Nationale Politie

Privacy assurance-rapport inzake Wet politiegegevens (Wpg)

NOREA Richtlijn 3000D, over de opzet en werking van privacy-beheersingsmaatregelen over de periode 1 januari 2022 tot en met 31 december 2022

KPMG Advisory N.V.

A2200026196 RA RFK/SP

12 september 2023

Dit rapport heeft 37 pagina's

Inhoud

1 Assurancerapport van de onafhankelijke auditor

In de Wpg zijn vereisten en regels opgenomen voor het verwerken van persoonsgegevens om de politietaak goed te kunnen uitvoeren. De Wpg zorgt daarbij voor een evenwicht tussen de belangen die met het uitvoeren van de politietaak gemoeid zijn enerzijds, en het beschermen van de privacy van burgers anderzijds. 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 externe controle moet volgens de 'Regeling periodieke audit politiegegevens' elke vier jaar plaatsvinden door een externe auditor. Deze controle is in de vorm van onderhavige privacy-audit uitgevoerd.

Wij hebben een audit uitgevoerd om te komen tot een oordeel met een redelijke mate van zekerheid over de wijze waarop de Nationale Politie in zowel opzet, bestaan als werking maatregelen en procedures heeft geïmplementeerd om naleving van de Wet Politiegegevens te borgen. Hierbij hebben wij de beheersingsmaatregelen zoals beschreven in de CIP Privacy Baseline (versie 3.3 zoals deze is aangevuld door politie voor de Wpg) als leidraad gebruikt. De verslagperiode betreft 1 januari 2022 tot en met 31 december 2022 waarbij de interne auditrapportages over de periode 2018 tot en met 2021 zijn bekeken.

De auditwerkzaamheden bestaande uit onder andere het inwinnen van inlichtingen (interviews), inspectie/verificatie van documentatie, waarneming ter plaatse en re-performance, hebben plaatsgevonden in de periode augustus 2022 tot en met april 2023. De details omtrent het object van onderzoek en de scope zijn toegelicht in paragraaf 1.3.

De informatie in hoofdstuk 3 van dit rapport genaamd 'Managementreactie Nationale Politie' is opgenomen door de Nationale Politie om additionele informatie te verschaffen aan de lezer van dit assurance-rapport. Deze informatie is geen onderdeel van ons onderzoek en wij brengen daarover geen oordeel tot uitdrukking.

1.1 Afkeurend oordeel

Naar ons oordeel, vanwege het belang van de bevindingen zoals beschreven onder 'Basis voor ons afkeurend oordeel', in alle van materieel belang zijnde aspecten:

a) zijn de interne beheersingsmaatregelen van de Nationale Politie om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens niet op afdoende wijze opgezet;

b) zijn de interne beheersingsmaatregelen van de Nationale Politie om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens niet op afdoende wijze geïmplementeerd gedurende de periode van 1 januari 2022 tot en met 31 december 2022;

c) hebben de getoetste interne beheersingsmaatregelen van de Nationale Politie om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens niet effectief gewerkt gedurende de periode van 1 januari 2022 tot en met 31 december 2022.

De specifieke, getoetste Wpg-domeinen zijn opgenomen in hoofdstuk 2 – Normenkader en testresultaten. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de beheersingsmaatregelen zoals vermeld in de CIP Privacy Baseline (versie 3.3 met Wpg). Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet.

1.2 Basis voor ons afkeurend oordeel

Wij hebben vastgesteld dat de beheersingsdoelstellingen bij de hieronder in de tabel benoemde Wpg-domeinen niet zijn behaald. Zoals opgenomen in de beschrijving van het normenkader en testresultaten (Hoofdstuk 2), waren (een deel) van interne beheersingsmaatregelen niet gedurende de gehele verslagperiode in afdoende mate opgezet, hebben niet bestaan en/of werkten niet effectief. Voor de volledigheid zijn de onderwerpen die afdoende zijn opgezet, geïmplementeerd en effectief werkten ook vermeld (groen).

Toelichting gebruikte kleuren:
Groen – interne beheersingsmaatregelen effectief.
Rood – interne beheersingsmaatregelen niet effectief.

Wpg-Beleidsdomein	O	B	W
B.01 Privacybeleid			
B.02 Organieke inbedding			
B.03 Risicomanagement, Privacy by Design en de DPIA			

Wpg-Uitvoeringsdomein	O	B	W
U.01 Doelbinding gegevensverwerking			
U.01.a Ter beschikking stellen			
U.01.b Verstrekken			
U.02 Register van verwerkingsactiviteiten			
U.03 Kwaliteitsmanagement			
U.04 Beveiligen van de verwerking van persoonsgegevens			
U.04.a Autorisaties			
U.04.b Logging			

Wpg-Uitvoeringsdomein	O	B	W
U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens			
U.06 Bewaren van persoonsgegevens			
U.07 Doorgifte persoonsgegevens			
U.08 Bevoegd functionaris			

Wpg-Control- of beheerdomein	O	B	W
C.01 Intern toezicht			
C.01.a Audits			
C.02 Toegang gegevensverwerking voor betrokkene			
C.03 Meldplicht Datalekken			

We hebben onze opdracht uitgevoerd overeenkomstig Richtlijn 3000D ('Direct-opdrachten'), uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland. Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en dat wij ons onderzoek zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen dat de informatie in de beschrijving geen afwijkingen van materieel belang bevat. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT auditor'.

Wij zijn onafhankelijk van de Nationale Politie zoals vereist in het 'Reglement Gedrags-code' ('Code of Ethics') van NOREA.

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

1.3 Object van onderzoek en scope

Het object van onderzoek van deze privacy-audit bestaat uit de beheersingsmaatregelen uit de CIP Privacy Baseline (versie 3.3 met Wpg) voor de verwerking van politiegegevens door de Nationale politie.

De (generieke) algehele beheersingsdoelstelling voor de Wpg privacy-audit is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens. 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 in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens.
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.

Indien wij bij de toetsing van de beheersingsmaatregelen relevante uitzonderingen hebben geconstateerd in Opzet en/of Bestaan, hebben wij voor deze beheersings-maatregelen niet de effectieve werking van deze beheersingsmaatregelen getoetst.

1.4 Beperkingen van interne beheersingsmaatregelen

De effectieve werking van de privacy-beheersingsmaatregelen zoals beschreven in hoofdstuk 2 is geen waarborg voor volledige compliance met de geldende wet- en regel-geving. Interne beheersingsmaatregelen bij een organisatie kunnen, vanwege hun aard, niet alle fouten of omissies bij het verwerken van persoonsgegevens voorkomen of ontdekken, waaronder de mogelijkheid van menselijke fouten en het omzeilen van interne beheersingsmaatregelen.

