Verbeterrapport

Externe Wpg audit 2019-2022

Door	5.1.2.e en 5.1.2.e
Afdeling	Gegevensautoriteit
Versienummer	1.0
Datum	29 januari 2024
Kenmerk	2024-0006311
Status	Definitief
Rubricering	Politie INTERN - Bedrijfsvoering

Typ Naam Dienst of Naam Eenheid
Typ Postadres Dienst of Postadres Eenheid

Inhoudsopgave

1 Inleiding

1.1 Wettelijk verplicht verbeterrapport

Eens in de vier jaar moet een externe privacy audit worden uitgevoerd.[1] De audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de Wet politiegegevens (Wpg) op adequate wijze uitvoering is gegeven. KPMG heeft de externe audit over de periode 2019 -2022 uitgevoerd en op 12 september 2023 een auditrapport opgeleverd. Indien bij het uitvoeren van de privacy audit tekortkomingen zijn geconstateerd stelt de verantwoordelijke binnen drie maanden een verbeterrapport op waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de geconstateerde tekortkomingen.[2] Dit verbeterrapport geeft invulling aan deze verplichting.

1.2 Achtergrond

Direct na het verschijnen van het vorige externe auditrapport (eind 2019) was duidelijk dat er nog veel tekortkomingen bij de naleving van de Wpg waren. In eerste instantie zijn het programma Privacy Compliance en de deelportefeuille privacy aan de slag gegaan met het sturen op verbetering van de geconstateerde tekortkomingen. Vanwege een behoefte aan intensivering en ondersteuning op een aantal cruciale thema's is in 2022 het Intensiveringsprogramma privacy gestart.

Inmiddels is het Intensiveringsprogramma privacy, zoals gepland, eind 2023 beëindigd en is décharge verleend.[3] Het Intensiveringsprogramma privacy heeft verschillende resultaten opgeleverd die ten minste wat betreft 'opzet' te beoordelen zijn. Momenteel wordt onder andere nog aandacht besteed aan de borging in de lijn en de inrichting van een systeem van monitoring en control. Een deel van de oplevering van het Intensiveringsprogramma privacy valt buiten de verslagperiode die loopt van 1 januari 2022 tot en met 31 december 2022. De audit kwam dus - in die zin - te vroeg om de resultaten van het Intensiveringsprogramma privacy te toetsen, maar deze resultaten zullen vanzelfsprekend wel bij dit verbeterrapport betrokken worden.

Het is goed om voor ogen te houden dat met de opvolging van de verbetermaatregelen uit dit rapport alsnog geen sprake is van volledige naleving van de Wpg. Voor de politie geldt nog steeds dat het kunnen naleven van de Wpg mede afhankelijk is van herziening van de huidige verouderde wetgeving, en vervanging of aanpassing van bestaande (oudere) systemen.

1.3 Leeswijzer

In hoofdstuk 2 van dit verbeterrapport wordt uiteengezet welke ontwikkelingen van invloed zijn op de wijze waarop de tekortkomingen moeten worden aangepakt. In hoofdstuk 3 wordt per onderwerp beschreven wat de bevindingen zijn van de externe auditor, wat de actuele stand van zaken is en welke verbetermaatregelen genomen moeten worden. In hoofdstuk 4 staat beschreven op welke wijze de voortgang van de door te voeren verbetermaatregelen gemonitord wordt.

1 Artikel 33, lid 1 Wet politiegegevens j° artikel 6:5, lid 1 Besluit politiegegevens
2 Artikel 4, lid 1 Regeling periodieke audit politiegegevens
3 In het KMTO van 13 december 2023.

2 Relevante ontwikkelingen

2.1 Intensiveringsprogramma privacy

In het KLO van 11 mei 2021 is geconstateerd dat er, ondanks korpsbrede inspanningen en eerdere programma's, onvoldoende voortgang was geboekt op een aantal cruciale privacy onderwerpen. De portefeuillehouder Ethiek & Privacy is verzocht een plan te maken om versnelling op privacy-compliance te realiseren. In januari 2022 is het Intensiveringsprogramma privacy gestart.
In de veelheid aan privacy onderwerpen zijn de volgende thema's geselecteerd, waarop versnelling mogelijk werd geacht:

1. Verwerkingenregister & GEB (AVG & Wpg)
2. PSbD/High Risk applicaties
3. Autorisaties
4. Kennis en awareness
5. Convenanten

Uit de déchargedocumenten van het intensiveringsprogramma is op te maken wat er voor deze onderwerpen is opgeleverd en wat er nog te doen staat. In hoofdstuk 3 wordt beschreven op welke manier een en ander tegemoetkomt aan de geconstateerde tekortkomingen in de Wpg-audit.

2.2 Verbetering privacygovernance

Naar aanleiding van het onderzoek van Capgemini in 2022 naar de privacygovernance bij de politie en gezien de uitkomsten van de recent opgeleverde externe en interne Wpg-audits is besloten te komen tot een verbetering van de privacygovernance. De Gegevensautoriteit (GA) bij de Staf Korpsleiding heeft de opdracht gekregen om te komen tot een voorstel tot verbetering van de governance zoals dat is vastgesteld in het *Privacybeleid* van de politie.[4] De notitie *De privacygovernance, voorstel tot verbetering* beschrijft een voorstel op hoofdlijnen. Een gedetailleerde beschrijving van functieprofielen en specifieke processen die hieruit voortvloeien (GEB, verwerkingenregister, etc.) zullen, als ingestemd is met deze verbeterde governance, worden uitgewerkt.

De voorgestelde privacygovernance sluit aan bij de korpsgovernance, die volop in ontwikkeling is. De verbetering van de governance beoogt de volgende geconstateerde knelpunten op te lossen.

<u>a. Diffuse governancestructuur</u>

- Er bestaat veel vrijheid in de eenheden waardoor er uiteenlopende opvattingen over privacyvraagstukken ontstaan.
- Onduidelijke belegging van verantwoordelijkheid waardoor 'eigenaarschap' voor verwerkingen niet wordt opgepakt en mitigerende maatregelen niet worden genomen.
- Er bestaat overlap van verantwoordelijkheden.

<u>b. Three-lines-of defence (3LoD) model</u>

- De tweede lijn is niet of slechts beperkt ingevuld.
- Daarnaast ontbreekt de verbindende laag tussen beleid en uitvoering.

4 Privacybeleid van 10 januari 2020

c. Capaciteit
Voor belangrijke werkzaamheden is te weinig capaciteit beschikbaar. Versnippering van verantwoordelijkheden leidt daarnaast tot inefficiënte inzet van schaarse middelen.

d. Rapportage- en verantwoordingslijnen
De rapportage- en verantwoordingslijnen binnen de privacygovernancestructuur zijn onvoldoende of ontbreken in zijn geheel. Ook ontbreken duidelijke KPI's en heldere dashboards.

e. Borgen, beheren en onderhouden van kennis
- Basale privacykennis bij de politie is laag.
- Kennismanagement is niet goed ingeregeld.
- Een specifieke voorziening ontbreekt.

Voorlopige hulpstructuur
De verbetering van de privacygovernance beoogt dus onder meer onduidelijkheid over verantwoordelijkheden en capaciteitsknelpunten op te lossen. Het zal echter nog enige tijd duren voordat de wijzigingen zijn doorgevoerd en effecten daarvan merkbaar zijn. Ondersteuning op de portefeuilles om privacy compliance voor verwerkingen te realiseren werd afgelopen periode door de eenheden en het programma geleverd. Dit is veelal een omvangrijke en complexe opgave. Met de décharge van het programma zijn aan de portefeuillehouders de GEB's opgeleverd. Het is aan de portefeuillehouder de geconstateerde risico's te mitigeren en hiervoor een plan van aanpak op te stellen. De portefeuillehouders hebben in het KMTO van 13 december 2023 nogmaals kenbaar gemaakt hierbij ondersteund te willen worden.

De deelportefeuillehouder privacy is hierover in gesprek gegaan met de korpsleiding. Naar aanleiding hiervan is besloten dat met ingang van 1 januari 2024 onder sturing van de deelportefeuillehouder een hulpstructuur wordt aangeboden, met als doel de producten te borgen in de organisatie en ondersteuning te verlenen aan de portefeuillehouders (GEB gerelateerd). Benodigd budget is geaccordeerd door de korpsleiding. Na zes maanden wordt geëvalueerd of de lijn het over kan nemen.

2.3 Verbetering korpsgovernance

De transitie van commissies naar vier strategische boards wordt als hefboom gebruikt bij de doorontwikkeling van de governance van het korps. Het Korpsmanagementteam (KMT) blijft verantwoordelijk voor strategie en visievorming, het vaststellen van kaderstellend (strategisch) beleid en grote verdelingsvraagstukken.

