke een relevante rol spelen in het onderhavige onderzoek. Vervolgens worden wekelijks landelijk de MRO mutaties en de daaraan gekoppelde objecten/subjecten vergeleken. In geval van overeenkomsten wordt op basis van een hit/no-hit, automatisch in de betrokken BVO registraties een zogenoemde MRO melding gegenereerd. In deze MRO melding wordt het overeenkomende onderzoek alsmede de betrokken contactpersoon vermeld. Inhoudelijke informatie over de aangetroffen overeenkomst wordt niet vermeld. Deze MRO melding is voor alle geautoriseerden van de onderhavige BVO registratie leesbaar.
2	Een "Procesbeschrijving inzake de verplichte schriftelijke vastlegging van de wettelijke genoemde gegevens, de termijn voor de ter inzage legging" is niet aanwezig. Uit verkregen informatie van de functioneel beheerder BVO blijkt dat MRO meldingen tot zes maanden, na de dag waarop een zogenoemde eindmutatie in een BVO registratie wordt gemaakt, worden gegenereerd. Na deze zes maanden worden geen MRO meldingen m.b.t. objecten en subjecten, voorkomende in de onderhavige BVO registratie, meer gegenereerd.
3	Dit onderwerp is niet onderzocht.
4	Een "Procesbeschrijving inzake het verwerken van gevoelige gegevens" is niet aanwezig bij de politie Zeeland. Uit verkregen informatie van de functioneel beheerder BVO blijkt dat het wel mogelijk is om, aan een in de BVO registratie voorkomende persoon een gevoelig kenmerk te koppelen. Dit kenmerk is dan wel leesbaar indien binnen de bewuste BVO registratie deze persoon wordt geraadpleegd. Een kenmerk heeft echter geen invloed op of toegevoegde waarde voor MRO meldingen. In een MRO melding wordt slechts kenbaar gemaakt dat dezelfde persoon in een ander onderzoek voorkomt. Het eventuele gevoelige kenmerk van die persoon komt in die MRO melding niet voor.
5	Een "Procesbeschrijving inzake de rechtmatigheid van de verkrijging" is niet aanwezig bij Politie Zeeland. Zoals eerder onder de artikel 9 en 10 verwerkingen werd verwoord, zijn medewerkers doordrongen van deze rechtmatigheid. Aangezien artikel 9 en artikel 10 gegevens in de BVO applicatie worden verwerkt, impliceert rechtmatige verwerking van artikel 9 en artikel 10 gegevens ook rechtmatige verwerking van bijbehorende VROS gegevens.
6	Een "Procesbeschrijving inzake het toereikend, ter zake dienend en niet bovenmatig zijn van politiegegevens" is niet aanwezig bij de politie Zeeland. Hiervoor is hetgeen onder de artikel 9 en artikel 10 verwerkingen wordt verwoord, ook van toepassing op de artikel 13 verwerking VROS met dien verstande dat de functioneel beheerder BVO de indruk heeft dat inhoudelijk beheer van MRO mutaties te wensen overlaat. Indien een verdachte in een BVO registratie niet langer als zodanig wordt beschouwd, wordt deze persoon zeer waarschijnlijk niet losgekoppeld van de MRO mutatie.
7	Een "Procesbeschrijving inzake het voor een ander doel verwerken van politiegegevens dan waarvoor ze zijn verkregen" is niet aanwezig bij Politie Zeeland. VROS betreft het verder verwerken van artikel 9 en/of artikel 10 gegevens en wordt gerealiseerd door een MRO mutatie aan te maken conform de Werkinstructie MRO, d.d. 23 juli 2009, versie 1.6.

ID	Aanbevelingen
1-7	Laat een aanvullende privacy audit uitvoeren om helder te krijgen of de onderhavige verwerking een VROS-verwerking is als bedoeld in artikel 13 WPG waarvoor de korpsbeheerder van de politie Zeeland de verantwoordelijke is. Stem de uitkomsten af met de korpsbeheerder van de KLPD omdat er over de vraag wie de verantwoordelijke in casu is op landelijk niveau geen consensus bestaat. Neem in de aanvullende privacy audit ook mee, wat er nu precies aan MRO-instructies is en welke onderdelen uit de WPG hier in wel en niet toereikend zijn geregeld.

1.10.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig				X
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn				X

ID	Beheersdoelstellingen	V	D	N	A
3	Politiegegevens worden adequaat organisatorisch en technisch beveiligd tegen verlies				X
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG				X
5	Toegang voor het CBP, de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens				X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt				X

ID	Bevindingen
1	Een "Procesbeschrijving inzake het juist en nauwkeurig verwerken van politiegegevens" is niet aanwezig. De applicatie is voorzien van een functionaliteit waarmee de juistheid en nauwkeurigheid van de politiegegevens wordt bevorderd, zoals verplichte velden, invoercontroles, referentietabellen. MRO meldingen zijn niet (alle) actueel bij artikel 9 verwerkingen.
2	Een "Procesbeschrijving inzake het verbeteren, vernietigen of aanvullen van gegevens indien deze onjuist of onvolledig blijken te zijn" is niet aanwezig. MRO meldingen zijn niet (alle) actueel bij artikel 9 verwerkingen.
3	Het implementeren en onderhouden van een stelsel van maatregelen en procedures tegen verlies of enigerlei vorm van onrechtmatige verwerking is niet getoetst.
4	Een "Procesbeschrijving inzake de toegang tot de politiegegevens ten behoeve van het toezicht door de verantwoordelijke op de naleving van het bij of krachtens de WPG bepaalde" is niet aanwezig. Dit onderwerp is niet verder onderzocht.
5	Een "Procesbeschrijving inzake de toegang tot politiegegevens voor degene die met de controle en het toezicht op de WPG zijn belast, zijnde de interne auditor, de auditor, de PF, het CBP en de FG, alsmede degenen die in opdracht van de verantwoordelijke technische werkzaamheden verrichten" is niet aanwezig. Dit onderwerp is niet verder onderzocht.
6	Het relevant zijn van een bewerkerovereenkomst is niet onderzocht.

ID	Aanbevelingen
1-6	Laat een aanvullende privacy audit uitvoeren naar alle onderwerpen.

1.10.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid				X
2	Politiegegevens worden slechts verwerkt door avps die door de verantwoordelijke zijn geautoriseerd				X
3	Voldoen aan specifieke autorisatieregels voor avps die onder het beheer van de verantwoordelijke vallen				X
4	Specifieke autorisatieregels in bijzondere gevallen voor niet avps die onder beheer van de verantwoordelijke vallen				X
5	Specifieke autorisatieregels in bijzondere gevallen voor avps die onder beheer van een andere verantwoordelijke vallen				X
6	Specifieke autorisatieregels tbv de eenheid die met de uitvoering van deze taak is belast				X

ID	Bevindingen
1-6	Geautoriseerden voor een BVO registratie hebben toegang tot de MRO mutatie alsmede eventuele MRO meldingen. Er is geen specifieke eenheid die met de uitvoering van de VROS-taak is belast. Zie de bevindingen bij het onderwerp autorisaties bij de artikel 9 verwerkingen. Het onderdeel autorisaties is verder niet onderzocht.

ID	Aanbevelingen
1-6	Laat een aanvullende privacy audit uitvoeren naar het verstrekken en beheren van autorisaties van MRO-meldingen.

1.10.4 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Tevoren schriftelijk vastleggen van termijn/gevallen voor beëindiging verwerking en de frequentie van de controle Hierop.				X

ID	Bevindingen
1	Een Procesbeschrijving inzake het van te voren schriftelijk vastleggen (protocolplicht) van de termijn waarbinnen dan wel de gevallen waarin het verder verwerken van de betreffende gegevens wordt beëindigd en de frequentie waarmee de gegevens ter voldoening aan die verplichting worden gecontroleerd is niet aanwezig. De eindmutatie in BVO wordt niet altijd correct gebruikt. Het aanmaken van een eindmutatie MRO in een BVO registratie heeft tot gevolg dat MRO meldingen nog maximaal zes maanden worden gegenereerd. Daarna worden de aan de MRO mutatie gekoppelde objecten en subjecten niet meer vergeleken met andere BVO registraties.

ID	Aanbevelingen
1	Laat een aanvullende privacy audit naar dit onderwerp uitvoeren.

1.10.5 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens 8, 9, 10 verwerking tbs VROS-taak				X
2	Gerelateerde gegevens verder verwerken na instemming bevoegde functionaris				X
3	Voldoen aan de uitzonderingsregels op de tbs				X
4	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld				X

ID	Bevindingen
1	Een MRO melding genereert slechts een vermelding dat een overeenkomst met een andere BVO registratie werd gevonden m.b.t. een object of subject. Inhoudelijke informatie wordt niet ontsloten. Voor inhoudelijke informatie dient men daadwerkelijk contact op te nemen met de vermelde contactpersoon van de BVO registratie waarmee een overeenkomst werd vastgesteld.
2	In geval een MRO melding en aansluitend overleg tussen de betrokken contactpersonen (waardoor tevens de rol van de betrokken bevoegd functionarissen kan worden gerespecteerd) kan in de Zuid-6 d.m.v. "labelen" van de onderhavige mutatie(s) de vermelde politiegegevens ter beschikking worden gesteld. Buiten de Zuid-6 is deze vorm van labelen niet mogelijk en dient het ter beschikking stellen op een alternatieve wijze (Outlook, toezenden van pv's, etc.) gerealiseerd te worden. VROS betreft het ter beschikking stellen en verder verwerken van artikel 9 en/of 10 gegevens voor geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon en wordt gerealiseerd door een MRO mutatie aan te maken conform de Werkinstructie MRO, d.d. 23-juli 2009, versie 1.6.
3	Een "Procesbeschrijving inzake de gevallen waarin de ter beschikking stelling van politiegegevens kan worden geweigerd of aan beperkende voorwaarden kan worden onderworpen" is niet aanwezig.
4	Bij indiensttreding leggen ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
1-3	Laat een aanvullende privacy audit uitvoeren, mede met het oog op de relevantie van alle in deze paragraaf genoemde onderwerpen.

1.10.6 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG				X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen				X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MIVD)				X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden				X

ID	Bevindingen
1-4	Verstrekkingen (=het beschikbaar stellen van politiegegevens buiten het politiedomein) van VROS gegevens komt, voor zover bekend, niet voor. Dit omdat een MRO melding slechts binnen het politiedomein m.b.v. de bij de politie gebruikte BVO applicatie wordt gegenereerd. Daarbij komt dat er geen sprake is van inhoudelijke politiegegevens, maar slechts een verwijzing op basis van hit/no-hit. Verstrekkingen van VROS gegevens buiten het politiedomein vinden, voor zover na te gaan, niet plaats.

ID	Aanbevelingen
1	Slot / overall aanbeveling: Neem in de aanvullende privacy audit mee op welke onderdelen in dit hoofdstuk nog procesbeschrijvingen of instructies moeten worden opgesteld.

1.11 Artikel 13 (Diensten Justitie)

1.11.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Beheersdoelstellingen	V	D	N	A
1	Overzicht verwerkingen ter ondersteuning van de politietaak voor het uitvoeren van taken ten dienste van de justitie				X
2	Schriftelijke vastlegging van wettelijke genoemde gegevens en het voldoen aan de termijn voor de ter inzage legging				X
3	Gemeenschappelijke verwerkingen schriftelijk aan het CBP melden				X
4	Gevoelige gegevens onvermijdelijk verwerken in aanvulling op andere politiegegevens				X
5	Politiegegevens slechts verwerken voor zover zij rechtmatig zijn verkregen				X
6	Politiegegevens zijn toereikend, terzake dienend en niet bovenmatig				X
7	Verkregen politiegegevens worden uitsluitend voor een ander doel verwerkt als de WPG daar uitdrukkelijk in voorziet				X

ID	Bevindingen
1	Taken ten dienste van justitie betreffen: • de uitvoering van wettelijke voorschriften waarmee Onze Minister van V & J is belast, zijnde de bepalingen ingevolge de Flora- en Faunawet, de Wet wapens en munitie, de Wet explosieven voor civiel gebruik (WECG), de Wet particuliere beveiligingsorganisaties en recherchebureaus (WBPR). Deze gegevens worden verwerkt m.b.v. de landelijke applicatie PSH-VM (Verona). Daarnaast is bij de medewerkers korpscheftaken een fysiek dossier, in de vorm van een uitdraai van PSH-VM (Verona), aanwezig in ordners. • de administratieve afhandeling Wet Mulder. Deze gegevens worden verwerkt door de afdeling Tobias. • Het betekenen van gerechtelijke mededelingen in strafzaken, het vervoer van rechtens van hun vrijheid beroofde personen, en de dienst bij de gerechten. Het vervoer en de dienst bij de gerechten wordt uitgevoerd door de parketpolitie. Het betekenen van gerechtelijke mededelingen wordt in Walcheren uitgevoerd door de parketpolitie, in het Oosterscheldebekken door het wijksecretariaat bureau Goes en in Zeeuws-Vlaanderen door het wijksecretariaat bureau Terneuzen. Alle gegevens worden verwerkt in de applicatie Papos. Tobias en Papos zijn verder niet onderzocht. Kortheidshalve wordt aanbevolen om hier een aanvullende privacy audit naar te laten uitvoeren. De onderstaande bevindingen zijn verkregen door het telefonisch interviewen van regionale gebruikers en betreffen uitsluitend de verwerking PSH-VM (Verona). Daarbij is niet gevraagd naar procesbeschrijvingen, maar hoe de gebruikers in de praktijk met de applicatie omgaan. De verkregen informatie is te summier om hier een oordeel op te kunnen baseren. Om die reden wordt ook aanbevolen om een aanvullende privacy audit te laten uitvoeren.
2	De medewerkers korpscheftaken maken gebruik van de op Politie Kennis Net gepubliceerde Releasenotes PSH-VM, versie 1.8.0, d.d. 28 juli 2010, uitgegeven door vtsPN, samengesteld door de landelijk functioneel beheerder.
3	PSH-VM (Verona) betreft een landelijke applicatie. De politieregio's zijn zelf verantwoordelijk voor de in deze applicatie opgeslagen politiegegevens. Dit betreft geen gemeenschappelijke verwerking. In Zeeland zijn de medewerkers korpscheftaken belast met het "voeden" van de applicatie.
4	Er worden (anders dan identiteitsgegevens) geen gevoelige gegevens verwerkt. Gevoelige gegevens zijn namelijk niet van belang voor de doelen.
5	Gegevens welke verwerkt worden, worden met name verkregen van de betrokkenen zelf. Ook worden relevante gegevens uit andere politieapplicaties (BVH) verder verwerkt indien dit relevant en noodzakelijk is. In ieder geval vindt jaarlijks, v.w.b. wapenverloven screening plaats van de verlofhouders. Hierbij wordt gebruik gemaakt van relevante BVH informatie, bijvoorbeeld in de vorm van een melding burenruzie, en wordt in PSH-VM verwezen naar deze BVH registratie. Op ad-hoc basis wordt BVH informatie verwerkt indien deze bij toeval wordt onderkend als zijnde relevant voor de doelstelling van PSH-VM.
6	Er worden niet meer gegevens verwerkt dan relevant is voor de doelstelling van PSH-VM.
7	De gegevens kunnen worden geraadpleegd door medewerkers meldkamer en infodesk. In de praktijk wordt hiervan gebruik gemaakt indien dit noodzakelijk is voor de politietaak. Voorbeelden hiervan zijn als volgt. Voordat tot aanhouding van een verdachte in diens woning wordt overgegaan, wordt bezien of er een vuurwapen in de woning aanwezig kan zijn. Indien een informant tegen een runner vertelt over de aanwezigheid van een vuurwapen bij een subject, wordt bezien of dit subject hiertoe gerechtigd is.