Vanwege deze inherente beperkingen kan een entiteit redelijke, maar niet absolute zekerheid verkrijgen dat alle privacy-incidenten die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving worden voorkomen en, voor wie die niet worden voorkomen, tijdig worden gedetecteerd.

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.

Ons onderzoek heeft geen betrekking op toekomstige perioden. Derhalve kunnen wij niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures of ertoe kunnen leiden dat de beheersingsmaatregelen ontoereikend worden als gevolg van veranderingen in de omstandigheden.

1.5 Beperkingen in gebruik en verspreidingskring

Ons assurance-rapport en de beschrijving van het nomenkader en testresultaten, zijn bestemd voor het betrokken management van de Nationale Politie, Ministerie van Justitie en Veiligheid en de Autoriteit Persoonsgegevens.

Het doel van deze privacy assurance-opdracht is om te komen tot een oordeel met een redelijke mate van zekerheid over de wijze waarop de Nationale Politie in zowel opzet, bestaan als werking maatregelen en procedures heeft geïmplementeerd om naleving van de Wet Politiegegevens te borgen. Het rapport dient dan ook niet te worden

behandeld als zijnde geschikt voor enige ander doel dan uiteengezet in dit assurance-rapport. Ons rapport moet derhalve niet worden beschouwd als geschikt om te worden gebruikt of erop te worden gesteund door andere partijen. Bekendmaking van het rapport aan derden is uitsluitend voorbehouden aan de Nationale Politie, wel vragen wij u dit in afstemming met ons te doen.

1.6 Verantwoordelijkheid van het management van de Nationale Politie

Het management van de Nationale Politie is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen om naleving van de Wet Politiegegevens te borgen gedurende de periode 1 januari 2022 tot en met 31 december 2022.

1.7 Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel over de opzet en werking van de interne beheersingsmaatregelen die verband houden met de beheersingsdoelstellingen zoals beschreven in de CIP Privacy Baseline (versie 3.3).

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten en fraude ontdekken.

Ons kantoor past het 'Reglement Kwaliteitsbeheersing NOREA (RKBN)' toe. Op grond hiervan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, auditrichtlijnen en andere relevante 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].

Ons onderzoek naar de opzet, implementatie en effectieve werking van interne beheersingsmaatregelen, bestond onder andere uit:

— het identificeren en inschatten van de risico's dat de interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet, geïmplementeerd of effectief werken om de beheersingsdoelstellingen te bereiken gedurende de periode van 1 januari tot en met 31 december 2022 als gevolg van fouten of fraude, het in reactie op deze risico's bepalen van assurance-werkzaamheden voor het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;

[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).

— het evalueren van de geschiktheid van de beheersingsdoelstellingen en de geschiktheid van de criteria;

— het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de getrouwe weergave van de beschrijving en de geschiktheid van de opzet van interne beheersingsmaatregelen om de beheersingsdoelstellingen te bereiken;

— het toetsen van de werking van de interne beheersingsmaatregelen die noodzakelijk zijn voor het verschaffen van een redelijke mate van zekerheid dat de beheersingsdoelstellingen werden bereikt.

Wij zijn gaarne bereid tot het geven van een nadere toelichting.

Amstelveen, 12 september 2023

KPMG Advisory N.V.

Digitaal ondertekend door:
Ronald Koorn
12 september 2023 16:08 +02:00...

drs. ing. R.F. Koorn RE CIPP/E

Partner

2 Normenkader en testresultaten

2.1 Beleidsdomein

Beleidsdomein	
Doelstelling	De doelstelling van het beleidsdomein is ervoor te zorgen dat op strategisch niveau afdoende randvoorwaarden en condities aanwezig zijn om de persoonsgegevens verantwoord te verwerken en opdat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.
Risico's	Door het ontbreken van een door het management uitgevaardigd beleid ontstaat het risico dat onvoldoende sturing wordt gegeven aan het verwerken van persoonsgegevens. Doorgaans zal dit een negatieve impact hebben op het realiseren van organisatiedoelstellingen (en het voldoen aan de eisen van privacywetgeving).

B.01 Privacybeleid	
Criterium	De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.
Doelstelling	Privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt.
Risico	Het ontbreken van een privacybeleid leidt ertoe dat de organisatie geen duidelijkheid heeft wat precies wordt verwacht, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden verwerkt (waaronder verzamelen, bewerken, inzien et cetera).
Wpg-artikelen	Art. 4a, lid 1

Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben geen relevante uitzonderingen geconstateerd bij de beheersings-maatregelen die vallen onder B.01. Privacybeleid.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

B.02 Organieke inbedding			
Criterium	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.		
Doelstelling	Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de wet- en regelgeving op het gebied van gegevensbescherming.		
Risico	Door het ontbreken van een goede en inzichtelijke taakverdeling en de daarvoor benodigde middelen en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de privacy- en sectorspecifieke wetgeving en het privacy-beleid niet effectief worden ingevuld.		
Wpg-artikelen	Art. 3, 4, 4a, lid 1, 6a, lid 3, 34, lid 1 en 36		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij geen relevante uitzonderingen geconstateerd bij de beheersingsmaatregelen die vallen onder B.02. Organieke inbedding.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