Portefeuillehouders zijn beleidsverantwoordelijk en intern en extern het 'boegbeeld' op het terrein van de portefeuille, binnen de vastgestelde (privacy)kaders. Zij zorgen voor de opbouw en borging van kennis.

De board adviseert als collectief het KMT over de richting en de prioriteiten, deelt raakvlakken en dilemma's en bewaakt samenhang. De board maakt één gezamenlijk geprioriteerd plan waarin onderwerpen over de portefeuilles heen terugkomen. Zij monitoren samenhang en voortgang van hoofdprogramma's in relatie tot de richting en prioriteiten van de board
De beleidsdirecteur ondersteunt en voert regie op de door de board vastgestelde prioriteiten en de bijbehorende ondersteuning.
De IV-keten regisseur stemt af met de beleidsdirecteur over impact, haalbaarheid en realisatie van geprioriteerde onderwerpen. Ook zorgt deze regisseur voor realisatie in de eigen IV-waardenketen en monitort dit. De IV-ketenregisseurs van de verschillende boards stemmen gezamenlijk af over de collectieve opgaven (bijv. autoriseren, logging).

2.4 Ontwikkeling korpsbrede visie risicomanagement

Risicomanagement vormt een belangrijke basis van de totale planning & control systematiek. Het gaat daarbij om het identificeren en waar mogelijk, kwantificeren van de risico's en het opstellen van beheersmaatregelen op periodieke basis. Waarbij nadrukkelijk geldt dat risicobeheersing niet tot doel heeft alle risico's te vermijden. In control zijn betekent dat de organisatie weet welke risico's ze loopt, maatregelen treft om de risico's te mitigeren en restrisico's bewust accepteert op het juiste niveau.

Binnen de directie Financiën en Control, cluster Risk en Compliance, wordt gewerkt aan een korpsbreed kader voor risicomanagement op strategisch, tactisch en operationeel niveau. De politie heeft besloten daarbij het ISO 31000 normenkader te volgen.[5] Veel rijksorganisaties werken al met dit model, zo ook het Ministerie van Justitie en Veiligheid.

Het risicomanagementproces wordt binnen de gehele organisatie in werking gebracht. In aanloop naar deze korpsbrede aanpak is de Directie IV gestart om voor de disciplines privacy, informatiebeveiliging en duurzame toegankelijkheid, een overzicht te genereren van de risico's binnen deze disciplines. Bij het opzetten van een operationeel systematisch risicomanagementproces worden de principes en uitgangspunten van het ISO 31000 normenkader als leidraad gehanteerd. Op deze manier worden de risico's op uniforme wijze geïdentificeerd, geanalyseerd, geëvalueerd, behandeld en gemonitord, binnen de drie disciplines, maar ook binnen de landelijke kaders.

Daarnaast heeft het intensiveringsprogramma het Centraal Risico Register (CRR) opgeleverd. Het CCR bevat een overzicht van privacyrisico's die zijn voortgekomen uit de GEB's die door het programma zijn uitgevoerd. Ook bevat het een overzicht van informatiebeveiligingsrisico's die zijn voortgekomen uit de IB-analyses die door het programma zijn uitgevoerd. CCR is een exceloverzicht dat tijdelijk in Vena wordt gezet. Binnen Vena is het mogelijk om vanuit een werkproces risico's te mitigeren. Vena is een tijdelijke oplossing er wordt gezocht naar een blijvende oplossing voor de toekomst.

2.5 Kaderbrief 2024-2028

Voor een aantal geconstateerde tekortkomingen geldt dat hiervoor reeds aandacht in de Kaderbrief 2024-2028 is gevraagd. Vooralsnog zijn er dan ook geen aanvullende verbetermaatregelen nodig als, met behulp van de nieuwe korpsgovernance, beter wordt gestuurd op de opgaven uit de kaderbrief en daarover wordt gerapporteerd. Het gaat dan meer specifiek om:

1. Voldoen aan en toetsbaar zijn op bestaande kaders en IV-beleid: architectuurkaders en informatiebeveiliging & privacy 'by design'. Cloudbeleid, ontwikkelstandaarden, etc.
2. De eenheden dragen actief bij aan het realiseren van de korpsambities van digitale transformatie, minimaal ten aanzien van digitaal vaardig worden maar ook met betrekking tot AVG-, Wpg- en cybersecurity kennis (Altijd alert).
3. Bij gebruik data voor Intel/opsporing werken de eenheden conform AVG en Wpg. Waar nodig worden risicoanalyses (GEB's) gemaakt, bijvoorbeeld ook bij het afsluiten van convenanten voor data-uitwisseling.

[5] Korpsbreed kader risicomanagement, KMTO 5 juli 2017

3 Verbetermaatregelen

De externe privacyaudit heeft tot doel om op systematische wijze te toetsen of op adequate wijze uitvoering is gegeven aan de Wpg. KPMG heeft hiervoor de beheersingsmaatregelen zoals beschreven in de CIP Privacy Baseline (versie 3.3 zoals deze is aangevuld door politie voor de Wpg) als leidraad gebruikt. KPMG benoemt in het auditrapport 19 onderwerpen waar onderzoek naar is gedaan en stelt dat de beheersingsdoelstellingen bij een aantal van deze onderwerpen niet zijn behaald en geeft daarom een afkeurend oordeel over de audit.

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).

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

Wpg Beleidsdomein	**Opzet**	**Bestaan**	**Werking**
B.01 Privacybeleid			
B.02 Organieke inbedding			
B.03 Risicomanagement, Privacy by Design en de DPIA			

Wpg Uitvoeringsdomein			
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			
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			
C.01 Intern toezicht			
C.01.a Audits			
C.02 Toegang gegevensverwerking voor betrokkene			
C.03 Meldplicht Datalekken			

3.1 Privacybeleid

Bevindingen audit

Bij dit onderwerp zijn geen relevante tekortkomingen geconstateerd.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Zoals beschreven in paragraaf 2.2. heeft de GA de opdracht gekregen om te komen tot een voorstel tot verbetering van de governance zoals dat is vastgesteld in het *Privacybeleid* van de politie. De notitie *Verbetering privacygovernance politie* beschrijft een voorstel op hoofdlijnen. Een gedetailleerde beschrijving van functieprofielen en specifieke processen die hieruit voortvloeien (GEB, verwerkingenregister, etc.) zullen, als ingestemd is met deze verbeterde governance, worden uitgewerkt in een geactualiseerd privacybeleid.

Daarnaast wordt 'privacybeleid' als thema meegenomen in de interne control cyclus.

	Verbetermaatregel	Verantwoordelijk	Gereed[6]
1	Actualiseren privacybeleid	Directeur IV (GA/privacy)	Q3 2024
2	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q2 2024

3.2 Organieke inbedding

Bevindingen audit

Bij dit onderwerp zijn geen relevante tekortkomingen geconstateerd.

Wel adviseert de auditor om de samenstelling, rollen en verantwoordelijkheden van de privacy-organisatie nader te specificeren. Meer concreet wordt geadviseerd om bijvoorbeeld een Centrale Privacy Officer (CPO) aan te stellen die verantwoordelijk is voor het opstellen en implementeren van privacybeleid. De overige privacyfunctionarissen, -adviseurs dienen te rapporteren aan de CPO. De rapportagelijnen dienen hierbij nader te worden uitgewerkt zodat de Functionaris voor Gegevensbescherming (FG) beter in staat is om haar taak als onafhankelijke toezichthouder te vervullen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Ook hiervoor geldt dat de GA, zoals beschreven in paragraaf 2.2., de opdracht heeft gekregen om te komen tot een voorstel tot verbetering van de governance. De notitie *Verbetering privacygovernance politie* beschrijft een voorstel op hoofdlijnen. Een gedetailleerde beschrijving van functieprofielen en specifieke processen die hieruit voortvloeien (GEB, verwerkingenregister, etc.) zullen, als ingestemd is met deze verbeterde governance, worden uitgewerkt in een geactualiseerd Privacybeleid. De suggestie om een CPO aan te stellen is in dit voorstel verwerkt, net als de rapportagelijnen tussen CPO, privacyfunctionarissen /adviseurs en de FG.

[6] Met 'gereed' wordt in beginsel gedoeld op 'opzet'. Indien opzet is bereikt kan Concernaudit bij de hercontrole beoordelen of bestaan ook aan de orde is.

De ‘organieke inbedding’ dient als thema meegenomen te worden in de interne control cyclus.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Actualiseren privacybeleid	Directeur IV (GA/privacy)	Q3 2024
2	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q2 2024

3.3 Risicomanagement, Privacy by Design en de GEB

Bevindingen audit

Het proces van risicomanagement is (nog) niet ingericht.

