|  |
| --- |
| **Assurance-rapport**  **NOREA Richtlijn 3000D** |
| **HERCONTROLE**  **o.g.v. artikel 4 Regeling periodieke audit politiegegevens (artikel 6:5, vierde lid Besluit Politiegegevens en artikel 33 vijfde lid Wet politiegegevens)**  **Privacy-audit Wet politiegegevens**  **[ORGANISATIE]** |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| Uitgebracht door | : |  |
| Onderzoeker(s) | : |  |
| Uitgebracht aan | : | [ORGANISATIE] |
| Contactpersoon | : |  |
| Datum | : | [DATUM] |
| Kenmerk | : | [ORGANISATIE][KENMERK] |
| Versie | : |  |
| Status | : |  |

Inhoud

[1 Assurance-rapport van de onafhankelijke auditor 5](#_Toc131395556)

[1.1 Opdracht 5](#_Toc131395557)

[1.2 Object van onderzoek 5](#_Toc131395558)

[1.3 Scope 6](#_Toc131395559)

[1.4 Verantwoordelijkheden [ORGANISATIE] 6](#_Toc131395560)

[1.5 Onze onafhankelijkheid en kwaliteitsbeheersing 6](#_Toc131395561)

[1.6 Verantwoordelijkheden van de auditor 7](#_Toc131395562)

[1.7 Gehanteerde criteria 7](#_Toc131395563)

[1.8 Beperkingen 7](#_Toc131395564)

[1.9 Ons oordeel met beperking 8](#_Toc131395565)

[1.10 De basis voor ons oordeel met beperking 8](#_Toc131395566)

[1.11 Beperkingen in gebruik en verspreidingskring 10](#_Toc131395567)

[2 Beschrijving privacy-doelstellingen 11](#_Toc131395568)

[3 Managementreactie 16](#_Toc131395569)

[Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen) 17](#_Toc131395570)

[Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische beheersingsmaatregelen) 22](#_Toc131395571)

**Colofon**

Voor u ligt het assurance-rapport inzake de hercontrole van de externe privacy audit op 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 de NOREA Handreiking Privacy audit Wpg voor boa’s, versie 1.0 d.d. 24 juni 2021, de Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors) en is opgesteld door [AUDITORGANISATIE]. 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 Bijlage 1 en 2 aanvullende informatie die uitsluitend bedoeld is voor [ORGANISATIE], zoals een overzicht van de getoetste interne beheersmaatregelen per boa domein en de door ons vastgestelde bevindingen en aanbevelingen.

# Assurance-rapport van de onafhankelijke auditor

## Opdracht

Ingevolge de opdracht van [ORGANISATIE] hebben wij een hercontrole uitgevoerd naar de opzet en het bestaan van de beheersingsmaatregelen die in het privacy audit rapport [KENMERK INITIEEL AUDITRAPPORT] van [AUDITORGANISATIE INITIELE AUDIT] als ‘voldoet deels’ of ‘voldoet niet’ zijn beoordeeld.

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 rechtmatig te kunnen uitvoeren. De wetgever heeft met de Wpg een evenwicht aangebracht 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 door een onafhankelijke auditor, moet laten vaststellen 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. In artikel 33 lid 3 is bepaald dat indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens de Wet politiegegevens bepaalde, de verwerkingsverantwoordelijke binnen een jaar een onafhankelijke hercontrole uit laat voeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. In het externe auditrapport is aangegeven dat de externe auditor de hercontrole zou moeten uitvoeren.

De verwerkingsverantwoordelijke zendt een afschrift van de hercontrolerapport aan de Autoriteit Persoonsgegevens.

## Object van onderzoek

Deze hercontrole heeft alleen betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tekortkomingen zijn geconstateerd tijdens het initiële onderzoek, zoals vastgelegd in het initiële externe auditrapport [KENMERK INITIEEL AUDITRAPPORT] d.d. [DATUM INITIEEL AUDITRAPPORT] van [AUDITORGANISATIE INITIELE AUDIT] en heeft tot doel op systematische wijze te toetsen of door de verantwoordelijke zodanige maatregelen zijn getroffen dat aan de uitvoering van het onderdeel of de betreffende onderdelen van de wet thans op adequate wijze uitvoering is gegeven.

## Scope

De scope van ons onderzoek bij [ORGANISATIE] bestond uit de hierna genoemde verwerking(en) van politiegegevens:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Organisatie-onderdeel | Domein | Processen/verwerkingen | Applicaties |
|  |  |  |  |  |
|  |  |  |  |  |

Wij hebben uitsluitend onderzoek uitgevoerd naar de bij de initiële privacy audit als ‘deels’ of ‘niet voldoende’ in opzet en bestaan beoordeelde beheersingsmaatregelen. Wij hebben geen onderzoek gedaan naar de bij de initiële audit niet beoordeelde normen en doen daar derhalve ook geen uitspraak over. Tevens doen wij geen uitspraak over de werking van de gerealiseerde verbetermaatregelen[[1]](#footnote-1).