B.03 Risicomanagement, Privacy by Design en de DPIA	
Criterium	De verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen.
Doelstelling	Beoordeling van de privacyrisico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht.
Risico	Privacyrisico's worden niet of niet tijdig gesignaleerd, waardoor de verwerking van de persoonsgegevens niet aan wet- en regelgeving op het gebied van gegevensbescherming voldoet en een grote(re) kans loopt op inbreuken op de beveiliging; dit kan leiden tot schade voor natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.
Wpg-artikelen	Art. 4a, 4b, 4c, art. 33b en art. 36, lid 3, onder c.
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben vastgesteld dat gedurende de verslagperiode nog niet voor alle hoog risico Wpg-verwerkingen een DPIA is afgerond en geconstateerde privacyrisico's zijn gemitigeerd. De organisatie heeft door deze achterstand nog geen proces geïmplementeerd om bij een verandering van het risico van een verwerking, tenminste een toetsing uit te voeren om te beoordelen of de verwerking overeenkomstig het privacybeleid wordt uitgevoerd (**B.03/01.03**). Als een gevolg hiervan hebben wij tevens niet kunnen vaststellen dat maatregelen blijvend passend zijn door het uitvoeren van gegevensbeschermingseffectbeoordelingen (GEB's c.q. DPIA's) (**B.03/02.03**). — Wij hebben vastgesteld dat op basis van uitgevoerde DPIA's niet voor alle systemen waarin politiegegevens worden verwerkt, passende maatregelen zijn genomen door bij het ontwerp de principes van gegevensbescherming te hanteren (zg. 'Privacy by Design') en door het hanteren van standaardinstellingen ('Privacy by Default') (**B.03/02.02**) en dat aantoonbaar opvolging heeft plaatsgevonden op de aanbevelingen/verbetervoorstellen uit de DPIA's (**B.03/03.03**). Zo hebben wij vastgesteld dat met name de (legacy) systemen niet over afdoende technische en organisatorische maatregelen beschikken (o.a. autorisaties, bewaartermijnen, logging, et cetera) om adequate gegevensbescherming te kunnen waarborgen.

	Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “B.03 Risicomanagement, Privacy by Design en de DPIA” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

2.2 Uitvoeringsdomein

Uitvoeringsdomein	
Doelstelling	In het uitvoeringsdomein worden persoonsgegevens daadwerkelijk verwerkt. De verantwoordelijke voor de verwerking moet hier de verwerking realiseren onder de condities en randvoorwaarden die in het beleidsdomein zijn gedefinieerd. Personen waarvan de persoonsgegevens worden verwerkt (betrokkenen) moeten de zekerheid kunnen krijgen dat de verwerking conform de wet- en regelgeving gebeurt.
Risico's	Wanneer richtlijnen voor de specifieke aspecten van de gegevensverwerking ontbreken dan bestaat het risico dat onvoldoende sturing wordt gegeven aan de specifieke aspecten bij de verwerking van persoonlijke gegevens. Dit geeft onduidelijkheid bij de technische en organisatorische inrichting van de gegevensverwerkingen.

U.01 Doelbinding gegevensverwerking	
Criterium	***Doelbinding*** — Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wet politiegegevens geformuleerde doeleinden. — Politiegegevens die zijn verkregen voor uitvoering van de politietaak, kunnen worden verwerkt voor een ander doel voor zover de Wet politiegegevens of Unierecht uitdrukkelijk daarin voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel. — Politiegegevens kunnen voor een ander doel dan voor de politietaak worden verwerkt door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen. — Voordat politiegegevens ten behoeve van de ondersteuning van de politietaak verder verwerkt worden is voldaan aan de vereisten van schriftelijke vastlegging.

U.01 Doelbinding gegevensverwerking	
	Noodzakelijkheid en rechtmatigheid — De verzameling en verwerking van politiegegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. Er wordt geborgd dat de persoonsgegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor artikel 9, 10 en 12 verwerkingen wordt vermeld. — Om te borgen dat alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking heeft de verwerkingsverantwoordelijk passende technische en organisatorische maatregelen gedefinieerd en geïmplementeerd. ***Bijzondere categorieën van politiegegevens*** Er vindt geen verwerking van bijzondere categorieën van politiegegevens, tenzij: — dat nodig is voor het doel van de verwerking, — dat in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon, en — de gegevens afdoende zijn beveiligd.
Doelstelling	Doelbinding waarborgt dat politiegegevens alleen worden verwerkt voor wettelijke doeleinden.
Risico	Het ongeoorloofd en onrechtmatig verwerken van politiegegevens.
Wpg-artikelen	Art. 3, art. 5, art. 8, lid 1, art. 9, lid 1 en 2, art. 10, lid 1, art. 11, art. 12, lid 1, art. 13 en art. 22.
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling:

U.01 Doelbinding gegevensverwerking			
	— Wij hebben vastgesteld dat de Nationale Politie niet beschikt over actuele werkinstructies die bekend en uitgedragen zijn waarin voor verwerkingen als bedoeld in de Wpg-artikelen 8, 9, 10 en 12 beschreven staat wat de noodzaak en doelbinding is van deze verwerkingen. De bestudeerde werkinstructies zijn of nog in concept en/of niet recent herzien (langer dan 3 jaar geleden) (**U.01/01.01**). — Wij hebben vastgesteld dat in het kader van toezicht geen structurele periodieke controles op doelbinding plaats-vinden (**U.01/01.03**). Dit betreft met name een ad-hoc proces in het geval van een calamiteit. — Voor de verwerking van gegevens met het oog op de controle op, en het beheer van informanten hebben wij vast-gesteld dat de Nationale Politie niet over actuele werkinstructies beschikt. De geldigheidsduur van de geldende documentatie is >5 jaar verstreken (**U.01/01.05**). — Vanuit de Politiesystemen is het niet mogelijk gebleken om ten behoeve van een deelwaarneming, totaalpopulatie lijsten te genereren van alle verwerkingen als bedoeld in de artikelen 8, 9, 10 en 12. Derhalve hebben wij de effectieve werking van de volgende beheersingsmaatregelen niet kunnen vaststellen: **U.01/01.05; U.01/01.06; U.01/01.07; U.01/01.08; U.01a/01.02 en U.01a/03.01**. — Wij hebben vastgesteld dat een actueel landelijk overzicht van artikel 13 verwerkingen (en wie de verwerkings-verantwoordelijke is) ontbreekt (**U.01/04.01**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.01 Doelbinding gegevensverwerking” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.01.a Ter beschikking stellen	
Criterium	— Geborgd is dat de verdere verwerking van artikel 9 en 10 gegevens alleen plaatsvindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. — Geborgd is dat de ter beschikking stelling van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in artikel 1, onderdeel a, conform de richtlijnen gesteld in de wet plaatsvindt.
Doelstelling	Het doel van 'Ter beschikking stellen' is het vrije verkeer van politiegegevens voor de uitvoering van de taak van bevoegde autoriteiten te bevorderen, behoudens uitzonderingen en in het geval van artikel 9 en 10 gegevens behoudens instemming.
Risico	Negatieve consequenties voor de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten en de bescherming van de openbare orde, of negatieve consequenties voor de persoonlijke levenssfeer van de betrokkene.
Wpg-artikelen	Art. 4.1, 8.4, 9.3, 10.5, 12.2, 15 en 15a.
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Bij verdere verwerking van persoonsgegevens (artikelen 9 of 10) dient de Bevoegd Functionaris in te stemmen met de terbeschikkingstelling voor die verdere verwerking. Op basis van onze werkzaamheden hebben wij niet kunnen vaststellen dat instemming van de BF ook daadwerkelijk adequaat heeft plaatsgevonden gedurende de verslagperiode omdat dit niet in alle gevallen aantoonbaar wordt vastgelegd in de operationele politiesystemen. Tevens vindt hier geen actief toezicht op plaats (**U.01a/02.01**). — Bij de doorzending van politiegegevens is de noodzakelijke informatie toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de mate van juistheid, volledigheid en betrouwbaarheid van politiegegevens kan beoordelen, alsmede de mate waarin zij actueel zijn (**U.01a/04.01**). Middels inspectie van de werkinstructies is vastgesteld dat niet wordt ingegaan op welke wijze de juistheid, volledigheid, actualiteit en daarmee de betrouwbaarheid kan worden beoordeeld.

