Auditdienst Rijk
Ministerie van Financiën

Privacy audit Wpg 2014
Rijksrecherche

Colofon

Titel	Privacy audit Wpg 2014 Rijksrecherche
Uitgebracht aan	Directeur Rijksrecherche
Datum	19 februari 2015
Kenmerk	ADR/2015/187

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1	**Assuranceverklaring**	**4**
2	**Samenvatting**	**5**
3	**Inleiding**	**6**
3.1	Aanleiding	6
3.2	Uitvoering privacy audit	6
3.3	Doelgroep van het rapport	7
4	**Bevindingen**	**8**
5	**Ondertekening**	**24**

1 Assuranceverklaring

In het najaar van 2014 heeft de Auditdienst Rijk (ADR) van het ministerie van Financiën in opdracht van de directeur van de Rijksrecherche een privacy audit uitgevoerd op grond van de Wet politiegegevens (Wpg) naar de verwerkingen die in de Wpg zijn beschreven bij de Rijksrecherche. De audit is uitgevoerd in de maanden oktober 2014 t/m januari 2015.

Deze privacy audit had tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij de Rijksrecherche.

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits) ' van juni 2006, van het NIVRA en de NOREA.

Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen bij de Rijksrecherche, naar de stand van januari 2015, in opzet, bestaan en werking niet volledig heeft voldaan aan de vereisten zoals genoemd in de Wpg.

Deze conclusie is onderworpen aan de inherente beperkingen die in paragraaf 3.2 van dit assurance-rapport zijn genoemd.

Het oordeel heeft betrekking op de zogenaamde verwerkingen genoemd in de Wpg. Het hierbij gehanteerde normenkader omvat de door de Rijksrecherche te nemen maatregelen.
Tekortkomingen op deze vlakken hebben uiteindelijk geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de directeur Rijksrecherche, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. De resultaten van het verbeterrapport en de uitgevoerde hercontrole zullen in de volgende privacy audit worden meegenomen.

Den Haag, d.d. 19 februari 2015,

Persoonsgebonden informatie

2 Samenvatting

Wij hebben geconcludeerd dat het stelsel van maatregelen en procedures ter bescherming van politiegegevens bij de Rijksrecherche, in opzet, bestaan en werking niet volledig heeft voldaan aan de eisen die de Wet politiegegevens daaraan stelt. Wij werken de belangrijkste bevindingen die hebben geleid tot deze conclusie hieronder uit.

Autorisaties
Er is geen autorisatieoverzicht beschikbaar waarin alle medewerkers zijn opgenomen. Daarnaast vindt geen vastlegging plaats van de toekenning, wijziging of verwijdering van autorisaties.
In Summ-IT worden medewerkers per onderzoek geautoriseerd en gedéautoriseerd door de bevoegd functionarissen. Je kunt dus slechts per onderzoek nagaan wie welke autorisaties heeft.
Een ander aandachtspunt is het verwijderen van autorisaties bij voltooide onderzoeken. Een voltooid onderzoek is weliswaar niet meer te raadplegen, maar als een voltooid onderzoek om een bepaalde reden na afsluiting nog geopend moet worden, krijgen alle tot dat onderzoek geautoriseerde medewerkers weer toegang.

Interne Audit
De Rijksrecherche beschikt niet over een eigen interne auditor. Er is geen interne audit uitgevoerd die voldoet aan de eisen die gesteld worden aan een interne audit. Bij wijze van interne audit heeft de privacyfunctionaris van de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) het jaarverslag 2013 van de privacyfunctionaris over de Rijksrecherche beoordeeld.

Ondanks deze tekortkomingen hebben wij geconstateerd dat privacybescherming binnen de Rijksrecherche als een belangrijk principe wordt gezien. In het strafvorderingsproces zijn veel waarborgen ingebouwd ter bescherming van persoonsgegevens. Ook het systeem Summ-IT draagt bij aan het handhaven van de voorschriften uit de Wpg.

3 Inleiding

3.1 Aanleiding

De Wet politiegegevens (Wpg) is op 1 januari 2008 in werking getreden en ook van toepassing op de verwerking van persoonsgegevens door de Rijksrecherche. De Wpg schrijft 'de verantwoordelijke' voor om periodiek een privacy audit uit te laten voeren op de naleving van de regels die als gevolg van die wet van toepassing zijn op het verwerken van politiegegevens (artikel 33 lid 1). Tevens dient 'deze verantwoordelijke' tijdig opdracht te verstrekken aan een auditinstelling om de vierjaarlijkse privacy audit uit te voeren.

De directeur van de Rijksrecherche is de verantwoordelijke voor de gegevensverwerking door de Rijksrecherche. De Rijksrecherche heeft de Auditdienst Rijk (ADR) gevraagd de privacy audit in 2014 uit te voeren.

De opdracht is beschreven in het document 'Plan van aanpak Wet Politiegegevens Rijksrecherche Privacy audit ' van 10 november 2014.

3.2 Uitvoering privacy audit

De privacy-audit is uitgevoerd conform de richtlijnen voor het uitvoeren van privacy-audits van de Nederlandse Orde van EDP Auditors (NOREA). Conform richtlijn 3600 van de NOREA.

Het onderzoek is gedaan volgens een door de ADR opgesteld werkprogramma. De uitgevoerde werkzaamheden bevatten onder meer: het beoordelen van het jaarverslag van de privacyfunctionaris, het houden van interviews onder medewerkers en leidinggevenden, het uitvoeren van deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie. De privacy-audit heeft zich gericht op het verkrijgen van een redelijke mate van zekerheid ten aanzien van de hieronder genoemde doelstelling en objecten.