## Verantwoordelijkheden [ORGANISATIE]

[ORGANISATIE] is verantwoordelijk voor de opzet en het bestaan van de aanvullende beheersingsmaatregelen om alsnog te kunnen voldoen aan het bij of krachtens de Wpg bepaalde binnen een jaar na de initiële externe privacy audit.

[ORGANISATIE] is ook verantwoordelijk om binnen drie maanden na afronding van de initiële externe privacy audit een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de geconstateerde tekortkomingen. Tijdens de hercontrole wordt beoordeeld of een verbeterrapport (verbeterplan) is opgesteld om de verbeteringen op te stellen.

## 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 politiegegevens[[2]](#footnote-2).

## Verantwoordelijkheden van de auditor

Wij hebben onze opdracht uitgevoerd in overeenstemming met de Richtlijn 3000D ‘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.

## 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 en bestaan door de IT-auditor worden getoetst. De IT-auditor maakt bij deze hercontrole gebruik van de volgende criteria:

|  |  |
| --- | --- |
| **Opzet** | De organisatie heeft de beheersingsmaatregen 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. |

## Beperkingen

Zoals hierboven staat vermeld, hebben wij bij deze hercontrole geen werkzaamheden uitgevoerd met betrekking tot de werking van de interne beheersmaatregelen die binnen de scope van ons onderzoek vallen. Wij achten de periode waarin de onderzochte beheersingsmaatregelen effectief hebben gewerkt daarvoor te kort. Wij brengen derhalve daarover geen oordelen tot uitdrukking.

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 beheersmaatregelen ineffectief kunnen worden.

## Ons oordeel met beperking

Wij hebben de hiernavolgende beheersingsmaatregelen, welke bij de initiële privacy audit als ‘voldoet deels’ of ‘voldoet niet’ zijn beoordeeld, opnieuw beoordeeld. Naar ons oordeel, uitgezonderd de aangelegenheden die hierna zijn beschreven in paragraaf 1.10 ‘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 en bestaan deze per [OORDEELSDATUM].

## De basis voor ons oordeel met beperking

Wij hebben de hiernavolgende beheersingsmaatregelen, die tijdens de initiële privacy audit als ‘voldoet deels’ of ‘voldoet niet’ zijn beoordeeld, opnieuw beoordeeld. Tijdens deze hercontrole hebben wij vastgesteld dat de hiernavolgende Wpg onderwerpen niet (rood) of niet geheel (oranje) zijn opgezet en/of bestaan.

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

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. Wij hebben geconstateerd dat door [ORGANISATIE] niet tijdig (dat wil zeggen binnen drie maanden na de initiële privacy audit) een verbeterrapport is opgesteld. Wij hebben bij de oordeelsvorming het door [ORGANISATIE] opgestelde verbeterrapport betrokken.

De specifiek getoetste beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in Bijlage 1 – Beschrijving van de beheersingsdoelstellingen, beheersingsmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsdoelstellingen, beheersingsmaatregelen en testresultaten (technische en organisatorische maatregelen).

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

*Toelichting gebruikte kleuren:*

G Groen - Voldoet aan de beheersingsmaatregel.

🗆 Oranje - Voldoet deels aan de beheersingsmaatregel. Om geheel aan de beheersingsmaatregel te voldoen dien(t)(en) de aanbeveling(en) te worden opgevolgd.

🗆 Rood - Voldoet niet aan de beheersingsmaatregel.

🗆 Grijs - Niet onderzocht (indien onderwerpen niet zijn onderzocht, wordt de reden hiervan aangegeven (bijvoorbeeld: niet onderzocht (NO) *of* Niet van toepassing. (NVT)).

