Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Privacyaudit WPG Agentschap Telecom

Definitief

Colofon

Titel	Privacy audit WPG Agentschap Telecom
Uitgebracht aan	Agentschap Telecom
Datum	20 december 2022
Kenmerk	2022-0000326303

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Inhoudsopgave

Colofon

Voor u ligt het assurance-rapport inzake de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van Agentschap Telecom 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 Auditdienst Rijk. 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 Agentschap Telecom, zoals een overzicht van de getoetste interne beheersmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen. Het voorliggende rapport is de 'short form' versie van ons rapport

1 Assurance-rapport van de onafhankelijke auditor

Aan: het Agentschap Telecom

1.1 Opdracht

Ingevolge de opdracht van het Agentschap Telecom 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 Agentschap Telecom bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht	VI	Optreden na constatering overtreding of van strafbare feiten	RP2000

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

1.4 Verantwoordelijkheden Agentschap Telecom

Agentschap Telecom is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de periode 01-01-2019 – 31-12-2021.

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 politiegegevens[1].

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] 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).

1.7 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 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.

1.8 Onderzoek naar de werking van beheersingsmaatregelen gedurende de verslagperiode

Ons onderzoek ten aanzien van opzet, bestaan en werking van beheersingsmaatregelen betreft de periode 01-01-2019 – 31-12-2021

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 het Agentschap Telecom 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 01-01-2019 – 31-12-2021[2], respectievelijk de 12 maanden voorafgaand aan de einddatum van de externe privacy audit Wpg 2021[3].
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).

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.

[2] Deze termijn geldt voor de in paragraaf 1.8 genoemde 'Toezichtmaatregelen'.
[3] Deze termijn geldt voor de overige, 'niet-Toezichtmaatregelen'.

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). Indien onderwerpen niet zijn onderzocht, wordt de reden hiervan aangegeven. De reden kan zijn 'niet onderzocht' (n.o) omdat opzet en/of bestaan ontoereikend is voor verdere onderzoek. Of 'niet van toepassing (n.v.t.) omdat het Agentschap Telecom alleen artikel 8 gegevens verwerkt en derhalve niet van toepassing is.

Toelichting gebruikte kleuren:
Groen - Voldoet aan de norm.
Oranje - Voldoet deels aan de norm. Om geheel aan de norm te voldoen dien(t)(en) de aanbeveling(en) te worden opgevolgd.
Rood - Voldoet niet aan de norm.
Grijs – Niet onderzocht indien onderwerpen niet zijn onderzocht, wordt de reden hiervan aangegeven (niet onderzocht (n.o) omdat opzet en/of bestaan ontoereikend is voor verdere onderzoek. Niet van toepassing (n.v.t.) omdat het Agentschap Telecom alleen artikel 8 gegevens verwerkt.).

Verwerking 1 Optreden na constatering overtreding of van strafbare feiten

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			n.o
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			n.o
4. Juistheid en volledigheid politiegegevens			n.o
5. Onderscheid feiten en oordeel			n.o
6. Gegevensbescherming door beveiliging en ontwerp			n.o
7. Gegevensbescherming door standaardinstellingen			n.o
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens	nvt	nvt	nvt
10. Autorisaties en toegang tot politiegegevens			n.o
11. Autorisaties: aanwijzen functionarissen	nvt	nvt	nvt
12. Onderscheid tussen verschillende categorieën van betrokkenen			n.o
13. Verwerker en Verwerkersovereenkomst			n.o
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming	nvt	nvt	nvt
16. Uitvoering van de dagelijkse politietaak			n.o
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein	nvt	nvt	nvt
18. Geautomatiseerd vergelijken en in combinatie zoeken	nvt	nvt	nvt
19. Ondersteunende taken	nvt	nvt	nvt
20. Bewaartermijnen, verwijderen en vernietigen		n.o	n.o
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee		n.o	n.o
22. Doorgiften aan derde landen	nvt	nvt	nvt
23. Verstrekking aan derden structureel voor samenwerkingsverbanden	nvt	nvt	nvt
24. Rechtstreekse verstrekking	nvt	nvt	nvt
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		n.o	n.o
26. Register			
27. Documentatie			n.o
28. Logging	nvt	nvt	nvt
29. Audits			n.o
30. Melding datalekken			n.o
31. Functionaris voor gegevensbescherming			n.o

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

1.12 Aanbeveling met betrekking tot de hercontrole

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

- Ten tijde van de audit was het Agentscap Telecom in proces om de openstaande vacature omtrent interne audit te vervullen. Aanwezigheid (en eventuele deskundigheid) van een interne auditfunctie met Wpg kennis derhalve niet volledig vervuld.
- Signifcant aantal tekortkomingen geconstateerd.

1.13 Beperkingen in gebruik en verspreidingskring

Het Agentschap Telecom dient ingevolge artikel 33 2e lid van de Wet politiegegevens een afschrift van de controleresultaten van de privacy audit aan de Autoriteit persoonsgegevens te zenden. In eerste instantie betreft dit het 'short form' rapport (rapport exclusief bijlagen). De Autoriteit persoonsgegevens kan, in het kader van haar toezichthoudende taak, het 'long form' rapport (rapport inclusief bijlagen) zonder opgaaf van redenen bij het Agentschap Telecom 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 het Agentschap Telecom en andere (rechts)personen.