ID	Aanbevelingen
1-7	Laat een aanvullende privacy audit uitvoeren naar de aanwezigheid van procesbeschrijvingen/instructies met betrekking tot de bovengenoemde onderwerpen en de omgang met de applicatie.

1.11.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig.				X
2	Politiegegevens worden verbeterd, vernietigd of aangevuld indien deze onjuist of onvolledig blijken te zijn.				X
3	Politiegegevens worden adequaat organisatorisch,technisch beveiligd tegen verlies of onrechtmatige verwerking.				X
4	Toegang van de verantwoordelijke tot politiegegevens ten behoeve van het toezicht op de naleving de WPG.				X
5	Toegang voor het CBP,de (interne) auditor, de privacyfunctionaris en technische medewerkers tot politiegegevens				X
6	Bewerkerovereenkomst ingeval politiegegevens met tussenkomst van die bewerker worden verwerkt.				X

ID	Bevindingen
1	De applicatie is voorzien van verplichte invoervelden. Daarnaast vind verificatie van persoonsgegevens plaats d.m.v. een verplichte toets met de GBA. De medewerkers korpscheftaken maken gebruik van de op Politie Kennis Net gepubliceerde Releasenotes PSH-VM, voornoemd.
2	In ieder geval jaarlijks vindt er, v.w.b. wapenverloven, screening plaats van de verlofhouders. Hierbij wordt gebruik gemaakt van relevante BVH informatie. Zie in dat verband de voorbeelden die hierboven zijn genoemd.
3	Toegang tot de applicatie wordt verkregen d.m.v. een persoonlijke inlogprocedure. Er is qua autorisaties onderscheid gemaakt in "schrijfrechten" (slechts toegekend aan de medewerkers korpscheftaken) en "raadpleegrechten" (toegekend aan medewerkers meldkamer en infodeskmedewerkers).
4	Een "Procesbeschrijving inzake de toegang tot de politiegegevens ten behoeve van het toezicht door de verantwoordelijke op de naleving van het bij of krachtens de Wpg bepaalde" is niet aanwezig.
5	Een "Procesbeschrijving inzake de toegang tot politiegegevens voor degene die met de controle en het toezicht op de WPG zijn belast, zijnde de interne auditor, de auditor, de privacyfunctionaris, het CBP en de functionaris gegevensbescherming, alsmede degenen die in opdracht van de verantwoordelijke technische werkzaamheden verrichten" is niet aanwezig bij Politie Zeeland.
6	Het onderdeel bewerkerovereenkomst is niet onderzocht.

ID	Aanbevelingen
1-6	Neem de hierboven vermelde onderwerpen in de aanvullende privacy audit mee.

1.11.3 Autorisaties

ID	Beheersdoelstellingen	V	D	N	A
1	Systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid				X
2	Politiegegevens worden verwerkt door avps die door de verantwoordelijke zijn geautoriseerd				X
3	Voldoen aan specifieke autorisatieregels voor avps die onder het beheer van de verantwoordelijke vallen.				X
4	Specifieke autorisatieregels in bijzondere gevallen voor niet avps die onder beheer van de verantwoordelijke vallen				X
5	Specifieke autorisatieregels in bijzondere gevallen voor avps die onder beheer van een andere verantwoordelijke vallen				X
6	Specifieke autorisatieregels tbv de eenheid die met de uitvoering van deze taak is belast				X

ID	Bevindingen
1-6	PSH-VM (Verona) bevat geen autorisaties die zijn toegekend aan niet-politieambtenaren. M.b.v. de toegekende autorisaties is het mogelijk om ook toegang te verkrijgen tot de gegevens van andere verantwoordelijken. Dit is inherent aan de inrichting van de applicatie. Er is geen aparte eenheid die met de uitvoering van deze taak belast. De geautoriseerden zijn door de regionaal functioneel beheerder geïnstrueerd m.b.t. het gebruik van de applicatie (zgn "knoppencursus").

ID	Aanbevelingen
1-6	Neem de bovengenoemde onderwerpen in de aanvullende privacy audit mee.

1.11.4 Bewaartermijnen en vernietiging

ID	Beheersdoelstellingen	V	D	N	A
1	Tevoren schriftelijk vastleggen van termijn/gevallen voor beëindiging verwerking en frequentie van controle hierop.				X

ID	Bevindingen
1	Door de medewerkers korpscheftaken wordt gewerkt aan de hand van de op Politie Kennis Net gepubliceerde Releasenotes PSH-VM, voornoemd. Vergunningen worden jaarlijks verlengd (m.u.v. de WBPR vergunningen, deze worden driejaarlijks verlengd). T.b.v. deze verlengingen worden de opgeslagen gegevens jaarlijks gecontroleerd en daar waar nodig geactualiseerd. Bij het vervallen van een vergunning (bijvoorbeeld bij beëindigen hobby, overlijden vergunninghouder) worden de gegevens niet verwijderd, maar krijgen deze de status van "vervallen". De applicatie kent voor de medewerkers korpscheftaken niet de mogelijkheid om in dit soort gevallen de gegevens te verwijderen. Dit verwijderen is voorbehouden aan de landelijk functioneel beheerder, maar aangezien de applicatie pas sinds 2005/2006 in gebruik werd genomen, vindt verwijdering momenteel niet plaats.

ID	Aanbevelingen
1	Neem het bovengenoemde onderwerp in de aanvullende privacy audit mee.

1.11.5 Ter beschikking stellen van politiegegevens

ID	Beheersdoelstellingen	V	D	N	A
1	Politiegegevens tbs aan geautoriseerde ambtenaren van politie indien nodig voor hun taakuitoefening				X
2	Gegevens landelijk raadpleegbaar stellen / tbs aan door verantwoordelijken geautoriseerde personen tbv politietaak				X
3	Voldoen aan de uitzonderingsregels op de tbs				X
4	Voldoen aan geheimhoudingsverplichting voor avps of de persoon aan wie politiegegevens ter beschikking zijn gesteld				X

ID	Bevindingen
1-2	D.m.v. de raadpleegautorisaties van infodeskmedewerkers en meldkamermedewerkers zijn alle gegevens landelijk beschikbaar en worden ter beschikking gesteld aan ambtenaren van politie indien nodig voor hun taakuitvoering.

ID	Bevindingen
3	Gelet op de uitzonderingsgronden zoals genoemd in art. 2:13 BP en de aard van de verwerkte gegevens zijn de uitzonderingsgronden niet van toepassing op de, in deze applicatie opgeslagen, politiegegevens.
4	Bij indiensttreding leggen alle ambtenaren van politie en andere personen de eed of belofte van geheimhouding af. Bij gelegenheid van de introductie van politieambtenaren en andere personen in hun werkomgeving wordt door leidinggevenden aandacht besteed aan de geheimhoudingsverplichting.

ID	Aanbevelingen
1-4	Neem de bovengenoemde onderwerpen naar relevantie in de aanvullende privacy audit mee.

1.11.6 Verstrekkingen

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de regels voor de verstrekkingen aan anderen dan de politie en de Marechaussee in par. 3 WPG				X
2	Voldoen aan de regels voor de protocolplicht voor de verstrekkingen				X
3	Voldoen aan de regels voor de uitzondering op de protocolplicht (OM, AIVD en MID)				X
4	Voldoen aan regels geheimhoudingsplicht bij verstrekkingen aan derden incidenteel en samenwerkingsverbanden				X

ID	Bevindingen
1	Er vinden geen verstrekkingen buiten het politiedomein plaats m.u.v.: • het mededelen dat een wapenverlof is ingetrokken aan de Koninklijke Nederlandse Schutter Associatie (KNSA). Deze verstrekking vindt plaats ingevolge punt 1.4.4.7 van het algemeen deel van de Circulaire Wapens en Munitie 2005, juridische achtergrond artikel 38, tweede lid van de Wet wapens en munitie. In Zeeland vindt dit jaarlijks 10 tot 15 maal plaats. • het op incidentele basis bevragen door de chef RID t.b.v. de AIVD taak. Hiertoe benadert hij een medewerker korpscheftaken.
2	Een verstrekking aan de KNSA wordt in het persoonsdossier van de betrokkene geprotocolleerd. De applicatie is echter niet zodanig ingericht dat deze verstrekkingen apart kunnen worden opgevraagd.
3	Een verstrekking t.b.v. de AIVD wordt niet geprotocolleerd.
4	Een verstrekking aan de KNSA wordt niet voorzien van een mededeling betreffende de geheimhoudingplicht.

ID	Aanbevelingen
1-4	Neem de bovengenoemde onderwerpen naar relevantie in de aanvullende privacy audit mee.

1.12 Rechten van betrokken

1.12.1 Verzoek om kennisneming

ID	Beheersdoelstellingen	V	D	N	A
1	Binnen de gestelde termijnen mededeling aan betrokkene op diens verzoek om kennisneming		X		X
2	Mededeling aan wettelijk benoemde personen conform wettelijke procedure	X			
3	Verzoek schriftelijk afwijzen conform de wettelijke gronden	X			

ID	Bevindingen
1	Een procesbeschrijving inzake het recht van betrokkenen op kennisneming van hun persoonsgegevens te verzoeken, is niet aanwezig bij politie Zeeland. In het kader van de toekomstige samenvoeging van de korpsen Midden-West Brabant en Zeeland wordt reeds samengewerkt tussen respectievelijk de Unit Veiligheid & Integriteit en de afdeling Integriteit & Veiligheid. In april/mei 2011 werd geïnventariseerd waar de overeenkomsten en verschillen in taken en werkwijzen zitten. Deze inventarisatie heeft geleid tot concrete voorstellen om te komen tot eenduidige procedures. In de zeer nabije toekomst zullen o.a. procedures t.b.v. kennisnemingsverzoeken en verstrekkingen worden ontwikkeld. Bij de politie Zeeland worden verzoeken omtrent de rechten van betrokkenen (kennisneming/verbetering/aanvulling/verwijdering/afscherming van politiegegevens) centraal behandeld door de afdeling privacy. (= de afdeling I & V). Politie Zeeland neemt daarbij de wettelijke bepalingen zoals verwoord in de artikelen 25 t/m 31 WPG in acht. Hierbij wordt gebruikgemaakt van de basisdocumenten, genoemd in het hoofdstuk Beleid. De Basisdocumenten zijn: • Toelichting kennisname; • Aanvraagformulier inzage verzoek; • Aanvraag inzage namens; • Aanvraag minder dan 16 jr; • Toelichting verwijdering E.A.; • Ontvangstbewijs contante betaling; • Verslag inzage. De politie Zeeland voldoet aan de wettelijke bepalingen betreffende inzageverzoeken. Inzageverzoeken worden binnen de wettelijke termijnen afgehandeld en de identiteit van de verzoeker wordt vastgesteld. Dit wordt, in verband met de personele capaciteit, gerealiseerd door veelvuldig gebruik te maken van de mogelijkheid om documenten te verstrekken. Van de tijd- en arbeidsintensieve methode van het in persoon inzage geven op een politiebureau wordt summier gebruik gemaakt. In 2010 werden 75 verzoeken tot kennisneming schriftelijk en 13 verzoeken mondeling en in persoon afgehandeld. Onder de genoemde 13 verzoeken vallen ook de verzoeken van nabestaanden van verkeersongevallen en zelfmoorden. Deze verzoeken worden in het kader van de rouwverwerking in persoon afgehandeld. De eventuele selectie van de te tonen documenten/foto's vindt plaats door de privacyfunctionaris. Hierbij kan worden geacht aan het niet tonen van schokkende close-up foto's van de bij het verkeersongeval betrokken en eveneens omgekomen tegenpartij. Deze foto's worden gemaakt door de Verkeers Ongevallen analyse (VOA) maar niet in het proces-verbaal opgenomen. Daar waar mogelijk wordt in overleg met de betrokken verbalisanten, de daadwerkelijke inzage door hen zelf uitgevoerd. Dit omdat nabestaanden mogelijk detailvragen stellen omtrent het plaatsgevonden incident welke slechts door de betrokken verbalisanten zijn te beantwoorden.
2	In de praktijk komen verzoeken tot kennisneming door wettelijk vertegenwoordigers slechts zeer sporadisch voor. In voorkomende gevallen worden deze in persoon afgehandeld met de wettelijk vertegenwoordigers.
3	De verzoeken tot kennisneming worden, met gebruikmaking van de bovengenoemde basisdocumenten, door de administratief medewerkster afgehandeld. De privacyfunctionaris is verantwoordelijk voor, en belast met, de afweging van de uitzonderingsgronden genoemd in artikel 27 WPG. In voorkomende gevallen vraagt hij, t.b.v. deze afweging, de betrokken verbalisanten en/of leidinggevenden beargumenteerd aan te geven of de goede uitvoering van de politietaak of gewichtige belangen van derden kennisneming verhinderen. Aangezien BVH documenten standaard worden afgedrukt met vermelding van BSN nummers en geheime telefoonnummers van derden, worden deze handmatig onleesbaar gemaakt om eventuele identiteitsfraude en/of ongewenst kennis kunnen nemen van een geheim telefoonnummer te vermijden. Tot op heden is van een gehele afwijzing van een verzoek tot kennisneming geen sprake geweest. Wel is incidenteel een inzageverzoek voor een deel geweigerd. De gedeeltelijke weigering wordt schriftelijk kenbaar gemaakt, waarbij verwoord wordt dat er gebruik wordt gemaakt van de uitzonderingsgronden van artikel 27 WPG. Tevens wordt de verzoeker in dit besluit gewezen op toepasselijkheid van de Awb zoals omschreven in artikel 29 WPG.

ID	Aanbevelingen
1	Stel procesbeschrijvingen vast voor de afhandeling verzoeken om kennisneming.

1.12.2 Verzoek om verbetering, aanvulling, verwijdering of afscherming

ID	Beheersdoelstellingen	V	D	N	A
1	Binnen gestelde termijn schriftelijke mededeling op verzoek om verbetering/ aanvulling/verwijdering/afscherming		X		X
1	Mededeling aan wettelijk benoemde personen conform wettelijke procedure	X			
1	De beslissing tot verbetering/ aanvulling/verwijdering/afscherming zo spoedig mogelijk uitvoeren	X			

ID	Bevindingen
1	Een procesbeschrijving inzake het recht van betrokkenen om verbetering, aanvulling, verwijdering of afscherming van diens persoonsgegevens te verzoeken is niet aanwezig bij de politie Zeeland. In 2010 werden slechts drie verzoeken tot verbetering/aanvulling/verwijdering of afscherming van politiegegevens ingediend. In twee gevallen werden deze verzoeken gehonoreerd. In één geval werd het verzoek geweigerd. Alle verzoeken werden schriftelijk binnen de wettelijke termijn afgehandeld. De weigering werd met redenen omkleed en voorzien van de mededeling over de toepasselijkheid van de Awb conform artikel 29 WPG. In de twee genoemde gevallen waarin de verzoeken werden gehonoreerd, werd de functioneel beheerder van de betreffende applicatie, nog voordat het besluit tot honorering aan de verzoeker werd verzonden, opdracht gegeven om e.e.a. te realiseren. De functioneel beheerders koppelden terug dat aan de opdracht werd voldaan.

ID	Aanbevelingen
1	Stel een procesbeschrijving vast voor de afhandeling van verzoeken inzake het recht op verbetering, aanvulling, verwijdering of afscherming.

