Oplegnota KMTO

Ingebracht door / Akkoord van:
Portefeuille Ethiek en Privacy
5.1.2.e , 5.1.2.e
5.1.2.e , 5.1.2.e
5.1.2.e @politie.nl
06-5.1.2.e

Let op: de inbrenger moet alle stukken geaccordeerd hebben

Onderwerp
Décharge programma + invulling ondersteuning borging en risicomitigatie

Rubricering
Politie INTERN - Bedrijfsvoering

Datum overleg In te vullen door secretaris
Agendapunt In te vullen door secretaris

Behandeld door 5.1.2.e
5.1.2.e @politie.nl
06-5.1.2.e

Bijlage(n) 1

Doel Ter besluitvorming

Het KMTO wordt gevraagd

1. décharge te verlenen aan de deelportefeuillehouder privacy ten aanzien van het intensiveringsprogramma privacy en daarbij
2. in te stemmen met verlenging van de (ingehuurde) capaciteit in ieder geval gedurende een half jaar met als doel de producten te borgen in de organisatie en ondersteuning te verlenen aan de portefeuillehouders (GEB gerelateerd);
3. kennis te nemen dat een voorstel voor de verbeterde privacy governance en het verbeterrapport naar aanleiding van de externe Wpg audit op 7 februari 2024 aan het KMTO worden voorgelegd.

** Bij een voorgenomen besluit moet het advies- of instemmingsverzoek bij de stukken worden gevoegd.*

Samenvatting
De doorlooptijd van het in januari 2022 gestarte intensiveringsprogramma privacy eindigt per eind 2023. Daarom wordt decharge gevraagd. Omdat nog een aantal zaken moet worden afgerond en de portefeuillehouders hebben aangegeven langer ondersteund te willen worden bij privacy verantwoordelijkheden, wordt vanaf 1 januari 2024, onder sturing van de deelportefeuillehouder privacy, een hulpstructuur aangeboden. Doel hiervan is de producten te borgen in de organisatie en ondersteuning te verlenen aan de portefeuillehouders (GEB gerelateerd). Benodigd budget is geaccordeerd door de korpsleiding. Na 6 maanden wordt geëvalueerd of de lijn het over kan nemen. Zo niet, dan dienen de contracten nogmaals te worden verlengd.

Aanleiding voor bespreking
In het KLO van 11 mei 2021 is geconstateerd dat er, ondanks korpsbrede inspanningen en eerdere programma's, onvoldoende voortgang is 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 Programma intensivering 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

De bijlage geeft een overzicht van de opgeleverde producten op deze thema's.

Verwerkingenregister & GEB

Bij de start van het programma is tijdens het KMTO van 26 januari 2022 besloten de verantwoordelijkheid voor bestaande verwerkingen en processen bij een portefeuillehouder te beleggen. Dit betekent dat de portefeuillehouder namens de korpschef optreedt als gemandateerd verwerkingsverantwoordelijke, zowel voor verwerkingen van de *legacy* als het traject *improvement*. De portefeuillehouder stuurt in dat verband als hoofdverantwoordelijke op privacy compliance van de verwerking en voert de rol van primus inter pares uit. Het is mogelijk dat de portefeuillehouder de rol van primus inter pares via ondermandaat bij een gemandateerde belegt. In die constructie stuurt de gemandateerde namens de portefeuillehouder op privacy compliance van de verwerking.

Ondersteuning op de portefeuilles wordt momenteel door de eenheid en het programma geleverd. Hoe meer portefeuilles een eenheid heeft, des te meer verwerkingen en complexer de opgave is om privacy compliant te worden. Met het einde van het programma in zicht, op 31 december 2023, worden de laatste GEB's opgeleverd en wordt het tijd voor de volgende fase; de risicomitigatie. De portefeuilles hebben nogmaals kenbaar gemaakt hierin ondersteund te willen worden.

Het programma is samen met de portefeuillehouder privacy hierover in gesprek gegaan met de korpsleiding. Naar aanleiding hiervan is besloten dat met ingang van 1 januari 2024 onder sturing van de portefeuillehouder een hulpstructuur kan worden 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 6 maanden wordt geëvalueerd of de lijn het over kan nemen. Zo niet, dan worden de contracten nogmaals verlengd.

