

**Externe privacy audit
Wet politiegegevens
Gemeente Meierijstad**



Controleperiode 1 januari 2022 tot en met 31 december 2024
NOREA Richtlijn 3000/D
Kenmerk BKBO/251103-02/EWPG

27 februari 2026
Dit assurancerapport heeft 20 pagina's
www.bkbo.nl

OGENSCHIJNLIJK

Ogenschijnlijk heeft het ene
niets te maken met het ander.

Ogenschijnlijk schuilt er
voordeel in een vaste baan.

Ogenschijnlijk zal er nog
een heleboel verand'ren.

Ogenschijnlijk staan de sterren
hier niet zo ver vandaan.

uit: 'Vrijwel alle gedichten', 2004
Jules Deelder

Colofon

Voor u ligt het assurancerapport van de externe audit inzake de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van de gemeente Meierijstad verwerken en die in een bestand zijn opgenomen, of die bestemd zijn daarin te worden opgenomen. Deze verwerkingen vallen onder de reikwijdte van de Wet politiegegevens (Wpg), het Besluit politiegegevens (Bpg) en het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (Bpgboa). Dit rapport is gebaseerd op Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors) en is opgesteld door BKBO bv. In dit rapport zijn de door ons vastgestelde bevindingen en conclusies beschreven.

Het 'long form' rapport bevat in Bijlage 1 en 2 aanvullende informatie die uitsluitend bedoeld is voor de gemeente Meierijstad, zoals een overzicht van de getoetste interne beheersingsmaatregelen per boa domein en de door ons vastgestelde bevindingen en aanbevelingen.

Dit rapport is opgesteld onder verantwoordelijkheid van de heer drs. M.B.H. Ijpelaar RE CEH CISA CIPP/E ingeschreven onder nummer 1252 als actief RE in het register van NOREA en geregistreerd als actief CISA met nummer 0126934 bij ISACA.

Inhoudsopgave

1	Assurancerapport van de onafhankelijke auditor	4
1.1	Ons afkeurend oordeel	4
1.2	De basis van ons afkeurend oordeel	4
1.2.1	Sub oordelen domein I Openbare ruimte	6
1.3	Criteria	7
1.4	Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek	8
1.4.1	Object van onderzoek	8
1.4.2	Specificatie van de controleperiode	8
1.4.3	Beperkingen	9
1.5	Beoogde gebruikers en doel	9
1.6	Verantwoordelijkheden van de opdrachtgever	9
1.7	Verantwoordelijkheden van de IT-auditor	10
1.8	Aanbeveling met betrekking tot de hercontrole	10
2	Beschrijving privacy doelstellingen	12
Bijlage 1	Beschrijving van de beheersingsmaatregelen en testresultaten	19
Bijlage 2	Beschrijving van de technische en organisatorische beheersingsmaatregelen en testresultaten	20

1 Assurancerapport van de onafhankelijke auditor

AAN: de gemeente Meierijstad

1.1 Ons afkeurend oordeel

Naar ons oordeel voldoen de door de gemeente Meierijstad getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens in opzet, bestaan en werking gedurende de controleperiode (zie sectie 1.4.2) in belangrijke mate niet aan de gestelde criteria (zie sectie 1.3). Vanwege het belang en de omvang van de aangelegenheden die hierna zijn beschreven, geven wij een afkeurend oordeel. Het overzicht met oordelen per beheersingsmaatregel is hierna in sectie 1.2 'De basis voor ons afkeurend oordeel' weergegeven.

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurancerapport zijn uiteengezet. De specifieke, getoetste beheersmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in de bijlage(n) 1 en 2.

1.2 De basis van ons afkeurend oordeel

Wij hebben vastgesteld dat een aanzienlijk deel van de hiernavolgende Wpg onderwerpen niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief werken. Omdat er bij een domein bij 10 of meer beheersingsmaatregelen¹ in opzet, bestaan en/of werking niet wordt voldaan aan de door de wetgever gestelde eisen, zijn deze aangelegenheden materieel en van diepgaande negatieve invloed op het beschermen van de privacy van betrokkenen. Ons afkeurend oordeel is gebaseerd op domein I.

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors (Directe-opdrachten)'. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 1.7 'Verantwoordelijkheden van de IT-auditor'.

¹ Hieronder worden zowel de algemene als de technische en organisatorische (IT) onderwerpen verstaan.

Wij zijn onafhankelijk van de gemeente Meierijstad en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen.