1.12.3 Mededeling van verbetering, aanvulling, verwijdering of afscherming

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan informatieplicht jegens personen/instanties die eerder gegevens over verzoeker ontvingen		X		X
1	Motiveren waarom niet aan de informatieplicht is voldaan	X			

ID	Bevindingen
1	Een procesbeschrijving inzake het doen van mededeling van verbetering, aanvulling, verwijdering of afscherming aan de ontvangers van politiegegevens is niet aanwezig. In 2010 werd slecht één dergelijk verzoek ontvangen. In dit geval was geen sprake van ontvangers van politiegegevens.

ID	Aanbevelingen
1	Stel een procesbeschrijving vast inzake het doen van mededeling van verbetering, aanvulling, verwijdering of afscherming aan de ontvangers van politiegegevens.

1.12.4 Vergoeding van kosten

ID	Beheersdoelstellingen	V	D	N	A
1	Niet meer dan de maximale vergoeding voor inzageverzoek in rekening brengen		X		X
1	Vergoeding aan verzoeker terugbetalen in de wettelijke benoemde gevallen	X			

ID	Bevindingen
1	Een procesbeschrijving voor het innen en terugbetalen van kosten inzake verzoeken om kennisneming is bij de Politie Zeeland niet aanwezig. Zie ook voorgaande opmerking m.b.t. gebruik basisdocumenten. In deze basisdocumenten wordt het bedrag, zijnde 4,50 euro, niet hoger dan het bij of krachtens amvb vastgestelde bedrag en de wijze van betaling vermeld. In de incidenteel voorkomende en wettelijke benoemde gevallen, zorgt de administratief medewerkster ervoor dat de vergoeding aan de verzoeker wordt terugbetaald.

ID	Aanbevelingen
1	Neem in de vast te stellen procesbeschrijvingen de vergoeding van kosten mee.

1.13 Audits

ID	Beheersdoelstellingen	V	D	N	A
1	Voldoen aan de periodieke verplichting uitvoeren privacy audit	X			
2	Afschrift zenden van de (her)controleresultaten van de privacy audit aan College bescherming persoonsgegevens	X			
3	Binnen een jaar uitvoeren van hercontrole op onderdelen die niet aan de voorwaarden voldeden	X			
4	Voldoen aan de geheimhoudingsverplichting voor alle betrokkenen bij de privacy audit	X			

ID	Bevindingen
1 2 3	Ten aanzien van de interne audit en de privacy audit heeft de korpsleiding van de politie Zeeland de volgende maatregelen genomen: • Een korpsbesluit voor het samenstellen van een intern audit team in 2010; • De deelname van de interne auditors aan een "in-house" training interne WPG-audits door Mazars in 2010; • Het vaststellen van een "Uitvoeringsdocument Interne Audit Wet politie gegevens"; • Een plannings - en uitvoeringsplan (bijlage in dossier); • Er is binnen politie Zeeland een "Regeling taken en bevoegdheden FG Politie Zeeland" waarin onderstaande punten zijn vastgelegd: • De aanstelling van een interne auditor; • De inrichting van de interne auditfunctie in de organisatie. In het" Uitvoeringsdocument Interne Audit Wet politie gegevens zijn geregeld: • Het jaarlijks uitvoeren van de interne audit en het éénmaal per vier jaar laten uitvoeren van een privacy-audit door externen; • het zenden van een afschrift zenden van de (her)controleresultaten van de privacy audit aan het College bescherming persoonsgegevens;

ID	Bevindingen
	• het zonodig binnen een jaar uitvoeren van hercontrole op onderdelen van de WPG die niet aan de voorwaarden voldeden. Een regeling voor het screenen van de interne auditors is niet formeel vastgelegd. Alle interne auditors zijn beëdigd ambtenaar, hebben een bepaalde screening ondergaan en hebben de eed of belofte voor geheimhouding afgelegd. De geheimhouding van de privacy auditor is in de overeenkomst geregeld.

ID	Aanbevelingen
	Geen.

1.14 Privacyfunctionaris

ID	Beheersdoelstellingen	V	D	N	A
1	Benoeming van de privacyfunctionaris		X		X
1	Toezicht en advisering door de privacyfunctionaris conform de wettelijke regels	X			
2	Toegang tot de politiegegevens voor zover nodig voor de uitvoering van zijn taak		X		X
3	Overzicht bijhouden van art.9 doelen en de daarover vast te leggen gegevens	X			
3	Overzicht van de gegevens krachtens artikel 13, 4 WPG (m.b.t. ondersteunende taken)		X		X
3	Overzicht bijhouden van de toekenning art. 6 autorisaties		X		X
3	Overzicht van par.3 verstrekkingen (m.u.v. verstrekkingen belang veiligheid staat)		X		X
3	Overzicht van verwerkingen ten aanzien waarvan aanwijzingen zijn over de onrechtmatigheid ervan	-			X
3	Overzicht van geautomatiseerde vergelijkingen op basis van artikel 11,5 WPG (met andere dan politiegegevens)		X		X
4	De volledigheid van de gegevens over de bedoelde art. 9 en 13 verwerkingen		X		X
5	Opstellen van een jaarverslag	X			
6	De aanmelding van de privacyfunctionaris bij het College bescherming persoonsgegevens	X			

ID	Bevindingen
1	De PF is officieel bij brief 09/01556, d.d. 01-04-2009 door de korpschef van de politie Zeeland benoemd en aangemeld bij het CBP. De functiebeschrijving komt niet overeen met de inhoud van de wet c.q. de opgestelde handreiking PF. Er is geen unieke functiebeschrijving voor de wettelijk verankerde functie van PF waarin wettelijke taken, bevoegdheden en verantwoordelijkheden omschrijven zijn. Er is, op initiatief van de FG, een taakverdeling gemaakt tussen de FG en de PF (beide hebben een functiebeschrijving) met deels gescheiden verantwoordelijkheden. De PF richt zich met name op advies, de FG op toezicht. De PF heeft, in afwijking van artikel 34 WPG, lid 1, de adviesfunctie en een beperkte toezichthoudende rol. De adviesrol van de PF bedraagt meer dan de helft van de tijd (ongeveer 60%). De PF is lid van de landelijke Expertgroep Politiegegevens en Privacy. Dit betreft een adviserend overleg voor de portefeuillehouder privacy binnen de Raad van Korpschefs. De PF is ontwerper van een mappenstructuur in de Word omgeving conform de WPG bepalingen. Deze mappenstructuur levert voor deze applicatie een bijdrage in het WPG conform verwerken van politiegegevens. De mappenstructuur werd vervolgens tot standaard voor de Zuid-6 verklaard. De check op de I-90-lijsten werd in het verleden (tot datum FLO juni 2010) door de FG uitgevoerd. De PF komt hier momenteel vanwege zijn andere reguliere werkzaamheden en het participeren in het interne- en externe auditteam niet aan toe. Wel is tijdens de interne audit een uitdraai van alle I90 mutaties gemaakt over de periode van 1-8-2009 – 1-8-2010 waarop deelwaarnemingen zijn uitgevoerd. Dit geldt ook voor de verantwoording van de verzoeken om politiegegevens en de uitgaande brieven in het postregistratiesysteem Corsa. In dat verband wordt verwezen naar par. 1.2.8 van dit rapport. Voor wat betreft zijn adviserende taak wordt verwezen naar de bijlage III geraadpleegde documenten, waaronder zich een groot aantal emails bevinden waaruit is afgeleid dat de PF zich intensief van de adviserende taak kwijt. De PF houdt toezicht op het proces van autoriseren binnen de politie Zeeland. De leidinggevende vult het autorisatieformulier in en stuurt dit naar de mailbox privacy. De aanvraag wordt door de IBF of de PF getoetst. Beiden kennen nagenoeg iedere medewerker bij naam en toenaam. Bij onduidelijkheid nemen zij contact op met verzoeker/leidinggevende. De autorisatieaanvraag wordt zo nodig door hen aangepast. Als er voor "blauwe" medewerkers autorisatie voor BVO wordt aangevraagd, wordt conform een informele afspraak met het hoofd RIO en de Korpsleiding besloten om de BVO autorisatie voor maximaal 6 maanden toe te kennen onder voorwaarde van de aanvraag van het P-veiligheidsonderzoek en het volgen van een e-learning cursus BVO. Het probleem voor het beheer van de autorisaties is dat er geen autorisatiebeheerserver is voor het intrekken van autorisaties. Vele malen is al bij leidinggevende aangedrongen om bij overplaatsing of het betrekken van een neventaak de autorisaties in te trekken, maar dat gebeurt marginaal. De PF kan met diverse mails aantonen dat hij dit signaleert. Dit gebeurt ook door de privacymedewerker. De afgelopen jaren is dit ongeveer 5 à 6 maal per jaar gebeurd. De PF kan autorisatie-uitdraaien regelen per team. Het pakket van eisen voor de autorisatieserver heeft betrekking op autorisaties voor: individuen, groepen, functies, afdelingen en organisatorische eenheden. De lokaal functioneel beheerder BVO kan inzage geven in de autorisaties per team. Ook van de CIE. De Teamchef CIE kent ook de autorisaties toe in zijn rol als CIE-chef. Er ligt een procesbeschrijving en pakket van eisen voor ABS. De vtsPN heeft opdracht om dit pakket te gaan kopen of een dergelijke server zelf te ontwikkelen. Beschikbaar is wel een regiorechtentool: per medewerker per afdeling is te zien welke autorisaties deze heeft. De tool is een schil over alle autorisaties in applicaties heen. De tool zoekt alle applicaties af en ziet welke autorisaties iemand heeft. De PF gebruikt de tool niet. De IBF wel om te zien welke rechten iemand heeft. Soms wordt ook even naar de vtsPN gebeld om te zien welke rechten iemand heeft. Maar de PF belt eigenlijk rechtstreeks met de functioneel beheerder of met de vtsPN. Regelmatig voeren de PF en IBF controles uit op de uitstaande autorisaties. Ingeval dit nodig is, wordt hierover met de geautoriseerde, leidinggevende of de proceseigenaar of functioneel beheer contact opgenomen. Er wordt ook veel via de "warme communicatie" gecommuniceerd.
2	Een procesbeschrijving m.b.t. de toegang van de PF tot de politiegegevens in het kader van diens toezichts- en controletaken is niet

ID	Bevindingen
	aanwezig. Bij politie Zeeland wordt deze rol hoofdzakelijk ingevuld door de FG. De PF heeft geen directe toegang tot de systemen BVH/BVO. Hij kan bij de functioneel beheerders van de desbetreffende systemen wel de nodige overzichten krijgen. De PF heeft geen zicht op / geen toegang tot de CIE-informatie. De PF heeft in het kader van zijn verantwoordelijkheden (m.u.v. de CIE) voldoende toegang tot de noodzakelijke informatie. Controle op de systemen BVO/BVH op het verwijderen van informatie (bijv. afloopberichten) is gewaarborgd. Controle op de andere, door de politie Zeeland gebruikte, systemen is niet gewaarborgd.
3	Ten aanzien van de verplichting voor de PF om een overzicht bij te houden van de schriftelijke vastlegging van de gegevens, als bedoeld in artikel 32, lid 1, WPG kan het volgende worden vermeld: 1. **Het overzicht artikel 9 verwerking** is aanwezig. De aan genoemd overzicht gekoppelde bewijsstukken (aanmelding WPG verwerking) zijn in het dossier bij de PF niet altijd compleet ingevuld. De belangrijkste opmerking is dat bij de deelwaarneming 7 formulieren niet getekend waren door de teamchef. Onder verwijzing naar par. 1.3.1.1 en 1.3.1.2 is af te leiden dat de PF inmiddels een goed overzicht heeft van de artikel 9 verwerkingen. 2. **Het overzicht artikel 13 verwerking is aanwezig.** Landelijk is overigens nog niet duidelijk/gedefinieerd wat nu eigenlijk als een artikel 13 verwerking moet worden beschouwd. 3. **Het overzicht van de artikel 6 autorisaties:** Dit deel van zijn taak is gemandateerd aan de IBF. Dit is formeel geregeld via het mandaatbesluit. De IBF geeft aan dat de lijsten niet actueel zijn. Lijsten zijn niet actueel te houden en zijn vaak van extern afkomstig. Overplaatsingen, verlopen autorisaties etc. worden door het korps niet adequaat bijgehouden. Een werkgroep op Zuid-6 niveau is bezig omissies te verzamelen en te analyseren teneinde de bestaande problematiek op te lossen. De opzet van de AO heeft hierin een hoge prioriteit. Uit de verslaglegging bij de onderwerpen autorisaties bij de verwerkingen artikel 8, en 9 komt naar voren, dat het proces van het autoriseren wel goed verloopt, maar het de-autoriseren niet. 4. **Het overzicht paragraaf 3 verstrekkingen:** de PF heeft toegang tot de I-90 overzichten (BVH) en verstrekkingenmutaties in BVO. Er vinden korpsbreed geen (geplande) controles plaats op de verstrekkingen / ter beschikkingstellingen. In de verstrekkingenmutaties is niet aangegeven welke mutaties verstrekkingen zijn (externe) en welke mutaties intern gericht zijn (ter beschikking stellingen). Uit de verslaglegging bij de onderwerpen verstrekkingen bij de verwerkingen artikel 8 blijkt, dat het gebruik van de I-90 functionaliteit in BVH over de teams heen een divers beeld geeft. De PF heeft over het afgelopen jaar de I-90 vastleggingen op aantallen bekeken. Voorzienbaar is, dat met het steekproefgewijs inhoudelijk bekijken van I-90 verstrekkingen veel tijd is gemoeid. 5. **Een overzicht van onrechtmatige bewerkingen** is niet bij de PF voorhanden. Dergelijke verstrekkingen zijn tot dusver niet bij de PF gemeld. Uit hoofde van zijn functie zijn onrechtmatige verwerkingen anders dan ingeval van vragen over verwerkingen uit de organisatie moeilijk voor de PF te detecteren. 6. Een **overzicht van geautomatiseerde vergelijkingen** (artikel 11) is niet aanwezig bij de PF. De PF heeft geen meldingen ontvangen van genoemde bewerkingen. [redacted]
4	De gegevens over artikel 9 verwerkingen zijn volledig bij de PF aanwezig. Een "Overzicht met verwerkingen van politiegegevens, waarin de verwerkingen ter ondersteuning van de politietaak met hun specifiek doelstellingen zijn opgenomen is bij de PF aanwezig. Dit zijn de verwerkingen HKS, HAVANK, PV's en rapporten en) die onderkend zijn als artikel 13, lid 1, verwerking. FCM, infodesk/ makelfunctie infodesk, moeten nog ter inzage worden gelegd.
5	De PF heeft het jaarverslag in april 2010 vastgesteld en aan de korpsleiding aangeboden.
6	De PF is formeel aangemeld bij het CBP.

ID	Aanbevelingen
1	Spits de functiebeschrijving van de PF op zijn wettelijke taken en bevoegdheden toe. Voorzie de PF van de benodigde ondersteuning om zijn toezichthoudende taak waar te maken. Overweeg om de taakverdeling tussen FG en PF te herzien.
2	Voorzie in een procesbeschrijving m.b.t. de toegang van de PF tot alle verwerkingen van politiegegevens.
3	Stel de PF in het kader van de protocolverplichting ingevolge artikel 32 en 34 WPG toereikende middelen ter beschikking.
4	Zorg er voor dat het overzicht van artikel 13 verwerkingen gecompleteerd wordt.