U.01.a Ter beschikking stellen			
	Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.01.a Ter beschikking stellen” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.01.b Verstrekken	
Criterium	— 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 art. 6:4 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. — De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt. — In de beslissing voor het verstrekken van politiegegevens ten behoeve van een samenwerkingsverband wordt vastgelegd: - ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, - ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt,

U.01.b Verstrekken	
	- 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 organisatie heeft passende technische en organisatorische maatregelen getroffen om te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art. 23.1, 23.2 en 23.3 Wpg. — De rechtstreekse verstrekking op basis van art 23.2 vindt alleen plaats aan de aangewezen personen. — Beperkte toegang tot politiegegevens tijdens de verzending verhindert op gepaste wijze onbevoegde openbaarmaking, schending, wijziging of vernietiging van politiegegevens. Encryptie en controles zijn gedefinieerd. (secure transmission).
Doelstelling	Het verstrekkingenregime van de Wpg heeft tot doel bij een zwaarwegend algemeen belang, voor zover noodzakelijk, verstrekking van politiegegevens mogelijk te maken. De afweging of verstrekking een zwaarwegend algemeen belang dient is zoveel mogelijk op regelgevingsniveau gelegd, maar dit is niet op voorhand in gedetailleerde regelgeving te vatten. Daarom voorziet de wet in enkele open geformuleerde bepalingen.
Risico	Vanwege de aard van politiegegevens kan verstrekking buiten de politie al snel gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene.
Wpg-artikelen	Art. 4.1, 7.2, 16, 18, 19, 20, 21, 22, 23 en 32, lid 1, onder b.
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben vastgesteld dat de Nationale Politie diverse preventieve maatregelen heeft getroffen om te waarborgen dat alleen die politiegegevens worden verstrekt aan die instanties en personen zoals bepaald in de Wpg en Bpg (o.a. het verstrekkingenbeleid, verstrekkingenwijzer, identificatie en authenticatie, et cetera). Tijdens onze auditwerkzaamheden hebben wij echter vastgesteld dat in de praktijk afspraken met partijen waaraan verstrekt kan worden (te) ruim

U.01.b Verstrekken			
	worden toegepast en dat de Nationale Politie over onvoldoende detectieve maatregelen beschikt om toezicht en controle te kunnen houden op welke politiegegevens aan welke instantie en personen zijn verstrekt. Zo hebben wij vastgesteld dat in de praktijk structureel politiegegevens worden verstrekt aan derden partijen/instanties zonder dat voor deze samenwerkingsverbanden een beslissing tot structurele verstrekking van politiegegevens op grond van artikel 20 van de Wet politiegegevens is overlegd (**U.01b/01.01**). Tevens ontbreken structurele controles die erop toezien dat bij verstrekkingen aan de documentatieplicht (conform art. 6:4 Bpg) wordt voldaan (**U.01b/01.04**). — Op basis van onze werkzaamheden hebben wij vastgesteld dat binnen de politieorganisatie geen afdoende maatregelen zijn ingericht om te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk (**U.01b/03.01**). Zo hebben wij vastgesteld dat indien bij de verstrekking geen sprake is van hit/no hit, politiegegevens die voor het doel van de rechtstreekse verstrekking niet relevant zijn niet worden afgeschermd (**U.01b/03.02**). Tevens ontbreekt het inzicht in rechtstreekse (geautomatiseerde) verstrekkingen welke gedurende de verslagperiode hebben plaatsgevonden op basis van art 23.2 (**U.01b/03.03 en U.01b/03.04**). — Wij hebben vastgesteld dat ten tijde van de verslagperiode een volledig centraal inzicht ontbrak in samenwerkingsovereenkomsten/convenanten waarbij een beslissing tot verstrekking van politiegegevensgegevens is genomen. Tevens was er sprake van samenwerkingsverbanden waarbij wel op structurele wijze politiegegevens werden verstrekt maar waarbij geen beslissing tot structurele verstrekking van politiegegevens op grond van artikel 20 van de Wet politiegegevens is overlegd (**U.01b/02.03**). Gedurende de verslagperiode was een project onderhanden om alle convenanten (zowel uit hoofde van Wpg als AVG) in kaart te brengen. Hierbij is een centraal convenantenportaal geïmplementeerd. Doel van dit portaal is om inzicht te verschaffen in geldende convenanten en artikel 20 Wpg-beslissingen. Op basis van het portaal kan beter gestuurd worden op doorlooptijden, doelmatigheid en rechtmatigheid. Tevens moet het portaal de verschillende eenheden helpen om strategische beslissingen te kunnen maken over het aangaan en continueren van samenwerkingsverbanden. Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.01.b Verstrekken” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.02 Register van verwerkingsactiviteiten	
Criterium	De verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.
Doelstelling	Het doel van een 'Register van verwerkingsactiviteiten' is inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens.
Risico	Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.
Wpg-artikelen	Art. 31d
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Op basis van onze werkzaamheden hebben wij vastgesteld dat het register van verwerkingsactiviteiten (Wpg) nog niet compleet was ten tijde van de verslagperiode. Tevens was er nog geen procedure opgesteld en geïmplementeerd om het register actueel te houden en periodiek te herzien. (**U.02/01.02 en U.02/01.04**). Via inspectie van het register van verwerkingsactiviteiten ten tijde van de verslagperiode hebben wij vastgesteld dat: - De onderlinge samenhang (gegevensstromen) en afhankelijkheden nog niet afdoende waren benoemd en beschreven tussen de bedrijfsprocessen; organisaties en organisatieonderdelen; de verwerkingen; de locaties waar persoonsgegevens worden opgeslagen; de gegevensuitwisselingen (binnen en buiten de eigen organisatie); en de systemen (**U.02/02.03**). - Bij wijzigingen in bestaande en nieuwe verwerkingen worden de resultaten vanuit de gegevensbeschermingseffectbeoordeling/DPIA nog niet afdoende meegenomen als onderdeel van de opname van de verwerking in het register (**U.02/02.04**).

