

**Assurance-rapport
NOREA Richtlijn 3000D**

Privacy-audit Wet politiegegevens
[VERSLAGPERIODE¹]

[ORGANISATIE]

Uitgebracht door:	
Onderzoeker(s):	
Uitgebracht aan:	[ORGANISATIE]
Contactpersoon:	
Datum:	[RAPPORTDATUM]
Rapportnummer:	[RAPPORTNUMMER]
Versie:	[VERSIENUMMER]
Status:	[STATUS]

¹ Verslagperiode is [9 maart 2019] tot [einddatum onderzoek externe privacy audit Wpg in 2021].

Inhoud

1	ASSURANCE-RAPPORT VAN DE ONAFHANKELIJKE AUDITOR.....	4
1.1	OPDRACHT.....	4
1.2	OBJECT VAN ONDERZOEK	4
1.3	SCOPE.....	4
1.4	VERANTWOORDELIJKHEDEN [ORGANISATIE].....	5
1.5	ONZE ONAFHANKELIJKHEID EN KWALITEITSBEHEERSING.....	5
1.6	VERANTWOORDELIJKHEDEN VAN DE AUDITOR	6
1.7	GEHANTEERDE CRITERIA	6
1.8	ONDERZOEK NAAR DE WERKING VAN BEHEERSINGSMATREGELEN GEDURENDE DE VERSLAGPERIODE	7
1.9	BEPERKINGEN	7
1.10	ONS OORDEEL MET BEPERKING	7
1.11	DE BASIS VOOR ONS OORDEEL MET BEPERKING	8
1.12	AANBEVELING MET BETREKKING TOT DE HERCONTROLE	12
1.13	BEPERKINGEN IN GEBRUIK EN VERSPREIDINGSKRING	12
2	BESCHRIJVING PRIVACY-DOELSTELLINGEN.....	14
3	MANAGEMENTREACTIE [OPTIONEEL].....	19
4	VERBETERRAPPORTAGE [OPTIONEEL].....	20
	BIJLAGE 1 – BESCHRIJVING VAN DE BEHEERSINGSMATREGELEN EN TESTRESULTATEN (WPG BEHEERSINGSMATREGELEN).....	21
	BIJLAGE 2 – BESCHRIJVING VAN DE BEHEERSINGSMATREGELEN EN TESTRESULTATEN (TECHNISCHE EN ORGANISATORISCHE BEHEERSINGSMATREGELEN)	34

Colofon

Voor u ligt het assurance-rapport inzake de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van [ORGANISATIE] 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) 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 [AUDIT ORGANISATIE]. In dit rapport zijn de door ons vastgestelde bevindingen, conclusies en aanbevelingen beschreven.

Ons rapport wordt uitgebracht in twee versies: Het 'short form' rapport bevat de basiselementen en is bedoeld voor de toezichthouder. Het 'long form' rapport bevat in Bijlagen 1 en 2 aanvullende informatie die in beginsel uitsluitend bedoeld is voor [ORGANISATIE], zoals een overzicht van de getoetste interne beheersmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen. Het voorliggende rapport is de 'long form' / 'short form' versie van ons rapport. *(opmerking: verwijder bij de 'short form' versie de bijlagen 1 en 2)*

1 Assurance-rapport van de onafhankelijke auditor

Aan: [ORGANISATIE]

1.1 Opdracht

Ingevolge de opdracht van [ORGANISATIE] hebben wij een onderzoek uitgevoerd naar de opzet, het bestaan en de werking van beheersingsmaatregelen die de wettelijke eisen van de in de Wet Politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpgboa) gestelde bepalingen waarborgen.

In de Wpg en het Bpgboa zijn vereisten en regels opgenomen voor het verwerken van persoonsgegevens die nodig zijn om de opsporing van strafbare feiten goed te kunnen uitvoeren. De Wpg zorgt daarbij voor een evenwicht tussen de belangen die met het uitvoeren van de opsporing van strafbare feiten gemoeid zijn en het beschermen van de privacy van burgers.

