|  |
| --- |
| **Assurance-rapport**  **NOREA Richtlijn 3000D** |
| Privacy-audit Wet politiegegevens  1 januari 2021 tot en met 31 december 2021  **Serviceorganisatie [ORGANISATIE]** |
|  |
|  |

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

Inhoud

[1 Assurance-rapport van de onafhankelijke auditor 4](#_Toc95192793)

[1.1 Opdracht 4](#_Toc95192794)

[1.2 Object van onderzoek 4](#_Toc95192795)

[1.3 Scope van de uitbestede processen/verwerkingen 5](#_Toc95192796)

[1.4 Verantwoordelijkheden serviceorganisatie [ORGANISATIE] 5](#_Toc95192797)

[1.5 Onze onafhankelijkheid en kwaliteitsbeheersing 5](#_Toc95192798)

[1.6 Verantwoordelijkheden van de auditor 5](#_Toc95192799)

[1.7 Gehanteerde criteria 6](#_Toc95192800)

[1.8 Onderzoek naar de werking van beheersingsmaatregelen gedurende de verslagperiode 7](#_Toc95192801)

[1.9 Beperkingen 7](#_Toc95192802)

[1.10 Ons oordeel met beperking 7](#_Toc95192803)

[1.11 De basis voor ons oordeel met beperking 7](#_Toc95192804)

[1.12 Beperkingen in gebruik en verspreidingskring 7](#_Toc95192805)

[2 Verantwoordelijkheden gebruikersorganisatie 9](#_Toc95192806)

[Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen) 11](#_Toc95192807)

[Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische beheersingsmaatregelen) 24](#_Toc95192808)

**Colofon**

Voor u ligt het assurance-rapport inzake de politiegegevens die serviceorganisatie [ORGANISATIE] voor clienten verwerkt 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.

# Assurance-rapport van de onafhankelijke auditor

**Aan: Serviceorganisatie [ORGANISATIE]**

## Opdracht

Ingevolge de opdracht van serviceorganisatie [ORGANISATIE] hebben wij een onderzoek uitgevoerd naar de opzet, het bestaan en de werking van relevante 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.

Cliënten van serviceorganisatie [ORGANISATIE] maken voor de verwerking van politiegegevens gebruik van de diensten/informatievoorziening/informatiesysteem van serviceorganisatie [ORGANISATIE]. Om de cliënten als verwerkingsverantwoordelijken, te ondersteunen bij de hiervoor beschreven privacy-audit heeft serviceorganisatie [ORGANISATIE] deze assurance-rapportage laten opstellen. In hoofdstuk 4 'Verantwoordelijkheid gebruikersorganisatie' is aangegeven welke aanvullende beheersingsmaatregelen de gebruikersorganisatie zou moeten treffen ten aanzien van de in Bijlage 1 genoemde beheersingsmaatregelen. De geschiktheid van de opzet of de werking van deze aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie hebben wij niet geëvalueerd.

## Object van onderzoek

Het object van onderzoek bestaat uit de beheersingsmaatregelen gericht op de ontwikkeling, het beheer, het onderhoud en de hosting van [APPPLICATIE EN VERSIE] welke de verwerking van politiegegevens door de cliënten van serviceorganisatie [ORGANISATIE] ondersteunt.

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 |

Specifiek zijn in scope de application controls, die het verwerkingsproces van de politiegegevens ondersteunen. Ook de verschillende vormen van ICT-beheer zijn in scope, voor zover relevant voor de doelstelling van de audit.

## Scope van de uitbestede processen/verwerkingen

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

|  |  |  |
| --- | --- | --- |
| # | Domein | Processen/verwerkingen |
| 1 | I/II/III/IV/V/VI |  |

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

## Verantwoordelijkheden serviceorganisatie [ORGANISATIE]

Serviceorganisatie [ORGANISATIE] is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de verslagperiode 1 januari 2021 tot en met 31 december 2021.

## 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 professionaliteit.

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.

## Verantwoordelijkheden van de auditor

Wij hebben onze opdracht uitgevoerd in overeenstemming met de Richtlijn 3000D ‘Assurance-opdrachten door IT-auditors’ van NOREA en wij hebben voldaan aan de specifieke vereisten voor de uitvoering van de externe privacy audit, zoals bepaald in artikel 5 van de Regeling periodieke audit politiegegevens[[1]](#footnote-1).

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 beheersingsmaatregelen 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 serviceorganisatie relevante 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 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. |
| **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. |

## Onderzoek naar de werking van beheersingsmaatregelen gedurende de verslagperiode

Ons onderzoek ten aanzien van de werking van beheersingsmaatregelen is beperkt tot de verslagperiode van 1 januari 2021 tot en met 31 december 2021.

## 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.

## 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 serviceorganisatie [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 [periode van 1 januari 2021 tot en met december 2021.

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 beheersingsmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische maatregelen).