Voortraject

Reeds besproken in: overleg stuurgroep Intensiveringsprogramma

Toelichting

De décharge van het programma en het borgen van de op te leveren producten in de organisatie, hangt nauw samen met twee andere trajecten die op 22 augustus 2023 in het KLO zijn besproken:

1) Verbetering privacy governance
2) Verbeterrapport naar aanleiding van de Wpg audit

1) Verbetering privacy governance

Mede naar aanleiding van een onderzoek van Capgemini in 2022, doet de Gegevensautoriteit in het KMTO van 7 februari 2024 een voorstel tot het actualiseren van de privacy governance bij de politie. Hierbij wordt ook rekening gehouden met aanpalende onderzoeken zoals het I-stelsel Rijk, de CIO-functie bij de politie (VKA), en de gedachten over de compliance-organisatie bij de politie. Over deze actualisering is met relevante betrokkenen gesproken. Uitgangspunten hierbij zijn: 'If it ain't broke, don't fix it', formele reorganisaties worden als het kan vermeden en geen inhuur meer op cruciale functies.

Dit leidt tot duidelijke rollen en verantwoordelijkheden binnen de politie. Het toezicht en de monitoring op de naleving van de privacy-regels worden beter vormgegeven. Daarnaast wordt het vraagstuk van kennisborging

geadresseerd. Er wordt hiertoe ook een Chief Privacy Officer (CPO) voorgesteld. Het op deze wijze structureel verbeteren van de processen en het duidelijker beleggen van verantwoordelijkheden zorgt dat de politie de privacyhuishouding beter op orde kan krijgen. Opgemerkt moet wel worden dat de eerste verantwoordelijkheid bij de lijn berust, dus dat dit ook van de lijn een stevig commitment vereist.

2) Verbeterrapport naar aanleiding van de Wpg audit

Omdat uit het externe auditrapport van KPMG (2019-2022) blijkt dat er tekortkomingen zijn bij de naleving van de Wpg, moet een verbeterrapport worden opgeleverd waaruit blijkt welke maatregelen zijn of worden genomen om de tekortkomingen op te lossen. Het verbeterrapport staat geagendeerd voor het KMTO van 7 februari 2024.

Inmiddels is geïnventariseerd welke maatregelen al in 2023 zijn genomen, onder andere door het hiervoor genoemde programma. Dat geldt voor onderwerpen als het verwerkingenregister, het uitvoeren van GEB's en de bevoegd functionaris. Ook is met relevante betrokkenen afstemming gezocht over de vormgeving van intern toezicht. Voor de onderwerpen die in opzet voldoende scoren, moet de focus komen te liggen op de implementatie en uitvoering van het beleid. Daarnaast moet overkoepelend aandacht worden besteed aan het inrichten van structurele periodieke controles van beheersingsmaatregelen.

Realisatie / consequenties

Consequenties	Toelichting (sta o.a. stil bij de volgende punten, indien relevant)	Akkoord van directeur:
☑ Personeel/ HRM:	De contracten van een aantal medewerkers die nu voor het programma intensivering privacy werkzaam zijn worden verlengd.	Ja
☑ Financieel:	Benodigd budget is geaccordeerd door de korpsleiding	Ja
☐ Informatievoorziening:	Vraagt het voorstel om wijzigingen op IV-gebied en hoe past het voorstel dan in het portfolio IV?	Ja/nee of n.v.t.
☐ Facility Management:	Zijn er consequenties t.a.v. huisvesting, uniformen of uitrusting?	Ja/nee of n.v.t.
☑ Communicatie:	Er is een communicatieadviseur betrokken bij de hulpstructuur.	Ja
☐ Juridisch:	Wat zijn de uitkomsten van de juridische toets van het voorstel? (denk bijvoorbeeld aan gegevensbescherming of geweldstoepassing)	Ja/nee of n.v.t.
☐ Politiek-bestuurlijk:	Wat is de uitstraling van het voorstel op politiek en bestuur (Tweede Kamer, burgemeesters, etc)?	Ja/nee of n.v.t.
☐ Operatie:	Wat is de impact van het voorstel op de taakuitvoering van de politie?	Ja/nee of n.v.t.
☑ PDC:	De uitvoerbaarheid is afgestemd.	Ja
☐ Anders …..		

Bijlagen

Décharge programma intensivering privacy dd. 5-12-2023

Vervolgtraject

Aankruisen wat van toepassing is.