Kleur	Omschrijving	Betekenis
	Groen	Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met het op die regel aangegeven onderwerp effectief zijn opgezet, bestaan op 31 december 2024 en geïmplementeerd gedurende de controleperiode".
	Oranje	Hierbij moet "voldoet deels" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met het op die regel aangegeven onderwerp deels effectief zijn opgezet, en/of niet volledig bestaan op 31 december 2024 en/of gedeeltelijk zijn geïmplementeerd gedurende de controleperiode". Om geheel aan de norm te voldoen dienen de dwingende aanbevelingen te worden opgevolgd.
	Rood	"Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met het op die regel aangegeven onderwerp niet in alle materiële opzichten effectief zijn opgezet en/of bestaan op 31 december 2024 en/of zijn geïmplementeerd gedurende de controleperiode".
	Grijs	De beheersmaatregelen zijn niet beoordeeld, hetzij omdat het onderwerp niet van toepassing was, hetzij omdat het onderwerp niet kon worden onderzocht.

Tabel 1 Toelichting gebruikte kleuren

1.2.1 Sub oordelen domein I Openbare ruimte

Domein	Verwerking
I	Gemeente - Openbare Ruimte
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de APV van de gemeente.
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot parkeeroverlast en -excessen
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Wet aansprakelijkheidsverzekering motorrijtuigen
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot het Vuurwerkbesluit en de Wet Milieubeheer
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de verwijzing voor vuurwerkoverlast door minderjarigen.
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Alcoholwet 2021.
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de wet hygiëne en veiligheid badinrichtingen en zwemgelegenheden
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de wet op de kansspelen
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Wet openbare manifestaties
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot noodverordeningen
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Wrakkenwet
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Wet buitengewone bevoegdheden burgerlijk gezag

Tabel Verwerkingen domein I

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Data protection impact assessment (DPIA)			
9. Bijzondere politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Weking
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken			
19. Ondersteunende taken			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			
24. Rechtstreekse verstrekking			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor Gegevensbescherming			

Tabel Sub oordelen domein I

Technische en organisatorische maatregelen	Oordelen		
	Opzet	Bestaan	Weking
1. GITC1. Wijzigingsbeheer			
2. GITC2. Logische toegangsbeveiliging			
3. GITC3. Beheer van kwetsbaarheden (patchmanagement)			
4. GITC4. Cryptografie			
5. GITC5. Vulnerability scans en penetratietesten			

Tabel Sub oordelen technische en organisatorische maatregelen domein I

1.3 Criteria

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van

politiegegevens door boa's. Hiertoe heeft de organisatie beheersingsmaatregelen getroffen die in opzet, bestaan en werking door de IT-auditor worden getoetst. De IT-auditor maakt bij deze toetsing gebruik van de volgende criteria:

Diepgang	Betekenis
Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is aan de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast, ingeval van handmatige beheersmaatregelen zijn deze toegepast door competente en bevoegde personen.

Tabel Gebruikte criteria

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1 Object van onderzoek

De scope van ons onderzoek bestond uit de hierna genoemde verwerkingen van politiegegevens:

Organisatieonderdeel	Domein	Processen	Applicaties
Team VTH	I. Openbare ruimte	Zie §1.2	City Control Office365 Djuma Zaaksysteem Zivver

Tabel Scope van het onderzoek

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde verwerkingen van politiegegevens en doen daar derhalve ook geen uitspraak over.

1.4.2 Specificatie van de controleperiode

Ons onderzoek ten aanzien van de werking van beheersingsmaatregelen is beperkt tot de periode 1 januari 2024 tot en met 31 december 2024. Uitzondering hierop vormen een aantal zogenaamde 'Toezichtmaatregelen'. Dit betreft de beheersingsmaatregelen:

- Planning, uitvoering, en rapportage van de interne audits (#29);
- Toezichttaken van de FG (#31).

Het onderzoeken van de 2 hiervoor genoemde 'Toezichtmaatregelen' strekte zich uit tot de volledige controleperiode, te weten de periode 1 januari 2021 tot en met 31 december 2024.

Hierbij merken wij op dat de controleperiode 1 januari 2021 tot en met 31 december 2021 bij een eerdere externe privacy audit (onder verwijzing naar kenmerk IAS 1652 2021_Wpg en de rapportdatum 5 december 2022 is onderzocht en aan de AP is gerapporteerd. Om "dubbeling" te voorkomen, maakt deze specifieke periode geen onderdeel uit van de thans onderzochte controleperiode. De controleperiode is daarmee de periode 1 januari 2022 tot en met 31 december 2024.