1.15 Functionaris gegevensbescherming

ID	Beheersdoelstellingen	V	D	N	A
1	De formele aanstelling van de Functionaris voor de gegevensbescherming (is niet verplicht)	X			X
2	Voldoen aan de wettelijke eisen van kennis en betrouwbaarheid	-			X
2	Voldoen aan de eisen van onafhankelijkheid	-			X
2	Vervuld zijn van de randvoorwaarden om de taak naar behoren te kunnen uitvoeren	-			X
2	Voldoen aan de verplichting tot aanmelding bij het College bescherming persoonsgegevens	-			X

ID	Beheersdoelstellingen	V	D	N	A
2	Voldoen aan de geheimhoudingverplichting	-			X
2	Opstellen jaarlijks verslag van werkzaamheden en bevindingen	-			X
3	Uitoefenen van het wettelijk bepaalde toezicht	-			X
4	Beschikken over bevoegdheden gelijkwaardig aan die in afd. 5.2 ABW	-			X

ID	Bevindingen
1 2	De FG is met ingang van juni 2010 met FLO gegaan en er was tot het einde van de interne audit nog geen vervanger. De nieuwe FG is recentelijk formeel door de korpschef aangesteld en bij het CBP aangemeld. De FG is nog aan zijn inwerkperiode bezig. Om die reden is tijdens de externe audit het onderwerp FG niet meegenomen. Dit zal het geval zijn bij de eerstvolgende privacy audit.

ID	Aanbevelingen
1-4	Laat de bovengenoemde onderwerpen meenemen in de eerst volgende privacy audit.

Bijlage II: Basisbeveiliging Politie

2.1 Gebruikersorganisatie

2.1.1 Informatievoorzieningproces

ID	Beheersdoelstellingen	V	D	N	A
1	Informatievoorzieningwijzigingen zijn gecontroleerd doorgevoerd zodat beschikbaarheid en integriteit gewaarborgd is		X		X
2	Het informatiesysteem blijft voldoen aan de huidige en toekomstige eisen die het gebruik hieraan stelt		X		X
3	Ingevoerde en vastgelegde gegevens zijn integer (juist, volledig, tijdige vastlegging, tijdige hersteltijd)		X		X
4	Verstoringen, die invloed op de beveiliging hebben of kunnen krijgen (beveiligingsincidenten) worden tijdig verholpen		X		X

ID	Bevindingen
1	Voor het wijzigingbeheer is bij Politie Zeeland alleen voor de grotere applicaties een procesbeschrijving aanwezig. (BVH / BVO / BVCM / KSA etc.), zoals in de vorm van het Handboek Functioneel Beheer BVO Zuid 6, versie 1.02, d.d. 24-06-2009, waarin aan dit onderwerp aandacht wordt besteed. Voor de kleine applicaties niet. De informatie voor FB (functioneel beheer) komt van de vtsPN. De FB op nationaal niveau maakt gebruikershandleidingen. Wijzigingsbeheer is geen continue proces bij de politie Zeeland doordat het niet verankerd is. Er is geen deelwaarneming op het wijzigingsbeheer uitgevoerd.
2	Een procesbeschrijving voor het functioneel applicatiebeheer is aanwezig in de vorm van het Handboek Functioneel Beheer BVO. Verder bestaan er veel operationele afspraken met de vtsPN maar deze zijn niet vastgesteld / vastgelegd. Taken, bevoegdheden en verantwoordelijkheden zijn tegen die achtergrond niet transparant. Controlemomenten en vastlegging hiervan ontbreken.
3	De procesbeschrijving inzake gegevensbeheer is aanwezig. In het Handboek Functioneel Beheer BVO wordt ook aandacht besteed aan de verantwoordelijkheid voor het gegevensbeheer. Zie verder de bevindingen en aanbevelingen in de voorgaande paragrafen met betrekking tot de kwaliteit van politiegegevens, zoals onder meer het gebruik van TrueBlue en het gegevensbeheer in BVO. Aan het belang van de kwaliteit van de gegevens wordt ook aandacht besteed in het Informatiebeveiligingsbeleid Zuid6. Aangegeven wordt, dat het bewaken van de kwaliteit mede wordt geborgd door een integraal gegevensbeheer voor informatiesystemen volgens het Business Information Service Library model (BiSL). Dit model waarborgt, dat gegevens integer, exclusief en beschikbaar zijn voor hen die daartoe zijn geautoriseerd. Hierop is tevens controle georganiseerd. Afhankelijk van de gegevensset is de verantwoordelijkheid hiervoor bovenregionaal of regionaal bepaald.
4	In het Beveiligingsbeleid Zuid6 staat onder meer beschreven, dat beveiligingsincidenten worden aangemeld bij de leidinggevende en de IBF. In Zuid-6 zijn afspraken gemaakt voor het registeren en afhandelen van beveiligingsincidenten. De uitwisseling binnen Zuid6 van beveiligingsincidenten is geregeld in de procedure IB-incidenten uitwisseling vtsPN – Zuid6. De politie Zeeland conformeert zich aan het beleid, met dien verstande dat nu het regionale beleid nog van kracht is. Daarin staat opgenomen dat iedere districtchef/diensthoofdverantwoordelijk is voor: • De melding van geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging bij de functionaris voor de gegevensbescherming; • De afdoening van incidenten en inbreuken op de informatiebeveiliging. Bij het zich voordoen van een incident zal door de districtchef/diensthoofd de functionaris voor de gegevensbescherming worden geconsulteerd omtrent de te nemen stappen ter verbetering van de informatiebeveiliging. Aan de korpsleiding zullen door de districtschef of door het diensthoofd ter beoordeling worden voorgelegd: • Incidenten die politiek gevoelig zijn, dit ter beoordeling van de verantwoordelijke lijnmanager; • Incidenten waarbij sprake is van strafbare feiten; • Materiele schade en immateriële schade boven een bepaald bedrag; • Incidenten die gevolgen kunnen hebben voor het imago van het korps. Gezien de ontwikkelingen in de organisatieveranderingen is het hierboven gehanteerde begrippenkader geheel gewijzigd. Binnen niet al te lange termijn, bij de vorming van de nationale politie, zal het begrippenkader wederom wijzigen. Registratie van opgetreden incidenten via signalen in de systemen zijn moeilijk te detecteren en is voornamelijk weggelegd bij de vtsPN. De ondersteuning van de vtsPN is steeds noodzakelijk. De logging van diverse applicaties is een steeds terugkerend item op bijeenkomsten en vergaderingen maar de vtsPN is nog niet in staat om maatwerk te leveren. Er bestaan weliswaar loggingsmogelijkheden doch om de gegevens te kunnen lezen is een tool nodig. De tooling is op dit moment in ontwikkeling. Er wordt een tool ontwikkeld waarin de IBF-ers dergelijke beveiligingsincidenten kunnen melden. De tool verkeert momenteel in de eindfase en zal nagenoeg gereed zijn om te worden geïmplementeerd. De implementatie is voorzien voor de zomer 2011.

ID	Aanbevelingen
1-4	Neem alle normen mee in de vormgeving en implementatie van het Informatiebeveiligingsbeleid Zuid6 en de periodieke controle op de uitvoering van dit beleid.

2.1.2 Medewerkers

ID	Beheersdoelstellingen	V	D	N	A
1	Beveiliging is integraal onderdeel van het functioneren van iedere medewerker	-			A
2	Medewerkers van de politie zijn betrouwbaar en gaan discreet om met de hen ter beschikking staande informatie	X			
3	Op gegevens waarvan het onwenselijk is dat deze in handen komen van onbevoegden rust een geheimhoudingsplicht	X			
4	Bij vervanging van een medewerker vindt geen doorbreking van functiescheiding plaats	-			A
5	Taken die van belang zijn voor de betrouwbaarheid van informatie(systemen) worden op juiste wijze uitgevoerd	-			A

ID	Bevindingen
1	In het Informatiebeveiligingsbeleid Politie Zeeland is de verantwoordelijkheid van de beveiliging van de informatievoorziening belegd op het niveau van de korpsleiding, de districtschefs en de diensthoofden. Iedere districtschef en diensthoofd is verantwoordelijk gesteld voor de medewerkers die binnen zijn district of dienst vallen.
2	Personen die bij het korps worden aangesteld of benoemd, worden vooraf onderworpen aan een onderzoek waaruit vast moet komen te staan dat de betreffende persoon geen strafbare feiten heeft gepleegd of directe contacten heeft met criminele personen. Onderwerpen binnen dit onderzoek betreffen milieuonderzoek, vastlegging onderzoeksuitkomsten en verklaring van goed gedrag. Het Hoofd I&V beschikt over processchema's inzake een uit te voeren "Betrouwbaarheidsonderzoek" en "Veiligheidsonderzoek". In de praktijk worden afhankelijk van de functie van een medewerker (periodiek) zogenaamde "A" en "P" onderzoeken uitgevoerd.
3	Iedere hiervoor in aanmerking komende medewerker legt bij in diensttreding de eed of belofte af voor de geheimhouding van politieinformatie. Documentatie die op dat onderwerp betrekking heeft, is aanwezig in de vorm van: • Het Korpsbesluit 03/02209 dd 18 april 2002; • Integriteitstatuut van de Nederlandse politie (Deltanet); • Het Draaiboek P&O introductieprogramma; • Arbeidsomstandigheden Eed / belofte (Deltanet).
4	Dit onderwerp is niet getoetst.
5	Anders dan in de vorige paragrafen reeds aan de orde is gekomen op het terrein van de kwaliteit van de verwerking van politiegegevens, is deze norm niet getoetst.

ID	Aanbevelingen
1 4 5	Neem alle normen mee in de vormgeving, uitwerking en implementatie van het Informatiebeveiligingsbeleid Zuid6 en de periodieke controle op de uitvoering van dit beleid.

2.1.3 Middelen

ID	Beheersdoelstellingen	V	D	N	A
1	Iedere locatie is afgeschermd voor onbevoegden		X		X
2	Onbevoegde personen kunnen geen inzicht krijgen in gegevens		X		X
3	Telewerkapparatuur voldoet aan alle beveiligingseisen die door de organisatie zijn opgesteld		X		X

ID	Bevindingen
1	Binnen de regio Zeeland wordt gebruik gemaakt van [redacted]. Alle gebouwen binnen de regiopolitie Zeeland zijn op dit toegangscontrolesysteem aangesloten. Toegangsdeuren zijn voorzien van een kaartlezer. Medewerkers worden door hun direct leidinggevende voor toegang geautoriseerd en aan hen wordt een toegangskaart (druppel) uitgegeven. De gecontroleerde toegang is gebaseerd op het Informatiebeveiligingsbeleid binnen de regiopolitie Zeeland. In het Besluit Autorisatieprocedure waarin de toegang tot gebouwen en terreinen van de regiopolitie Zeeland is dit verder uitgewerkt. De afdeling Bedrijfsvoering verzorgt [redacted]. Het systeem kent verschillende autorisatieniveaus, waaronder het hoogste niveau voor het technisch beheer, een niveau voor het functioneel beheer en een niveau voor medewerkers van de receptie en het wijksecretariaat die hiermee slechts bezoekers kunnen registreren. De beheerprocedure voor het systeem verkeert in de conceptfase. Taken, bevoegdheden, verantwoordelijkheden en functiescheiding zijn nog niet belegd. Een calamiteiten- of incidentenregeling of paragraaf ontbreekt. Er wordt gewerkt met autorisatieformulieren en uit praktische overwegingen ook met mondelinge afspraken met een beperkt aantal teamchefs. Toegang wordt verleend door een medewerker van de afdeling Bedrijfsvoering die zelfstandig en naar eigen inzicht handelt. Een procesbeschrijving inzake het beheer van toegang binnen een locatie is op de afdeling niet aanwezig. Een autorisatie wordt door de medewerker ingetrokken op basis van hetgeen hem ter ore komt. Gezien het geringe aantal verzoeken om autorisaties wordt vermoed dat er autorisaties in het systeem voorkomen die inmiddels ingetrokken hadden moeten zijn. Hiernaar is verder geen onderzoek ingesteld. Door de IBF is bij onderzoek geconstateerd dat de computerruimten goed beveiligd zijn en dat de toegangsregeling op dat onderdeel op orde is. Volgens het Informatiebeveiligingsbeleid politie Zeeland 2008 is het diensthoofd FEB verantwoordelijk voor de facilitaire voorzieningen, waaronder de fysieke toegangsbeveiliging van de gebouwen.
2	Een procesbeschrijving of instructie inzake het adequaat beveiligen van werkplekken is niet aanwezig. Uit de gehouden interviews komt naar voren dat de PC beveiliging (wachtwoord, booten, schermbeveiliging, randapparatuur) op orde is. Niet op orde zijn: Clean desk policy (wordt niet stringent toegepast), controle op de werkplekbeveiliging en de wachtwoordpolicy. Binnen het LOIB (Landelijk Overleg Informatie Beveiliging) is een werkgroep bezig met de actie "Password Reset". Tevens wordt in deze werkgroep aandacht besteed aan de omgang met social media. De IBF is trekker van deze werkgroep. De activiteiten zijn gericht op een adequate en veilige wijze in het omgaan met passwords en een eenduidige en uniforme wijze van het toekennen, wijzigen en verwijderen van passwords van cliënts. Er ligt een voorstel voor een landelijke regeling om te komen tot een adequate passwordreset. Het beheer van apparatuur, m.n. (afvoeren van) gegevensdragers en printerbeheer (alleen printen op gedefinieerde netwerkprinters) is niet onderzocht.
3	De politie Zeeland beschikt over een Gebruikershandleiding Telewerken van de vtsPN. Het beleid dan wel instructies op dit terrein op korpsniveau is nog niet door de korpsleiding vastgesteld. Aan dergelijk beleid c.q. instructie wordt nog gewerkt. Specifieke aandachtspunten die worden uitgewerkt zijn: • Gebruikersauthenticatie; • Gegevensdragers (m.n. usb-sticks); • Uitsluiting van het via telewerken gebruik maken van data waaraan hogere eisen dan gemiddeld aan exclusiviteit zijn gesteld; • Procedures omtrent telewerken vanuit huis; • Beveiligde verbindingen. Binnen de Politie Zeeland mogen slechts enige mensen telewerken.

ID	Aanbevelingen
1	Voer aanvullend onderzoek uit op toegangscontrolesysteem en stel een beheerprocedure vast.
2	Stel een instructie op voor de werkplekbeveiliging. Voer onderzoek uit naar het beheer van apparatuur / gegevensdragers.
3	Stel een instructie voor het telewerken vast.