☐ KMTO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming	☐ KLO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming
☐ BBVO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming	☐ BOO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming
☐ COR (WOR)	☐ ter informatie ☐ voor instemming ☐ voor advies	☐ Vakbonden	☐ formeel, via CGOP ☐ informeel via overleg KL-vakbonden
☐ Combi MT	☐ ter besluitvorming ☐ ter bespreking/opinievorming ☐ ter kennisgeving	☐ LOVP	☐ ter informatie ☐ ter opinievorming ☐ ter besluitvorming

Archivering

Her vul je in waar het vastgestelde document wordt gearchiveerd.

Décharge programma intensivering privacy

KMTO 13 december 2023

5.1.2.e , 5.1.2.e

Versie 5 december 2023

« waakzaam en dienstbaar »

1. Project verwerkingenregister, GEB & IB
2. Project kennis & awareness
3. Project privacydesk & convenanten
4. Project autorisaties & privacy rapportages

1. Project verwerkingenregister, GEB & IB

	Opdracht	Opgeleverd?
1.	Uitvoeren van GEB's incl. IB-analyse op bestaande verwerkingen:	
-	Privacy en Ethiek (1 GEB)	Opgeleverd
-	Arrestantentaken (1 GEB)	Opgeleverd
-	Crisisbeheersing (1 GEB)	Opgeleverd
-	CTER (1 GEB)	Opgeleverd
-	Dienstverlening (2 GEB's)	Opgeleverd
-	Executie (0 GEB's)	Opgeleverd
-	Generieke Opsporing (5 GEB's)	4 opgeleverd, 1 on hold
-	GGP (5 GEB's)	Opgeleverd
-	Intelligence (10 GEB's)	3 opgeleverd, 7 lopend (waarvan 2 complexe)
-	Landelijke Meldkamer Samenwerking (0 GEB's)	Opgeleverd
-	Operationeel Centrum (1 GEB)	Opgeleverd
-	Specialistische Opsporing (5 GEB's)	2 afgerond, 3 bij int. review
-	Vreemdelingenzaken (5 GEB's)	Opgeleverd
-	Thematische Opsporing (3 GEB's)	Opgeleverd
-	VIK (4 GEB's)	Opgeleverd
-	Zorg & Veiligheid (3 GEB's)	Opgeleverd

1. Project verwerkingenregister, GEB & IB

	Opdracht	Opgeleverd?
2.	Advies aan portefeuillehouders t.a.v. risico mitigerende maatregelen op basis van de GEB's incl. IB-analyse	Opgeleverd*
3.	Bestaande verwerkingen registreren in verwerkingenregister	Opgeleverd*
4.	Notitie voorziening privacy	Opgeleverd
5.	Landelijk format: GEB-formulier	Opgeleverd

2. Project kennis & awareness

Opdracht	Opgeleverd?
1. Leermiddel en toets Basis AVG, IB, Wpg	Opgeleverd
2. Leermiddel en toets Toepassen AVG, IB, Wpg	Buiten scope geplaatst
3. Leermiddel en toets Expert AVG, IB, Wpg	Buiten scope geplaatst
4. Beheer leermiddelen en toetsen	Memo opgeleverd