## De basis voor ons oordeel met beperking

Wij hebben vastgesteld dat de hiernavolgende relevante beheersingsmaatregelen niet (rood) of niet volledig (oranje) door serviceorganisatie [ORGANISATIE] zijn opgezet, bestaan en/of effectief werken. Zoals opgenomen in de beschrijving van de beheersingsmaatregelen en testresultaten (Bijlage 1 en Bijlage 2), waren deze interne beheersingsmaatregelen niet gedurende de gehele verslagperiode in afdoende mate opgezet, hebben niet bestaan en/of werkten niet effectief.

## Beperkingen in gebruik en verspreidingskring

Deze rapportage en de beschrijving van toetsingen van interne beheersingsmaatregel in de bijlagen zijn uitsluitend voor cliënten die gebruik hebben gemaakt van de dienstverlening van serviceorganisatie [ORGANISATIE] en hun auditors, die voldoende inzicht hebben om het in aanmerking te nemen bij het inschatten van de risico’s op afwijkingen van materieel belang, tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregel die door cliënten zelf worden uitgevoerd.

Dit rapport wordt alleen aan de Autoriteit persoonsgegevens ter beschikking gesteld als deze daar, in het kader van haar toezichthoudende taak, om verzoekt. Voor de verstrekking van de rapportage geldt als voorwaarde dat de rapportage origineel, volledig en ongewijzigd ter inzage wordt aangeboden.

Het is, zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming, niet toegestaan deze rapportage met anderen dan cliënten en 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 serviceorganisatie [ORGANISATIE] en andere (rechts)personen.

|  |  |
| --- | --- |
| [PLAATS], [RAPPORTDATUM] |  |
| [AUDIT ORGANISATIE] |  |
| [NAAM AUDITOR] |  |
| [HANDTEKENING AUDITOR] |  |

# Verantwoordelijkheden gebruikersorganisatie

Uitgangspunt is dat de privacyrisico’s pas worden afgedekt als de beheersingsmaatregelen van de gebruikersorganisatie samen met de serviceorganisatie effectief zijn. In onderstaande tabel wordt aangegeven welke aanvullende beheersingsmaatregelen de gebruikersorganisatie zou moeten treffen ten aanzien van de in Bijlage 1 genoemde beheersingsmaatregelen. De opzet, het bestaan en de werking van deze aanvullende interne beheersingsmaatregelen hebben wij niet geëvalueerd.

**LET OP! ONDERSTAANDE TABEL IS SLECHTS EEN VOORBEELD**

| **#** | **Criteria** | **Gewenste interne beheersingsmaatregelen van de gebruikersorganisatie** |
| --- | --- | --- |
| **De onderstaande beheersingsmaatregelen vallen gedeeltelijk onder de verantwoordelijkheid van de gebruikersorganisatie:** | | |
| 1 | 1, 9, 11, 13, 25, 26 | De gebruikersorganisatie dient als verwerkingsverantwoordelijke, conform de wettelijke vereisen, organisatorische maatregelen te treffen zoals:   * het identificeren en documenteren van alle verwerkingen van politiegegevens binnen de organisatie (#1); * het identificeren van verwerking van bijzondere categorieën en het vaststellen van regels hieromtrent (#9); * het aanstellen van een (of meerdere) bevoegde functionaris(sen) en het vaststellen van de daarbij behorende taken, bevoegdheden en verantwoordelijkheden (#11); * het vaststellen en vastleggen van afspraken met de leverancier(s) (verwerker(s)) (#13); * het vaststellen en implementeren van een proces dat ziet op de informatievoorziening aan de betrokkene, recht op inzage, rectificatie en verwijdering (#25); * het bijhouden van een register conform artikel 31d lid 1 (#26). |
| 2 | 2, 3, 17, 21 | De gebruikersorganisatie dient ervoor te zorgen dat:   * boa’s de BOA applicatie gebruiken conform de wettelijke bepalingen en de gebruikershandleiding(en), zoals:   + het voorkomen van het zonder noodzaak aanleggen van registraties van politiegegevens buiten de boa applicatie (zgn. 'schaduwsystemen') (#2);   + het achterwege laten van alle gegevensinvoer die niet absoluut noodzakelijk is op grond van de in de wet genoemde doeleinden (#3);   + het alleen verstrekken van politiegegevens aan de bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties als bedoeld in art. 15a voor zover dat voortvloeit uit een rechtsinstrument op grond van het verdrag betreffende de werking van de Europese Unie (#17);   het alleen verstrekken van politiegegevens aan anderen dan politie en Koninklijke marechaussee voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd (#21). |
| 3 | 6 | De gebruikersorganisatie dient:   * gegevensbeschermingsbeleid en procedures te ontwikkelen en vast te stellen, en, waar nodig geacht en DPIA’s uit te voeren (#6); * maatregelen te implementeren die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) (#6). |
| 4 | 10, 28 | De gebruikersorganisatie dient:   * regels vast te stellen voor het zorgvuldig omgaan met accounts en wachtwoorden (zoals het niet delen hiervan e.d.) (#10); * periodiek (minimaal jaarlijks) controles uit te voeren op de uitgegeven rechten (accountcontrole) (#10); * periodiek (minimaal jaarlijks) controles uit te voeren op het rechtmatig gebruik van deze rechten (m.g.v. de logging) (#28). |
| 5 | 27, 30 | De gebruikersorganisatie dient als verwerkingsverantwoordelijke:   * te zorgen voor de schriftelijke vastlegging van inbreuken op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie (#27); * een procedure voor beheer van privacy-incidenten en -inbreuken op te stellen en te implementeren (#30); * met <opdrachtgever> afspraken te maken over de behandeling van (vermoede) privacy-incidenten en -inbreuken (bijvoorbeeld in de Verwerkersovereenkomst) (#30). |
| **De onderstaande beheersingsmaatregelen vallen geheel onder de verantwoordelijkheid van de gebruikersorganisatie** | | |
| 6 | 15, 18, 19, 22, 23, 24, 27, 29, 31 | De gebruikersorganisatie dient als verwerkingsverantwoordelijke:   * processen vast te leggen en te implementeren m.b.t.:   + geautomatiseerde individuele besluitvorming (#15);   + geautomatiseerd vergelijken en in combinatie zoeken #18);   + voor artikel 13 verwerkingen vooraf voldaan wordt aan de wettelijke vereisten (#19);   + het vastleggen van doorgiften aan derde landen (#22), met inbegrip van de schriftelijke vastlegging van de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf (#27);   + verstrekking aan derden structureel voor samenwerkingsverbanden (#23);   + rechtstreekse verstrekking (#24);   + een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1 (#27); * conform de Regeling periodieke audit politiegegevens jaarlijks interne audit, en periodiek (na 2 jaar en vervolgens om de 4 jaar) externe audits te laten uitvoeren (#29); * een functionaris gegevensbescherming (FG) aan te stellen voor de Wpg en de daarbij behorende taken, bevoegdheden en verantwoordelijkheden vast te stellen (#31). |