2.1.4 Strategie & Beleid

ID	Beheersdoelstellingen	V	D	N	A
1	Informatievoorziening en beveiliging staat in de strategie en komt in het informatiebeveiligingsbeleid tot uitvoer	X			X
2	Medewerkers van het korps zijn op de hoogte van de afspraken die gelden ten aanzien van de informatiebeveiliging	X			X

ID	Bevindingen
1	Er is informatiebeveiligingsbeleid van kracht binnen de regio Zeeland (Informatiebeveiligingsbeleid Politie Zeeland 2008). De Autorisatieprocedure politie Zeeland maakt integraal onderdeel uit van dat beleid. In het Informatiebeveiligingsbeleid zijn de taken en verantwoordelijkheden voor de informatiebeveiliging op het niveau van de korpsbeheerder/korpschef, de districtschefs, de diensthoofden, de taakaccenthouders en de portefeuillehouder informatiebeveiliging en privacy belegd. In de afgelopen jaren is steeds meer de nadruk komen te liggen op de inspanningen binnen Zuid-6. Een projectplan aangaande het bevorderen van het informatiebeveligingbeleid en de informatiebeveiliging in Zuid6 is in uitvoering. Zo zijn tal van documenten ontwikkeld: • Integraal informatiebeveiligingsbeleid Zuid-6. Hierin is voor de 6 zuidelijke regio's het informatiebeveiligingsbeleid geregeld; • De regeling IB-incidenten; • Het autorisatiebeleid Zuid Nederland met een accountbeheer en volledige procesbeschrijving. Daarvan maakt deel uit de procesbeschrijving met de omschrijving van de producten en de standaardautorisatieprofielen ten einde rol-gebaseerd te kunnen autoriseren op een eenduidige wijze; • De ontwikkeling voor de invoering van een Autorisatie Beheer Server waarin aan de hand van standaardprofielen autorisaties geautomatiseerd verlopen. De toekenning van autorisaties gebeurt dan rol en functiegebaseerd en niet op naam; • Het regionale informatiebeveiligingsbeleid met de regionale autorisatieprocedure; • De gedragscode aangaande informatiedragers; • Regeling voor beveiligd printen; • De rubriceringregeling geldend in de 6 zuidelijke regio's; • Regelingen voor de vernietiging van informatiedragers; • Richtlijnen ten behoeve van digitaal anonimiseren. In de loop van de afgelopen jaren zijn de inzichten veranderd als het gaat om de informatiebeveiliging. Was eerst de situatie zo dat er: 'nee, tenzij' werd verkocht. Nu is de mening dat 'ja, mits' veel beter zal werken. Dat is de reden dat een landelijk project gestart is in het begin 2010, onder de naam 'Samen Beveiligen' met als doelstelling: 'de situatie op het gebied van (informatie)beveiliging bij politie Nederland te verbeteren en zorg te dragen voor een homogeen niveau van beveiliging in het gehele politiedomein' De volgende doelstelling is het actualiseren van de leidraad BBNP: • Ontwikkeling van een weeginstrument; • Toetsen middels het weeginstrument; • Tekortkomingen blootleggen; • Ondersteunen bij implementatie ontbrekende controle; • Toets van de implementatie, waarbij de uitgangspunten zijn: • Actualisatie en toets beperkt tot de gebruikersorganisatie; • Leidend zijn de controls niet de maatregelen; • Maatregelen worden getoetst op relevantie.
2	Een bewustwordingsprogramma is aanwezig in de vorm van het aandacht besteden aan de onderwerpen privacy en (informatie)beveiliging in het begeleidingstraject van de aspiranten. Op die manier wordt geleerd dat beveiliging een integraal onderdeel is van elke medewerker van het korps. Volgens het Integraal (informatiebeveiligingsbeleid Zuid6 is één van de belangrijkste onderdelen van informatiebeveiliging bij de politie Zeeland het bevorderen van het bewustzijn onder de gebruikers van de informatie. Als de gebruikers namelijk niet op de hoogte zijn van de richtlijnen en regels hebben deze geen enkele uitwerking. Het risico is dan dat er fouten worden gemaakt waardoor beveiligingsincidenten ontstaan. Onderkend wordt dat door medewerkers bewust te maken van het belang van de veiligheid van de door hen gebruikte informatie, veel van die fouten kunnen worden voorkomen. Het beveiligingsbewustzijn wordt op de volgende wijze bevorderd: • Het publiceren van artikelen en informatie in nieuwsbrieven, op het intranet en in speciale handreikingen; • Aandacht besteden aan informatiebeveiliging in de verschillende interne opleidingen; • Directe aandacht van leidinggevenden door het ter sprake brengen op de werkvloer; • Organisatie van speciale workshops en presentaties rond beveiligingsthema's voor verschillende doelgroepen waaronder lijnmanagers, taakaccenthouders, maar ook eindgebruikers; • Voeren van periodiek overleg tussen alle in het korps aanwezige taakaccenthouders, onder voorzitterschap van de proceseigenaar informatie met ondersteuning van de IBF en de regionale privacy functionaris; • Terugkoppelen van de resultaten van gehouden controles en afhandeling van incidenten om zodanig mensen attent te maken op het belang van de informatiebeveiliging; • Voeren van periodiek Zuid6 overleg tussen alle IBF-ers en taakacccenthouders van de korpsen; • Deelnemen aan het landelijke IBF-netwerk c.q. virtueel kantoor door IBF of taakaccenthouder om ervaringen landelijk uit te wisselen. Een ander uitgangspunt van voornoemd informatiebeveiligingsbeleid is het "need-to-know, need-to-share" principe. Elke medewerker krijgt uitsluitend toegang tot de informatie die hij voor het uitvoeren van zijn functie en taken nodig heeft. De werkwijze is vastgelegd in het Autorisatiebeleid Zuid6. Onderkend wordt dat door de groeiende samenwerking zowel binnen als buiten de Nederlandse politie de noodzaak en verplichting om informatie te delen groter wordt dan ooit. Dit wordt ook vanuit de WPG voorgeschreven. In dat kader groeit ook het besef van het belang dat de gegevens die als basis dienen voor het delen van informatie betrouwbaar moeten zijn met het oog op de verbeterde samenwerking. Binnen het bestek van de privacy audit is niet meer getoetst of medewerkers op de hoogte zijn van hun taken, bevoegdheden en

ID	Bevindingen
	verantwoordelijkheden met betrekking tot de informatiebeveiliging.

ID	Aanbevelingen
1-2	Ga door op de ingeslagen weg van de vormgeving van informatiebeveiligingsbeleid en de implementatie ervan in Zuid6 verband.

2.1.5 Leiderschap

ID	Beheersdoelstellingen	V	D	N	A
1	Periodiek vaststellen dat beveiligingsmaatregelen naar behoren functioneren		X		X

ID	Bevindingen
1	Korpsbrede controle van beveiligingsmaatregelen is tot nu toe niet opgenomen in de planning- en controlcyclus van de politie Zeeland en wordt tot nu toe ook niet uitgevoerd. Eind 2008 is een Informatiebeveiligingsfunctionaris (IBF) aangesteld bij de regiopolitie Zeeland. Zijn functie houdt onder meer in: • Het adviseren van de portefeuillehouder inzake het te voeren (opstellen, bijstellen, herzien) informatiebeveiligingsbeleid en inzake het afstemmen van het informatiebeveiligingsbeleid van het korps met dat van andere korpsen; • Het uitdragen in het korps van de noodzaak van informatiebeveiliging en van de daarbij geldende beleidsbepalingen; • Het rapporteren aan de portefeuillehouder over de situatie van de informatiebeveiliging in het korps in het algemeen en van beveiligingsincidenten in het bijzonder; • Het adviseren van leidinggevenden, verantwoordelijk voor informatiesystemen of gemeenschappelijke IT-diensten, bij de uitwerking van het informatiebeveiligingsbeleid van het korps in informatiebeveiligingsplannen en bij de implementatie van die plannen; • Het adviseren van de portefeuillehouder en leidinggevenden inzake het maken van afspraken bij uitwisseling van gegevens; • Het evalueren, selecteren en voorstellen van toe te passen producten of werkwijzen met betrekking tot informatiebeveiliging; • Het bijhouden van de ontwikkelingen op het gebied van informatiebeveiliging. De IBF adviseert gevraagd en ongevraagd aan de hand van vraagstukken op zijn werkterrein. Van structurele controles op het terrein van de informatiebeveiliging conform een vooropgezet jaarplan of meerjarenplanning is geen sprake. De IBF houdt zich vooralsnog structureel bezig met bijdragen aan het beveiligingsbeleid en thans vooral op de gezamenlijk beleidsvorming in Zuid6 verband. Een recent voorbeeld hiervan is het concept Autorisatiebeleid Zuid-Nederland, versie 9 maart 2011. In het Informatiebeveiligingsbeleid Zuid 6 wordt aandacht besteed aan de toetsing en evaluatie van het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid is na inwerking treding twee jaar geldig, en wordt na de evaluatie geactualiseerd. IBF-Zuid onderhoudt dit beleid. Verder wordt aangegeven, dat in de jaarcyclus de evaluatie plaatsvindt aan de hand van controle-, interne audit-, incident- en managementrapportages op het gebied van invoering, naleving effectiviteit en efficiency. In de meerjarencyclus beoordeelt een onafhankelijke deskundige de opzet, bestaan en de werking van het informatiebeveiligingsbeleid en de beveiligingsmaatregelen. Deze externe audit vindt in het jaar voorafgaand aan een volgende cyclus plaats.

ID	Aanbevelingen
	Neem informatiebeveiliging als een vast onderdeel op in de managementcontrolcyclus. Neem de monitoring van de informatiebeveiliging in de politiepraktijk als een vast onderdeel op in de periodieke privacy audits.

Bijlage III: Overzicht geraadpleegde documenten

- Korpsbeschrijving Politie Zeeland
- Zelfevaluatie Politie Zeeland
- Jaarring 2008 Politie Zeeland (werkplan) politie Zeeland
- Jaarring 2009 Politie Zeeland (werkplan)
- Mappenstructuur O-schijf
- Jaarverslag PF + FG 2008
- Jaarverslag PF + FG 2009
- Jaarverslag Politie Zeeland 2008
- Jaarverslag Politie Zeeland 2009
- Jaarplan 2010 Politie zeeland
- Meerjarenbeleidplan 2008-2011 Politie Zeeland
- Korpsbekendmaking nr. 19
- Aanwijzing Bevoegd Functionarissen
- Inrichtingsplan Politie Zeeland
- Korpsbekendmaking nr. 21 Politie Zeeland
- Marap 2008 Politie Zeeland
- Marap 2009 Politie Zeeland
- Convenanten
- Overzicht E-learning WPG
- Implementatie WPG Politie Zeeland
- Samenwerkingsverbanden / Convenanten
- WPG in de mandaat regeling
- "Groene lijst"(overzicht applicaties)
- Werkplannen Teams 2010
- Korpsinformatie m.b.t. de invoering WPG
- Aanwijzing Interne auditor Politie Zeeland
- Overzicht maatschappelijke klassen BV
- Herverdeling portefeuilles
- Regeling Convenanten
- Modelconvenant JCO
- Nieuwsbrief KMT inzake IT-onderwerpen
- Zie verder de lijst met documenten in het interne auditdossier
- Informatiebeveiligingsbeleid Politie Zeeland 2008
- Integraal (informatie) beveiligingsbeleid Zuid6, 01-12-2010
- Gebruikershandleiding Telewerken vtsPN, 25-04-2011
  Autorisatiebeleid Zuid-Nederland, concept, 09-03-2011
- Jaarverslag Privacyfunctionaris 2010, 14-04-2011
- Besluit autorisatieprocedure Politie Zeeland, versie 1.0, 01-10-2008
- Handleiding procesdossier Zeeland, versie 2.0, 01-05-2005
- Werkproces Infodesk, Project Implementatie Wpg, versie 2.0 15 juli 2010
- [redacted]
- Handboek RID Politie Zeeland
- Gedragscode rechtstreekse verstrekking van politiegegevens aan leden van het Openbaar Ministerie Arrondissement Middelburg
- Handleiding/uitleg mappenstructuur O:schijf, versie 0.2, 03-05-2011
- Autorisatiematrix onderzoeksmappen Zuid6
- Autorisatiematrix beheer rollen onderzoeksmappen Zuid6
- Tabel 3: Standaard functie / rollen / schalen t.o.v. BlueView autorisaties
- Procesbeschrijving verwerking van politiegegevens artikel 8 en 9, versie 3.0, 24-06-2010.
- Instellingsprotocol voor het verder verwerken van politiegegevens ex artikel 13, eerste, tweede of derde lid, Wet politiegegevens, herkenningsdienstsysteem, art. 13.1 WPG
- Brief van Politie Taakorganisatie Vreemdelingen aan Regiopolitie Zeeland, inzake Landelijk reglement ex artikel 13 WPG d.d. 23 maart 2010

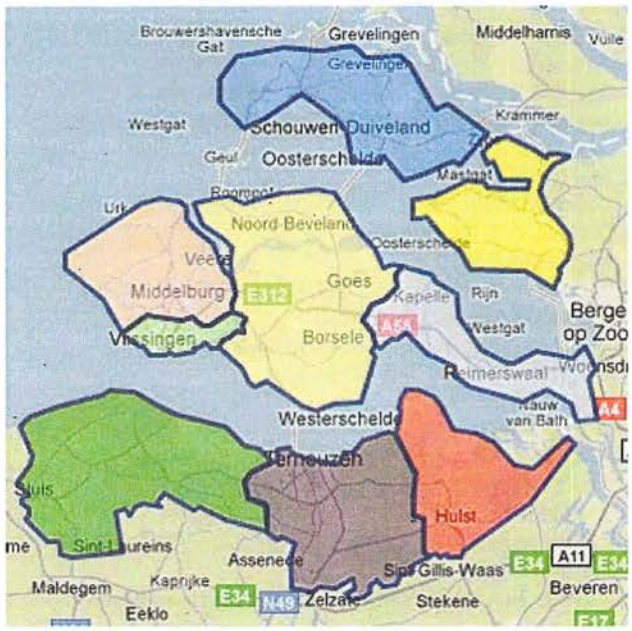
- Schriftelijke vastlegging als bedoeld in artikel 13, lid 4 van de Wet politiegegevens, genaamd Forensisch Opsporings Informatie Systeem, van de politieregio
- Schriftelijke vastlegging als bedoeld in artikel 13, lid 4 van de Wet politiegegevens, genaamd Verwijzingsindex Recherche Onderzoeken en Subjecten, van de politieregio
- Rapportage Definitieve Bevindingen van het College Bescherming Persoonsgegevens inzake Politie Infodesk II, juli 2009
- CBP Richtsnoeren ANPR De toepassing van automatische kentekenherkenning door de politie, januari 2009
- Landelijk afsprakenboek HKS, versie 4.7 definitief, d.d. oktober 2010
- Update procesmodel en –beschrijving "veiligheidsinformatie genereren", Programma Intelligence, versie 1.0, d.d. 4-12-2009
- Mail PF inzake schriftelijke vastlegging als bedoeld in art. 13, lid 4 van de Wet politiegegevens Protocol herkenningsdienstsysteem en P.V.'s, versie 0.4
- Mail met bijlagen van de PF: memo 18-5-2009 inzake Convenant 2009, memo 9-7-2008 inzake Aanwijzing PG's Reactieprotocol, Memo 3-3-2009 inzake inzet vertrouwenspersonen in interne onderzoeken, memo 17-2-2009 inzake Kernteam Stichting Welzijn X, memo 9-11-2009 inzake OGGZ (Wijktafel) X, memo 16-2-2009 inzake Werkafspraken risicoscreening vrouwenopvang, memo 28-1-2009 inzake intentieverklaring bevordering sociale veiligheid gemeente X, memo 10-2-2009 inzake Politie & schoolveiligheid, memo 23-6-2009 inzake veiligheidshuis, memo 20-1-2009 inzake Wijkscan gemeente X, memo 21-12-2010 inzake verstrekking aan burgemeester, memo 3-3-2010 inzake Cameratoezicht Koninginnedag 2010, memo 2-4-2007 inzake Mutaties huiselijk geweld, memo 17-2-2010 inzake gegevensuitwisseling t.b.v. fraudebestrijding, memo 25-3-2010 inzake Samenwerkingsovereenkomst Zeeland / X, memo 3-11-2010 inzake Stelsel bewaken en beveiligen
- Mail PF inzake gebruikersinstructie integrale bevraging III, januari 2011 versie 3.5
- Schriftelijke vastlegging als bedoeld in artikel 13, lid 4 van de Wet politiegegevens, genaamd Processen-verbaal en rapporten, van de politieregio
- Basis Voorziening Handhaving, Afspraken BVH en Handleiding gebruiker, versie 1.0 Zeeland, d.d. 1-10-2010 (2x)
- Lijst Maatschappelijke Klassen, BVH Servicepack 5, versie 2.1, d.d. 25-7-2010 (2x)
- Basis Voorziening Handhaving, gebruikersafspraken BVH, d.d. 28-9-2010
- Basis Voorziening Handhaving, Handleiding HOvJ, versie 1.0, 2009
- Matrix opdrachtverstrekking gegevensbeheer
- Schema mailverkeer True Blue na geconstateerde (mogelijke) fout in BVH
- Opdrachtverstrekking gegevensbeheer politie Zeeland, versie 2.3, d.d. september 2009
- Basis voorziening handhaving, Gebruikersafspraken BVH
- Power Point Presentatie BVH re-training oktober, november, december 2010
- Convenant inzake verstrekking van politiegegevens aan de AIVD
- De verstrekkingsgrondslag van artikel 7 van de Wet politiegegevens
- Mail IBF inzake Verstrekking gemeente en informatieverzoek Operationeel adviseurs
- Brief van Politie Zeeland aan College bescherming Persoonsgegevens d.d. 31-3-2009, inzake aanmelden privacy functionaris
- Besluit Informatie uitwisseling politie Zeeland in het kader van het samenwerkingsverband ROVZ, d.d. 1-12-2008, memo d.d. 26-1-2009 inzake discriminatie,
- Memo 23-4-2009, inzake Samenwerkingsovereenkomst Zeeland / X,
- Brief van Politie afdeling Politieberaden aan de leden van de Raad van korpschefs, d.d. 10-2-2011 inzake Convenant autorisatie RID voor CIE-info
- Mail PF d.d. 4-8-2010, bijlage Def. Verslag KMT d.d. 13-4-2010
- Mail PF inzake Gebruik BVO door collegae wijkteam in onderzoek, d.d. 9-11-2010
- Mail PF inzake Gegevensopslag woninginbraken, d.d. 20-1-2011
- Mail PF inzake Sepotafhandeling in BVH, d.d. 3-1-2011
- Mail PF inzake Overvallers op Deltanet, d.d. 7-2-2011
- Mail PF inzake Verstrekken politiegegevens, d.d. 25-1-2011
- Mail PF inzake Afloopberichten, d.d. 9-2-2011
- Mail PF inzake Gegevensopslag HG-EGG-SBB, d.d. 6-1-2011