De opdrachtgever, hoofd spectrummanagement, is eigenaar van dit rapport. De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdracht gevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

Den Haag, 20 december 2022

[redacted]

[redacted]

Senior Adviseur Bedrijfsvoering

Auditdienst Rijk

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 het Agentschap Telecom 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.
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 • De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. • Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.
5. Onderscheid feiten en oordeel Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
6. Gegevensbescherming door beveiliging en ontwerp • Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan. • De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd. • Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen). • De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.
7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: • alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking; • politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.
8. Gegevensbeschermings-effectbeoordeling / 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.

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

Onderwerpen en beheersingsmaatregelen
• Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. • Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.
18. Geautomatiseerd vergelijken en in combinatie zoeken • Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11. • Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4. • Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn. • Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.
19. Ondersteunende taken • Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).
20. Bewaartermijnen, verwijderen en vernietigen • Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. • De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd. • Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen zoals genoemd in de Archiefwet voldaan.
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee • Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd. • Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg). • Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. • 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: o Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, o Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, o Het doel waartoe dit is opgericht, o Welke gegevens worden verstrekt, o De voorwaarden onder welke de gegevens worden verstrekt en o Aan welke personen of instanties de gegevens worden verstrekt. • De daadwerkelijke verstrekking van gegevens wordt vastgelegd.

Onderwerpen en beheersingsmaatregelen
24. Rechtstreekse verstrekking • De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen. • De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering • De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de 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.
26. 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.
27. Documentatie • De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard. • De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie. • De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.
28. Logging • De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1. • De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.
29. Audits Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.
30. Melding datalekken • De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen. • De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd. • De melding van een datalek aan de Autoriteit Persoonsgegevens vindt tijdig en volledig plaats. • Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.
31. Functionaris voor gegevensbescherming • Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op: 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.

Onderwerpen en beheersingsmaatregelen
• 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.

Auditdienst Rijk
Postbus 20201 2500 EE Den Haag (070) 342 77 00

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Managementreactie auditrapport ADR Wpg

RDI en de Wpg
De Rijksinspectie Digitale Infrastructuur (RDI) heeft BOA's in dienst voor onder andere het handhaven van de Telecommunicatiewet. Sinds 2019 geldt de Wet politiegegevens (Wpg) voor organisaties met BOA's in dienst. Om te voldoen aan de Wpg heeft de RDI het programma Wpg gestart. Binnen dat programma wordt gewerkt aan de inbedding van de processen die worden geraakt door de Wpg in het RDI zaaksysteem Genius. Daarnaast vinden binnen het programma verschillende verbeteracties plaats. Het programma is gestart in 2019 en loopt tot eind 2023.

Externe audit Wpg
In het najaar van 2022 heeft de ADR een audit uitgevoerd op de naleving van de Wpg. De audit betrof de periode 2020 en 2021. Deze audit is de eerste externe audit op de Wpg nadat de wet is gaan gelden voor de RDI. De ADR constateert dat de RDI in de verslagperiode niet (geheel) voldoet aan de Wpg. Naar aanleiding van de bevindingen en aanbevelingen levert de RDI in maart een verbeterrapportage. In het najaar van 2023 volgt een her-audit door de ADR. De RDI verwacht dan stappen te hebben gezet in het voldoen aan de Wpg.

Genomen maatregelen
De RDI vindt het belangrijk om zorgvuldig om te gaan met persoonsgegevens en heeft al maatregelen genomen vanuit het programma Wpg. De verslagperiode loopt tot en met 2021, in 2022 en 2023 genomen maatregelen zijn nog niet zichtbaar in de auditrapportage. In de verbeterrapportage neemt de RDI al genomen maatregelen en aanvullende maatregelen op. De belangrijkste al genomen maatregelen worden hieronder toegelicht en hebben betrekking op het verbeteren van het vastleggen van processen, procesbeheersing, interne audit / controle en de inbedding van de processen die worden geraakt door de Wpg in het zaaksysteem Genius.

Verbeteren vastleggen processen
De RDI werkt aan het verbeteren van de vastlegging van processen en procedures. In het eerste half jaar van 2023 rondt de RDI dit af voor de processen en procedures waarvoor de Wpg geldt. Het beeld dat wordt geschetst in het auditrapport, waarbij op verschillende normen bevindingen zijn gedaan in opzet en bestaan, is herkenbaar. Met het verbeteren van de vastlegging van processen en procedures verwacht de RDI stappen te hebben gezet.

Procesbeheersing
Procesbeheersing is een onderwerp waar dit jaar meer aandacht voor zal zijn, onder andere door het verder ontwikkelen van de rol Chief Privacy Officer (CPO). De functie CPO is nieuw binnen de RDI en heeft een belangrijke rol in procesbeheersing.

Interne audit / control
Door personeelsverloop is in de afgelopen jaren druk komen te staan op de interne auditfunctie. In 2023 wil de RDI acties ondernemen om capaciteit en kennis binnen interne audit te vergroten.

Inbedding in het zaaksysteem
De RDI is bezig met het inbedden van de processen die de Wpg raken in het zaaksysteem Genius. De audit heeft zich gericht op het oude systeem RP2000. De implementatie van het nieuwe systeem lost een aanzienlijk deel van de bevindingen op. De start van de implementatie staat gepland in 2023.

Een investering in het oude systeem is niet haalbaar. Dat betekent dat de RDI nog niet geheel voldoet aan de Wpg totdat ook deze processen zijn geïmplementeerd en aantoonbaar worden gevolgd.

Functionaris voor gegevensbescherming
Over de invulling van norm 31 Functionaris voor gegevensbescherming en de bevindingen hierop gaat de RDI in gesprek met de ADR. Beelden over de invulling van de functie Functionaris voor gegevensbescherming verschillen.