**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 inllustratieve 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 3 | Nood-  zakelijkheid & rechtmatig-heid, 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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.  Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 6 | Gegevens-bescherming door beveiliging en ontwerp | Art 4a lid 1 t/m 5 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 7 | Gegevens-bescherming door standaard-instellingen | Art 4b lid 1a en lid 1b | De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:   1. alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking; 2. politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 8 | Gegevens-beschermings-effectbeoordeling/ 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 9 | Bijzondere categorieën van politie-gegevens | Art 5 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 11 | Autorisaties: aanwijzen functionaris-sen | Art 6 lid 7 | Er is een actuele lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 13 | Verwerker en Verwerkers-overeenkomst | Art 6c | 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.  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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 14 | Geheim-houdings-plicht | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 15 | Geauto-matiseerde individuele besluit-vorming | Art 7a | 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.  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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 16 | Uitvoering van de dagelijkse politietaak | Art 8 lid 1 en 2 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 17 | Ter beschikking stellen van politie-gegevens binnen het WPG-domein | Art 4 lid 1 Art 8 lid 4 Art 9 lid 3 Art 15 lid 1 en 2 Art 15a lid 1 en 2 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 18 | Geautomati-seerd 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 | 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 19 | Onder-steunende 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). | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 20 | Bewaar-termijnen, verwijderen en vernietigen | Art 4 lid 2 Art 8 lid 6 Art 9 lid 4 Art 14 | 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 als genoemd in de Archiefwet voldaan. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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.  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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 23 | Verstrekking aan derden structureel voor samen-werkings-verbanden | Art 20 | De verantwoordelijke 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 24 | Rechtstreekse verstrekking | Art 23 | 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 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 | 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 26 | Register | Art 31d lid 1 en 2 | De verwerkingsverantwoordelijke houdt een register bij dat de volgende gegevens bevat:   1. de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming; 2. de doelen van de verwerking; 3. de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties; 4. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens; 5. **in voorkomend geval, het gebruik van profilering;** 6. in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie; 7. **een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn;** 8. zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd; 9. zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a; 10. **de toekenning van de autorisaties, bedoeld in artikel 6.**   De verwerker houdt een register bij dat de volgende gegevens bevat:   1. 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; 2. de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn uitgevoerd; 3. 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 4. indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 27 | Documentatie | Art 32 lid 1 t/m 4 | 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 29 | Audits | Art 33 | Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 30 | Melding datalekken | Art 33a | 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 AP 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |
| 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 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 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. | (DOORGAANS) GEEN VERANTWOORDELIJKHEID VAN DE SERVICEORGANISATIE | N.v.t. |

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

| **#** | **Onderwerp** | **Beheersingsmaatregelen** | **Testwerkzaamheden / Bevindingen** | **Conclusies / 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 4 | Cryptografie | Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersingsmaatregelen 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |
| 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. | BESCHRIJF DE TESTWERKZAAMHEDEN/BEVINDINGEN T.A.V. (ONDERSTEUNENDE) BEHEERSINGSMAATREGELEN DIE DOOR DE SERVICEORGANISATIE ZIJN OPGEZET EN GEIMPLEMENTEERD. |  |

1. 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 politiegegegevens). [↑](#footnote-ref-1)