**Verwerking 1 Domein … (****Strafrechtelijke handhaving in het kader van de …).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Onderwerpen** | **Initiële audit** | | | **Her-controle** | |
| **Opzet** | **Bestaan** | **Werking** | **Opzet** | **Bestaan** |
| 1.       Reikwijdte |  |  |  | NO | NO |
| 2.       Doelbinding |  |  |  | NO | NO |
| 3.       Noodzakelijkheid en rechtmatigheid, vermelding herkomst |  |  |  | NO | NO |
| 4.       Juistheid en volledigheid politiegegevens |  |  |  | NO | NO |
| 5.       Onderscheid feiten en oordeel |  |  |  | NO | NO |
| 6.       Gegevensbescherming door beveiliging en ontwerp |  |  |  |  |  |
| 7.       Gegevensbescherming door standaardinstellingen |  |  |  | NO | NO |
| 8.       Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA) |  |  |  |  |  |
| 9.       Bijzondere categorieën van politiegegevens |  |  |  | NO | NO |
| 10.    Autorisaties en toegang tot politiegegevens |  |  |  |  |  |
| 11.    Autorisaties: aanwijzen functionarissen |  |  |  | NO | NO |
| 12.    Onderscheid tussen verschillende categorieën van betrokkenen |  |  |  | NO | NO |
| 13.    Verwerker en Verwerkersovereenkomst |  |  |  | NO | NO |
| 14.    Geheimhoudingsplicht |  |  |  | NO | NO |
| 15.    Geautomatiseerde individuele besluitvorming |  |  |  | NO | NO |
| 16.    Uitvoering van de dagelijkse politietaak |  |  |  | NO | NO |
| 17.    Ter beschikking stellen van politiegegevens binnen het WPG-domein |  |  |  | NO | NO |
| 18.    Geautomatiseerd vergelijken en in combinatie zoeken |  |  |  | NO | NO |
| 19.    Ondersteunende taken |  |  |  | NO | NO |
| 20.    Bewaartermijnen, verwijderen en vernietigen |  |  |  | NO | NO |
| 21.    Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee |  |  |  | NO | NO |
| 22.    Doorgiften aan derde landen |  |  |  | NO | NO |
| 23.    Verstrekking aan derden structureel voor samenwerkingsverbanden |  |  |  | NO | NO |
| 24.    Rechtstreekse verstrekking |  |  |  | NO | NO |
| 25.    Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering |  |  |  | NO | NO |
| 26.    Register |  |  |  | NO | NO |
| 27.    Documentatie |  |  |  | NO | NO |
| 28.    Logging |  |  |  |  |  |
| 29.    Audits |  |  |  |  |  |
| 30.    Melding datalekken |  |  |  | NO | NO |
| 31.    Functionaris voor gegevensbescherming |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Technische en organisatorische maatregelen**  **Informatiesysteem: …** | **Initiële audit** | | | **Her-controle** | |
| **Onderwerpen** | **Opzet** | **Bestaan** | **Werking** | **Opzet** | **Bestaan** |
| 1.       Wijzigingenbeheer |  |  |  | NO | NO |
| 2.       Logische toegangsbeveiliging |  |  |  | NO | NO |
| 3.       Beheer van kwetsbaarheden (patchmanagement) |  |  |  | NO | NO |
| 4.       Cryptografie |  |  |  | NO | NO |
| 5.       Vulnerability scans en penetratietesten |  |  |  | NO | NO |

## Beperkingen in gebruik en verspreidingskring

[ORGANISATIE] dient ingevolge artikel 33 2e lid van de Wpg een afschrift van de controleresultaten van deze hercontrole 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 [ORGANISATIE] opvragen. Voor de verstrekking van beide rapportages geldt als voorwaarde dat de rapportage origineel, volledig en ongewijzigd ter inzage wordt aangeboden.

<Opdrachtgever> verwerkt ook Wpg gegevens voor andere bestuursorganen, en heeft daarom ook onze toestemming het ‘long form’ rapport te delen met deze bestuursorganen.

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.

[AUDITORGANISATIE]

[PLAATS], [DATUM]

[AUDITOR] RE

# 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 illustratieve beheersingsmaatregelen weergegeven.

| **Onderwerpen en beheersingsmaatregelen** |
| --- |
| 1. **Reikwijdte**   De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd. |
| 1. **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. |
| 1. **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. |
| 1. **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. |
| 1. **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. |
| 1. **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. * 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. |
| 1. **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. |
| 1. **Gegevensbeschermingseffectbeoordeling / 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. |
| 1. **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. |
| 1. **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. |
| 1. **Autorisaties: aanwijzen functionarissen**   Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen. |
| 1. **Onderscheid tussen verschillende categorieën van betrokkenen**   De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen. |
| 1. **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. |
| 1. **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. |
| 1. **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 bewustwordingssessies binnen de organisatie. |
| 1. **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. |
| 1. **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. |
| 1. **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. |
| 1. **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). |
| 1. **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. |
| 1. **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. |
| 1. **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. |
| 1. **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   + Aan welke personen of instanties de gegevens worden verstrekt. * De daadwerkelijke verstrekking van gegevens wordt vastgelegd. |
| 1. **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. |
| 1. **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 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 uitsluitsel 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. |
| 1. **Register**  * 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. |
| 1. **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. |
| 1. **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. |
| 1. **Audits**   Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens. |
| 1. **Melding datalekken**  * 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. |
| 1. **Functionaris voor gegevensbescherming**  * Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:   + 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;   + 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. |