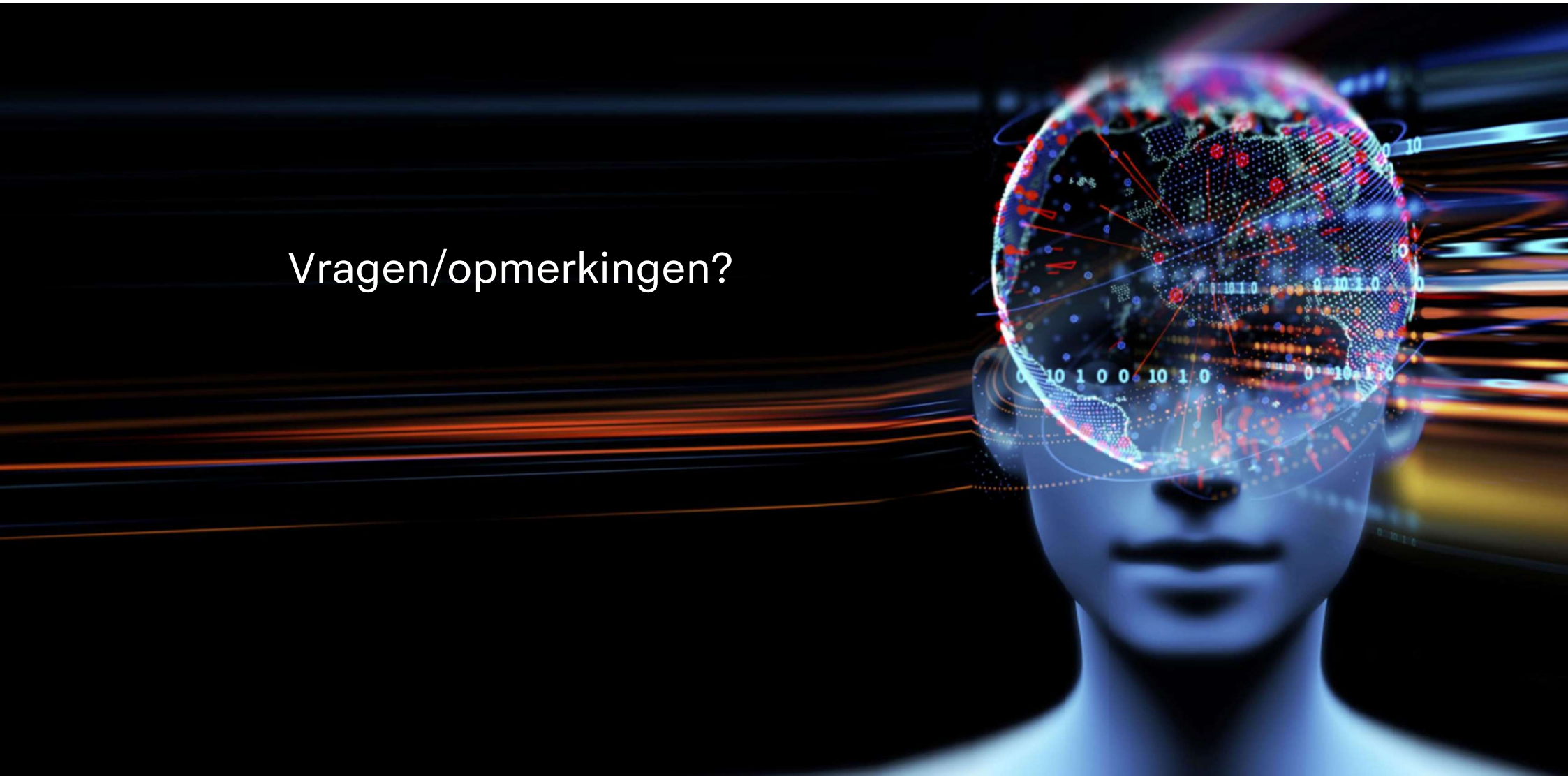
3. Project privacydesk & convenanten

	Opdracht	Opgeleverd?
1.	Uitvoeren kruiscontroles en opleveren lijst 0-metingen convenanten	Opgeleverd
2.	Plan van aanpak interventiestrategie non compliant convenanten	Opgeleverd
3.	Opstellen van een plan van aanpak t.b.v. herstel convenanten voor de eenheden	Deze maand enkel nog Noord-Nederland en dan opgeleverd
4.	Beleidskader convenanten inclusief proces en overige bijlagen	Opgeleverd
5.	Ontwikkelen aanvraagprocedure rechten van betrokkenen	Buiten scope geplaatst
6.	Verdiepende training privacydesk	Opgeleverd

4. Project autorisaties & privacy rapportages

	Opdracht	Opgeleverd?
1.	Privacy dashboard bouwen	Opgeleverd
2.	Bevoegd Functionaris	Opgeleverd
3.	Schoning Direct Assigns	Opgeleverd
4.	Verbetering privacy rapportages	Opgeleverd

Vragen/opmerkingen?



« waakzaam en dienstbaar »

Projecteindrapport

Verwerkingenregister, GEB & IB

Projectmanager	5.1.2.e
Versienummer	1.0
Datum	11 december 2023
Status	Definitief
Rubricering	Politie INTERN - Bedrijfsvoering

Documentinformatie

Met dit projecteindrapport rapporteert de projectleider over het afsluiten van het project aan de programmamanager. Hierin wordt gerapporteerd over het verloop van het project en de bereikte projectresultaten, gerelateerd aan de opdracht en het projectplan. Als de programmamanager akkoord is, dient deze het rapport in bij de stuurgroep. Waar het vastgesteld wordt (opnemen in de documentinformatie).