Om te kunnen beoordelen of dit evenwicht wordt gehandhaafd, is in artikel 33 van de Wpg bepaald dat de verwerkingsverantwoordelijke voor het verwerken van politiegegevens periodiek, door middel van het uitvoeren van audits, moet controleren of de bij of krachtens deze wet gegeven regels worden nageleefd. Een dergelijke controle moet volgens de Regeling periodieke audit politiegegevens twee jaar na inwerkingtreding van de wet en vervolgens elke vier jaar plaatsvinden. Deze controle is in de vorm van onderhavige privacy-audit uitgevoerd.

1.2 Object van onderzoek

Het object van onderzoek van deze privacy audit Wpg bestaat uit de beheersingsmaatregelen voor de verwerkingen van politiegegevens die onder verantwoordelijkheid van de verwerkingsverantwoordelijke worden verwerkt. Verwerkingen kunnen plaatsvinden in de volgende domeinen:

Domein	Boa-werkterrein
I	Openbare ruimte
II	Milieu, welzijn en infrastructuur
III	Onderwijs
IV	Openbaar vervoer
V	Werk, inkomen en zorg
VI	Generieke opsporing

1.3 Scope

De scope van ons onderzoek bij [ORGANISATIE] bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1		I/II/III/IV/V/VI		
2				

3				
4				

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

Of:

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde verwerkingen van politiegegevens maar geconstateerd dat er ook in andere domeinen dan vermeld Wpg verwerkingen plaatsvinden. Aangezien [ORGANISATIE] deze domeinen niet heeft opgenomen in onze opdracht doen we derhalve hierover geen uitspraak over.

Optioneel:

[ORGANISATIE] verwerkt Wpg gegevens ook voor een aantal andere bestuursorganen, te weten: <lijst opnemen in geval van inbesteding>.

1.4 Verantwoordelijkheden [ORGANISATIE]

[ORGANISATIE] is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de periode [VERSLAGPERIODE].

1.5 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professioneel gedrag.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden wij een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde 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.

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).

1.6 Verantwoordelijkheden van de auditor

Wij hebben onze opdracht uitgevoerd in overeenstemming met de Richtlijn 3000D (Herzien) 'Assurance-opdrachten door IT-auditors' van NOREA.

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid, voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

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.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel met een redelijke mate van zekerheid te bieden.

1.7 Gehanteerde 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

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 beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast, ingeval van handmatige beheersingsmaatregelen zijn deze toegepast door competente en bevoegde personen.

1.8 Onderzoek naar de werking van beheersingsmaatregelen gedurende de verslagperiode

Ons onderzoek ten aanzien van de werking van beheersingsmaatregelen is beperkt tot de periode [VAN – TOT] Vul hier in: de periode van 1 jaar (12 maanden) voorafgaand aan de einddatum van het onderzoek externe privacy audit Wpg 2021 (uiterlijk 31 december 2021)]. Uitzondering hierop vormen een aantal zogenaamde 'Toezichtmaatregelen'. Dit betreft de beheersingsmaatregelen:

- Jaarlijks Toezicht van de FG op de doelbinding (#2);
- Controles op de noodzakelijkheid en rechtmatigheid door de FG (of PO) (#3);
- Controles op het vernietigen en rectificeren van politiegegevens (#4);
- Controles op uitvoering DPIA's (#6 en #31);
- Beschikbaarheid logbestanden (#28);
- Planning, uitvoering, en rapportage van de interne audits (#29);
- Overige toezichttaken van de FG (#31).

Het onderzoeken van de hiervoor genoemde 'Toezichtmaatregelen' strekte zich uit tot de volledige verslagperiode (9 maart 2019 tot [EINDDATUM ONDERZOEK]).

1.9 Beperkingen

Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen 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.