1.4.3 Beperkingen

Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersmaatregelen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

1.5 Beoogde gebruikers en doel

De gemeente Meerijstad dient ingevolge artikel 33 2e lid van de Wet politiegegevens een afschrift van de controleresultaten van de privacy audit aan de Autoriteit persoonsgegevens te zenden. In eerste instantie betreft dit het 'short form' rapport (rapport exclusief bijlagen). De Autoriteit persoonsgegevens kan, in het kader van haar toezichthoudende taak, het 'long form' rapport (rapport inclusief bijlagen) zonder opgaaf van redenen bij de gemeente Meerijstad opvragen. Voor de verstrekking van beide rapportages geldt als voorwaarde dat de rapportage origineel, volledig en ongewijzigd ter inzage wordt aangeboden.

Het is, zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming, niet toegestaan de rapportages met anderen dan de Autoriteit persoonsgegevens te delen. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

1.6 Verantwoordelijkheden van de opdrachtgever

De gemeente Meerijstad is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersmaatregelen gedurende de controleperiode 1 januari 2022 tot en met 31 december 2024, om te voldoen aan de wettelijke eisen van de in de Wet Politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa) gestelde bepalingen.

1.7 Verantwoordelijkheden van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken.

Wij passen het 'Reglement Kwaliteitsbeheersing NOREA' (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsmanagement inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere relevante wet- en regelgeving. Wij voldoen aan de specifieke vereisten voor de uitvoering van de externe privacy audit, zoals bepaald in artikel 5 van de Regeling periodieke audit politiegegevens².

De werkzaamheden zijn afhankelijk van de door de IT-auditor toegepaste professionele oordeelsvorming en bestonden uit een combinatie van inspectie van documentatie, het houden van interviews, het evalueren van de resultaten van de uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden. Onze bevindingen zijn opgenomen in de bijlagen 1 en 2.

1.8 Aanbeveling met betrekking tot de hercontrole

De verantwoordelijke is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterplan op te stellen waarin de maatregelen worden beschreven en gepland, ter verbetering van de bij de externe privacy audit geconstateerde tekortkomingen.

Hoewel er sprake is van een afkeurend oordeel hebben we geconstateerd dat de interne auditfunctie door de gemeente Meierijstad inmiddels op orde is gebracht (zie norm 29), en derhalve bevelen we aan dat de hercontrole op de effectiviteit van de verbetermaatregelen door de *interne auditor* wordt uitgevoerd.

De hercontrole moet plaatsvinden binnen één jaar na de rapportagedatum van deze audit. De resultaten van het verbeterplan en de uitgevoerde hercontrole worden in de volgende externe privacy audit meegenomen.

² Zie hiervoor 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 (Regeling periodieke audit politiegegevens).

Vlijmen d.d. 27 februari 2026

BKBO B.V.



2 Beschrijving privacy doelstellingen

Om de privacy van de verwerkte politiegegevens ten behoeve van de wettelijke taak te kunnen waarborgen en te kunnen voldoen aan de eisen die de wet daaraan stelt, heeft de gemeente Meierijstad beheersingsmaatregelen getroffen in lijn met het normenkader uit de vigerende NOREA Handreiking Audit Wet politiegegevens (boa). Die illustratieve beheersingsmaatregelen zijn gebaseerd op de Wet politiegegevens en het Besluit politiegegevens buitengewoon opsporingsambtenaren en omvatten de te verwachten onderwerpen en -beheersingsmaatregelen, gericht op beheersing van privacy in gegevensverwerkende processen en indicatieve controles, in lijn met de geldende wet- en regelgeving.

Onderstaand zijn deze onderwerpen en mogelijke beheersingsmaatregelen weergegeven.

Onderwerpen en beheersingsmaatregelen	
1. Reikwijdte	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.
2. Doelbinding	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een, met die doeleinden onverenigbare wijze, worden verwerkt.
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst	Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.
4. Juistheid en volledigheid politiegegevens	De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.
5. Onderscheid feiten en oordeel	Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
6. Gegevensbescherming door beveiliging en ontwerp	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.

Onderwerpen en beheersingsmaatregelen

De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.

Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).

De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.