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Markering Ja/Nee
0.1	05-12-2023	Eerste concept IB	Nee
0.2	07-12-2023	Toevoeging Privacy	Nee
1.0	11-12-2023	Definitieve versie	Nee

Distributie / Akkoord

Versie	Verzend datum	Naam	Afdeling / Functie	Datum akkoord
0.1	08-12-2023	5.1.2.e	5.1.2.e	
0.2	11-12-2023	5.1.2.e	5.1.2.e	

Projectevaluatie

1. Doelstelling

Onderstaande tabel geeft de doelstelling, aanleiding, opdracht en beoogde resultaten en effecten weer, zoals beschreven in het projectplan

Doelstelling	Aanleiding	Opdracht
Doelstelling is om alle processen te clusteren tot verwerkingen en deze in het centrale SmartPIA register te registeren en te classificeren als hoog- of laagrisico. Van de hoog-risico verwerkingen zal een GEB (GegevenbeschermingEffectBeoordeling) worden opgesteld waarbij de privacy risico's zullen worden gedocumenteerd en overgedragen. Daarnaast is de doelstelling om van alle geregistreerde hoog-risico verwerkingen inzicht te hebben in de informatiebeveiligingsrisico's en hieraan gekoppeld de mitigerende maatregelen Het opleveren van geadviseerde maatregelen bij de aangetroffen risico's aan de portefeuillehouder. Er wordt een landelijk Wpg GEB formulier ontwikkeld.	Het programmaplan intensivering privacy 2023 geeft een beschrijving van de weg die afgelegd dient te worden om volledige privacy compliance en inbedding daarvan in de organisatie te bereiken. Privacy compliance betreft het aantoonbaar voldoen aan de Algemene verordening gegevensbescherming (AVG) en Wet Politiegegevens (Wpg). Hierin staat beschreven dat persoonsgegevens goed moeten worden beveiligd. Als de informatiebeveiliging niet op orde is, bestaat het gevaar dat persoonsgegevens op straat komen te liggen.	Privacy draagt zorg voor de definitie en classificatie van de verwerkingen en het opstellen van de GEB's voor de hoog-risico verwerkingen Informatiebeveiliging onderzoekt of passende technische en organisatorische maatregelen zijn getroffen om verwerkingen van persoonsgegevens goed te beveiligen. Het bestaande GEB formulier aanpassen aan de Wpg.
Resultaat	▪ Privacy: Voor de hoogrisico-verwerkingen waar een GegevensbeschermingEffectBeoordeling (GEB) voor geschreven is, zijn voor de onderliggende applicaties Informatiebeveiligs(IB) analyses opgesteld inclusief dossiervorming ▪ IB: Na oplevering van de IB analyses zijn dossiers versleuteld waarbij de gebruikte wachtwoorden in de standaard password manager "Keepass" zijn opgeslagen. ▪ Bij het uitblijven van een standaard GRC omgeving is een begin gemaakt van een Centraal Risico Register in Excel op basis waarvan de eerste rapporten zijn opgemaakt. ▪ Er is een Wpg GEB formulier beschikbaar voor het uitvoeren van GEB's.		
Effecten	▪ De privacy- en informatiebeveiligingsrisico's binnen de verwerkingen en onderliggende systemen zijn in kaart		

	gebracht en overgedragen aan de portefeuillehouders en product owners. ▪ De risico's zijn begroot (kans x impact) en geprioriteerd ▪ Per risico zijn mitigerende maatregelen geadviseerd om het risico te verminderen of weg te nemen. ▪ Navraag leert dat er nog geen aanvang is gemaakt met het implementeren van de aanbevolen mitigerende maatregelen (uitzonderingen bevestigen hier de regel). ▪ Het beschikbaar hebben van een Wpg GEB formulier vergroot de uniformiteit bij het uitvoeren van een GEB.