1.10 Ons oordeel met beperking

Naar ons oordeel, uitgezonderd de aangelegenheden die hierna zijn beschreven in paragraaf 1.11 'De basis voor ons oordeel met beperking', in alle van materieel belang zijnde aspecten, zijn de door de [ORANISATIE] getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's op afdoende wijze opgezet, bestaan deze en hebben deze effectief gewerkt gedurende de [VERSLAGPERIODE]³, respectievelijk de 12 maanden voorafgaand aan de einddatum van de externe privacy audit Wpg 2021⁴.

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. De specifieke, getoetste beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in Bijlage 1 – Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (technische en organisatorische maatregelen).

³ Deze termijn geldt voor de in paragraaf 1.8 genoemde 'Toezichtmaatregelen'.

⁴ Deze termijn geldt voor de overige, 'niet-Toezichtmaatregelen'.

1.11 De basis voor ons oordeel met beperking

Wij hebben vastgesteld dat de hiernavolgende Wpg onderwerpen niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief werken. Zoals opgenomen in de beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (Bijlage 1 en Bijlage 2), waren deze interne beheersmaatregelen niet gedurende de gehele verslagperiode in afdoende mate opgezet, hebben niet bestaan en/of werkten niet effectief.

Voor de volledigheid zijn de onderwerpen die afdoende zijn opgezet, geïmplementeerd en effectief werkten ook vermeld (groen). Dit geldt eveneens voor de onderwerpen die niet zijn onderzocht (grijs).

Omdat binnen [ORGANISATIE] meerdere verwerkingen van politiegegevens plaatsvinden, waarbij de oordelen per onderwerp onderling afwijken, hebben we ons oordeel per verwerking weergegeven.

Verwerking 1 (Proces/verwerking)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
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 politie-gegevens 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. Recht-streekse verstrekking aan inlichtingen- of veiligheidsdiensten			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
30. Melding datalekken			
31. Functionaris voor gegevensbescherming			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

Verwerking 2 (Proces/verwerking)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
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 politie-gegevens 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. Recht-streekse verstrekking aan inlichtingen- of veiligheidsdiensten			

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
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			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

Verwerking 3 (Proces/verwerking)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
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 politie-gegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken			
19. Ondersteunende taken			
20. Bewaartermijnen, verwijderen en vernietigen			

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			
24. Recht-streekse verstrekking aan inlichtingen- of veiligheidsdiensten			
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			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

Verwerking 4 (Proces/verwerking)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en Verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming			

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politie-gegevens 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. Recht-streekse verstrekking aan inlichtingen- of veiligheidsdiensten			
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			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

Indien uit de resultaten van de privacy audit blijkt dat niet of niet geheel wordt voldaan aan het bij of krachtens de wet bepaalde, dient de auditor hier een aanbeveling op te nemen inzake de uitvoering van een hercontrole door een externe dan wel interne auditor (art.2 lid 5d Regeling periodieke audits politiegegevens).

1.12 Aanbeveling met betrekking tot de hercontrole

Wij hebben vastgesteld dat [ORGANISATIE] niet (geheel) voldoet aan het bij of krachtens de wet bepaalde. Inzake de uitvoering van de hercontroles, bevelen wij [ORGANISATIE] aan om deze door een interne / externe auditor te laten uitvoeren. Wij baseren deze aanbeveling op het volgende:

- Overwogen aspect(en) voor de aanbeveling (zie paragraaf 2.4 van de Handreiking)

1.13 Beperkingen in gebruik en verspreidingskring

[ORGANISATIE] 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 opgave van redenen bij [ORGANISATIE] 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. Het is niet toegestaan deze rapportage te gebruiken in juridische conflicten tussen [ORGANISATIE] en andere (rechts)personen.

[PLAATS], [RAPPORTDATUM]

[AUDIT ORGANISATIE]

[NAAM AUDITOR]

[HANDTEKENING AUDITOR]

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 [ORGANISATIE] beheersingsmaatregelen getroffen in lijn met de illustratieve beheersingsmaatregelen uit de NOREA Handreiking Privacy audit Wpg (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 illustratievebeheersingsmaatregelen 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 en 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 <ul style="list-style-type: none">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 <ul style="list-style-type: none">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.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: <ul style="list-style-type: none">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. Gegevensbeschermings-effectbeoordeling / Data protection impact assessment (DPIA) <ul style="list-style-type: none">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.