U.02 Register van verwerkingsactiviteiten			
	Wij zijn door afgevaardigden van het verbeterprogramma geïnformeerd dat momenteel een project onderhanden is om het register van verwerkingsactiviteiten te actualiseren. Fase 1, het herzien en opvoeren van alle Wpg-verwerkingen was medio maart 2023 reeds afgerond. Het uitvoeren van DPIA's op de hoog risico verwerkingen (Fase 2.) en het mitigeren van privacyrisico's (Fase 3.) was ten tijde van het schrijven van dit rapport nog onderhanden en dienen eind 2023 te zijn afgerond. De voortgang van dit project wordt gemonitord met een dashboard. Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake "U.02 Register van verwerkingsactiviteiten" gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.03 Kwaliteitsmanagement	
Criterium	De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de gegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit gebeurt op verzoek van betrokkene dan wordt deze over de status van de afhandeling geïnformeerd.
Doelstelling	'Kwaliteitsmanagement' moet ervoor zorgen dat een gegevensverwerking correct en in overeenstemming met de wens van betrokkenen is.
Risico	Wanneer de gegevens onjuist of onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene getrokken met negatieve consequenties of naar het oordeel van betrokkene ongewenste verwerking van zijn of haar persoonsgegevens tot gevolg.
Wpg-artikelen	Art. 4, 6b, 24a, 28
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling:

U.03 Kwaliteitsmanagement			
	— Op basis van onze werkzaamheden hebben wij vastgesteld dat bij de registratie van gegevens in (operationele) politiesystemen onvoldoende technische en organisatorische maatregelen zijn ingericht om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen. Zo wordt binnen de belangrijkste politiesystemen veelal gewerkt met vrije tekstvelden en ontbreken systeemtechnische checks op juistheid en/of een handmatige vier-ogen controle bij de invoer waardoor de datakwaliteit binnen de registratie derhalve afhankelijk is van de initiële (handmatige) invoer door de politieambtenaar. Tevens ontbreekt onafhankelijk toezicht op de juistheid en nauwkeurigheid (**U.03/01.01**). — Via inspectie van de handleiding rechten van betrokkene vastgesteld dat in de rectificatieprocedure niet is opgenomen dat indien de verwerkingsverantwoordelijke politiegegevens heeft gerectificeerd, vernietigd of afgeschermd, de ontvangers daarvan in kennis dienen te worden gesteld (**U.03/03.01**). — Vastgesteld dat in werkinstructies regels worden aangereikt om bij de registratie van politiegegevens onderscheid te maken tussen politiegegevens die op feiten zijn gebaseerd enerzijds, en politiegegevens die op een persoonlijk oordeel zijn gebaseerd anderzijds. Via waarneming ter plaatse in de systemen echter vastgesteld dat systeem-technisch geen onderscheid gemaakt wordt tussen politiegegevens die op feiten en op oordeel zijn gebaseerd. De inhoud is derhalve afhankelijk van de wijze waarop de politieambtenaar hier invulling aan geeft. Tevens is hier ook geen sprake van onafhankelijk toezicht. — Vanuit de politiesystemen is het niet mogelijk gebleken om ten behoeve van een deelwaarneming, totaal-populatielijsten te genereren om zo te kunnen vaststellen of onderscheid wordt gemaakt tussen feiten en persoonlijk oordeel (**U.03/04.01**) en verschillende categorieën van betrokkenen (**U.03/05.01**). Derhalve hebben wij de effectieve werking van deze beheersingsmaatregelen niet kunnen vaststellen. Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.03 Kwaliteitsmanagement” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.04 Beveiligen van de verwerking van persoonsgegevens			
Criterium	De verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen voor de verwerking van persoonsgegevens op een passend beveiligingsniveau		
Doelstelling	Het doel van 'beveiligen van de verwerking van persoonsgegevens' is persoonsgegevens te beschermen tegen verlies, onbeschikbaarheid, corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.		
Risico	Het ongewenst openbaar worden, manipulatie, misbruik en niet beschikbaar zijn van gegevens.		
Wpg-artikelen	Art. 4a		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Op basis van onze werkzaamheden hebben wij vastgesteld dat gedurende de verslagperiode nog niet alle risico-analyses (o.a. DPIA's) voor de hoog risico Wpg-verwerkingen waren afgerond. Deze risicoanalyses vormen de basis om te identificeren of aanvullende technische en organisatorische maatregelen dienen te worden getroffen voor de verwerking van persoonsgegevens op een passend beveiligingsniveau. Voor de DPIA's die wel zijn afgerond hebben wij vastgesteld dat het daadwerkelijk implementeren van de geïdentificeerde passende technische en organisatorische maatregelen en het monitoren van de voortgang hierop slechts nog beperkt plaatsvindt (**U.04/01.04**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake "U.04 Beveiligen van de verwerking van persoonsgegevens" gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.04.a Autorisaties	
Criterium	— Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: politiegegevens worden slechts verwerkt door ambtenaren van politie die zijn belast met de politietaak, die daartoe door de verwerkingsverantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt (zg. need-to-know-basis). — 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. — Er is een proces voor het verlenen van toegang tot de politiegegevens t.b.v. de controle en het toezicht op de naleving van de wet. — Er is een proces voor het verlenen van de benodigde toegang aan een verwerker en aan functionarissen die in opdracht van de verwerkingsverantwoordelijke technische werkzaamheden verrichten.
Doelstelling	Beoogd wordt te waarborgen dat politiegegevens uitsluitend worden verwerkt voor zover dat noodzakelijk is ten behoeve van de uitvoering van de politietaak. De verwerkingsverantwoordelijke is daartoe verplicht een systeem van autorisaties te onderhouden. Door middel van het systeem van autorisaties is de verantwoordelijke in staat de verwerking van politie-gegevens bewust toe te delen aan de personen die onder zijn beheer vallen en voor wie de verwerking noodzakelijk is voor de vervulling van hun taken, zijnde onderdelen van de politietaak.
Risico	Te ruime autorisatie brengt het risico met zich mee dat gegevens onrechtmatig verwerkt worden, doelbinding niet nageleefd wordt en daardoor inbreuk gepleegd wordt op de rechten en vrijheden van betrokkenen.
Wpg-artikelen	Art. 6, lid 1 t/m 6 en art. 6a
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Op basis van onze werkzaamheden hebben wij vastgesteld dat de Nationale Politie beschikt over een actuele autorisatiematrix die aansluit bij de organisatiestructuur. Deze autorisatiematrix geeft inzicht in de basis de benodigde autorisatiecodes weer per verwerkingsdoel. Voor de belangrijkste (operationele) politiesystemen waarin Wpg-