Uit de uitgevoerde GEB’s blijkt dat niet voor alle systemen waarin politiegegevens worden verwerkt, passende maatregelen zijn genomen. De principes van privacy by design en privacy by default zijn weliswaar goed uitgewerkt in het *Beleidskader Privacy Security & Duto by design*, maar zijn nog niet overal toegepast. Ook wordt niet aantoonbaar opvolging gegeven aan de aanbevelingen/ verbetervoorstellen uit de GEB’s. Met name de (legacy) systemen beschikken niet over afdoende technische en organisatorische maatregelen (o.a. autorisaties, bewaartermijnen, logging, et cetera) om adequate gegevensbescherming te kunnen waarborgen.

Geadviseerd wordt om GEB’s uit te voeren voor alle hoog risicoverwerkingen van politiegegevens en deze op een centrale plaats te administreren (bijvoorbeeld in SmartPIA). Daarnaast wordt geadviseerd een PDCA-cyclus in te richten voor het periodiek herzien van de GEB’s en het monitoren of de in de GEB’s beschreven maatregelen om de geïdentificeerde privacyrisico’s te mitigeren ook daadwerkelijk worden geïmplementeerd.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Status project risicomanagement
Hierbij moet onderscheid worden gemaakt tussen enerzijds de strategische en tactische kant van risicomanagement. Dat gaat over de onderwerpen die bij de naleving van de Wpg nog onvoldoende beheerst worden, zoals het actueel houden van het verwerkingenregister. En anderzijds de meer operationele en uitvoerende kant van risicomanagement. Dat gaat over de risicoanalyses die moeten worden uitgevoerd voorafgaand aan de start van een verwerking van persoons-en politiegegevens. Waarna erop gestuurd moet worden dat deze risico’s voor de rechten en vrijheden van personen ook worden gemitigeerd of geaccepteerd.

Zoals beschreven in paragraaf 2.3. is de directie IV in 2023 gestart met een uniforme aanpak bij het onderwerp risicomanagement voor de disciplines privacy, informatiebeveiliging en duurzame toegankelijkheid. Vanwege de samenhang en soms afhankelijkheid tussen deze drie disciplines is een uniform operationeel proces op het mitigeren van risico’s zeer wenselijk. Ook is het door de uniforme aanpak mogelijk om de voortgang op het mitigeren van de risico’s beter te monitoren.

Daarbij wordt ingezet op een meer volwassen vorm van risicomanagement, waarbij ook een mate van risicobereidheid wordt geformuleerd (met name voor ‘legacy-systemen’).[7] Risico’s voor de rechten en vrijheden van personen moeten bovendien in beeld blijven en bij wijzigingen in de verwerking opnieuw worden beoordeeld zodat maatregelen blijvend passend zijn. Naar aanleiding van het

[7] Zie ook speerpunt 1 van de Informatiebeveiligingsstrategie 2026.

auditrapport zal dit in de actualisering van het *Beleidskader registerplicht en GEB* ook expliciet terugkomen.

Privacy by design and default
Zoals de externe auditor ook al aangeeft zijn de principes van privacy by design en privacy by default, net als de principes van informatiebeveiliging en duurzame toegankelijkheid, uitgewerkt in het *Beleidskader Privacy Security & Duto by design*. Deze principes zijn ook opgenomen in de Organisatie Definition of Done (ODoD) die door het Compliance Office van de dienst IV wordt gehanteerd. Dat betekent dat bij softwareontwikkeling een increment pas als 'done' kan worden bestempeld als dit voldoet aan alle kwaliteitseisen. De ODoD is een referentiekader voor de ontwikkelteams.

Daarnaast is twee jaar geleden binnen de dienst IV het Expertisecentrum Privacy (ECP) opgericht, met als primair doel om de IV-organisatie te ondersteunen op het gebied van privacy. In dat kader is de afgelopen jaren een proces ingericht waarbij GEB's en IB-risicoanalyses worden uitgevoerd op de (door)ontwikkeling van (door IV ondersteunde) applicaties waarin verwerkingen van persoons- en politiegegevens plaatsvinden.

Op het gebied van privacy by design en privacy by default heeft het ECP een belangrijke adviserende rol binnen de dienst IV. In dat kader is het *Beleidskader Privacy, Security en Duurzame toegankelijkheid by Design* het afgelopen jaar vertaald naar werkbare procedures en werkinstructies. Deze zullen het komende jaar binnen de IV-organisatie geïmplementeerd worden.

Ook draagt het ECP in belangrijke mate bij aan het implementeren van privacy by design in het IV-voortbrengingsproces door deel te nemen aan het Readiness-traject van het IV Control Framework. Voorafgaand aan de initiatie van een IV-project beoordeelt het ECP of voldoende rekening wordt gehouden met de privacyrisico's die kunnen ontstaan bij de inrichting en ingebruikname van projectproducten waarmee persoons- en politiegegevens kunnen worden verwerkt.

Daarnaast heeft het ECP eind 2023 de Cloud Privacy Risicoanalyse (CPRA) ontwikkeld. Een CPRA biedt inzicht in de cloudgerelateerde privacy risico's die kunnen ontstaan bij de ingebruikname van cloudtoepassingen binnen de politie. De CPRA wordt uitgevoerd voorafgaand aan een GEB, of wanneer het uitvoeren van een GEB niet noodzakelijk is.

GEB's
Vanuit het Intensiveringsprogramma privacy is afgelopen periode extra capaciteit beschikbaar gekomen voor het uitvoeren van GEB's en het optimaliseren van het verwerkingenregister. Bij de décharge van het intensiveringsprogramma is per portefeuille een memo geschreven met daarin een overzicht van de afgeronde GEB's en de meest recente status van de overige GEB's. Daarbij is aanvullende informatie opgenomen die nodig is om die GEB's af te kunnen ronden. Deze afrondende memo's zijn eind december 2023 per mail aangeboden aan de portefeuillehouders.

In bijlage 1 van het *Projecteindrapport Verwerkingenregister, GEB & IB*[8] is de stand van zaken met betrekking tot de Wpg GEB's per 7 december 2023 weergegeven.

De verbetering van de privacygovernance moet eraan bijdragen dat voorafgaand aan de start van nieuwe hoog risico verwerkingen voortaan een GEB wordt uitgevoerd.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Start project risicomanagement	Directeur IV (CIO office/GA) Diensthoofd IV	Q1 2024
2	Actualiseren *Beleidskader registerplicht en GEB*	Directie IV (GA/privacy)	Q3 2024

[8] Projecteindrapport Verwerkingenregister, GEB & IB van 11 december 2023

3	Sturen op toepassen principes PSDbD	Politiechefs/ Portefeuillehouders/ Diensthoofd IV (SCBE)	Doorlopend
4	Afronden en uitvoeren GEB's voor resterende en nieuwe hoog risico-verwerkingen	Politiechefs/ Portefeuillehouders/ Diensthoofd IV (Sector IB)	Doorlopend
5	Prioriteren en uitvoeren mitigerende maatregelen	Politiechefs/ Portefeuillehouders/ Diensthoofd IV (SCBE)	Doorlopend

3.4 Doelbinding gegevensverwerking

Bevindingen audit

1) De politie beschikt niet 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 de doelbinding is van deze verwerkingen. De bestudeerde werkinstructies zijn of nog in concept en/of niet recent herzien (langer dan 3 jaar geleden).
2) In het kader van toezicht is er geen structurele periodieke controles op doelbinding. Dit betreft met name een ad-hoc proces in het geval van een calamiteit.
3) Voor de verwerking van gegevens met het oog op de controle op, en het beheer van informanten is vastgesteld dat de politie niet over actuele werkinstructies beschikt. De geldigheidsduur van de geldende documentatie is >5 jaar verstreken.
4) 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.
5) Er is geen actueel landelijk overzicht van artikel 13 verwerkingen (en wie de verwerkings-verantwoordelijke is).

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

De Redactieraad AVG en Wpg is samengesteld uit deskundigen uit de kring van privacyfunctionarissen, de GA en de Politieacademie. De Redactieraad is ten aanzien van Wpg documentatie verantwoordelijk voor beschikbaarheid, consistentie en beheer en onderhoud. Het actualiseren van werkinstructies is reeds opgestart door de Redactieraad.
Voor wat betreft de werkinstructie voor de verwerking van gegevens met het oog op de controle op, en het beheer van informanten (artikel 12 Wpg) geldt dat de afspraken en eisen hieromtrent zijn vastgelegd in de *Handleiding Bronnen en Inwinning (SummIT)* en de *Handleiding Subjecten (SummIT)* van 14 februari 2020. De Redactieraad beoordeelt of aanvullend een werkinstructie nodig is.

Om tegemoet te komen aan enkele basisbeginselen van de Wpg wordt daarnaast een *Kwaliteitshandboek Wpg* opgesteld. Daarin wordt aandacht besteed aan de vereiste noodzakelijkheid en rechtmatigheid bij de verwerking van politiegegevens. Ook wordt uitgewerkt op welke wijze de juistheid en nauwkeurigheid van politiegegevens moet worden gewaarborgd. Waaronder het, waar mogelijk, vastleggen van onderscheid tussen politiegegevens die op feiten en op oordeel zijn gebaseerd op een wijze waarop (onafhankelijk) toezicht mogelijk is.

Wat betreft de bevinding over de artikel 13-verwerkingen wordt verwezen naar paragraaf 3.7. Deze verwerkingen zijn immers in het register van verwerkingsactiviteiten opgenomen, net als alle andere verwerkingen.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Actualiseren en beschikbaar stellen werkinstructies	Directeur IV (GA/privacy/Redactieraad) Directeur PDC (afdeling privacy)	Q2 2024
2	Opstellen Kwaliteitshandboek Wpg	Directeur IV (GA/privacy)	Q2 2024
3	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q1 2024
4	Opnemen artikel 13-verwerkingen in register	Politiechefs/ Portefeuillehouders	Doorlopend

3.5 Ter beschikking stellen

Bevindingen audit

1) Bij verdere verwerking van persoonsgegevens (artikelen 9 of 10) is het niet mogelijk gebleken vast te stellen dat instemming van de bevoegd functionaris (BF) ook daadwerkelijk adequaat heeft plaatsgevonden omdat dit niet in alle gevallen aantoonbaar wordt vastgelegd in de operationele politiesystemen. Tevens vindt hier geen actief toezicht op plaats.
2) Bij 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. 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.

Geadviseerd wordt om op basis van een risicoanalyse vast te stellen welke aanvullende technische en/of organisatorische (preventieve, detectieve en correctieve) maatregelen benodigd zijn om meer grip te verkrijgen op de processen voor het ter beschikking stellen van (gevoelige) gegevens.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Zoals ook aan de auditor is benadrukt, is het van belang te realiseren dat de Wpg uitgaat van ‘delen, tenzij…’. Dat houdt in dat politiegegevens ter beschikking gesteld moeten worden aan politieambtenaren dan wel Wpg-partners voor zover zij die nodig hebben voor de uitvoering van hun taak, tenzij een weigeringsgrond aan de orde is. Dit principe wordt mogelijk gemaakt door een systeem van autorisaties. Dit systeem/model bepaalt onder meer welke politieambtenaren gelet op hun werkzaamheden en plek in de organisatie een bepaalde rol hebben, met bijbehorende autorisatieniveaus. Aan de hand van dit systeem kunnen sommige politieambtenaren bepaalde politiegegevens vinden, en anderen niet. Denk bijv. aan een wijkagent die geen art. 9-gegevens kan zien, maar een analist van DRIO wel ziet ‘dat’ er mogelijk relevante artikel 9-gegevens zijn zodat deze opgevraagd kunnen worden bij de BF. De afspraak is dat de persoon die gegevens uit een artikel 9- of artikel 10-verwerking wil gebruiken altijd terug moet naar de bron en instemming moet vragen aan de BF.[9] Het systeem van autorisatie voorziet dus in een vorm van ‘generieke instemming van de BF’ om terbeschikkingstelling mogelijk te maken.

Op dit moment is het in SummIT inderdaad functioneel niet mogelijk gestructureerd vast te leggen dat politiegegevens met instemming van de BF verder worden verwerkt. Dit is overigens ook geen verplichting op grond van de Wpg, maar vanuit het perspectief van te nemen beheersmaatregelen wenselijk.

[9] Zie ook paragraaf 1.39 op p. 18 van de *Landelijke werk- en invoerafspraken SummIT*

Dit vraagstuk kan bijvoorbeeld opgelost worden door:
a) alle inhoudelijke informatie (journaalmutaties, pv's, tapverslagen etc.) direct te laten beoordelen door de BF op deelbaarheid en laten voorzien van een code op grond van art. 2:12 Besluit politiegegevens (Bpg), of
b) door de afspraak in stand te laten om gegevens die worden gevonden pas te gebruiken na instemming van de BF. Deze instemming moet dan anders dan nu op gestructureerde wijze vastgelegd worden (bijv. in het journaal).

Maar wellicht zijn meer oplossingen te bedenken. Deze vraag kan voorgelegd worden aan de Adviesgroep SummIT. De kans bestaat dat de oplossingen een aanpassing van SummIT vereist, dit moet worden opgestart via een Request For Change (RFC). Vervolgens kunnen rapportages gedraaid worden teneinde monitoring/toezicht mogelijk te maken. Aangezien de stuurgroep SummIT 8 op 21 december 2023 heeft besloten de livegang uit te stellen omdat er allerlei knelpunten moeten worden opgelost, wordt er begin 2024 een nieuwe planning verwacht. Tot die tijd worden geen RFC's opgepakt. Daarna zullen de RFC's die er liggen voorrang krijgen. De verwachting is dan ook dat een nieuwe RFC in 2024 niet zal worden opgepakt.

Om tegemoet te komen aan enkele basisbeginselen van de Wpg wordt daarnaast een *Kwaliteitshandboek Wpg* opgesteld. Daarin wordt aandacht besteed aan de vereiste noodzakelijkheid en rechtmatigheid bij de verwerking van politiegegevens. Ook wordt uitgewerkt op welke wijze de juistheid en nauwkeurigheid van politiegegevens moet worden gewaarborgd. Waaronder op welke wijze de juistheid, volledigheid, actualiteit en daarmee de betrouwbaarheid bij doorzending van gegevens kan worden beoordeeld.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Impactanalyse vastleggen ter beschikking stellingen	Productowner/Adviesgroep SummIT	Q3 2024
2	Prioritering mogelijk RFC (comply or explain)	Productowner SummIT	Q3 2024
3	Opstellen Kwaliteitshandboek Wpg	Directeur IV (GA/privacy)	Q2 2024

3.6 Verstrekken

Bevindingen audit

1) Door de auditor is vastgesteld dat in de praktijk afspraken met partijen waaraan verstrekt kan worden (te) ruim worden toegepast en dat de politie over onvoldoende detectieve maatregelen beschikt om toezicht en controle te kunnen houden op welke politiegegevens aan welke instantie en personen zijn verstrekt. Soms ontbreekt een art. 20 Wpg-beslissing. Tevens ontbreken structurele controles die erop toezien dat bij verstrekkingen aan de documentatieplicht wordt voldaan.
2) Er zijn geen afdoende maatregelen ingericht om te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk. Zo is 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. Tevens ontbreekt het inzicht in rechtstreekse (geautomatiseerde) verstrekkingen op basis van art 23.2 Wpg.
3) Er ontbreekt een volledig centraal inzicht in samenwerkingsovereenkomsten/convenanten waarbij een beslissing tot verstrekking van politiegegevens is genomen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

In het *Projecteindrapport voor deelproject 4 Convenanten* van het Intensiveringsprogramma privacy staat beschreven dat met de décharge van het programma het volgende is opgeleverd:

- Er zijn landelijke kaders beschreven om kwalitatief, goede convenanten op te kunnen leveren die compliant zijn aan wetgeving en beleid.
- Er is kennisverbreding in de organisatie ontstaan over convenanten en gebruik 0-meting.
- Toegankelijk maken informatie m.b.t. het proces convenanten aan de medewerkers Privacydesk.
- Er is inzicht ontstaan in de kwaliteit op bestaande convenanten op het convenantenportaal.
- De eenheden kunnen het plan van aanpak op convenanten gebruiken voor de roadmap privacy.
- De politie is in staat om convenanten en verwerkingen in het verwerkingsregister te koppelen.
- Er is een methodiek rondom convenanten ontwikkeld waardoor de politie de actieve informatieplicht en de Wet open overheid kan naleven.[10]

Met bovengenoemde wordt tegemoetgekomen aan bevindingen 1 en 3.

De bevinding over rechtstreekse verstrekkingen ziet op verstrekkingen aan leden van het Openbaar Ministerie (OM). De politie is op grond van artikel 16, lid 1, onder a Wpg verplicht hen politiegegevens te verstrekken voor zover zij deze behoeven in verband met hun gezag of zeggenschap over de politie of over andere personen of instanties die met de opsporing van strafbare feiten zijn belast, of voor de uitvoering van andere hun bij of krachtens de wet opgedragen taak.
In artikel 23, lid 1 Wpg is vervolgens bepaald dat verstrekking rechtstreeks kan plaatsvinden voor zover noodzakelijk met het oog op strafvorderlijke beslissingen omtrent opsporing en vervolging en de hulp aan slachtoffers van strafbare feiten. Voorop staat dus dat de politie verplicht is de noodzakelijke politiegegevens te verstrekken.
De rechtstreekse verstrekking aan leden van het OM wordt vormgegeven via autorisaties.[11] De toegang van leden van het OM tot BVH is wel degelijk zo ingericht dat zij slechts bij die registraties kunnen waar zij aan gekoppeld zijn, namelijk via de voorziening Betere Opsporing door Sturing op Zaken (BOSZ). De toegang tot SummIT is ingericht via een aparte autorisatierol voor externen met niveau 1, waardoor alleen geraadpleegd kan worden binnen de onderzoeken waar de OM-medewerker aan is toegevoegd. Aan de hand van loggegevens kan vastgesteld worden welke gegevens geraadpleegd zijn.

Het is de vraag in hoeverre het nodig is om deze autorisaties nog ‘strakker’ in te richten en wat daarvoor de mogelijkheden zijn. Deze vraag moet voorgelegd worden aan de portefeuillehouder Intelligence, als verantwoordelijke voor het autorisatiemodel. Indien zo’n oplossing een aanpassing van SummIT vereist moet dit via een Request For Change (RFC). Vervolgens kunnen rapportages gedraaid worden teneinde monitoring/toezicht mogelijk te maken. Aangezien de stuurgroep SummIT 8 op 21 december 2023 heeft besloten de livegang uit te stellen omdat er allerlei knelpunten moeten worden opgelost, wordt er begin 2024 een nieuwe planning verwacht. Tot die tijd worden geen RFC’s opgepakt. Daarna zullen de RFC’s die er liggen voorrang krijgen. De verwachting is dan ook dat een nieuwe RFC in 2024 niet zal worden opgepakt.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Impactanalyse rechtstreeks verstrekken OM	Portefeuillehouder Intelligence (SCBE)	Q3 2024
2	Prioritering RFC (comply or explain)	Productowner SummIT	Q3 2024

[10] Voor een volledige beschrijving van de activiteiten zie: Projecteindrapport voor deelproject 4 Convenanten van 12 december 2023.
[11] Let op: het gaat hier om autoriseren in technische zin, niet in de zin van artikel 6 Wpg

3.7 Register van verwerkingsactiviteiten

Bevindingen audit

1) Het register van verwerkingsactiviteiten is nog niet compleet. Tevens is er nog geen procedure opgesteld en geïmplementeerd om het register actueel te houden en periodiek te herzien.
2) De onderlinge samenhang (gegevensstromen) en afhankelijkheden tussen de bedrijfsprocessen zijn nog niet afdoende benoemd en beschreven; organisaties en organisatieonderdelen; de verwerkingen; de locaties waar persoonsgegevens worden opgeslagen; de gegevensuitwisselingen (binnen en buiten de eigen en de systemen).
3) Bij wijzigingen in bestaande en nieuwe verwerkingen worden de resultaten vanuit de GEB nog niet afdoende meegenomen als onderdeel van de opname van de verwerking in het register.

Geadviseerd wordt om het project voor de herziening van het register van verwerkingsactiviteiten (Fasen 1 t/m 3) conform planning af te ronden en erop toe te zien dat dit ook gedegen gebeurt. Daarnaast adviseert de auditor om de integratie en consistentie tussen enerzijds het register van verwerkingsactiviteiten en anderzijds de GEB's en QuickScans te waarborgen. Een GRC-tool biedt de mogelijkheid om beter grip te houden op het actueel houden van het register en het periodiek herzien/actualiseren van de uitgevoerde GEB's.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

In het register van verwerkingsactiviteiten zijn in totaal 314 verwerkingen vastgelegd. Deze zijn gebaseerd op de bedrijfs-/werkprocessen die zijn beschreven door de directie Operatien. De 314 verwerkingen zijn, op basis van gesprekken die zijn gevoerd met de materiedeskundigen van de 15 landelijke hoofdportefeuilles, samengevoegd tot 107 verwerkingen. Voorts is een procedure ontwikkeld om het register van verwerkingsactiviteiten (SmartPia) actueel te houden.
Begin 2024 vindt overdracht plaats van de door het intensiveringsprogramma opgeleverde producten aan de Afdeling Privacy van het PDC. Deze afdeling beoordeelt welke acties nodig zijn om het register compleet te maken en actueel te houden.

De verbetering van de korps- en privacygovernance moet eraan bijdragen dat verantwoordelijken beter in staat zijn het register actueel te houden.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Overdracht register aan PDC	Deelportefeuillehouder privacy	Q2 2024
2	Compleet maken en actueel houden register	Portefeuillehouders/ Politiechefs	Doorlopend
3	Beheer register	Directeur PDC (Afdeling Privacy)	Doorlopend
4	Actualiseren *Beleidskader registerplicht en GEB*	Directie IV (GA/privacy)	Q3 2024

3.8 Kwaliteitsmanagement

Bevindingen audit

1) Bij de registratie van gegevens in (operationele) politiesystemen zijn onvoldoende technische en organisatorische maatregelen ingericht om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen. Tevens ontbreekt onafhankelijk toezicht op de juistheid en nauwkeurigheid.
2) In de rectificatieprocedure is niet opgenomen dat indien de verwerkingsverantwoordelijke politiegegevens heeft gerectificeerd, vernietigd of afgeschermd, de ontvangers daarvan in kennis dienen te worden gesteld.
3) Er is vastgesteld dat in systemen systeemtechnisch 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.
4) Vanuit de politiesystemen is het niet mogelijk gebleken om ten behoeve van een deelwaarneming, totaalpopulatielijsten te genereren om zo te kunnen vaststellen of onderscheid wordt gemaakt tussen feiten en persoonlijk oordeel en verschillende categorieën van betrokkenen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Om tegemoet te komen aan enkele basisbeginselen van de Wpg die ook de kwaliteit van gegevens raken wordt een *Kwaliteitshandboek Wpg* opgesteld. Daarin wordt aandacht besteed aan de vereiste noodzakelijkheid en rechtmatigheid bij de verwerking van politiegegevens. Ook wordt uitgewerkt op welke wijze de juistheid en nauwkeurigheid van politiegegevens moet worden gewaarborgd. Waaronder het, waar mogelijk, vastleggen van onderscheid tussen politiegegevens die op feiten en op oordeel zijn gebaseerd op een wijze waarop (onafhankelijk) toezicht mogelijk is.

Daarnaast zijn in 2023 de *Landelijke werk- en invoerafspraken SummIT*[12] geactualiseerd. In dit document staan de werk- en invoerafspraken op een rij. Daaruit blijkt dat er wel degelijk technische en organisatorische maatregelen zijn ingericht om de kwaliteit van persoonsgegevens te waarborgen. Zoals de aansluiting bij basisregistraties (paragraaf 2.3) en het afdwingen van invoer door verplichte velden (bijv. paragraaf 1.1., 1.8 en 2.5).

Ook voor de Basisvoorziening Handhaving (BVH) zijn landelijke werk- en invoerafspraken gemaakt. Deze zijn te vinden op de agorapagina *BVH Gebruikersondersteuning*.

Zodra het kwaliteitshandboek gereed is zal het worden gedeeld met de Adviesgroep SummIT (AGS), het Landelijke Gebruikersoverleg BVH en de Teams Kwaliteit van Informatie. Bij toekomstige actualiseringen kan rekening worden gehouden met de eisen uit het kwaliteitshandboek.

Voor bevinding 2 geldt dat de *Handleiding Rechten van Betrokkene voor de politieorganisatie* is geactualiseerd. In paragraaf 3.7 is opgenomen dat de ontvangers van politiegegevens geïnformeerd moeten worden als de politiegegevens zijn gerectificeerd, vernietigd of afgeschermd. Hiervoor is ook een modelbrief ontwikkeld en in gebruik genomen.

[12] Landelijke werk- en invoerafspraken SummIT, 1 februari 2023

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Opstellen Kwaliteitshandboek Wpg	Directeur IV (GA/privacy)	Q2 2024
2	Sturen op toepassen landelijke werk- en invoerafspraken SummIT	Politiechefs (hoofden Operatien)	Doorlopend
3	Meenemen in ontwerp RAPP	Programmamanager PVR	Doorlopend

3.9 Beveiligen van de verwerking van persoonsgegevens

Bevindingen audit

1) Nog niet alle risicoanalyses (o.a. GEB's) voor de hoog risico Wpg-verwerkingen zijn 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.
2) Voor de GEB's die wel zijn afgerond is vastgesteld dat het daadwerkelijk implementeren van de geïdentificeerde passende technische en organisatorische maatregelen en het monitoren van de voortgang hierop slechts nog beperkt plaatsvindt.

Geadviseerd wordt om aanvullende aandacht te besteden aan het daadwerkelijk implementeren van de geïdentificeerde passende technische en organisatorische maatregelen voortkomend uit het GEB-proces. Daarnaast adviseert de auditor om ook de binnen de organisatie uitgevoerde data-analyses, risicoselecties en ongestructureerde dataverwerkingen in kaart te brengen en hierbij na te gaan of aanvullende maatregelen benodigd zijn.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

In het *Projecteindrapport Verwerkingenregister, GEB & IB*[13] van het Intensiveringsprogramma privacy staat voor dit onderwerp beschreven dat het volgende is opgeleverd:

- Voor de hoog risico-verwerkingen waar een GEB voor geschreven is, zijn voor de onderliggende applicaties Informatiebeveiligingsanalyses (IB-analyses) opgesteld, inclusief dossiervorming.
- Bij het uitblijven van een standaard GRC-omgeving is een begin gemaakt met een Centraal Risico Register in Excel op basis waarvan de eerste rapporten zijn opgemaakt.
- De privacy- en informatiebeveiligingsrisico's binnen de verwerkingen en onderliggende systemen zijn in kaart gebracht en overgedragen aan de portefeuillehouders en productowners.

Voor een uitgebreidere toelichting wordt verwezen naar het projecteindrapport. En voor de maatregelen ten aanzien van het uitvoeren van GEB's naar paragraaf 3.3. van dit rapport.

Hiermee zijn de risico's van verschillende hoog risico-verwerkingen beoordeeld (kans x impact) en geprioriteerd. Per risico zijn mitigerende maatregelen geadviseerd om het risico te verminderen of weg te nemen. 5.1.2.i [redacted]

[13] Projecteindrapport Verwerkingenregister, GEB & IB van 11 december 2023

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Uitvoeren IB-analyses voor resterende en nieuwe hoog risico-verwerkingen	Diensthoofd IV (Sector IB) Portefeuillehouders/ Politiechefs	Doorlopend
2	Prioriteren en implementeren mitigerende maatregelen op grond van het plan van aanpak	Portefeuillehouders (SCBE)/ Politiechefs	Doorlopend

3.10 Autorisaties

Bevindingen audit

1) Bij de belangrijkste (operationele) politiesystemen waarin Wpg-gegevens worden verwerkt ontbreekt een actuele autorisatiematrix waarin rollen, rechten en kritieke functiescheidingsconflicten staan beschreven.
2) De documentatie ten aanzien van het autorisatieproces (toekennen, wijzigen en intrekken van rechten) is niet recent herzien (in afgelopen drie jaar).
3) 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) is onvoldoende vastgesteld en vastgelegd.
4) Een periodieke controle (minimaal jaarlijks) waarbij de huidige autorisatie-inrichting in (IST-situatie) wordt getoetst ten opzichte van de normautorisatiematrix (SOLL-Matrix) ontbreekt.

In opzet is een procesbeschrijving aanwezig van het autorisatieproces. Deze betreft het toekennen, aanpassen en stopzetten van toegang tot de politiesystemen. Echter mist er een actuele autorisatiematrix voor de belangrijkste politiesystemen waarin Wpg-gegevens verwerkt worden. Documentatie ten aanzien van het autorisatieproces is recent niet herzien. Monitoring en control op het proces en het autorisatiesysteem ontbreekt in opzet. De monitoring en control op het uitgeven van en van de uitgegeven autorisaties ontbreekt in zijn geheel. De auditor wijst erop dat het aanpakken van deze tekortkomingen een meerjarig project betreft.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

In 2023 zijn (beleids-)kaders en procesbeschrijving geactualiseerd. Daarnaast is er de afgelopen jaren veel energie 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.

In het Bestemmingsplan IV 2022-2026 is de richting voor Informatiebeveiliging bepaald. Daaruit volgt dat de autorisatiemethodiek verschuift van toepassingen naar de gegevens zelf. In het plangebied Politiewerk vertaalt dat zich voor veel facetten van beveiliging naar het koppelen van gegevens die bedrijfsfuncties in de capabilities gebruiken met autorisatiekenmerksets.
De toegestane wijze van gebruik van gegevens wordt gestuurd door de autorisatiematrix. In de autorisatiematrix wordt, voor combinaties van autorisatiekenmerken van de gegevens, bijgehouden welke rol/mandaat de eindgebruiker (min of meer initiator van de bedrijfsfunctie) in de organisatie moet hebben voor een specifiek gebruik (zoals aanmaken, vernietigen, inzien). Dit is vaak voorzien van een extra conditie gerelateerd aan de verbondenheid/betrokkenheid/verantwoordelijkheid (zoals teamlid of onderzoeksleider) tot een specifiek gegeven.

Bovenstaande betekent dat de politie een bewuste keuze maakt om niet altijd per politiesysteem een actuele autorisatiematrix bij te houden, maar dat de autorisatiemethodiek dus op de gegevens wordt toegepast.
Om dit te realiseren zijn beleids- en ontwerpkaders gemaakt (deelarchitectuur, bestemmingsplan, referentie architectuur IAM), waaruit volgt dat:

- Applicaties moeten zijn aangesloten op de generieke voorziening IAM, waardoor het mogelijk wordt gemaakt een actuele status van autorisaties per persoon te geven;
- IAM-betrokkenheid 5.1.2.i zal worden gebruikt om inzichtelijk te maken welke rol een geautoriseerde ten aanzien van een verzameling registraties (bijvoorbeeld voor een onderzoek, incident of evenement) heeft.
- De IAM-autorisatieservice bepaalt op basis van de Autorisatiematrix welk gebruik voor een geautoriseerde toegestaan is.

De realisatie van IAM-betrokkenheid 5.1.2.i en de IAM-autorisatieservice is georganiseerd via de regiegroep Generieke Voorzieningen. 5.1.2.i Tot die tijd regelt elke applicatie op haar eigen manier de toegang tot data.

Geef prioriteit aan:
1. de aansluiting van applicaties op IAM;
2. de realisatie van IAM-betrokkenheid 5.1.2.i en de IAM-autorisatieservice, en
3. het inrichten van een monitoring-/controlproces op beide.

Als hier geen prioriteit aan wordt gegeven, dan zal het overzicht op een andere manier verkregen moeten worden, en zal alsnog binnen elke applicatie een autorisatiematrix moeten worden opgesteld. Dit is gelet op de alle beleids- en ontwerpkaders en de daarvoor nodige (beheer)capaciteit echter niet wenselijk.

Ten aanzien van de tweede bevinding zijn inmiddels stappen gezet. Verschillende documenten zijn ontwikkeld of geactualiseerd. Zoals:

- Bestemmingsplan IV 2022-2026
- Deelarchitectuur Autorisatiemanagement
- IAM Tactisch Beveiligingsbeleid (wordt binnenkort vastgesteld)

Voor de derde bevinding geldt dat het verlenen van toegang aan onder meer de korpschef en toezichthouders op grond van art. 6a Wpg voor zover zij dat nodig hebben voor hun onderzoek, niet in het autorisatiemodel kan worden ingepast. In een werkproces moet geregeld worden in welke gevallen, onder welke voorwaarden aan dergelijke functionarissen de benodigde toegang kan worden verleend.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Aansluiting applicaties op IAM (incl RAPP)	Portefeuillehouders/ Politiechefs	Doorlopend
2	Realisatie IAM-betrokkenheid 5.1.2.i en IAM-autorisatieservice	Diensthoofd IV (SPO autoriseren)	2025
3	Inrichting monitoring-/controlproces op IAM-betrokkenheid en -autorisatieservice	Diensthoofd IV (SPO autoriseren)	2025
4	Actualiseren Autorisatiebeleid en -procedures (incl. toegang logging)	Directeur IV (GA/CISO) Diensthoofd IV (IB)	Q4 2024
5	Inrichting werkproces toegang verlenen art. 6a Wpg	Directeur IV (GA/privacy) Diensthoofd IV	Q3 2024

3.11 Logging

Bevindingen audit

1) De vereisten ten aanzien van de toegang tot de loggegevens zijn onvoldoende bepaald en vastgelegd.
2) De huidige (operationele) politiesystemen (legacy) waarin Wpg-gegevens worden verwerkt beschikken over onvoldoende functionaliteiten 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.
3) Daarnaast ontbreekt actief toezicht op logging.

Geadviseerd wordt om in samenspraak met de systeemeigenaren per politiesysteem logging-en auditvereisten te definiëren en te implementeren. Hierbij dienen eerst de richtlijnen voor logging en monitoring te worden gedefinieerd. Denk hierbij aan kritieke handelingen die kunnen worden verricht in het systeem waarop logging dient te worden geactiveerd, wijze waarop logging wordt weggeschreven en bewaard, vernietigingsprocedures voor logging in lijn met bewaartermijnen en de wijze waarop de logging al dan niet geautomatiseerd gemonitord kan worden.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

5.1.2.i [redacted]

Bovenstaande is beschreven in het geactualiseerde *Beleidskader logging 2.0*, dat eind december 2023 is geaccordeerd bij de Beleidstafel IV.

Wat betreft de eerste bevinding is het zo dat in het beleidskader wel is beschreven wie er toegang tot de loggegevens mogen hebben, maar niet onder welke voorwaarden. Het is de bedoeling aan te sluiten bij het autorisatiebeleid en de bijbehorende processen rond aanvragen, goedkeuren en uitvoeren van toegang tot gegevens. Voorkomen moet worden dat aparte procedures voor toegang tot loggegevens worden ontwikkeld.

Om tegemoet te komen aan de tweede bevinding van de auditor moet worden gestuurd op 5.1.2.i [redacted] en betekent dat applicaties in overeenstemming moeten worden gebracht met het *Beleidskader logging 2.0* en de auditlogstandaard. 5.1.2.i [redacted] Daarover zal periodiek gerapporteerd worden aan de CTO. Aan de hand daarvan moeten de portefeuillehouders gaan sturen op realisatie van bruikbare logging.

Voor wat betreft de legacy moet geconstateerd worden dat sommige systemen nog jaren zullen worden gebruikt. 5.1.2.i [redacted]

5.1.2.i [redacted]

De derde bevinding gaat over toezicht op de logging. Met *Protective Monitoring*[14] wordt controle van de logging voor alle systemen en applicaties die politiegegevens verwerken ingericht. De bedoeling is om het model en de werkwijze die ontwikkeld zijn tijdens de pilot atypische signalen in 2024 landelijk in te voeren. In de jaren daarna zullen dan meer applicaties worden aangesloten op deze monitoring en zullen nieuwe detectieregels en indicatoren worden toegevoegd. 5.1.2.i [redacted]

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Actualiseren Autorisatiebeleid en -procedures (incl. toegang logging)	Directeur IV (GA/CISO) Diensthoofd IV (IB)	Q4 2024
2	Aansluiting applicaties op LaaS	Portefeuillehouders/ Politiechefs	Doorlopend
3	5.1.2.c [redacted]	Diensthoofd IV (IB)	Q3 2024
4	Doorontwikkeling LaaS	Diensthoofd IV (CTO)	Doorlopend
5	Uitrol Protective Monitoring	Diensthoofd IV (IB)	2026

3.12 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens

Bevindingen audit

Bij dit onderwerp zijn geen relevante tekortkomingen geconstateerd.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Geen specifieke aanbevelingen vanuit de audit.

	Verbetermaatregel	Verantwoordelijk	Gereed
	Nvt		

3.13 Bewaren van persoonsgegevens

Bevindingen audit

De 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[15] 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.

[14] Het KLO is op 5 december 2023 akkoord gegaan met de eerste fase van protective monitoring (2024).
[15] Brief Aanpak cold cases (kenmerk 2487378), 4 februari 2019

Geadviseerd wordt een procedure op te stellen en te implementeren voor het controleren, verwijderen en vernietigen van politiegegevens in lijn met het bewaartermijnenbeleid. Tevens dienen aanvullende technische en organisatorische maatregelen te worden geïmplementeerd om te waarborgen dat gegevens kunnen worden verwijderd in lijn met het bewaartermijnenbeleid. Dit stelt de politie in staat om te kunnen voldoen aan het bewaartermijnenbeleid indien besloten wordt om weer politiegegevens te vernietigen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Op 14 november 2023 is in het kader van het traject Herziening Wpg een bijeenkomst geweest tussen een afvaardiging van het Ministerie van JenV, de korpsleiding en het College van Procureurs-Generaal over verwerkings-en bewaartermijnen. Daar is nog geen definitieve beslissing uit voortgekomen, dus de opvolging van het standpunt in de kamerbrief duurt voort.
Dat neemt niet weg dat het advies van de auditor moet worden opgevolgd om ervoor te zorgen dat de politie in staat moet zijn politiegegevens te verwijderen en vernietigen als dat aan de orde is, bijvoorbeeld naar aanleiding van een verzoek in het kader van rechten van de betrokkene. Daarvoor moeten waar mogelijk technische en organisatorische maatregelen worden genomen en moet ook een procedure worden ontwikkeld.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Technische en organisatorische maatregelen in politiesystemen (incl. RAPP) om gegevens conform wettelijke termijnen te kunnen verwijderen en vernietigen (incl. poortwachterfunctionaliteit).	Politiechefs/ Portefeuillehouders/ Diensthoofd IV	Doorlopend
2	Opstellen procedure controleren, verwijderen en vernietigen politiegegevens	Directie IV (GA/privacy) Diensthoofd IV (FB)	Q3 2024

3.14 Doorgifte persoonsgegevens

Bevindingen audit

De politie beschikt over een tijdelijke werkinstructie voor de doorgifte van politiegegevens aan derde landen. Deze is ongedateerd. Er vindt geen actief toezicht plaatsvindt op de naleving van de werkinstructie. Daardoor is er geen inzicht in welke politiegegevens zijn doorgegeven aan derde landen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

De werkgroep derde landen, bestaande uit vertegenwoordigers van de politie, KMar, BOD's (vertegenwoordigd door de FIOD) en OM, heeft besloten de 'Tijdelijke instructie' te herzien. Het idee is om deze instructie meer te richten op de eindgebruiker dus ook wat meer handvatten voor de praktijk mee te geven. Daarnaast zal in de instructie het onderscheid tussen politieel en justitieel aangescherpt worden. Het is dus een integrale herziening waarbij de ervaring van de afgelopen jaren uit de praktijk wordt verwerkt.

De 0.1 versie is gereed en wordt besproken in de werkgroep. Aangezien hier meerdere partijen bij betrokken zijn is de duur van het afstemmings- en vaststellingstraject lastig in te schatten. Het streven is om dit in Q2 af te ronden.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Actualiseren werkinstructie	Directeur IV (GA/privacy) Politiechef LE (LIRC)	Q2 2024
2	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q1 2024

3.15 Bevoegd functionaris

Bevindingen audit

De politie beschikt niet over een actueel overzicht van functionarissen die als Bevoegd Functionaris (BF) zijn aangewezen. Vanwege het ontbreken van deze administratie is niet vastgesteld of alle BF-en voldoen aan de vastgestelde vakbekwaamheidseisen.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Dit onderwerp is door het Intensiveringsprogramma privacy opgepakt. In het *Projecteindrapport Bevoegd Functionaris*[16] staat dat de volgende resultaten zijn opgeleverd. Voor nadere informatie wordt naar dit document verwezen.

Landelijk gedefinieerd BF-proces en initiëring van de verbetering van het beleid.
Voor de BF-administratie is een landelijk uniform proces opgesteld dat is opgenomen in de systemen van Bedrijfsarchitectuur BV met als eigenaar de deelportefeuillehouder privacy. Aanscherping van het beleid is besproken met de GA die het beleid zal actualiseren. Er zijn drie voorwaarden om een medewerker de BF rol uit te kunnen laten voeren:
1) Aangewezen (voldoet aan functieprofiel/aanwijsbesluit)
2) Bekwaam (is de medewerker opgeleid)
3) Toegewezen (is de rol toegewezen aan de medewerker)

Proces in gebruik genomen
Op 12 mei 2023 is het proces inclusief achterliggende systemen live gegaan en in gebruik genomen. Teamchefs zijn geïnformeerd via de landelijke nieuwsbrief leidinggevenden en via de portefeuilleondersteuners binnen de eenheden. Ter ondersteuning zijn werkinstructies opgesteld die gepubliceerd zijn op het intranet en in beheer zijn genomen door de afdeling privacy PDC.

IV-inrichting
- Vanuit HRM is in Youforce de rol ‘Bevoegd Functionaris’ opgenomen in de ‘Rollen en middelen’-functionaliteit waar de teamchef de toewijzing kan beheren.
- Binnen BICC bedrijfsvoering is een cognosrapport ontwikkeld om inzicht in de BF administratie te verkrijgen.
- Initiële vulling van de systemen op basis van de huidige BF-administratie.

Ondersteunende rapportages tbv het proces
Voor zowel de teamchef als de privacyfunctionaris is cognosrapportage 5014: Bevoegd Functionaris gerealiseerd die diverse gegevens ontsluit:
- Functie gegevens HRM (Youforce).
- BF Rol gegevens HRM (Youforce).
- Opleidingsgegevens van de Politieacademie (Osiris).

[16] Projecteindrapport Bevoegd Functionaris van 28 juni 2023

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Actualiseren Beleidskader BF (incl. aanwijsbesluit)	Directeur IV (GA/privacy)	Q2 2024
2	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q2 2024

3.16 Intern toezicht

Bevindingen audit

1) Er is geen documentatie (bijvoorbeeld evaluatierapportages, jaarplan FG, jaarverslag FG, etc.) aangetroffen waaruit blijkt dat de FG van de politie recent aantoonbare controles en/of privacy compliance-assessments heeft uitgevoerd om vast te stellen of de gegevensverwerkingen voldoen aan de wettelijke verplichtingen.
2) Over de verslagperiode is in onvoldoende mate aangetoond via bijvoorbeeld toezicht en/of verantwoordings-rapportages dat voldaan wordt aan de basisbeginselen van de Wpg.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Zoals beschreven in paragraaf 2.2. heeft de GA de opdracht gekregen om te komen tot een voorstel tot de verbetering van de governance zoals dat is vastgesteld in het Privacybeleid van de politie. De notitie *Verbetering privacygovernance politie* beschrijft een voorstel op hoofdlijnen. Een gedetailleerde beschrijving van functieprofielen en specifieke processen die hieruit voortvloeien (GEB, verwerkingenregister, etc.) zullen, als ingestemd is met deze verbeterde governance, worden uitgewerkt in een geactualiseerd Privacybeleid.

De verbeterde privacygovernance gaat uit van de het three lines of defence-model voor het managen van de privacyrisico's.

1e lijn: Eigenaar van risico's: identificeert en beoordeelt risico's. De 1e lijn neemt mitigerende maatregelen of accepteer de risico's.

2e lijn: Stelt kaders en richtlijnen op, ondersteunt en adviseert de eerste lijn in het toepassen van kaders. Bewaakt of de eerste lijn zijn verantwoordelijkheden ook daadwerkelijk neemt (controle/monitoring).

3e lijn: Voert onafhankelijke audits uit en houdt onafhankelijk toezicht. De 3e lijn opereert los van de andere organisatieonderdelen.
Daarnaast kunnen externe audits worden uitgevoerd en toezichthouders op de naleving van de privacy wet- en regelgeving toezien.

Meer concreet is het jaarverslag van de FG over 2022 inmiddels aangeboden aan de referent KL. Tevens wordt voor 2024 een toezichtplan opgesteld.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Geactualiseerd Privacybeleid (incl 3LoD-model)	Directeur IV (GA/privacy)	Q3 2024
2	Jaarverslag en toezichtplan FG	FG	Q4 2024 Q1 2025

3.17 Audits

Bevindingen audit

1) Er is vastgesteld dat interne audits (Wpg-audit) niet worden uitgevoerd conform een formeel auditplan.
2) In het geval van geconstateerde tekortkomingen gedurende de privacy-audits geen formele hercontrole wordt uitgevoerd door een externe auditor zoals de norm voorschrijft.[17] Tevens vastgesteld dat bij recente Wpg-audits niet binnen drie maanden na dagtekening van het auditrapport een verbeterrapport is opgeleverd.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

1) Ten behoeve van cyclus 5 (2023-2026) wordt een meerjarig auditplan opgesteld door de interne auditor waarin per jaar is aangegeven welk auditactiviteiten met betrekking tot de Wpg worden uitgevoerd. Dit auditplan wordt afgestemd met de GA en behoeft de goedkeuring van de referent KL. In dit auditplan wordt beschreven wat de precieze scope en diepgang van de auditactiviteiten is, welk normenkader wordt gehanteerd, de benodigde auditcapaciteit en in welke periode de auditactiviteiten worden uitgevoerd.
2) In de meest recente privacyaudit heeft de auditor (KPMG) niet aangegeven dat de hercontrole moet worden uitgevoerd door een externe auditor. De hercontrole zal derhalve door de interne auditor worden uitgevoerd en richt zich uitsluitend op de onderdelen waarvoor tekortkomingen zijn geconstateerd in de privacyaudit en die zijn geadresseerd in dit verbeterrapport. De hercontrole zal plaatsvinden in de tweede helft van 2024.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Opstellen auditplan	Concernaudit	Q1 2024
2	Uitvoeren hercontrole	Concernaudit	Q4 2024

3.18 Toegang gegevensverwerking voor betrokkene

Bevindingen audit

Bij dit onderwerp zijn geen relevante tekortkomingen geconstateerd.

Wel wordt in het kader van kwaliteitsmanagement geadviseerd om, in lijn met het Besluit Digitale Overheid, op basis van een risicoanalyse vast te stellen of het haalbaar is om de toegankelijkheid voor betrokkenen te verhogen door ook een digitale ingang te creëren voor verzoeken in het kader van rechten van betrokkenen. Hierbij dienen dan wel afdoende technische waarborgen te worden getroffen voor (online) identificatie en authenticatie om te waarborgen dat de identiteit van de betrokkene adequaat wordt vastgesteld.

Conclusie	Opzet	Bestaan	Werking

[17] Artikel 4, lid 3 Regeling periodieke audit politiegegevens

Stand van zaken en verbetermaatregelen

Het digitaliseren van de verzoeken om inzage en correctie in het kader van rechten van betrokkenen was in beginsel onderdeel van het Intensiveringsprogramma privacy. De stuurgroep van het programma is echter op 5 september 2023 akkoord gegaan met het buiten scope plaatsen van dit onderwerp. Door het intensiveringsprogramma zijn diverse ontwikkelmogelijkheden met relevante stakeholders besproken. Alle opties kennen zo hun voor- en nadelen. De voorkeur gaat uit naar de optie die het mogelijk maakt via politie.nl een verzoek in te dienen. Dat moet via het portfolioproces in gang gezet worden en zou een co-productie kunnen zijn van de deelportefeuille privacy en de portefeuille Dienstverlening. De stuurgroep voorzag dat dit niet voor het einde van het programma gerealiseerd zou kunnen worden. Vandaar de keuze om dit onderwerp door te schuiven.

De gesprekken tussen de deelportefeuille privacy, de productowner van politie.nl en de SCBE van de portefeuille Dienstverlening moeten hervat worden om tot een businesscase te komen die tot een plaats op het portfolio kan leiden. Overigens is daarbij randvoorwaardelijk dat de ‘mijn-‘ en ‘mijn zakelijk-’omgeving zijn afgerond.

Rechten van betrokkenen als thema dient ook meegenomen te worden in de interne control cyclus.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Verzoek indienen bij politie.nl	Deelportefeuillehouder privacy	Q1 2024
2	Opstellen businesscase en doorlopen portfolioproces	Deelportefeuillehouder privacy/ Portefeuillehouder Dienstverlening (SCBE)	Q3 2024
3	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q1 2024

3.19 Meldplicht Datalekken

Bevindingen audit

Bij dit onderwerp zijn geen relevante tekortkomingen geconstateerd.

Conclusie	Opzet	Bestaan	Werking

Stand van zaken en verbetermaatregelen

Geen specifieke aanbevelingen vanuit de audit. Meldplicht datalekken als thema dient wel meegenomen te worden in de interne control cyclus.

	Verbetermaatregel	Verantwoordelijk	Gereed
1	Opnemen in monitoring- en controlcyclus	Directeur IV (GA/privacy)	Q1 2024

4 Monitoring opvolging verbeterrapport

De in hoofdstuk 3 beschreven verbetermaatregelen worden gemonitord door de GA in de vorm van een tertaalrapportage, aansluitend bij de reguliere cyclus van managementrapportages. Deze zullen worden aangeboden aan de strategische boards en input vormen voor de managementgesprekken.

Overeenkomstig artikel 33, lid 3 van de Wpg zal Concernaudit na een jaar een hercontrole uitvoeren.

Overigens geldt voor alle onderwerpen dat een proces van continue verbetering wordt ingezet middels borging van privacy in de reguliere planning- & controlcyclus. Dat geldt dus ook voor de onderwerpen waarvoor bij de audit geen concrete tekortkomingen zijn geconstateerd, maar bijvoorbeeld door de interne auditor wel risico's zijn geïdentificeerd. Deze maatregelen vallen buiten het bestek van dit verbeterrapport.