7. Gegevensbescherming door standaardinstellingen

De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:

- Alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.
- Politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

8. Data protection impact assessment (DPIA)

Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet.

De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.

9. Bijzondere politiegegevens

Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:

- Dat onvermijdelijk is voor het doel van de verwerking.
- Dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon.
- De gegevens afdoende zijn beveiligd.

10. Autorisatie en toegang tot politiegegevens

Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: de verwerkingsverantwoordelijke heeft die personen, die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens, geautoriseerd voor alleen die gegevens (need-to-know).

- Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.
- Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.

11. Autorisaties: aanwijzen functionarissen

Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.

Onderwerpen en beheersingsmaatregelen**12. Onderscheid tussen verschillende categorieën van betrokkenen**

De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.

13. Verwerker en Verwerkersovereenkomst

- De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen in de verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken.
- De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen.
- Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling.
- Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging.
- Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.

14. Geheimhoudingsplicht

Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.

15. Geautomatiseerde individuele besluitvorming

- Besluiten uitsluitend gebaseerd op geautomatiseerde verwerking, die voor de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet.
- Het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.

16. Uitvoering van de dagelijkse politietaak

- Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst), dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis).
- Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstreken geautomatiseerd worden vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden

Onderwerpen en beheersingsmaatregelen

bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaken.

17. Ter beschikking stellen (voor verdere verwerking)

- Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris.
- Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.

18. Geautomatiseerd vergelijken en in combinatie zoeken

- Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11.
- Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4.
- Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn.
- Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.

19. Ondersteunende taken

Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).

20. Bewaartermijnen, verwijderen en vernietigen

- Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.
- De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.
- Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen zoals genoemd in de Archiefwet voldaan.

21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee

- Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.
- Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg).
- Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.

Onderwerpen en beheersingsmaatregelen

- Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.
- De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij.
- Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.

22. Doorgiften aan derde landen

- De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.
- De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).
- Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet.
- Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.

23. Verstrekking aan derden structureel voor samenwerkingsverbanden

- De verwerkingsverantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.
- In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd:
 1. Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is,
 2. Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt,
 3. Het doel waartoe dit is opgericht,
 4. Welke gegevens worden verstrekt,
 5. De voorwaarden onder welke de gegevens worden verstrekt en
 6. Aan welke personen of instanties de gegevens worden verstrekt.
- De daadwerkelijke verstrekking van gegevens wordt vastgelegd.

24. Rechtstreekse verstrekking

- De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen.
- De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.

25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering

- De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de

Onderwerpen en beheersingsmaatregelen

- betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2.
- Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd.
- Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.
- De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid een klacht in te dienen bij de AP.
- Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.

26. Register

De verwerkingsverantwoordelijke houdt een register bij van alle categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Het register voldoet aan de eisen gesteld in de wet (art 31d lid 1). Het register dient te worden bijgehouden met de relevante informatie om inzicht te verschaffen in de compliance status en de beoordeling van de mate waarin de waarborgen passend zijn voor de verwerking.

27. Documentatie

De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard.

- De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie.
- De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.

28. Logging

De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1. De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.

29. Audits

Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.

30. Melding datalekken

Onderwerpen en beheersingsmaatregelen

De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen.

- De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd.
- De melding van een datalek aan de Autoriteit Persoonsgegevens vindt tijdig en volledig plaats.
- Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.

31. Functionaris voor Gegevensbescherming

Er is een functionaris voor gegevensbescherming (= FG) aangesteld die toezicht houdt op:

1. het naleven van de Wpg;
 2. het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;
 3. de toewijzing van de autorisaties, bedoeld in art 6;
 4. de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens;
 5. de audits;
 6. de uitvoering van de DPIA's.
- De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.
 - De FG is aangemeld bij de Autoriteit Persoonsgegevens.

De bijlagen van dit rapport zijn vertrouwelijk en opgenomen als aparte PDF-bestanden en vormen samen met dit rapport het "long form" rapport. De bijlagen zijn uitsluitend bestemd voor de gemeente Meerijstad.

Bijlage 1 Beschrijving van de beheersingsmaatregelen en testresultaten

Deze bijlage van dit rapport is vertrouwelijk en uitsluitend bestemd voor de gemeente Meierijstad. Deze bijlage heeft betrekking op domein I.

Bijlage 2 Beschrijving van de technische en organisatorische beheersingsmaatregelen en testresultaten

De bijlage 2 van dit rapport is vertrouwelijk en uitsluitend bestemd voor de gemeente Meierijstad.