U.04.a Autorisaties			
	gegevens worden verwerkt hebben wij vastgesteld dat een actuele autorisatiematrix waarin rollen, rechten en kritieke functiescheidingsconflicten staan beschreven ontbreekt (**U.04.a/01.01**). Wij hebben derhalve niet kunnen vaststellen dat alle in de norm beschreven beperkingen adequaat zijn ingericht binnen de autorisatie-inrichting (**U.04.a/01.01a**). — Wij hebben vastgesteld dat de documentatie ten aanzien van het autorisatieproces (toekennen, wijzigen en intrekken van rechten) niet recent is herzien (in afgelopen drie jaar)(**U.04.a/01.02**). — Wij hebben vastgesteld dat het proces voor het verlenen van toegang voor het kunnen uitvoeren van controle en toezicht op de naleving van de Wpg (voor de verwerkingsverantwoordelijke, auditors, PF, FG en AP) onvoldoende is vastgesteld en vastgelegd (**U.04.a/01.03 en U.04a/01.04**). — Wij hebben vastgesteld dat een periodieke controle (minimaal jaarlijks) waarbij de huidige autorisatie-inrichting in (IST-situatie) wordt getoetst ten opzichte van de normautorisatiematrix (SOLL-Matrix) ontbreekt (**U.04.a/01.05**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.04.a Autorisaties” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.04.b Logging	
Criterium	— De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a, lid 1, Wpg. — De organisatie detecteert en onderzoekt toegang of toegangspogingen tot persoonsgegevens door personeel, derden of hackers die kunnen leiden tot een inbreuk, sabotage van systemen, invoeging van schadelijke code, diefstal van persoonlijke gegevens, enzovoort. — 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.

U.04.b Logging			
Doelstelling	De logging vindt plaats ten behoeve van de controle van de rechtmatigheid van de gegevensverwerking, de waarborging van de integriteit van de beveiliging van de gegevens en voor strafrechtelijke procedures.		
Risico	Zonder logging bestaat het risico dat de organisatie de rechtmatigheid en onrechtmatigheid van verwerkingen en inbreuken in verband met de beveiliging niet kan aantonen.		
Wpg-artikelen	Art. 32a		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Op basis van onze werkzaamheden hebben wij vastgesteld dat de vereisten ten aanzien van de toegang tot de log gegevens onvoldoende is bepaald en vastgelegd (**U.04.b/01.01**). — Wij hebben vastgesteld dat de huidige (operationele) politiesystemen (legacy) waarin Wpg-gegevens worden verwerkt over onvoldoende functionaliteiten beschikken om toegang (pogingen), het wijzigen of vernietigen, inbreuken en onbevoegde pogingen te loggen en te bewaren met een detailniveau en bewaartermijn die toereikend is voor analyse en onderzoek (**U.04.b/02.01; U.04b/02.02; en U.04b/02.03**). Daarnaast ontbreekt actief toezicht op logging. Toezicht op logging betreft met name een ad hoc proces in het geval van een calamiteit (**U.04.b/02.02**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.04.b Logging” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens			
Criterium	De verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig en op een vastgestelde wijze informatie aan de betrokkene beschikbaar.		
Doelstelling	Het doel van 'Informatieverstrekking aan betrokkene bij verzameling van persoonsgegevens' is om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking, zodat de betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.		
Risico	De organisatie is niet transparant, waardoor de organisatie niet kan verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking.		
Wpg-artikelen	Art. 24a, lid 1, 24b, 27		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij geen relevante uitzonderingen geconstateerd bij de beheersingsmaatregelen die vallen onder “U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens”.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.06 Bewaren van persoonsgegevens	
Criterium	Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.
Doelstelling	Het doel van 'Bewaren persoonsgegevens' is te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel.
Risico	Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.

U.06 Bewaren van persoonsgegevens			
Wpg-artikelen	Art. 8, lid 6, art. 9, lid 4, art. 10, lid 6, art. 12, lid 6, art. 13, lid 4, onder c, art. 14		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: Wij hebben vastgesteld dat de Nationale Politie beschikt over een retentiebeleid waarin de maximale bewaartermijnen zijn uitgewerkt en handvatten zijn beschreven om te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel. Naar aanleiding van een Kamerbrief van de Minister van Justitie en Veiligheid is echter door de Korpsleiding besloten om tot nader besluit geen politiegegevens meer te vernietigen. Het bewaartermijnenbeleid wordt derhalve niet gehandhaafd (**U.06/01.01; U.06/03.01; U.06/03.02; U.06/03.03; U.06/03.04; U.06/03.05; U.06/03.06; U.06/03.08**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.06 Bewaren van persoonsgegevens” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.07 Doorgifte persoonsgegevens	
Criterium	**Doorgifte van politiegegevens aan derde landen** — De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatheidsbesluit 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 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 een derde landen is de toestemming van de verantwoordelijke autoriteit van dit lidstaat beschikbaar.
Doelstelling	Het doel van de vereisten bij 'Doorgifte persoonsgegevens' is te waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid ingeregeld blijft.
Risico	Als een organisatie niet voldoet aan dit criterium is het niet duidelijk voor de organisatie wat exact wordt verwacht bij het doorgeven van persoonsgegevens waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig verder worden verwerkt en gebrek is aan het nemen van verantwoordelijkheid en controle.
Wpg-artikelen	Art. 6c en 17a
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben vastgesteld dat de Nationale Politie beschikt over een tijdelijke werkinstructie voor de doorgifte van politiegegevens aan derde landen. Dit protocol is ongedateerd. Wij zijn geïnformeerd dat geen actief toezicht plaatsvindt op de naleving van de werkinstructie. Mede hierdoor ontbreekt het inzicht in welke politiegegevens zijn doorgegeven aan derde landen (**U.07/01.01**).