Onderwerpen en beheersingsmaatregelen

- 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 categorieën van 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. Autorisaties 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.

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 gebaseerd uitsluitend op geautomatiseerde verwerking dat voor de betrokkene nadelige rechtsgevolgen heeft 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 bewustwordings sessies 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 bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.

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.

Onderwerpen en beheersingsmaatregelen

- 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.
- 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:
 - Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is,
 - Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt,
 - Het doel waartoe dit is opgericht,
 - Welke gegevens worden verstrekt,
 - De voorwaarden onder welke de gegevens worden verstrekt en

Onderwerpen en beheersingsmaatregelen
<ul style="list-style-type: none">○ Aan welke personen of instanties de gegevens worden verstrekt.• De daadwerkelijke verstrekking van gegevens wordt vastgelegd.
24. Rechtstreekse verstrekking <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de 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 <ul style="list-style-type: none">• De verwerkingsverantwoordelijke houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 1.• De verwerker houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 2.
27. Documentatie <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <p>Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.</p>
30. Melding datalekken <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:<ul style="list-style-type: none">○ het naleven van de Wpg;○ het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;○ de toewijzing van de autorisaties, bedoeld in art 6;○ de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens;

Onderwerpen en beheersingsmaatregelen

- de audits;
- de uitvoering van de DPIA's.
- De Functionaris Gegevensbescherming stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.
- De Functionaris voor Gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens.

3 Managementreactie [OPTIONEEL]

Toelichting: De verwerkingsverantwoordelijke kan (mag, maar is niet verplicht!) een reactie geven op het auditrapport. Hiermee wordt bewerkstelligd dat de ontvanger (de AP) wordt geïnformeerd over de (voorgenomen of reeds uitgevoerde) opvolgingen van de bevindingen en eventuele ontwikkelingen die zich hebben voorgedaan na de wettelijke periode.

Betreft: Managementreactie [ORGANISATIE] op het Assurance-Rapport Privacy Audit Wpg van [AUDIT ORGANISATIE].

[VOORBEELDTEKST]

[ORGANISATIE] heeft kennisgenomen van het voorliggende assurance-rapport. Het rapport sluit aan bij de situatie per 31 december 2021 van [ORGANISATIE] inzake verwerking van politiegegevens. We delen de conclusies zoals weergegeven in het rapport. Het rapport geeft een aantal aandachtspunten waaraan [ORGANISATIE] de komende periode aandacht zal gaan schenken.

De aandachtspunten bevinden zich vooral in het onderdeel / de onderdelen ... die intern geformaliseerd(moeten) zijn binnen de [ORGANISATIE] om de betrouwbare verwerking van politiegegevens te kunnen borgen. Ook is het bestaan en/of de werking op sommige onderdelen niet voldoende aantoonbaar.

Voor komend jaar zal allereerst aandacht worden besteed aan

- A
- B
- C

De reeds in 2022 gerealiseerde/geïmplementeerde maatregelen zijn:

- D
- E

4 Verbeterreportage [OPTIONEEL]

Toelichting: De verwerkingsverantwoordelijke dient drie maanden na de afronding van de externe audit een verbeterreportage op te stellen op basis van de conclusies in het assurance-rapport. De verwerkingsverantwoordelijke kan de auditor vragen om hierover te rapporteren zonder een uitspraak te doen of de verbetermaatregelen bestaan of effectief zijn.

Betreft: Verbeterplan voor de ontbrekende beheersmaatregelen naar aanleiding van het assurance-Rapport Privacy Audit Wpg van [AUDIT ORGANISATIE].

Wij hebben vastgesteld dat alle door ons geconstateerde tekortkomingen zijn geadresseerd door [ORGANISATIE] en dat de planning erin voorziet dat deze zullen zijn gerealiseerd ultimo [jaartal of plandatum invullen].