# Managementreactie

*Betreft: Managementreactie [ORGANISATIE] op het Assurance-Rapport ‘Hercontrole Privacy Audit Wpg’ van [AUDITORGANISATIE]*

[MANAGEMENTREACTIE]

**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 die zijn getoetst tijdens de hercontrole. In de hiernavolgende tabellen hebben wij in de kolom *‘Bevindingen’* de resultaten van onze werkzaamheden gericht op het vaststellen van de opzet en het bestaan van de beheersingsmaatregelen vastgelegd. In de kolom *‘Conclusies en aanbevelingen’* 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.

Zoals in paragraaf 1.3 is aangegeven, verwerkt [ORGANISATIE] politiegegevens in Domein …..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Organisatie-onderdeel | Domein | Processen/verwerkingen | Applicaties |
|  |  |  |  |  |

[NEEM IN DE ONDERSTAANDE TABELLEN ALLEEN DE NORMEN OP DIE IN HET KADER VAN DE HERCONTROLE ZIJN BEOORDEELD]

| **1. Strafrechtelijke handhaving in het kader van de Wet Natuurbescherming en storten afval buiten inrichting (natuurgebied)** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr** | **Onderwerp** | **Verwijzing artikel** | **Beheersingsmaatregel** | **Bevindingen hercontrole** | **Opzet** | **Bestaan** | **Conclusies en aanbevelingen** |
| 6 | Gegevens-bescherming door beveiliging en ontwerp | Art 4a, lid 1 t/m 5 | Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt m.b.t. ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.  De verwerkingsverantwoordelijke 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). |  |  |  |  |
| 8 | Gegevens-bescherming-effect-beoordeling/ Data protection impact assessment (DPIA) | Art 4c | 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. |  |  |  |  |
| 10 | Autorisaties en toegang tot politie-gegevens | Art 6 lid 1 t/m 6 Art 6a | 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. |  |  |  |  |
| 28 | Logging | Art 32a | 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 | Art 33 | Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens. |  |  |  |  |
| 31 | Functionaris voor gegevens-bescherming | Art 36 | Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:   * het naleven van de WPG; * het beleid van de verwerkings-verantwoordelijke met betrekking tot de bescherming van persoonsgegevens; * de toewijzing van de autorisaties, bedoeld in art 6; * de bewustmaking en opleiding van de boa’s betrokken bij de verwerking van politiegegevens; * de audits; * 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 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)**

Zoals in paragraaf 1.3 is aangegeven, verwerkt [ORGANISATIE] politiegegevens in Domein ….

[ORGANISATIE] maakt voor deze verwerkingen gebruik van de volgende informatiesysteem:

|  |  |  |  |
| --- | --- | --- | --- |
| **Verwerking** | **Informatiesysteem** | **Beheerorganisatie** | **Leverancier** |
|  |  |  |  |

## 

| **#** | **Onderwerp** | **Beheersingsmaatregelen** | **Bevindingen** | **Opzet** | **Bestaan** | **Conclusies en aanbevelingen** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Wijzigingenbeheer | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van applicaties tijdig, geautoriseerd en getest worden doorgevoerd.    Doelstelling:  Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.  Scope:  Applicatie-, hosting (verwerker)- of SAAS leverancier van de WPG-geclassificeerde verwerkende systemen. |  |  |  |  |
| 2 | Logische toegangs-beveiliging | 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.    Doelstelling:  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.    Scope:  Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen. |  |  |  |  |
| 3 | Beheer van kwetsbaarheden  (patch-management) | 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.    Doelstelling:  Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.    Scope:  Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen. |  |  |  |  |
| 4 | Cryptografie | Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.    Doelstelling:  Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid,  authenticiteit en/of integriteit van politiegegevens te beschermen.    Scope:  Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen. |  |  |  |  |
| 5 | Vulnerability scans en  Penetratietesten | Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.    Doelstelling:  Het verkrijgen van inzicht in de weerstand die de systemen kunnen bieden aan pogingen om het te compromitteren.  Scope:  Hosting, leverancier van de WPG-geclassificeerde verwerkende systemen. |  |  |  |  |

1. De hercontrole heeft in beginsel alleen betrekking op opzet en bestaan, omdat de tijdspanne om een gewogen oordeel te geven over de werking in veel gevallen te kort zal zijn. [↑](#footnote-ref-1)
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). [↑](#footnote-ref-2)