U.07 Doorgifte persoonsgegevens			
	Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.07 Doorgifte persoonsgegevens” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

U.08 Bevoegd functionaris	
Criterium	Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.
Doelstelling	Het doel van de instemming van de bevoegde functionaris is om te toetsen of tussen het oorspronkelijke doel en het doel waarvoor de gegevens verder kunnen worden verwerkt — mede gelet op de tactische belangen van de opsporing en de inbreuk op de privacy van betrokkenen — proportioneel is. De BF dient daartoe te voldoen aan de deskundigheidseisen en te zijn aangewezen door de verwerkingsverantwoordelijke.
Risico	Schade aan tactische belangen van de opsporing en de inbreuk op de privacy van betrokkenen.
Wpg-artikelen	Art. 6:7
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben vastgesteld dat de Nationale Politie niet over een actueel overzicht beschikt van functionarissen die als BF zijn aangewezen (**U.08/01.01**). Vanwege het ontbreken van deze administratie hebben wij tevens niet kunnen vaststellen of alle BF-en voldoen aan de vastgestelde vakbekwaamheidseisen (**U.08/01.03**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “U.08 Bevoegd functionaris” gedurende de gehele verslagperiode is behaald.
Conclusie	**Opzet** / **Bestaan** / **Werking**

2.3 Control- of Beheerdomein

Control- of Beheerdomein	
Doelstelling	De doelstelling van Intern toezicht is te zorgen voor en/of vast te stellen dat maatregelen ter waarborging van de privacy afdoende zijn ingericht (control, beheersing).
Risico's	Door het ontbreken van noodzakelijke maatregelen binnen het beheersingsdomein is het niet zeker dat de verwerking aan de vereisten voldoet en dat de governance van die omgeving toereikend is ingericht.

C.01 Intern toezicht	
Criterium	Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.
Doelstelling	Het doel van 'Intern toezicht' is het garanderen van een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, het garanderen van naleving van wet- en regelgeving betreffende de gegevensbescherming, en het garanderen en aantoonbaar maken van naleving van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens.
Risico	Als de verwerking van persoonsgegevens niet voldoet aan wet- en regelgeving betreffende gegevensbescherming, dan zijn de risico's tweeledig: de betrokkene loopt persoonlijke privacyrisico's en de verwerkingsverantwoordelijke wordt geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago als gevolg van communicatieve of handhavende maatregelen van betrokkenen, derden en/of de toezichthoudende autoriteiten.

C.01 Intern toezicht	
Wpg-artikelen	Art. 3 en 4a, lid 1, 36, lid 4 en 34, lid 3
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben geen documentatie (bijvoorbeeld evaluatierapportages, jaarplan FG, jaarverslag FG, etc.) aangetroffen waaruit blijkt dat de FG van de Nationale Politie recent aantoonbare controles en/of privacy compliance-assessments heeft uitgevoerd om vast te stellen of de gegevensverwerkingen voldoen aan de wettelijke verplichtingen (**C.01/01.01**; **C.01/01.02; C.01/01.03; C.01/01.04; C.01/02.09 en C.01/02.10**). — Over de verslagperiode is in onvoldoende mate aangetoond via bijvoorbeeld toezicht en/of verantwoordings-rapportages dat: - persoonsgegevens uitsluitend voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden zijn verzameld en niet op een met die doeleinden onverenigbare wijze zijn verwerkt (doelbinding) (**C.01/02.01**). - de verwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking) (**C.01/02.02**). - de verwerking ten aanzien van de betrokkene rechtmatig is (**C.01/02.03 en C.01/02.04**) - passende technische en organisatorische maatregelen op een dusdanige manier worden verwerkt, dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwe-lijkheid) (**C.01/02.05**). - de persoonsgegevens juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (kwaliteitsmanagement) (**C.01/02.06**). - de wijze van verwerken ten aanzien van de betrokkene 'behoorlijk' is (**C.01/02.07**). - de persoonsgegevens op een wijze worden verwerkt die voor de betrokkene transparant is (**C.01/02.08**).

C.01 Intern toezicht			
	Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “C.01 Intern toezicht” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

C.01.a Audits	
Criterium	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit Politiegegevens.
Doelstelling	Met behulp van een systeem van monitoring (evaluaties en privacy audits) dient de verantwoordelijke na te gaan in hoeverre de getroffen verwerkingsmaatregelen en -procedures de doelstelling van de wettelijke normen en het geformuleerde privacybeleid realiseren. De resultaten van de uitgevoerde monitoring vormen de basis voor eventuele correctieve acties, aanpassing van getroffen maatregelen en procedures, dan wel bijstelling van het geformuleerde beleid.
Risico	Onvoldoende uitvoering geven aan de auditverplichting kan leiden tot risico’s voor betrokkenen die niet inzichtelijk zijn voor de verwerkingsverantwoordelijke en de toezichthouder (Autoriteit Persoonsgegevens).
Wpg-artikelen	Art. 33
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij de volgende uitzonderingen geconstateerd welke impact hebben op het behalen van deze beheersingsdoelstelling: — Wij hebben vastgesteld dat interne audits (Wpg-audit) niet worden uitgevoerd conform een formeel auditplan (**C.01.a/02.02**). — Vastgesteld dat in het geval van geconstateerde tekortkomingen gedurende de privacy-audits geen formele her-controle wordt uitgevoerd door een externe auditor zoals de norm voorschrijft (**C.01a/02.04**). Tevens vastgesteld dat

C.01.a Audits			
	bij recente Wpg-audits niet binnen drie maanden na dagtekening van het auditrapport een verbeterrapport is opgeleverd (**C.01a/04.01**). Op basis van deze geconstateerde uitzonderingen is niet aangetoond dat de beheersingsdoelstelling inzake “C.01.a Audits” gedurende de gehele verslagperiode is behaald.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

C.02 Toegang gegevensverwerking voor betrokkene			
Criterium	De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.		
Doelstelling	Het doel van 'Toegang gegevensverwerking voor betrokkene' is om zo nodig transparantie te bieden over de gegevens-verwerking, zodat de betrokkene zijn rechten kan uitoefenen en zo de verantwoordelijke kan aanspreken bij onrecht-matigheid van een gegevensverwerking, opdat deze onrechtmatigheid beëindigd wordt.		
Risico	De organisatie is niet transparant, waardoor het inzicht in de rechtmatigheid van de verwerkingen door de organisatie ontbreekt, waardoor het vertrouwen in een organisatie verloren gaat.		
Wpg-artikelen	Art. 24a, 25, 26, 27		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij geen relevante uitzonderingen geconstateerd bij de beheersingsmaat-regelen die vallen onder “C.02 Toegang gegevensverwerking voor betrokkene”.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