OF

Wij hebben vastgesteld dat alle door ons geconstateerde tekortkomingen -behalve onderstaande uitzonderingen- zijn geadresseerd door [ORGANISATIE] en volgens planning zullen zijn gerealiseerd ultimo [jaartal of plandatum invullen].

- [eventuele uitzonderingen]

De bijlagen van dit rapport zijn vertrouwelijk en uitsluitend bestemd voor [ORGANISATIE].

Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen)

In deze bijlage zijn de beheersingsmaatregelen opgenomen zoals die zijn overeengekomen met [ORGANISATIE] (opmerking: hieronder zijn de illustratieve beheersingsmaatregelen uit de NOREA Handreiking overgenomen. Deze illustratieve beheersingsmaatregelen dienen zo nodig klant specifiek worden gemaakt). In de onderstaande tabel hebben wij in de kolom 'Bevindingen' de resultaten van onze werkzaamheden gericht op het vaststellen van de opzet, het bestaan en/of de werking van de beheersingsmaatregelen vastgelegd. In de kolom 'Conclusie en aanbeveling' geven wij aan of aan de criteria voor de opzet, het bestaan en/of de werking wordt voldaan (eventueel) aangevuld met een aanbeveling ter verbetering.

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
1	Reikwijdte	Art 2 lid 1 en 2	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.		
2	Doelbinding	Art 3 lid 1, 3 en 4 Art 8 lid 1 Art 9 lid 1 en 2 Art 11 lid 1	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 onrechtmatige wijze, worden verwerkt.		
3	Noodzakelijkheid & rechtmatigheid, vermelding herkomst	Art 3 lid 2 en 5	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 politie-gegevens	Art 4 lid 1	De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens.		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.		
5	Onderscheid feiten en persoonlijk oordeel	Art 4 lid 3	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	Art 4a lid 1 t/m 5	<p>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.</p> <p>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.</p> <p>Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/wijzigingen).</p> <p>De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.</p>		
7	Gegevensbescherming door standaardinstellingen	Art 4b lid 1a en lid 1b	<p>De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:</p> <p>a) alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking;</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			b) politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.		
8	Gegevens-beschermings-effectbeoordeling/ Data protection impact assessment (DPIA)	Art 4c	<p>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.</p> <p>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.</p>		
9	Bijzondere categorieën van politie-gegevens	Art 5	<p>Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:</p> <ul style="list-style-type: none"> • 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	Autorisaties en toegang tot politie-gegevens	Art 6 lid 1 t/m 6 Art 6a	<p>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) .</p> <p>Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			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 functionaris-sen	Art 6 lid 7	Er is een actuele lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.		
12	Onderscheid tussen verschillende categorieën van betrokkenen	Art 6b	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.		
13	Verwerker en Verwerkers-overeenkomst	Art 6c	<p>De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking heeft 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.</p> <p>De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen.</p> <p>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.</p> <p>Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging.</p> <p>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.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
14	Geheimhoudingsplicht	Art 7	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	Art 7a	<p>Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet.</p> <p>Het verbod op het gebruik van profilering dat 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.</p>		
16	Uitvoering van de dagelijkse politietaak	Art 8 lid 1 en 2	<p>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).</p> <p>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 bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.</p>		
17	Ter beschikking stellen van politiegegevens	Art 4 lid 1 Art 8 lid 4 Art 9 lid 3 Art 15 lid 1 en	Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris.		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
	binnen het WPG-domein	2 Art 15a lid 1 en 2	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	Art 11 lid 1, 3, 4 en 5 Art 8 lid 3 Art 2:1 en 2:2 lid 1 Bpg	<p>Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11.</p> <p>Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4.</p> <p>Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn.</p> <p>Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.</p>		
19	Ondersteunende taken	Art 13	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	Art 4 lid 2 Art 8 lid 6 Art 9 lid 4 Art 14	<p>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.</p> <p>De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			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 als genoemd in de Archiefwet voldaan.		
21	Verstrekking van politie-gegevens aan anderen dan politie en Koninklijke marechaussee	Art 16 Art 18 Art 19 Art 21 Art 22 Art 7 lid 1 Art 4	<p>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.</p> <p>Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg).</p> <p>Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.</p> <p>Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.</p> <p>De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij.</p> <p>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.</p>		