- Mail PF inzake Bijwonen werkoverleg RT1, d.d. 20-1-2011
- Mail PF inzake Opslag 9e verwerking O-schijf, d.d. 9-2-2011
- Mail PF inzake procesbeschrijving art 8+9.doc, d.d. 9-2-2011
- Mail PF inzake Convenant, d.d. 15-4-2009
- Mail PF inzake Uitnodiging projectleidersdag 13 februari, d.d. 28-1-2009
- Mail PF inzake Presentatie Bevoegd Functionaris, d.d. 19/1/2009, bijlage Seminar BF(1).PPT
- Mail PF inzake Map kantoorautomatisering, d.d. 6-2-2009
- Mail PF inzake Mappenstructuur O-schijf, d.d. 26-1-2009
- Mail PF inzake Notitie beslotenheid BVH, d.d. 5-3-2009, bijlagen: 250708 Aanwijzing Wet Politiegegevens.pdf; meldingsformulier embargo-onderzoek.doc
- Mail PF inzake Link naar verstrekkingenwijzer, d.d. 27-4-2009
- Mail PF inzake Brief aanmelding privacyfunctionaris, d.d. 2-3-2009
- Mail PF inzake X, d.d. 18-2-2009
- Mail PF inzake Opslag gegevens, d.d. 21-1-2009
- Mail PF inzake Overzichtlijst art. 9 verwerkingen, d.d. 3-3-2009
- Mail PF inzake Politie & Veiligheid, d.d. 10-2-2009, bijlagen Memo advies Samenwerking en incidentele verstrekkingen
- Mail PF Presentatie werkgroep recherche, d.d. 20-4-2009
- Mail PF inzake 2 daagse wpg training, d.d. 5-3-2009
- Mail PF inzake Samenwerkingsverband aanpak huurdersoverlast gemeente Middelburg.doc, d.d. 16-3-2009
- Mail PF inzake Artikel 8, d.d. 16-2-2009
- Mail PF inzake Bewijs goed gedrag, d.d. 21-1-2009
- Mail PF inzake Info m.b.t. winkeldiefstal, d.d. 5-2-2009
- Mail PF inzake Informeren school, d.d. 12-3-2009
- Mail PF inzake Kennis, d.d. 16-3-2009
- Mail PF inzake Lijsten met telefoonnummers, d.d. 2-2-2009
- Mail PF inzake Mappen structuur, d.d. 23-3-2009
- Mail PF inzake Nieuwe onderzoeksregistratie, d.d. 9-4-2009
- Mail PF inzake Overleg Zuid-6, d.d. 16-2-2009
- Mail PF inzake Overzicht mee te nemen registraties.xls, d.d. 2-2-2009
- Mail PF inzake Privacy, d.d. 12-2-2009
- Mail PF inzake Reminder PD, d.d. 22-1-2009
- Mail PF inzake Seminar bevoegd functionaris, d.d. 5-1-2009
- Mail PF inzake Ter beschikking stellen, d.d. 20-1-2009
- Mail PF inzake Uitwisselen gegevens, d.d. 18-3-2009
- Mail PF inzake Vernietiging vingerafdrukken en verdachtenfoto's, d.d. 27-3-2009
- Mail PF inzake Verstrekken aan nabestaande, d.d. 22-1-2009
- Mail PF inzake Verstrekken PV bevindingen, d.d. 5-2-2009
- Mail PF inzake Vraagje m.b.t. privacy, d.d. 4-2-2009
- Mail PF inzake Vraagje over verstrekking, d.d. 2-3-2009
- Mail PF inzake Werkafspraken politie / vrouwenopvang, d.d. 16-2-2009, bijlage memo werkafspraken risicoscreening 16/2/2009.doc
- Mail PF inzake Werkgroep Zuid-6 autorisaties, d.d. 5-1-2009
- Mail PF inzake WPG, d.d. 5-3-2009
- Mail PF inzake Regeling periodieke audit politiegegevens, d.d. 6-1-2009
- Mail PF inzake ROVZ verstrekkingen, d.d. 17-3-2009
- Mail PF inzake SOZ, d.d. 16-4-2009, bijlage Wijziging uitvoeringsregeling AWR.htm
- Mail PF inzake Stukje intranet, d.d. 27-4-2009, bijlage Publicatie Deltanet 2009.doc
- Mail PF inzake Ter beschikking stellen, d.d. 20-1-2009
- Mail PF inzake Terugkoppeling, d.d. 21-1-2009
- Mail PF inzake Toezending stukken ROVZ, d.d. 3-3-2009
- Mail PF inzake Tolken, d.d. 4-3-2009
- Mail PF inzake Vernietiging vingerafdrukken en verdachtenfoto's, d.d. 25-3-2009
- Mail PF inzake Verstrekken personalia aan ambulancedienst, d.d. 24-3-2009
- Mail PF inzake DL S ZLD Communicatie, betreft verstrekkingenwijzer, d.d. 27-4-2009, bijlage verstrekkingenwijzer Definitief 17042009.pdf
- Mail PF inzake Voorlichting aspiranten, d.d. 5-1-2009

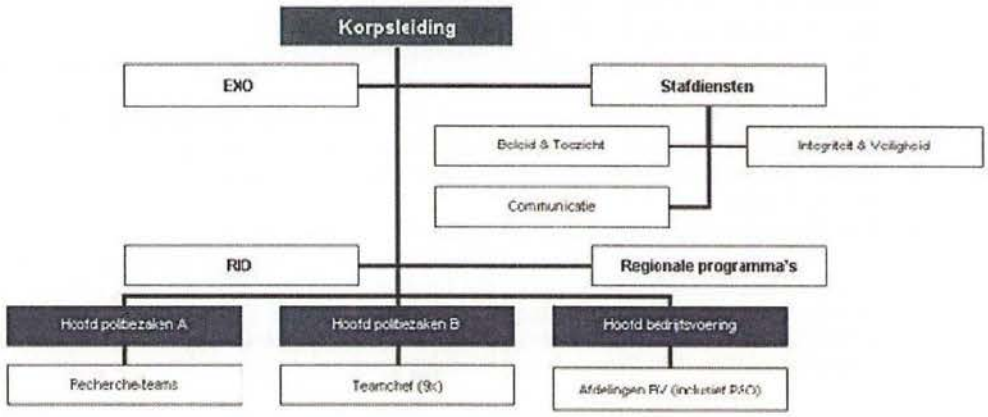
- Mail PF inzake Aanwijzing bevoegd functionaris CIE.doc
- Mail PF inzake Dossiernr PL XXX, d.d. 13-1-2009
- Mail PF inzake Privacyvraagstuk, d.d. 13-1-2009
- Mail PF inzake Diepteonderzoek naar ernstige bermongevallen, d.d. 2-2-2009
- Mail PF inzake Wapenregistratiesysteem, d.d. 1-4-2009
- Mail PF inzake Var Project.ppt, d.d. 12-1-2009
- Mail PF inzake Bijeenkomst Zuid 6, d.d. 17-2-2009
- Mail PF inzake Bsn benadeelden, d.d. 19-1-2009
- Mail PF inzake Bijeenkomst Zuid 6, d.d. 17-2-2009
- Mail PF inzake Vernietiging vingerafdrukken verdachtenfoto's, d.d. 25-3-2009
- Mail PF inzake Beantwoording vragen WOB verzoek, d.d. 23-3-2009, bijlagen 20090303.beantwoording WOB.doc, 20090203.WOB verzoek, 13-3-2009 concept p b wob.DOC
- Mail PF inzake Bijeenkomst Zuid 6, d.d. 17-2-2009
- Mail PF inzake Inspoelen PDA´s, d.d. 3-3-2009
- Mail PF inzake Mappenstructuur O-schijf, d.d. 26-1-2009
- Mail PF inzake uitwisselen gegevens, d.d. 17-3-2009
- Mail PF inzake Huurdersoverlast Gemeente X, d.d. 25-3-2009, bijlage Besluit informatie-uitwisseling Huurdersoverlast Middelburg 2009.doc
- Mail PF inzake Huurdersoverlast, d.d. 1-4-2009, bijlage Convenant en Besluit informatie-uitwisseling Huurdersoverlast Gemeente X 2009.doc
- Mail PF inzake Interventieteam X, d.d. 31-3-2009
- Mail PF inzake Inzageverzoek, d.d. 26-1-2009
- Mail PF inzake WPG Audit, d.d. 9-8-2010
- Mail PF inzake Servicedesk-Zuid, betreft Opvragen autorisaties, d.d. 5-1-2009
- Mail PF inzake Autorisaties, d.d. 5-1-2009
- Mail PF inzake Overzicht mee te nemen registraties ZLD.xls, d.d. 21-1-2009, bijlage Overzicht mee te nemen registraties ZLD.xls
- Mail PF inzake Tolken accounts en het overspringen van tekst naar raadpleegmodus, d.d. 28-1-2009
- Mail PF inzake Overzicht mee te nemen registraties ZLD.xls, d.d. 2-2-2009, bijlage Overzicht mee te nemen registraties ZLD.xls
- Mail PF inzake Overzichten, d.d. 5-2-2009, bijlage CC0000002596460.doc, CC0000002596460.xls
- Mail PF inzake Accounts welke na 31/12 expired zijn, d.d. 6-2-2009
- Mail PF inzake WPG/stadswachten, d.d. 9-2-2009
- Mail PF inzake Tolkenaccounts, d.d. 12-2-2009
- Mail PF inzake Intrekken autorisaties (herhaling), d.d. 17-2-2009
- Mail PF inzake Implementeren WPG, d.d. 18-2-2009
- Mail PF inzake Autorisatieformulier GBA online, d.d. 3-3-2009, bijlage AutorisatieformulierGBAonline Politie Zeeland.doc
- Mail PF inzake Privacy d.d. 4-3-2009
- Mail PF inzake Casus autorisatie, d.d. 4-3-2009, bijlage vragenformulier helpdesk.doc
- Mail PF inzake rectificatie, d.d. 5-3-2009
- Mail PF inzake BlueView voor analyse, d.d. 9-3-2009, bijlage AF0903091015.doc
- Mail PF inzake Autorisatie verstrekken aan uitzendkrachten, d.d. 12-3-2009
- Mail PF inzake Bevragingen door gebruikers Verificatie Module (v/h GBA-Online), d.d. 23-3-2009
- Mail PF inzake Wachtwoord, d.d. 25-3-2009
- Van PF inzake Toegangscontrole, d.d. 7-4-2009, bijlagen concept toegangscontrole Zeeland.doc, Zeeland Advies autorisatie toegangscontrole-1.doc, Zeeland Advies autorisatie toegangscontrole-2.doc, Zeeland Advies autorisatie toegangscontrole-3.doc, Concept Leidraad Rubricering.doc, Bijlage 1 Groepsindeling toegangscontrole.doc, Bijlage 3 Autorisatietabel toegangscontrole.xls

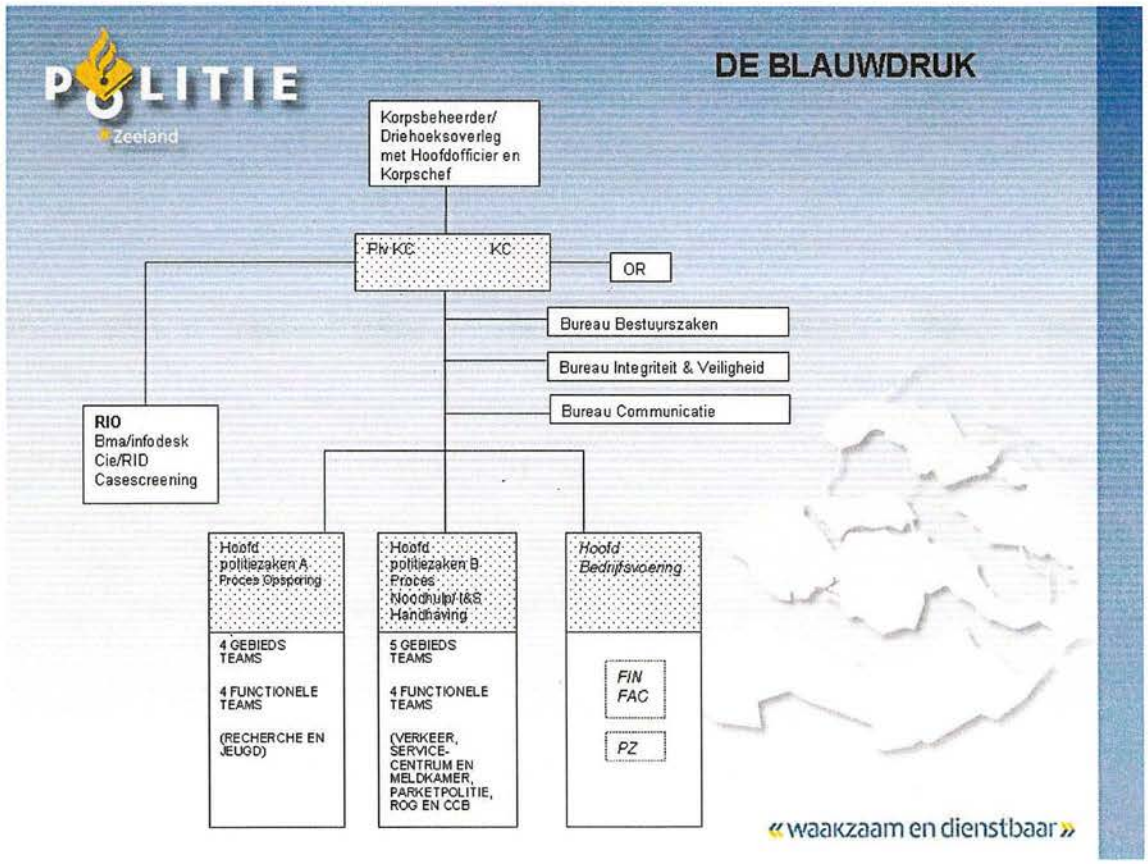
Bijlage IV: Overzicht van de organisatie- en informatiestructuur van Politie Zeeland

Politie Zeeland geografisch



Organogram werkorganisatie Politie Zeeland





Politie Zeeland is onderverdeeld in 9 werkgebieden:

- Schouwen-Duiveland;
- Tholen;
- Kapelle / Reimerswaal;
- Goes / Borsele / Noord-Beveland;
- Middelburg / Veere;
- Sluis;
- Terneuzen;
- Hulst;
- Vlissingen.

De divisie Recherche bestaat uit:

- Rechercheteam 1 (Walcheren);
- Rechercheteam 2 (Oosterscheldebekken);
- Rechercheteam 3 (Zeeuws-Vlaanderen);
- Regionaal Recherche Team (RRT);
- Bureau Project Voorbereiding (BPV);
- Bureau Bijzondere Recherche Expertise (BBRE);
- Bureau Bijzondere Recherche Ondersteuning (BBRO);
- Regionaal Milieu Team (RMT).

(Het Bureau Project Voorbereiding is niet in de privacy audit meegenomen)

De Regionale Informatie Organisatie (RIO) bestaat uit:
- Bureau Casescreening (BSC);
- Bureau Misdaad Analyse (BMA);
- Infodesk;
- Criminele Inlichtingen Eenheid (CIE);
- Regionale Inlichtingen Dienst (RID).

(Het Bureau Casescreening is niet in de privacy audit meegenomen.)

De divisie Executieve Ondersteuning (EXO) bestaat uit:
- Forensische Opsporing (FO);
- Jeugdpolitie;
- Regionale Ondersteunings Groep (ROG);
- Servicecentrum;
- Conflict- en Crisis Beheersing (CCB);
- Parketpolitie;
- Verkeerspolitie;
- Vreemdelingenpolitie (VP);
- Totaal Bekeuring Informatie Afhandelings Systeem (Tobias).

(De divisie EXO is met uitzondering van de Forensische opsporing, de Jeugdpolitie, de Vreemdelingenpolitie en de Verkeerspolitie niet in de privacy audit meegenomen.)

Verdeling processen & portefeuilles

Indien specifieke beleidsterreinen (doorgaans) tijdelijk maar soms ook langdurig, extra aandacht vergen kan het KMT besluiten tot het aanstellen van een portefeuillehouder. Het gaat daarbij doorgaans om producten waarvan het niet leveren politiek bestuurlijk gevoelig ligt en daarom aandacht of begeleiding vragen. De portefeuillehouder adviseert de proceseigenaar over de inrichting van het proces.

Portefeuillehouders kunnen worden belast met taken zoals het voeren van overleg in- en extern, het voorbereiden van het veiligheidsbeleid, het monitoren van het werk etc.
Zoveel mogelijk wordt de opzet in lijn gebracht met de verdeling van de portefeuilles op landelijk niveau onder de hoofdprocessen Intake, Noodhulp, Handhaving, Opsporing en adviseren signaleren. De hoofdprocessen zijn eigendom van de KMT-leden.

1. De **korpschef** is verantwoordelijk voor het proces besturen en de portefeuilles:
- Veilige Publieke taak;
- Publiek Private Samenwerking;
- Control;
- Integriteit en omgangsvormen.

2. De **plv korpschef** is verantwoordelijk voor de processen voorbereiden en verbeteren en de portefeuilles Intelligence en terrorisme, portefeuille opsporing (verantwoordelijkheid KL)

3. Het **hoofd bedrijfsvoering** voor het proces ondersteunen waaronder:
- In-door-uitstroom, ontwikkeling processen en opleiding;
- Personeelszorg en arbeidsvoorwaarden;
- Financiën;
- Facility management.

4. Het **hoofd politiezaken A** voor het uitvoerende proces Opsporing waaronder:
- Tactische opsporing;
- Forensische Opsporing;
- Vermogenscriminaliteit;
- Zeden, veelpleger en openlijk geweld;
- Milieucriminaliteit;
- Rechtshulp;

- Vreemdelingen.

5. Het **hoofd politiezaken B** voor de uitvoerende processen Intake Noodhulp en handhaving waaronder:
- Verkeer;
- Milieu(handhaving) en Bijzondere wetten;
- Jeugd;
- Conflict en crisisbeheersing;
- Meldkamerdomein.

Bijlage V: Transponeringstabel WPG / BPG

Toelichting

Deze transponeringstabel volgt de hoofdstukken met de onderwerpen en de id nrs in de bijlage I.
Toegevoegd zijn de scores:
OV= de opzet is voldoende;
OD= deficiëntie in de opzet;
BV= het bestaan is voldoende;
BD= deficiëntie in het bestaan.

1.1 GO: Gebruikersorganisatie

1.1.1 Inrichting van de organisatie

ID	Artikel	Toelichting	V	D	N	A
1	4.3 WPG	OD/BD		X		X
1		OD/BD		X		X
2		OD/BD		X		X
3		OD/BD		X		X
4		OD/BD		X		X
5		OD/BD		X		X
6	6.7 WPG;	OV/BD		X		X
6	2:10 BPG	OV/BD		X		X

1.2 Artikel 8 (verwerking voor de dagelijkse politietaak)

1.2.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	3.1 WPG	OV/BV	X			
2	8.1 WPG	OV/BD		X		X
3	1 WPG; 32.2 WPG	-	-			
4	5 WPG	OD/BV		X		X
5	3.2 WPG	OD/BV		X		X
6	3.2 WPG	OV/BV	X			
7	3.3 WPG	OD/BV		X		X

1.2.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OV/BV	X			
2	4.2 WPG	OV/BD (=i24)		X		X
3	4.3 WPG	OD/BD		X		X
4	4.4 WPG	OD/BV		X		X
5	4.5 WPG	OD/BV		X		X
6	4.6 WPG	OD/BD		X		X

1.2.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BD (BD v.w.b. de-autoriseren)		X		X
2	6.2 WPG	OV/BD		X		X
3	6.3 WPG	OV/BD		X		X
4	6.4 WPG	OV/BD		X		X
5	6.5 WPG	OV/BD		X		X

1.2.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	8.1 WPG;8.1 MVT	OD/BD (BD v.w.b. informatiesystemen niet ingericht)		X		X
1	8.1 WPG;8.1 MVT	OD/BD		X		X
2	8.2 WPG	OD/BD		X		X
2	8.2 WPG	OD/BD		X		X
3	8.4 WPG	OD/BD		X		X

1.2.5 In combinatie met elkaar verwerken

ID	Artikel	Toelichting	V	D	N	A
1	8.3 WPG	-	-			X
2	8.4 WPG	-	-			
3	32 WPG; 6:4.2 BPG	-	-			
4	2:1 BPG	-	-			
5	2:9 BPG	-	-			

1.2.6 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	8.6 WPG; 4.2 WPG	OD/BD		X		X
2	14.1 WPG	OD/BD		X		X
3	14.2 WPG	OD/BD		X		X
4	14.3 WPG	OD/BD		X		X
5	32 WPG; 6:4.2 BPG; 6:4.3 BPG	OD/BD		X		X
6	14.4 WPG	OD/BD		X		X

1.2.7 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG	OD/BV		X		X
2	8.4 WPG	OD/BV		X		X
3	13.1 WPG	OD/BV		X		X
4	13.2 WPG; 6:2 BPG	OD/BV		X		X
5	13.3 WPG	OD/BV		X		X
6	15.2 WPG; 2:13.1 BPG	OD/BV		X		X
7	7 WPG; 4:8 BPG	OV/BV	X			

1.2.8 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG	OD/BD		X		X
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG	OD/BD		X		X
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG	OD/BD		X		X
4	7 WPG; 4:8 BPG	OD/BD		X		X

1.3 Artikel 9 (verwerking voor de rechtsorde in een bepaald geval)

1.3.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	9.1 WPG; 3.1 WPG	OV/BV	X			
2	9.2 WPG; 32.1 WPG;6:4.1 BPG	OV/BV	X			
3	1 WPG; 32.2 WPG	-	-			
4	5 WPG	OD/BV		X		X
5	1 WPG; 32.2 WPG	OD/BV		X		X
6	3.2 WPG	OD/BV		X		X
7	3.2 WPG	OD/BV		X		X
8	3.3 WPG	OD/BV		X		X

1.3.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OD/BD		X		X
2	4.1 WPG	OD/BD		X		X
3	4.3 WPG	OD/BD		X		X
4	4.4 WPG	OD/BD		X		X
5	4.5 WPG	OD/BV		X		X
6	4.6 WPG	OD/BD		X		X

1.3.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BD (BD v.w.b. de autoriseren)		X		X
2	6.2 WPG	OV/BD		X		X
3	6.3 WPG	OV/BD		X		X
4	6.4 WPG	OV/BD		X		X
5	6.5 WPG	OV/BD		X		X

1.3.4 Geautomatiseerd vergelijken

ID	Artikel	Bevindingen	V	D	N	A
1	11.1 WPG; 2:10 BPG	OV/BD	X			X
2	2:2.1 BPG	OV/BD	X			
3	2:9 BPG	OV/BD	X			
4	2:11 BPG; 2:10.1 BPG; 2:13.1 BPG	OV/BD	X			
5	2:10.1 BPG; 2:12 BPG	OV/BD	X			
6	11.5 WPG	OV/BD	X			
7	6:4.2 BPG	OV/BD	X			
8	6:4.3 BPG	OV/BD	X			

1.3.5 In combinatie met elkaar verwerken

ID	Artikel	Toelichting	V	D	N	A
1	11.4 WPG; 2:10.1 BPG	-	-			X
2	2:2.2 BPG; 2:2.3 BPG	-	-			
3	2:9 BPG	-	-			
4	2:11 BPG	-	-			
5	2:12 BPG	-	-			
6	6:4.2 BPG	-	-			
7	6:4.3 BPG	-	-			

1.3.6 Bewaartermijnen en vernietiging

ID	Artikel	Bevindingen	V	D	N	A
1	9.4 WPG; 4.2 WPG	OD/BD		X		X
2	14.1 WPG	OD/BD		X		X
3	14.2 WPG	OD/BD		X		X
4	14.3 WPG	OD/BD		X		X
5	6:4.3 BPG	OD/BD		X		X
6	14.4 WPG	OD/BD		X		X

1.3.7 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG	OD/BD		X		X
2	9.3 WPG; 2:10.1 BPG	OD/BD		X		X
3	13.1 WPG; 6:2 BPG	OD/BD		X		X
4	13.2 WPG	OD/BD		X		X
5	13.3 WPG	OV/BV	X			
6	15.2 WPG; 2:13.1 BPG	OD/BV		X		X
7	7 WPG; 4:8 BPG	OD/BV		X		X

1.3.8 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG	OD/BV		X		X
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG	OD/BV		X		X
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG	OD/BV/-		X		X
4	7 WPG; 4:8 BPG	OD/BV		X		X

1.4 Artikel 10,1A CIE (verkrijgen van inzicht in betrokkenheid personen)

1.4.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	10.1 WPG; 3:1 BPG	OV-BV	X			
2	10.2 WPG	OV/BV	X			X
3	1 WPG; 32.2 WPG	-	-			
4	5 WPG	OV/BV	X			
5	3.2 WPG	OV/BV	X			
6	3.2 WPG	OV/BV	X			
7	3.3 WPG	OV/BV	X			
8	3.4 WPG	OV/BV	X			

1.4.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OV-BV	X			
2	4.1 WPG	OV/BD		X		X
3	4.3 WPG	OV/BV	X			
4	4.4 WPG	OD/BV		X		X
5	4.5 WPG	OD/BV		X		X
6	4.6 WPG	OD/BV		X		X

1.4.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BV	X			X
2	6.2 WPG	OV/BV	X			X
3	2:5.1 BPG	OV/BV	X			
4	2:6 BPG	OV/BD		X		X
5	2:9 BPG	OV/BV	X			

1.4.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	11.2 WPG; 2:10.1 BPG	OV/BV	X			X
2	2:2.2 BPG; 2:2.3 BPG	OV/BV	X			
3	2:9 BPG	OV/BV	X			
4	2:11 BPG	OV/BV	X			
5	2:10.1 BPG; 2:12 BPG	OV/BV	X			
6	11.5 WPG	OV/BV	X			
7	6:4.2 BPG	OV/BV	X			
8	6:4.3 BPG	OV/BV	X			

1.4.5 In combinatie met elkaar verwerken

ID	Artikel	Toelichting	V	D	N	A
1	11.4 WPG; 2:10.1 BPG	OV/-	X			
2	2:2.2 BPG; 2:2.3 BPG	-	-			
3	2:9 BPG	-	-			
4	2:11 BPG	-	-			
5	2:12 BPG	-	-			
6	6:4.2 BPG	-	-			
7	6:4.3 BPG	-	-			

1.4.6 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	10.6 WPG; 4.2 WPG	OV/BD		X		
2	14.1 WPG	OV/BD		X		
3	14.2 WPG	OV/BV	X			
4	14.3 WPG	OV/BV	X			
5	6:4.3 BPG	OV/BV	X			
6	14.4 WPG	OD/BV		X		X

1.4.7 Ter beschikking stellen van politiegegevens

ID	Artikel	Bevindingen	V	D	N	A
1	15.1 WPG; 6.2 WPG	OV/BV/	X			
2	10.5 WPG; 2:10 BPG	OV/BV	X			
3	13.1 WPG; 6:2 BPG	OV/BV	X			
4	13.2 WPG	OV/BV	X			
5	13.3 WPG	OV/BV	X			
6	15.2 WPG; 2:13.1 BPG	OV/BV	X			
7	7 WPG; 4:8 BPG	OV/BV	X			

1.4.8 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG	OV/BV	X			
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG	OV/BV	X			
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG	OV/BV	X			
4	7 WPG; 4:8 BPG	OV/BV	X			

1.5 Artikel 10,1B Themaverwerking (verkrijgen van inzicht in betrokkenheid personen)

1.5.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Bevindingen	V	D	N	A
1	10.1 WPG; 3:1 BPG	Tijdens de interne audit maar ook tijdens de privacy audit is geruime tijd aandacht besteed aan de vraag of er bij de Vreemdelingenpolitie sprake is van een verwerking als bedoeld in artikel 10, lid 1, onder b, WPG, de zogenaamde themaverwerking op het terrein van mensensmokkel / mensenhandel. Uiteindelijk is voorzichtig de conclusie getrokken, dat er bij de VP sprake zou kunnen zijn van een verwerking als bedoeld in voornoemd artikel voor zover het betreft mensenhandel als bedoeld in art. 273f WvSr en mensensmokkel als bedoeld in art. 197a WvSr. Door capaciteits- en tijdgebrek zijn een aantal onderwerpen bij de VP niet toereikend in de interne audit en de externe audit onderzocht. Om die reden wordt in deze paragraaf en de hierna volgende paragrafen waar dit relevant is volstaan met de weergave van de bevindingen en de aanbevelingen.				X
2	10.3 WPG					X
3	1.f.6° WPG; 32.2 WPG					X
4	5 WPG					X
5	3.2 WPG					X
6	3.2 WPG					X
7	3.3 WPG					X
8	3.4 WPG					X