C.03 Meldplicht Datalekken			
Criterium	De verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de Autoriteit Persoonsgegevens, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.		
Doelstelling	Het doel van 'Meldplicht datalekken' is negatieve consequenties van een datalek te beperken en waar mogelijk te voorkomen.		
Risico	Negatieve consequenties die de persoonlijke levenssfeer van de betrokkene treffen.		
Wpg-artikelen	Art. 33a, art. 32, lid 1, onder d en art. 6c, lid 5		
Belangrijkste afwijkingen	Op basis van onze werkzaamheden hebben wij geen relevante uitzonderingen geconstateerd bij de beheersingsmaatregelen die vallen onder “C.03 Meldplicht Datalekken”.		
Conclusie	**Opzet**	**Bestaan**	**Werking**

3 Managementreactie Nationale Politie

In augustus 2022 is aan KPMG de opdracht verleend om, overeenkomstig de verplichting in de Wet politiegegevens (Wpg) en de Regeling periodieke audit politiegegevens, een externe privacy audit uit te voeren. Het Privacy assurance rapport over de opzet en werking van privacy beheersingsmaatregelen dat in dit kader door KPMG is opgemaakt hebben wij in goede orde ontvangen en met belangstelling gelezen. Hierbij onze reactie op het rapport.

Auditcyclus

De externe Wpg audit moet eens in de vier jaar worden uitgevoerd. Voorgaande jaren heeft de Auditdienst Rijk (ADR) de externe Wpg audit voor de politie uitgevoerd. Het laatste rapport is door de ADR voor de periode 2015 – 2018 opgemaakt en in 2019 opgeleverd. Het voorliggende auditrapport van KPMG is in het kader van de periode 2019 – 2022 opgemaakt. De verslagperiode loopt van 1 januari 2022 tot en met 31 december 2022.

Resultaat ten opzichte van vorige audit

De audit geeft helaas een afkeurend oordeel. In vergelijking met het vorige externe auditrapport uit 2019 valt op dat het aantal onderwerpen dat in opzet voldoet is toegenomen. Ook het aantal onderwerpen dat zowel in opzet, bestaan als werking voldoet is toegenomen. Dat de beheersingsmaatregelen voor belangrijke onderwerpen zoals rechten van betrokkenen en de meldplicht datalekken (blijvend) voldoen, toont aan dat de verbeteractiviteiten effect hebben gesorteerd.

Tegelijkertijd is het zorgelijk dat het bij een aantal andere thema's niet is gelukt het bestaan en ook de werking aan te tonen. Gezien het feit dat eerder al prioriteit moest worden gegeven aan 'autorisaties', is het vooral zorgelijk dat dit onderwerp in opzet, bestaan en werking onvoldoende scoort. In het vorige rapport stond dit in opzet op oranje (er wordt niet geheel voldaan aan de norm)[2].

Intensiveringsprogramma privacy

Het Intensiveringsprogramma privacy, dat in 2019 is gestart en eind 2023 eindigt, heeft bijgedragen aan een verbeterslag op onderwerpen als het verwerkingen-register, verstrekken (convenanten), bevoegd functionaris, autorisaties (de-autoriseren) en Gegevensbeschermingseffectbeoordelingen (GEB's). Ook is ingezet op kennisontwikkeling, het realiseren van een Wpg e-learning en een opleiding voor privacy deskmedewerkers bij de Politieacademie. Dit komt helaas alleen (nog) niet nadrukkelijk tot uiting in de auditresultaten, omdat de verslag-periode voor de audit 2022 is.

[2] KPMG scoort alleen 'rood' of 'groen', terwijl de ADR ook de score 'oranje' hanteerde.

Reactie op bevindingen

Op een paar onderwerpen willen wij specifiek ingaan.

Autorisatie

Het afkeurend oordeel heeft onder andere te maken met het feit dat documentatie over het autorisatieproces sterk verouderd is (opzet). Ook ontbreekt een periodieke controle op de toepassing van de autorisatiematrix. Dit moet de komende periode gerealiseerd worden.

Over het eerste punt merken wij op dat in 2023 (beleids-)kaders en proces-beschrijvingen zijn geactualiseerd. Daarnaast wensen wij te benadrukken dat de afgelopen jaren veel energie is gestoken in de schoning van uitgereikte autorisaties, zowel intern als bij ketenpartners, en het in werking brengen van Identity & Access Management (IAM)-tooling. Beide ontwikkelingen maken dat er wel degelijk meer grip is op de toegang tot gegevens.

Risicomanagement

Vanuit het Intensiveringsprogramma privacy is afgelopen periode extra capaciteit beschikbaar gekomen voor het uitvoeren van GEB's en het optimaliseren van het verwerkingenregister. Hoewel er veel GEB's voor belangrijke basisprocessen zijn afgerond, is nog niet voor alle hoog risico-verwerkingen een GEB uitgevoerd. Hier wordt de komende periode aandacht aan besteed.

Daarnaast wordt ingezet op een meer volwassen vorm van risicomanagement, waarbij ook een mate van risicobereidheid wordt geformuleerd (met name voor 'legacy-systemen'). Risico's moeten bovendien in beeld blijven en bij wijzigingen in de verwerking opnieuw worden beoordeeld zodat maatregelen blijvend passend zijn. Naar aanleiding van het auditrapport zal dit in de actualisering van het Beleid registerplicht en GEB zal dit expliciet terugkomen.

Intern toezicht

Met een intern toezichtstelsel wordt georganiseerd dat beheersmaatregelen ter waarborging van privacy voldoende zijn ingericht. Ik onderschrijf de aanbeveling dat het interne toezichtstelsel bij de politie moet worden versterkt. De privacy governance wordt op korte termijn geactualiseerd en aangescherpt. Dat betekent onder andere een duidelijkere beschrijving van rollen, taken en verantwoordelijk-heden rond intern toezicht en structurele periodieke controles van beheersings-maatregelen. Hierbij zal nadrukkelijk ook het three-lines-model worden betrokken.

Verbeterrapport

De Wpg verplicht om drie maanden na oplevering van de auditrapportage in een verbeterrapport aan te geven welke maatregelen worden genomen ter verbetering van de geconstateerde tekortkomingen. In dit verbeterrapport zal bovenstaande nader uitgewerkt worden.