22	Doorgiften aan derde landen	Art 17a	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.		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			<p>De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).</p> <p>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.</p> <p>Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.</p>		
23	Verstrekking aan derden structureel voor samenwerkingsverbanden	Art 20	<p>De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.</p> <p>In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd:</p> <ul style="list-style-type: none"> • Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, • Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, • Het doel waartoe dit is opgericht, • Welke gegevens worden verstrekt, • De voorwaarden onder welke de gegevens worden verstrekt en • Aan welke personen of instanties de gegevens worden verstrekt. <p>De daadwerkelijke verstrekking van gegevens wordt vastgelegd.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
24	Rechtstreekse verstrekking	Art 23	<p>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.</p> <p>De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.</p>		
25	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering.	Art 24a lid 1 t/m 4 Art 24b Art 25 Art 26 Art 27 Art 28	<p>De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2.</p> <p>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.</p> <p>Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.</p> <p>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.</p> <p>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.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
26	Register	Art 31d lid 1 en 2	<p>De <u>verwerkingsverantwoordelijke</u> houdt een register bij dat de volgende gegevens bevat:</p> <ul style="list-style-type: none"> a) de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming; b) de doelen van de verwerking; c) de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties; d) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens; e) in voorkomend geval, het gebruik van profilering; f) in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie; g) een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn; h) zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd; i) zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a; j) de toekenning van de autorisaties, bedoeld in artikel 6. <p>De <u>verwerker</u> houdt een register bij dat de volgende gegevens bevat:</p> <ul style="list-style-type: none"> a) de naam en de contactgegevens van de verwerker of verwerkers en van iedere verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming; 		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			<p>b) de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn uitgevoerd;</p> <p>c) indien van toepassing, doorgiften van politiegegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd</p> <p>d) indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.</p>		
27	Documentatie	Art 32 lid 1 t/m 4	<p>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.</p> <p>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.</p> <p>De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.</p>		
28	Logging	Art 32a	<p>De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1.</p> <p>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.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
29	Audits	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.		
30	Melding datalekken	Art 33a	<p>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.</p> <p>De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd.</p> <p>De melding van een datalek aan de AP vindt tijdig en volledig plaats.</p> <p>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.</p>		
31	Functionaris voor gegevensbescherming	Art 36	<p>Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:</p> <ul style="list-style-type: none"> o het naleven van de WPG; o het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens; o de toewijzing van de autorisaties, bedoeld in art 6; o de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens; o de audits; o de uitvoering van de DPIA's. <p>De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.</p>		

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			De functionaris voor gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en de contactgegevens van de FG zijn openbaar gemaakt.		

Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische beheersingsmaatregelen)

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
1	Wijzigingenbeheer	<p>Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.</p> <p><u>Doelstelling:</u> Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.</p> <p><u>Scope:</u> Applicatie-, hosting (verwerker)- of SAAS leverancier van de WPG-geclassificeerde verwerkende systemen.</p>		
2	Logische toegangsbeveiliging	<p>De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.</p> <p><u>Doelstelling:</u> Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.</p> <p><u>Scope:</u> Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen.</p>		

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
3	Beheer van kwetsbaarheden (patchmanagement)	<p>Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.</p> <p><u>Doelstelling:</u> Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.</p> <p><u>Scope:</u> Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen.</p>		
4	Cryptografie	<p>Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.</p> <p><u>Doelstelling:</u> Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van politiegegevens te beschermen.</p> <p><u>Scope:</u> Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen.</p>		
5	Vulnerability scans en Penetratietesten	<p>Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.</p> <p><u>Doelstelling:</u> Het verkrijgen van inzicht in de weerstand die de systemen kunnen bieden aan pogingen om het te compromitteren.</p> <p><u>Scope:</u> Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen.</p>		

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen