Afzender
Gegevensautoriteit
Typ Telefoonnr. afzender

Ontvanger(s)
Typ naam of namen

Rubricering
Politie INTERN - Bedrijfsvoering

Datum	14 augustus 2023	**Behandeld door**	Birgit Vredendaal
Ons kenmerk	Typ Ons kenmerk	**Kopie aan**	Typ Kopie aan
Uw kenmerk	Typ Uw kenmerk	**Bijlage(n)**	-

Onderwerp Managementreactie externe Wpg audit 2022

Geachte heer Koorn,

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 heb ik in goede orde ontvangen en met belangstelling gelezen. Hierbij geef ik u mijn 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)[1].

Intensiveringsprogramma privacy
Het Intensiveringsprogramma privacy, dat in 2019 is gestart en eind 2023 eindigt, heeft bijgedragen aan een verbeterslag op onderwerpen als het verwerkingenregister, 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

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

de Politieacademie. Dit komt helaas alleen (nog) niet nadrukkelijk tot uiting in de auditresultaten, omdat de verslagperiode voor de audit 2022 is.

Reactie op bevindingen
Op een paar onderwerpen wil ik 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 merk ik op dat in 2023 (beleids-)kaders en procesbeschrijvingen zijn geactualiseerd. Daarnaast wens ik 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 verantwoordelijkheden rond intern toezicht en structurele periodieke controles van beheersingsmaatregelen. 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.

Hoogachtend,

H.G. Geveke
Lid korpsleiding