Het doel[1] van de de privacy-audit is op systematische wijze te toetsen of aan de bepalingen van de Wet politiegegevens op adequate wijze uitvoering is gegeven.

Concreet betekent dit het beantwoorden van de vraag in hoeverre is geborgd dat voldaan wordt aan wetsartikelen van de Wpg die betrekking hebben op de Rijksrecherche. Het gaat hierbij om de volgende vier hoofdgebieden:

- Algemene uitgangspunten Wpg (art. 1-7)
- Verwerking van politiegegevens (art. 8-15)
- Verstrekking van politiegegevens (art. 16-24)
- Toezicht (art. 32-36)

In de door de ADR uitgevoerde privacy-audit is alleen de Rijksrecherche beoordeeld. De ADR heeft geen onderzoek verricht naar de door de VtsPN aan de Rijksecherche geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij de VtsPN of bij anderen dan de Rijksrecherche.
In de audit zijn de Wpg artikelen die op de Rijksrecherche van toepassing zijn, meegenomen. Voor de beoordeling van de opzet en het bestaan is uitgegaan van de peildatum van 1 november 2014. De beoordeling van de werking omvat de maatregelen en procedures die in de borging van de wettelijke eisen uit hoofde

1 Conform artikel 2, lid 2 Regeling periodieke audit politiegegevens

van de Wpg moeten voorzien. De werking is, voor zover mogelijk, beoordeeld over de periode van 1 november 2013 tot 1 november 2014.

Het conceptrapport is op 5 februari 2015 afgestemd met de Rijksrecherche.

3.3 Doelgroep van het rapport

Het auditrapport is vertrouwelijk en niet bestemd voor het maatschappelijk verkeer.

Het rapport wordt aangeboden aan de directeur Opsporing van de Rijksrecherche, die voor verdere verspreiding zorg draagt.

4 Bevindingen

In dit hoofdstuk zijn de bevindingen vanuit de privacy audit samengevat per artikellid van de Wpg die van toepassing zijn op de Rijksrecherche. De bevindingen zijn verwerkt in een matrix waarbij in kleur de scores zijn aangegeven van de beoordeling van de opzet, het bestaan en de werking. Daarbij hebben we de volgende criteria gehanteerd:
Groen: Er wordt in hoofdlijnen voldaan aan de norm.
Oranje: Er wordt niet of niet geheel voldaan aan de norm of er is een acceptabel actieplan.
Rood: Er wordt niet voldaan aan de norm en er is geen acceptabel actieplan.
Grijs: Niet vast te stellen of niet van toepassing.

Norm	Aspect	Bevindingen en oordeel	O	B	W
Paragraaf 1 Algemene uitgangspunten (artikel 1 tm 7 Wpg Toezicht)					
4.1 en 34	De verantwoordelijke heeft organisatorische (toezichtshoudende) maatregelen genomen zodat hij indien nodig maatregelen kan nemen.	**Privacy Functionaris** Opzet: De privacyfunctionaris van de Rijksrecherche is benoemd en aangemeld bij het CBP. De privacyfunctionaris is geautoriseerd voor alle relevante modules in Summ-IT en kan zelfstandig controlewerkzaamheden uitvoeren. Bestaan en werking: De privacyfunctionaris wordt in voldoende mate in staat gesteld zijn werkzaamheden uit te voeren. Hij heeft de benodigde autorisaties en heeft in overleg met de kerninstructeurs Summ-IT bepaald hoe hij zijn controle op o.a. autorisaties en bewaartermijnen kan opzetten en uitvoeren. Er is een plan van aanpak voor de privacy controle (augustus 2013). De controle heeft zich gericht op: • Doelbinding • Autorisaties • Ter beschikking stellen • Bewaartermijnen • Verwerken van politiegegevens op gezamenlijke schijven en persoonlijke mappen. De privacyfunctionaris voert zijn controles uit in samenwerking met de kerninstructeurs Summ-IT. De resultaten van de controles liggen vast in het jaarverslag over 2013.			
4.1 en 33.1		**Interne Audit** Opzet De Rijksrecherche beschikt niet over een eigen interne auditor en zoekt in de toekomst mogelijk samenwerking met BOD'en om de interne audit vorm te kunnen geven. Bestaan en werking: Bij wijze van interne audit heeft de privacyfunctionaris van de FIOD het jaarverslag 2013 van de privacyfunctionaris beoordeeld. Er is geen interne audit uitgevoerd die voldoet aan de eisen die gesteld worden aan een interne audit.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
Paragraaf 1 Algemene uitgangspunten (artikel 1 tm 7 Wpg uitvoering TCI)					
3	Noodzakelijkheid, rechtmatigheid en doelbinding	Zie paragraaf 2			
4.1	Er zijn maatregelen genomen die moeten borgen dat politiegegevens juist en nauwkeurig zijn. Indien politiegegevens onjuist of onvolledig zijn, worden deze gecorrigeerd, aangevuld of vernietigd.	Opzet: De organisatie rondom de eerste vastlegging van gegevens is goed geregeld. Opsporingsambtenaren zijn gerechtigd om te werken met politiegegevens (Strafvordering 142) en hebben in hun opleiding voldoende meegekregen over het belang van juistheid en nauwkeurigheid voor het strafproces. Voor de vastlegging wordt gebruik gemaakt van Summ-IT en daarin zijn verplichte invoervelden opgenomen: soort onderzoek, doel van het onderzoek, afdeling, onderzoeksnaam. Bestaan: De voortgang van de onderzoeken heeft de aandacht van het management en wordt 1x per 2 weken besproken in het operationeel overleg. De juistheid en nauwkeurigheid komen daar ook aan de orde. Werking: Toetsing van de werking van deze norm is ingebed in het werkproces. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
4.2	Verwijderen en vernietigen	Zie paragraaf 2			
4.3	Er zijn passende technische en organisatorische maatregelen genomen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Dat geldt vooral indien gegevens via een netwerk worden verzonden of beschikbaar gesteld via directe geautomatiseerde toegang.	Opzet: De Rijksrecherche sluit voor wat betreft het informatiebeveiligingsbeleid aan op het integraal beveiligingsbeleid van het Openbaar Ministerie. De fysieke beveiliging is onderdeel van de beveiliging van het Openbaar Ministerie. De toegangsbeveiliging maakt onderdeel uit van de beveiliging van het Paleis van Justitie. Op de afdeling zelf is sprake van zonering, waarbij alleen geautoriseerde medewerkers toegang hebben tot een bepaalde zone. Vanwege de geringe omvang van de IT-afdeling bestaat onvoldoende scheiding tussen de ICT-functie en de gebruikersorganisatie. Hierdoor ontstaat het risico op onrechtmatig gebruik. Volledige functiescheiding is binnen deze afdeling van 6 personen niet haalbaar gebleken. Er is toch getracht om functiescheiding aan te brengen door 2 onderhoudsmedewerkers in een flexibele schil te plaatsen. Al naar gelang de behoefte kunnen deze medewerkers met aparte rollen (systeembeheer en applicatiebeheer) worden ingezet. Bestaan: Tot en met 2013 werd een jaarlijkse quick scan uitgevoerd op de naleving van de normen uit het 'normenkader informatiebeveiliging OM'. Op dit moment is het alarmsysteem van de Rijksrecherche nog niet aangesloten op het Openbaar Ministerie. Dit komt doordat de Rijksrecherche onlangs is verhuisd. In dit kader is een Security Assessment Herhuisvesting Rekencentrum Rijksrecherche uitgevoerd.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
		De toegangsbeveiliging is strikt geregeld. Bij binnenkomst in het Paleis van Justitie dient men zich aan te melden bij de beveiliging. De afdeling waar de Rijksrecherche is gehuisvest kan alleen onder begeleiding betreden worden. Bij het verlaten van een afdeling moet men door een sluis. De zonering van de afdeling is uitgewerkt in een lijst, waarin per medewerker is opgenomen tot welke zone hij/zij toegang heeft. Werking: Uit de quick scan zijn zes onvolkomenheden gebleken waarop actie is ondernomen voor zover dat relevant en binnen de middelen van de Rijksrecherche haalbaar was. Er zijn geen beveiligingsissues geweest in de onderzochte periode. Doordat de Rijksrecherche onlangs (in november 2014) is verhuisd, hebben wij de werking van de fysieke beveiliging niet kunnen toetsen.			
		Autorisaties Zie paragraaf 6.1			
4.4, 4.5	Toegang van verantwoordelijke, interne auditor, externe privacy auditor, privacyfunctionaris, functionaris gegevensbescherming, bewerker tot gegevens etc.	Zie paragraaf 5			
4.6	Duidelijk is vastgelegd wat de bevoegdheden en verantwoordelijkheden zijn van de externe bewerker.	De Rijksrecherche heeft geen externe bewerker. Niet van toepassing.			
5	Gevoelige gegevens	Zie paragraaf 2			
6.1	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verantwoordelijke heeft die personen die vanuit hun functie toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens. Let hierbij ook op personen die niet onder de verantwoordelijke vallen.	Opzet: In het systeem Summ-IT worden autorisaties uitgegeven, gewijzigd en ingetrokken. Er kan geen historisch overzicht worden gegenereerd van autorisatieverstrekkingen, met datum van uitgifte en intrekking autorisatie. Deze functionaliteit zal niet in Summ-IT worden ingebouwd. (prioriteitstelling politie en teveel belasting van serverruimte). Mocht er onverhoopt een lekincident plaatsvinden, dan kan wel per onderzoek worden achterhaald welke personen toegang tot het onderzoek hadden in een bepaalde periode. Hiermee is het ontbreken van een historisch overzicht niet risicovol. De coördinator TCI is altijd op de hoogte van de toegang tot de TCI gegevens. De privacyfunctionaris heeft voldoende bevoegdheden om autorisaties te monitoren en hier controle op uit te voeren.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
		Bestaan en werking: In Summ-IT worden medewerkers geautoriseerd en gedéautoriseerd door de bevoegd functionarissen. Deze handeling maakt deel uit van het reguliere werkproces. Autorisaties zijn gekoppeld aan rollen en aan de rollen zijn personeelsnummers gekoppeld. Medewerkers die uit dienst zijn getreden worden automatisch gedéautoriseerd doordat autorisaties gekoppeld zijn aan het personeelsnummer. Uit de controle van de privacyfunctionaris over 2013 blijkt dat in het algemeen zorgvuldig wordt omgegaan met het autoriseren en de-autoriseren van medewerkers. Deze controle vindt 2x per jaar plaats door de privacyfunctionaris, ondersteund door een kerninstructeur Summ-IT. Een aandachtspunt is het verwijderen van autorisaties bij voltooide onderzoeken. Een voltooid onderzoek is weliswaar niet meer te raadplegen, maar als een voltooid onderzoek om een bepaalde reden na afsluiting nog geopend moet worden, krijgen alle tot dat onderzoek geautoriseerde medewerkers weer toegang. Dat is een onwenselijke situatie.			
6.7, voor 9.3, 10.5, 11.1, 11.2, 11.4, 12.4, 12.5, en 13.3 Wpg	Bepaalde verwerkingen vereisen de toestemming door een bevoegd functionaris, of mogen alleen door een bevoegd functionaris worden uitgevoerd. (art. 9.3, 10.5 (verdere verwerking), 11.1, 11.2 en 11.4 (geautomatiseerd vergelijken) 12,4 en 12,5 (controle en beheer van informanten) en 13.3 (ter beschikking stellen voor ondersteuning politietaak) De verantwoordelijke wijst deze bevoegd functionarissen aan.	**Bevoegd functionaris** Opzet: Bij de start van een onderzoek is het regiohoofd van de betreffende regio bevoegd functionaris. Dit is in Summ-IT vastgelegd. Bestaan en Werking: Deze handeling maakt deel uit van het reguliere werkproces. Afzonderlijke toetsing van de werking van deze norm heeft in het kader van de privacyaudit niet plaatsgevonden.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
7	De persoon die politiegegevens verwerkt is verplicht tot geheimhouding.	Opzet: Het schenden van de geheimhoudingsplicht is een misdrijf (art. 272 SR). Binnen de Rijksrecherche vindt bij iedere indiensttreding een A-screening plaats. Daarnaast wordt de eed afgelegd en krijgt iedere werknemer een cursusmap waarin de Wpg wordt behandeld. Bestaan: Er zijn geen schendingen van de geheimhoudingsplicht bekend binnen de Rijksrecherche. De soort werkzaamheden brengt met zich mee dat medewerkers zorgvuldig en integer omgaan met persoonsgegevens. Ethiek wordt in sessies met het MT besproken. De zaaks OvJ moet toestemming geven om medewerkers van buiten het politiedomein mee te laten werken aan een onderzoek. In die gevallen wordt een geheimhoudingsverklaring getekend. Werking: De aard van de norm maakt dat het niet mogelijk is de werking ervan te toetsen.			
Paragraaf 2 Verwerking (artikel 8 tm 15 Wpg)					
Artikelen 8 t/m 15 Wpg die betrekking hebben op verwerking van politiegegevens.					
3.1, 8.1, 9.1, 9.2, 10.1, 12.1	Bij het verwerken van politiegegevens moet altijd sprake zijn van doelbinding. Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden, dus: • Art. 8 dagelijkse politietaak; • art. 9 onderzoek voor rechtshandhaving in een bepaald geval • art. 10 inzicht in betrokkenheid bij bedreigingen van de rechtsorde (NCIE) • art. 12 controle en beheer van informanten (NCIE)	Opzet: Artikel 9 onderzoeken worden in Summ-IT opgestart. Daarbij is altijd sprake van doelbinding. Bij de start van een onderzoek wordt soms een globaal doel opgevoerd dat na de voorbereidingsfase wordt aangescherpt. Leiding RIS en TCI officier van Justitie hebben voor controledoeleinden toegang tot het informantenregister. Bestaan en werking: Er is door de privacyfunctionaris een onderzoek uitgevoerd naar doelbinding in onderzoek. De eisen uit het strafvorderingsproces waarborgen dat niet meer informatie wordt opgenomen dan noodzakelijk is voor het doel van de vastlegging. Het vastleggen van het doel van het onderzoek volgt automatisch uit het aanmaken van een onderzoek. Toetsing werking informantenregister nemen wij niet mee in deze audit.			
9.2, 13.4	Van landelijk raadpleegbare politiegegevens (VROS, HAVANK, HKS) wordt vooraf vastgelegd: • Het specifieke doel • De categorieën van personen en de gevallen waarin of de termijnen waarbinnen het verwerken wordt beëindigd	Opzet: In de instructie 'WPG :proces opsporing' is beschreven dat de bevoegd functionaris bij afronding van een onderzoek gegevens in de landelijk toegankelijke bakken laat plaatsen. De Rijksrecherche maakt altijd een bewuste keuze of gegevens worden overgedragen aan landelijke ondersteunende systemen. Als gegevens beschikbaar worden gesteld gebeurt dat via Summ-IT. De infodesk registreert dit. Bestaan: Beschikbaar stellen gebeurt zelden, maar men is zich er wel van bewust dat dit via de infodesk moet lopen.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
		Werking: Omdat deze handeling zelden voorkomt, hebben wij de werking van deze norm niet kunnen beoordelen.			
3.3	De gegevens mogen alleen voor een ander doel worden gebruikt als de Wpg daarin voorziet.	Doelafwijkend gebruik wordt uitgewerkt in paragraaf 3 (Verstrekkingen).			
3.1, 3.2 en 3.4	Voor artikel 9, 10 en 12 verwerkingen geldt dat de herkomst van de gegevens en de wijze van verkrijging vermeld moet zijn.	Opzet: Summ-IT heeft een verplicht invoerveld herkomst. Bestaan en werking: Vermelding van herkomst zit in strafvordering ingebakken. Als de herkomst van materiaal niet vermeld is, dan blijf een zaak niet overeind in de rechtbank. Werking: Toetsing van de werking van deze norm is ingebed in het werkproces. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
5	Gevoelige gegevens worden alleen vastgelegd als dat nodig is voor het doel van de verwerking.	Opzet: Het Wetboek van Strafvordering bepaalt dat geen gevoelige gegevens gevorderd mogen worden (Art. 126nd en nf). Bestaan: Alleen wanneer het voor een onderzoek relevant is, worden gevoelige gegevens opgenomen. Doordat meerdere personen aan een zaak in Summ-IT werken, geldt hier het vier-ogenprincipe. Werking: Toetsing van de werking van deze norm is ingebed in het werkproces. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
2.9 Bpg	De ambtenaren van politie die geautomatiseerd gegevens vergelijken dienen over voldoende kennis en vaardigheden te beschikken op het gebied van: a. (verschillende vormen van verwerking van politiegegevens, b. de wet- en regelgeving die relevant is voor de verwerking van politiegegevens, en c. methoden en technieken van informatieanalyse	Binnen de Rijksrecherche vindt het geautomatiseerd vergelijken van gegevens niet plaats. De Rijksrecherche doet altijd eigenstandig onderzoek. Als informatie van een politie-eenheid nodig is, dan wordt deze ter beschikking gesteld door of gevorderd bij de politie.			

Norm	Aspect	Bevindingen en oordeel	O	B	W
11.1, 11.2 en 11.3 2.11 Bpg	Als dat nodig is voor het onderzoek kunnen politiegegevens die voor dat onderzoek (art 9) zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 om vast te stellen of verbanden bestaan tussen de betreffende gegevens. Hetzelfde geldt voor een artikel 10 verwerking. Deze kunnen geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van de artikelen 8, 9 of 10. De gerelateerde gegevens kunnen, na instemming van de daartoe bevoegde functionaris, zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder worden verwerkt.	n.v.t.			
Norm/ Bevindingen *9.1, 10.1,* 11.4	In bijzondere gevallen kunnen in opdracht van het bevoegd gezag (officier van justitie of burgemeester), politiegegevens in combinatie met elkaar worden verwerkt teneinde vast te stellen of verbanden bestaan tussen de gegevens. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens, na instemming van een daartoe bevoegde functionaris voor dat onderzoek of die verwerking verder worden verwerkt.	<u>Opzet:</u> In de werkinstructie 'WPG : proces opsporing' is de procedure voor het in combinatie met elkaar verwerken opgenomen. Het gaat dan om gevorderde gegevens en niet om gegevens die de Rijksrecherche door geautomatiseerd vergelijken heeft verkregen. <u>Bestaan:</u> De werkinstructie benadrukt dat uitsluitend in bijzondere gevallen gegevens in combinatie met elkaar worden verwerkt. Deze procedure is in het werkproces meegenomen. Tot op heden is het niet voorgekomen. <u>Werking:</u> Tot op heden niet van toepassing en daarom niet getoetst.			

8.4, 9.3 en 10.5	Artikel 8, 9 en 10 gegevens kunnen ter beschikking worden gesteld voor verdere verwerking op grond van de artikelen 8, 9, 10 en 12. Voor verdere verwerking van artikel 9 en 10 gegevens geldt dat hiervoor toestemming nodig is van een daartoe bevoegde functionaris.	Binnen de Rijksrecherche vindt dit type verwerking niet plaats.			
10.1 en 10.2 10.3, 10.4, 11.5, 12, 4, 12.5, 13,1	Politiegegevens kunnen gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij het beramen of plegen van misdrijven. De verwerking vindt slechts plaats omtrent a. verdachten van die misdrijven b. personen t.a.v. wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van die misdrijven c. personen die in een bepaalde relatie staan tot a en b Ambtenaren van politie of buitengewoon opsporingsambtenaren als bedoeld in artikel 142, eerste lid van het Wetboek van Strafvordering.	Toetsing van de opzet van deze normen is ingebed in het werkproces/strafvordering. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			

Artikelen 8 t/m 15 Wpg die betrekking hebben op het ter beschikking stellen van politiegegevens.					
12.2	Artikel 12 gegevens kunnen gedurende een periode van maximaal vier maanden na de datum van eerste verwerking ter beschikking worden gesteld voor verdere verwerking op grond van de artikelen 8, 9 of 10. (Binnen deze termijn moet de betrouwbaarheid van de informant zijn vastgesteld, anders dreigt door toepassing van artikel 12 vermenging met artikel 10 onderzoeken).	Opzet: In de TCI werkinstructie is opgenomen dat informatie binnen vier maanden ter beschikking moet worden gesteld. In Summ-IT krijgt men een melding, een maand voordat deze vier maanden verstreken zijn. Bestaan: De TCI instructie is bekend bij medewerkers TCI. De TCI OvJ houdt toezicht op het naleven van deze termijn. Werking: Toetsing van de werking van deze normen is ingebed in het werkproces/strafvordering. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
15.1	De verantwoordelijke stelt politiegegevens ter beschikking aan personen die door zichzelf dan wel door een andere verantwoordelijke zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze nodig hebben voor de uitvoering van hun taak	Opzet: De procedure is beschreven in de 'instructie WPG: proces opsporing'. Bestaan: De bevoegd functionaris geeft in overleg met de zaaksofficier toestemming voor deze terbeschikkingstelling. Deze terbeschikkingstellingen worden gemuteerd in het algemeen journaal. Werking: Toetsing van de werking van deze norm is ingebed in het werkproces/strafvordering. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
15.2, 4 Bpg	Er zijn aan het ter beschikking stellen van politiegegevens weigeringsgronden verbonden	Opzet: De weigeringsgronden zijn opgenomen in de 'instructie WPG: proces opsporing'. Bestaan: De bevoegd functionaris voert een toets uit om te beoordelen of er weigeringsgronden zijn. Werking: Toetsing van de werking van deze norm is ingebed in het werkproces/strafvordering. Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden			

Artikelen 8 t/m 15 Wpg die betrekking hebben op de (bewaar)termijnen van politiegegevens					
	De applicatie is voorzien van een functionaliteit waarmee de politiegegevens binnen de gestelde termijnen worden verwijderd en vernietigd. Indien deze functionaliteit ontbreekt, zijn andere maatregelen getroffen en beschreven voor de verwijdering en vernietiging. Indien niet aanwezig is er een werkinstructie voor het toezicht op verwijdering en vernietiging. Hierin is aangegeven wie hier voor verantwoordelijk is en met welke periodiciteit controle plaatsvindt.	Opzet: Met de beheermodule van Summ-IT is het mogelijk de bewaartermijnen te beheren. Bestaan en werking: Zie volgende normen die bewaartermijnen betreffen.			
8.1, 8.2, 8.3 en 8.6	Normen die betrekking hebben op de dagelijkse politietaak.	Bij de Rijksrecherche is geen sprake van artikel 8 verwerkingen, waardoor deze normen niet van toepassing zijn.			
9.4	De politiegegevens die zijn verwerkt op grond van artikel 9.1, 10 en 12 en niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of gedurende een periode van maximaal een halfjaar verwerkt ten einde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in artikel 10.1 of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn verwijderd.	Opzet: Na afsluiting van een onderzoek kunnen de vastgelegde gegevens gedurende maximaal een jaar worden geraadpleegd. Dit is nodig om na te gaan of de gegevens aanleiding kunnen geven tot een nieuw onderzoek. Doordat het Openbaar Ministerie geen afloopberichten verstuurd is binnen de Rijksrecherche door het management bepaald dat na het intern afsluiten van een onderzoek een termijn wordt aangehouden van een jaar. Het vervolgens handhaven van de bewaartermijnen wordt automatisch bewaakt door Summ-IT die op de relevante momenten een signaal afgeeft voor het veiligstellen c.q. verwijderen van de opgeslagen gegevens. Bestaan: Uit het jaarverslag van de privacyfunctionaris blijkt dat niet in alle gevallen de voorziening Wpg in de beheermodule van Summ-IT bekend was. Met deze voorziening kan snel overzicht worden gegenereerd van onderzoeken die op raadplegen moeten worden gezet. Werking: Uit het jaarverslag van de privacyfunctionaris blijkt dat door de onbekendheid met de voorziening Wpg in de beheermodule van Summ-IT, onderzoeken niet altijd tijdig op raadplegen worden gezet.			

10.6	De politiegegevens, die worden verwerkt op basis van Art. 10 en 12, worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens periodiek gecontroleerd (art 10) en halfjaarlijkse controle art. 12. De gegevens worden verwijderd uiterlijk vijf jaar (art. 10) en 10 jaar (art 12) na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de politiegegevens van betrokkene.	<u>Opzet en bestaan:</u> Zie artikel 9.4 <u>Werking:</u> Toetsing van de werking van deze norm is ingebed in het werkproces/strafvordering (incl. toetsing door TCI officier). Afzonderlijke toetsing in het kader van de privacyaudit heeft niet plaatsgevonden.			
12.6	Artikel 12 gegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens elk half jaar gecontroleerd. De gegevens worden vernietigd uiterlijk tien jaar na de datum van laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van politiegegevens van betrokkene op grond van het doel, bedoeld in het eerste en vijfde lid.	<u>Opzet:</u> In Summ-IT wordt de startdatum ingevoerd en kan ingesteld worden dat je een signaal krijgt een maand voordat de viermaandentermijn verloopt. Je hebt dan nog een maand de tijd om nieuwe informatie te genereren zodat de termijn verlengd wordt. Met Summ-IT wordt ook de vernietingingstermijn gehandhaafd. Dit staat beschreven in de instructie 'WPG : proces opsporing'. <u>Bestaan:</u> De TCI officier is primair verantwoordelijk voor de controle op de handhaving van de bewaartermijnen. Hij maakt hiervan schriftelijk verslag en levert dat in bij de hoofdofficier. <u>Werking:</u> Gezien de gevoeligheid van gegevens die bij het TCI zijn opgeslagen, hebben wij de werking van deze norm niet getoetst. In het proces zijn naar onze mening in opzet en bestaan voldoende waarborgen ingebouwd voor de handhaving van de bewaartermijnen.			
14	Politiegegevens mogen na verwijdering maximaal vijf jaar worden bewaard en voor geen ander doel worden gebruikt dan voor de afhandeling van klachten en de verantwoording van verrichtingen. Verwijderde gegevens moeten na afloop van de bewaartermijn worden vernietigd.	<u>Opzet:</u> In de 'instructie WPG: proces opsporing' is de procedure beschreven. <u>Bestaan en werking:</u> De bewaartermijnen kunnen met Summ-IT beheerd worden. In Summ-IT worden de termijnen geautomatiseerd verwerkt. Met startdatum, einddatum, datum laatste verwerking en aantal dagen overschrijding. De directeur Opsporing tekent de vernietigingslijsten.			

14.2	Verwijderde gegevens worden gedurende de bewaartermijn niet verstrekt aan opsporingsambtenaren en gezagsdragers (16), inlichtingendiensten en buitenlandse opsporingsinstanties (17), derden structureel voor alle regio´s (18), derden incidenteel voor alle regio´s (19), derden structureel voor samenwerkingsverban den (20), rechtstreekse verstrekking (23) en rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten (24).	Dit komt bij de Rijksrecherche niet voor.			
14.3	In bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10, kunnen politiegegevens gedurende de bewaartermijn van 5 jaar na verwijdering, in opdracht van de Politiewet 1993 bevoegde gezag ter beschikking worden gesteld voor hernieuwde verwerking op grond van artikel 9 of 10.	<u>Opzet:</u> Hernieuwde verwerking komt zelden voor bij de Rijksrecherche. De privacyfunctionaris is zich bewust van het feit dat een opdracht van de Officier van Justitie nodig is voor hernieuwde verwerking (onderwerp in controleverslag privacyfunctionaris). <u>Bestaan en werking:</u> De handelswijze bij hernieuwde verwerking is bekend. Hernieuwde verwerking komt zelden voor bij de Rijksrecherche. Wij hebben de werking van deze norm daarom niet kunnen beoordelen.			
14.4	Van de vernietiging wordt afgezien als de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. In dat geval worden de gegevens zo spoedig mogelijk overgebracht naar een archiefbewaarplaats. Met toepassing van artikel 15 van de Archiefwet 1995 worden beperkingen aan de openbaarheid gesteld.	<u>Opzet:</u> In de 'instructie WPG : proces opsporing' is vastgelegd dat de documentalist met de directeur Opsporing afstemt of een dossier in aanmerking komt voor archivering in het Nationaal Archief als gevolg van cultureel of historisch belang. <u>Bestaan en werking:</u> De Rijksrecherche is momenteel bezig met het opschonen van het archief en het overbrengen naar het Nationaal Archief van dossiers die van cultureel of historisch belang zijn. Gezocht wordt nog naar een manier waarop de dossiers onder embargo kunnen blijven zonder dat per dossier te moeten motiveren.			

Paragraaf 3 Verstrekkingen (artikel 16 t/m 24 Wpg)					
Art. 16 t/m 24 Wpg)	Politiegegevens worden alleen 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.	Opzet: Structurele verstrekking komt niet voor bij de Rijksrecherche (Instructie WPG : proces opsporing). Binnen de Rijksrecherche worden in uitzonderingsgevallen politiegegevens verstrekt buiten het politiedomein. Ten behoeve van de incidentele gegevensuitwisseling met de belastingdienst, is een convenant afgesloten waarmee het verstrekken van gegevens formeel is geregeld. Verder is binnen de Rijksrecherche afgesproken dat alle verstrekkingen lopen via de privacyfunctionaris waarbij de uiteindelijke goedkeuring door de verantwoordelijke wordt afgestemd met de zaaksofficier. Bestaan en werking: Verstrekkingen wijzer is aanwezig en vastgelegd in een ordner. Verstrekkingen vinden zelden plaats. Wij hebben de werking van deze norm niet beoordeeld.			
17	Politiegegevens kunnen worden verstrekt aan buitenlandse Inlichtingen en Veiligheidsdiensten, en aan politieautoriteiten in andere landen, en de BES-eilanden, als bij de ontvangende instantie voldoende waarborgen aanwezig zijn voor een juist gebruik van de verstrekte gegevens, en bescherming van de privacy.	Opzet, bestaan en werking: De Rijksrecherche heeft in dit kader nog geen verzoeken gehad.			
20	De verantwoordelijke heeft geborgd dat alleen informatie in samenwerkingsverbanden wordt verstrekt met de volgende doeleinden: Het voorkomen en opsporen van strafbare feiten Het handhaven van de openbare orde Het verlenen van hulp aan hen die dat nodig hebben Het uitoefenen van toezicht op het naleven van regelgeving	Opzet, bestaan en werking: Verstrekking in samenwerkingsverbanden komt tot op heden niet voor bij de Rijksrecherche.			

7	Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.	Opzet, bestaan en werking: In het protocol met de belastingdienst is geheimhoudingsplicht vastgelegd. Bij verstrekkingen is de integriteit van de ontvangende partij een vereiste. Bij twijfel wordt niet verstrekt. Er wordt uitsluitend verstrekt na toestemming van de zaaksofficier. De ontvangende partij moet een geheimhoudingsverklaring tekenen.			
Art. 6.1, 6.2 en 6.3 Bpg-BOD 4.1 t/m 5.1 Bpg	Bijzondere opsporingsdiensten kunnen (met instemming van de bevoegd functionaris) politiegegevens verstrekken etc...	De Rijksrecherche is geen BOD.			
Rechtsbescherming (artikel 25 t/m 31 WPG					
25, 26, 27	Als een persoon daarom schriftelijk verzoekt deelt de verantwoordelijke binnen zes weken mee of, en zo ja welke, politiegegevens over deze persoon zijn vastgelegd. Desgevraagd meldt hij of in een periode van vier jaar voorafgaand aan het verzoek gegevens zijn verstrekt, en aan welke ontvangers of categorieën van ontvangers is verstrekt. De verantwoordelijke kan vier weken uitstel nemen, of hoogstens zes weken, indien bij een andere eenheid gegevens over de verzoeker worden verwerkt.	Opzet: De procedure ten aanzien van de rechten van betrokkene is adequaat beschreven in de 'werkinstructie WPG : proces opsporing'. Gegevensverzoek in het kader van Wpg/WOB wordt bij de staf ingediend. In geval van bezwaar: college van procureurs generaal. Bestaan: De privacyfunctionaris ontvangt vrijwel geen typische Wpg verzoeken. Het gaat eerder om de vraag of iemand in systemen voorkomt. Veelal wordt daarvoor door de verzoeker de WOB als grondslag gebruikt. Werking: In de onderzoeksperiode is slechts 1 keer een verzoek binnengekomen. Het verzoek is vastgelegd in een ordner bij de privacyfunctionaris.			
28 + 30	Een persoon kan verzoeken gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt.	Opzet: De procedure ten aanzien van de rechten van betrokkene is adequaat beschreven in de 'werkinstructie WPG : proces opsporing'. Bestaan en werking: Verzoeken tot wijziging van gegevens zijn tot dusver niet voorgekomen.			