1.5.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG					X
2	4.1 WPG					X
3	4.3 WPG					X
4	4.4 WPG					X

ID	Artikel	Toelichting	V	D	N	A
5	4.5 WPG					X
6	4.6 WPG					X

1.5.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG					X
2	6.2 WPG					X
3	2:4.1 BPG; 2:4.2 BPG					X
4	2:6 BPG					X
5	2:9 BPG					X

1.5.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	11.2 WPG; 2:10.1 BPG					X
2	2:2.2 BPG; 2:2.3 BPG					X
3	2:9 BPG					X
4	2:11 BPG					X
5	2:10.1 BPG; 2:12 BPG					X
6	11.5 WPG					X
7	6:4.2 BPG					X
8	6:4.3 BPG					X

1.5.5 In combinatie met elkaar verwerken

ID	Artikel	Toelichting	V	D	N	A
1	11.4 WPG; 2:10.1 BPG					
2	2:2.2 BPG; 2:2.3 BPG					
3	2:9 BPG					
4	2:11 BPG					
5	2:12 BPG					
6	6:4.2 BPG					
7	6:4.3 BPG					

1.5.6 Bewaartermijnen en vernietiging

ID	Artikel	Bevindingen	V	D	N	A
1	10.6 WPG; 4.2 WPG					X
2	14.1 WPG					X
3	14.2 WPG					X
4	14.3 WPG					X
5	6:4.3 BPG					X
6	14.4 WPG					X

1.5.7 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG					X
2	10.5 WPG; 2:10.1 BPG					X
3	13.1 WPG; 6:2 BPG					X
4	13.2 WPG					X
5	13.3 WPG					X
6	15.2 WPG; 2:13.1 BPG					X
7	7 WPG; 4:8 BPG					X

1.5.8 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG					X
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG					X
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG					X

ID	Artikel	Toelichting	V	D	N	A
4	7 WPG; 4:8 BPG	.				X

1.6 Artikel 10,1C RID (verkrijgen van inzicht in betrokkenheid personen)

1.6.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	10.1 WPG; 3:1 BPG	OV-BV	X			
2	10.4 WPG	OV/BV	X			
3	1.f.6° WPG; 32.2 WPG	-	-			
4	5 WPG	OV/BV	X			
5	3.2 WPG	OV/BV	X			
6	3.2 WPG	OV/BV	X			
7	3.3 WPG	OV/BV	X			
8	3.4 WPG	0V/BV	X			

1.6.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OV/BV	X			
2	4.1 WPG	OV/BV	X			
3	4.3 WPG	OV/BV	X			
4	4.4 WPG	OD/BD		X		X
5	4.5 WPG	OD/BD		X		X
6	4.6 WPG	-	-			

1.6.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BV	X			
2	6.2 WPG	OV/BV	X			
3	2:5.2 BPG; 2:5.3 BPG	-	-			
4	2:6 BPG	OV/BV	X			
5	2:9 BPG	OV/BV	X			

1.6.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	11.2 WPG; 2:10.1 BPG	OV/BV	X			X
2	2:2.2 BPG; 2:2.3 BPG	OV/BV	X			
3	2:9 BPG	OV/BV	X			
4	2:11 BPG	OV/BV	X			
5	2:10.1 BPG; 2:12 BPG	OV/BV	X			
6	11.5 WPG	OV/BV	X			
7	6:4.2 BPG	OV/BV	X			
8	6:4.3 BPG	OV/BV	X			

1.6.5 In combinatie met elkaar verwerken

ID	Artikel	Toelichting	V	D	N	A
1	11.4 WPG; 2:10.1 BPG	OV/-	X			
2	2:2.2 BPG; 2:2.3 BPG	-	-			
3	2:9 BPG	-	-			
4	2:11 BPG	-	-			
5	2:12 BPG	-	-			
6	6:4.2 BPG	-	-			
7	6:4.3 BPG	-	-			

1.6.6 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	10.6 WPG; 4.2 WPG	OV/BD		X		X

ID	Artikel	Toelichting	V	D	N	A
2	14.1 WPG	OV/BD		X		X
3	14.2 WPG	OV/BV	X			
4	14.3 WPG	OV/BV	X			
5	6:4.3 BPG	OV/BV	X			
6	14.4 WPG	OD/BD		X		X

1.6.7 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG	OV/BV	X			
2	10.5 WPG; 2:10.1 BPG	OV/BV	X			
3	13.1 WPG; 6:2 BPG	OD/BD		X		X
4	13.2 WPG	OD/BD		X		X
5	13.3 WPG	OD/BD		X		X
6	15.2 WPG; 2:13.1 BPG	OV/BV	X			
7	7 WPG; 4:8 BPG	BV	X			

1.6.8 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG	OV/BV	X			
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG	OV/BV	X			
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG	OV/BV	X			
4	7 WPG; 4:8 BPG	OV/BV	X			

1.7 Artikel 12 Informanten CIE

1.7.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	12.1 WPG; 12.7 WPG	OV/BV	X			
2	12.3 WPG	OV/BV	X			
3	1.f.6° WPG; 32.2 WPG	-	-			
4	5 WPG	OV/BV	X			
5	3.2 WPG	OV/BV	X			
6	3.2 WPG	OV/BV	X			
7	3.3 WPG	OV/BV	X			
8	3.4 WPG	OV/BV	X			

1.7.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OV/BV	X			
2	4.1 WPG	OV/BV	X			
3	4.3 WPG	OV/BV	X			
4	4.4 WPG	OD/BD		X		X
5	4.5 WPG	ODBD		X		X
6	4.6 WPG	OD/-		X		X

1.7.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BV	X			
2	6.2 WPG	OV/BV	X			
3	2:3.1 BPG	OV/BV	X			
4	2:3.6 BPG	OV/BV	X			
5	2:6 BPG	OV/BV	X			
6	2:9 BPG	OV/BV	X			

1.7.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	12.4 WPG	OV/BV	X			X
2	2:3.4 BPG; 2:3.5 BPG	OV/BV	X			
3	2.9 BPG	OV/BV	X			

1.7.5 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	12.6 WPG; 4.2 WPG	0V/BV	X			

1.7.6 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 12.2 WPG	OV/BV	X			
2	15.2 WPG; 2:13.1 BPG	OV/BV	X			
3	7 WPG; 4:8 BPG	OV/BV	X			

1.8 Artikel 12 Informanten RID

1.8.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	12.1 WPG; 12.7 WPG	OV-BV	X			
2	12.3 WPG	OV/BV	X			
3	1 WPG; 32.2 WPG	-	-			
4	5 WPG	OV/BV	X			
5	3.2 WPG	OV/BV	X			
6	3.2 WPG	OV/BV	X			
7	3.3 WPG	OV/BV	X			
8	3.4 WPG	OV/BV	X			

1.8.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG	OV/BV	X			
2	4.1 WPG	OV/BV	X			
3	4.3 WPG	OV/BV	X			
4	4.4 WPG	OD/BD		X		X
5	4.5 WPG	OD/BD		X		X
6	4.6 WPG	-	X			

1.8.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG	OV/BV	X			
2	6.2 WPG	OV/BV	X			
3	2:3.1 BPG	OV/BV	X			
4	2:3.6 BPG	OV/BV	X			
5	2:6 BPG	-	-			
6	2:9 BPG	OV/BV	X			

1.8.4 Geautomatiseerd vergelijken

ID	Artikel	Toelichting	V	D	N	A
1	12.4 WPG	OV/BV	X			
2	2:3.4 BPG; 2:3.5 BPG	OV/BV	X			
3	2.9 BPG	OV/BV	X			

1.8.5 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	12.6 WPG; 4.2 WPG	OV/BV	X			

1.8.6 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 12.2 WPG	OV/BV	X			
2	15.2 WPG; 2:13.1 BPG	OV/BV	X			
3	7 WPG; 4:8 BPG	OV/BV	X			

1.9 Artikel 13 (landelijke registers)

1.9.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	13.1 WPG	Over artikel 13 verwerkingen is landelijk discussie gaande. De onderwerpen in dit hoofdstuk zijn in de interne audit en de privacy audit vanwege capaciteits- en tijdgebrek niet toereikend onderzocht. Volstaan is met summiere bevindingen en aanbevelingen.				X
2	13.4 WPG; 31.1 WPG: 32.3 WPG; 33.4 WPG; 6:2 BPG					X
3	1° WPG; 32.2 WPG		-			
4	5 WPG					X
5	3.2 WPG					X
6	3.2 WPG					X
7	3.3 WPG					X

1.9.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG					X
2	4.1 WPG					X
3	4.3 WPG					X
4	4.4 WPG					X
5	4.5 WPG					X
6	4.6 WPG					X

1.9.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG					X
2	6.2 WPG					X
3	6.3 WPG					X
4	6.4 WPG					X
5	6.5 WPG					X

1.9.4 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	4.2 WPG; 13.4 WPG; 32.1 WPG; 32.3 WPG; 32.4 WPG; 6:2 BPG	-				X

1.9.5 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG	-				X
2	13.1 WPG; 6:2 WPG	-				X
3	15.2 WPG; 2:13.1 BPG	-				X
4	7 WPG; 4:8 BPG	-				X

1.9.6 Verstrekkingen

ID	Artikel	Bevindingen	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG	-				X
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG	-				X
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG	-				X
4	7 WPG; 4:8 BPG	-				X

1.10 Artikel 13 (VROS-taak)

1.10.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	13.3 WPG; 2:10.1 BPG	Over artikel 13 verwerkingen is landelijk discussie gaande. De onderwerpen in dit hoofdstuk zijn in de interne audit en de privacy audit vanwege capaciteits- en tijdgebrek niet toereikend onderzocht. Volstaan is met summiere bevindingen en aanbevelingen.				X
2	13.4 WPG; 31.1 WPG; 32.3 WPG; 33.4 WPG; 6:2 BPG					X
3	1 WPG; 32.2 WPG		-			
4	5 WPG					X
5	3.2 WPG					X
6	3.2 WPG					X
7	3.3 WPG					X

1.10.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG					X
2	4.1 WPG					X
3	4.3 WPG					X
4	4.4 WPG					X
5	4.5 WPG					X
6	4.6 WPG					X

1.10.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG					X
2	6.2 WPG					X
3	6.3 WPG					X
4	6.4 WPG					X
5	6.5 WPG					X
6	6.6 WPG; 2:8 BPG					X

1.10.4 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	4.2 WPG; 13.4 WPG; 32.1 WPG; 32.3 WPG; 32.4 WPG; 6:2 BPG					X

1.10.5 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG					X
2	13.3 WPG; 2:10.1 BPG; 5.7 WPG					X
3	15.2 WPG; 2:13.1 BPG					X
4	7 WPG; 4:8 BPG					X

1.10.6 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG					X

ID	Artikel	Toelichting	V	D	N	A
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG					X
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG					X
4	7 WPG; 4:8 BPG					X

1.11 Artikel 13 (diensten Justitie)

1.11.1 Noodzakelijkheid, rechtmatigheid en doelbinding

ID	Artikel	Toelichting	V	D	N	A
1	13.1 WPG	Over artikel 13 verwerkingen is landelijk discussie gaande. De onderwerpen in dit hoofdstuk zijn in de interne audit en de privacy audit vanwege capaciteits- en tijdgebrek niet toereikend onderzocht. Volstaan is met summiere bevindingen en aanbevelingen.				X
2	13.4 WPG; 31.1 WPG; 32.3 WPG; 33.4 WPG; 6:2 BPG					X
3	1.f.6° WPG; 32.2 WPG					X
4	5 WPG					X
5	3.2 WPG					X
6	3.2 WPG					X
7	3.3 WPG					X

1.11.2 Juistheid, volledigheid en beveiliging politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	4.1 WPG					X
2	4.1 WPG					X
3	4.3 WPG					X
4	4.4 WPG					X
5	4.5 WPG					X
6	4.6 WPG					X

1.11.3 Autorisaties

ID	Artikel	Toelichting	V	D	N	A
1	6.1 WPG					X
2	6.2 WPG					X
2	6.3 WPG					X
4	6.4 WPG					X
5	6.5 WPG					X
6	6.6 WPG; 2:8 BPG					X

1.11.4 Bewaartermijnen en vernietiging

ID	Artikel	Toelichting	V	D	N	A
1	4.2 WPG; 13.4 WPG; 32.1 WPG; 32.3 WPG; 32.4 WPG; 6:2 BPG					X

1.11.5 Ter beschikking stellen van politiegegevens

ID	Artikel	Toelichting	V	D	N	A
1	15.1 WPG; 6.2 WPG					X
2	13.1 WPG; 6:2 BPG					X
3	15.2 WPG; 2:13.1 BPG					X
4	7 WPG; 4:8 BPG					X

1.11.6 Verstrekkingen

ID	Artikel	Toelichting	V	D	N	A
1	16 t/m 24 WPG; 4:1 t/m 5:5 BPG					X
2	32 WPG; 6:4.4 BPG; 6:4.6 BPG					X

ID	Artikel	Toelichting	V	D	N	A
3	32 WPG; 6:4.5 BPG; 6:4.6 BPG					X
4	7 WPG; 4:8 BPG					X

1.12 Rechten van betrokkenen

1.12.1. Verzoek om kennisneming

ID	Artikel	Toelichting	V	D	N	A
1	25 WPG	OD/BV		X		X
2	26 WPG	BV	X			
3	27 WPG	BV	X			

1.12.2. Verzoek om verbetering, aanvulling, verwijdering of afscherming

ID	Artikel	Toelichting	V	D	N	A
1	28 WPG	OD/BV		X		X
1		BV	X			
1		BV	X			

1.12.3. Mededeling van verbetering, aanvulling, verwijdering of afscherming

ID	Artikel	Toelichting	V	D	N	A
1	30 WPG	OD/BV		X		X
1		BV	X			

1.12.4. Vergoeding van kosten

ID	Artikel	Toelichting	V	D	N	A
1	31 WPG	OD/BV		X		X
1		BV	X			

1.13 Audits

ID	Artikel	Toelichting	V	D	N	A
1	33.1 WPG; 33.5 WPG; 6:5 BPG	BV	X			
2	33.2 WPG	BV	X			
3	33.3 WPG	BV	X			
4	33.4 WPG	BV	X			

1.14 Privacyfunctionaris

ID	Artikel	Toelichting	V	D	N	A
1	34.1 WPG	OD/BV		X		X
1		OV/BV	X			
2	4.5 WPG	OD/BD		X		X
3	34.2 WPG	OD/BV	X			
3		OD/BD		X		X
3		OD/BD		X		X
3		OD/BD		X		X
3		-	-			X
3		OD/BD		X		X
4	13.4 WPG; 31.1 WPG; 32.3 WPG; 32.4 WPG; 6:2 BPG	OD/BD		X		X
5	34.3 WPG	OV/BV	X			
6	34.4 WPG	OV/BV	X			

1.15 Functionaris gegevensbescherming

ID	Artikel	Toelichting	V	D	N	A
1	36 WPG	OV/BV	X			X
2	63 WBP		-			X
3	64 WBP		-			X
4	5.2 ABW		-			X