Toezicht (artikel 32 t/m 36 Wpg)					
32 6.4.2. Bpg, 6.4.3 Bpg	Protocolplicht De privacyfunctionaris houdt een overzicht bij van de schriftelijke vastlegging van de volgende gegevens:	Zie hieronder			
	Vastleggen doel	Opzet: Nieuwe onderzoeken worden in Summ-IT aangemaakt. Daarbij is het doel van het onderzoek ook vastgelegd. Bestaan en werking: De privacyfunctionaris houdt voor het zaaksoverleg een overzicht bij van de doelen van lopende onderzoeken. De doelen liggen vast in Summ-IT.			
	Art. 13 verwerkingen	Opzet: Art. 13 verstrekkingen worden via de infodesk in Summ-IT vastgelegd. Bestaan en werking: De privacyfunctionaris houdt geen afzonderlijk overzicht bij, maar kan dit wel bij de infodesk opvragen. Wij hebben de werking niet getoetst.			
	Autorisaties	Opzet: Autorisaties worden niet gelogd. Er is daardoor geen overzicht beschikbaar. Bestaan en werking: De toekenning van autorisaties wordt niet gelogd en dus ook niet vastgelegd bij de privacyfunctionaris.			
	Geautomatiseerde vergelijking of in combinatie met elkaar verwerken	Deze handelingen worden door de Rijksrecherche niet verricht.			
	Hernieuwde verwerking	Opzet: Een hernieuwde verwerking moet worden vastgelegd in Summ-IT. In het jaarverslag van de privacyfunctionaris zijn de eisen voor vastlegging opgenomen. Bestaan en werking: Hernieuwde verwerking komt zelden voor.			
	Verstrekkingen	Opzet: De privacyfunctionaris houdt een overzicht bij van verstrekkingen. Bestaan en werking: Er is een overzicht van de verstrekkingen.			
	Onrechtmatige verwerkingen	Opzet: Indien een onrechtmatige verwerking zich voordoet moet dit worden vastgelegd in Summ-IT en melding worden gedaan bij de privacyfunctionaris. Bestaan en werking: De privacyfunctionaris is zich bewust van zijn rol bij het registreren van onrechtmatige verwerkingen. Hij kan hier alleen op basis van signalen handelen. Dat heeft zich nog niet voorgedaan.			

	Geautomatiseerd vergelijken met andere dan politiegegevens	De Rijksrecherche vergelijkt niet geautomatiseerd met andere dan politiegegevens.			
	Gemeenschappelijke verwerkingen	<u>Opzet:</u> De Rijksrecherche kent geen gemeenschappelijke verwerkingen. In het jaarverslag wordt er wel aandacht aan gegeven. Mocht een gemeenschappelijke verwerking nodig zijn, dan dient dit gemeld te worden bij de privacyfunctionaris die dit vervolgens in Summ-IT opneemt.			
33 Audits 33.1, 33.2, 33.5 wpg 6.5 bpg 3 RPAP	Twee jaar na inwerkingtreding van de wet, en vervolgens eenmaal in de vier jaar, laat de verantwoordelijke een privacy audit door een onafhankelijke auditor uitvoeren. Tenminste jaarlijks vindt een interne audit plaats. De interne audit en de interne auditor voldoen aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens. De interne auditor heeft toegang tot alle voor zijn audit benodigde gegevens.	<u>Opzet:</u> De Rijksrecherche beschikt niet over een eigen interne auditor en zoekt in de toekomst mogelijk samenwerking met BOD'en om de interne audit vorm te kunnen geven. Aan de eis van de privacyaudit is wel voldaan. <u>Bestaan en werking:</u> De interne audit heeft nog geen vorm gekregen. Aan de eis van de privacyaudit is wel voldaan. In 2012 is een review uitgevoerd op het verbeterplan door externen. Bij wijze van interne audit heeft de privacyfunctionaris van de FIOD het jaarverslag 2013 van de privacyfunctionaris beoordeeld. Dit was een pragmatische oplossing voor het feit dat de Rijksrecherche (of het OM) geen eigen interne auditafdeling heeft. In de bijlage van het Jaarverslag zijn de bevindingen en aanbevelingen van de interne auditor van de FIOD opgenomen. Er is geen interne audit uitgevoerd die voldoet aan de eisen die gesteld worden aan een interne audit.			

5 Ondertekening

Den Haag, 19 februari 2015

Persoonsgebonden informatie

Projectleider

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