Doelstelling	Aanleiding	Opdracht
Op aangeven van de portefeuillehouder Ethiek en Privacy wordt door het programma een voorstel gedaan voor een landelijke voorziening privacy. Het doel van deze voorziening is om de portefeuilles en de uitvoering in de eenheden te ondersteunen bij hun privacytaken. Een van de uitgangspunten hierbij is de groei volgens het CIP volwassenheidsmodel van de privacy organisatie.	Aanleidingen hiervoor zijn onder andere: - Vraag portefeuillehouders om ondersteund te worden - Visie op de privacy functie ontbreekt waardoor versnippering is ontstaan t.a.v. het privacylandschap - De privacy functie in de eenheden is niet geformaliseerd - Capaciteit en belasting van de privacyfunctionaris staat onder druk - Privacy beleid en kaders zijn beschreven maar onvoldoende geïmplementeerd - Er is een toenemende groei aan inzageverzoeken, adviesaanvragen, samenwerkingsverbanden, innovaties, complexiteit (big data, cloud oplosingen, intelligence ….) - Programma maskeert en verwerkt veel privacyvraagstukken - Legacy wordt weggewerkt maar de kraan staat open - Toezicht AP wordt geïntensiveerd.	Doe een voorstel voor een landelijke voorziening privacy.
Resultaat	▪ De portefeuilles en de uitvoering in de eenheden worden ondersteund bij hun privacytaken	
Effecten	▪ De privacytaken kunnen beter worden opgepakt waardoor ook groei plaatsvindt volgens het CIP volwassenheidsmodel van de privacy organisatie.	

Effecten en resultaten

Effecten

Onderstaande tabel geeft aan in welke mate het project de beoogde effecten heeft opgeleverd

Nr.	Beoogd effect conform projectplan	Realisatie
1	Het aantoonbaar voldoen aan de Algemene verordening gegevensbescherming (AVG) en Wet Politiegegevens (Wpg). Daarnaast het inzicht hebben in de privacy- en informatiebeveiligingsrisico's en hieraan gekoppelde mitigerende maatregelen	Voor de hoog-risico verwerkingen zijn GEB's opgesteld. Voor applicaties binnen deze verwerkingen is een IB analyse opgesteld, tenzij de applicatie op korte termijn uitgefaseerd of vervangen zou worden. Ook wanneer een andere partij (zoals de sector IB) al een informatiebeveiligingsanalyse aan het maken was, is er niet nog een IB analyse binnen het programma gemaakt, maar zijn de gevonden risico's overgenomen.
2	Betrokken partijen zoals de portefeuillehouders en productowners zijn op de hoogte gebracht van de risico's in hun verwerking(en) resp. applicatie(s).	De GEB's zijn besproken en gedeeld met de portefeuillehouders voor verdere opvolging (inclusief de onderliggende IB analyses)
3	Het beschikbaar hebben van een Wpg GEB formulier vergroot de uniformiteit bij het uitvoeren van een GEB.	Het Wpg GEB formulier is in de eerste fase van het programma opgeleverd waarna conform dit formulier de GEB's zijn uitgevoerd.
4	De privacytaken kunnen middels een landelijke voorziening privacy beter worden opgepakt waardoor ook groei plaatsvindt volgens het CIP volwassenheidsmodel van de privacy organisatie.	De effecten blijven vooralsnog uit omdat het vanuit het programma gedane voorstel meegaat in de verbetering van de privacy governance, hetgeen nog niet gereed is.

Resultaten

Onderstaande tabel geeft aan in welke mate het project de beoogde resultaten heeft opgeleverd

Nr.	Beoogd resultaat conform projectplan	Realisatie
1	Beoogd resultaat: Een gevuld verwerkingen register (SmartPIA) en GEB's voor de hoog-risico verwerkingen waarmee inzicht in de Privacy risico's wordt verkregen. Daarnaast het inzicht hebben in de informatiebeveiligingsrisico's en hieraan gekoppelde mitigerende maatregelen	De privacy risico's zijn gedocumenteerd in de GEB's en opgeslagen in verwerkingenregister SmartPIA. Voor een gespecificeerd overzicht van de opgeleverde GEB's per portefeuille en een overzicht van de status per GEB: **zie Bijlage-A** Doordat het programma per 31-12-2023 formeel stopt, is het niet mogelijk om de externe reviews voor alle GEB's af te wachten. Feedback vanuit de externe reviews zal in 2024 moeten worden verwerkt. Een gecombineerd overzicht van de privacy en IB risico's is opgesteld inclusief een aantal basis rapportages: het Centraal Risico Register (CRR). Omvang van dit overzicht op hoofdlijnen: - 5000 privacy- en IB risicoregels met geadviseerde mitigerende maatregelen waar nodig - 200 applicaties onderzocht en beschreven - 46 AVG GEB's Zie het Centraal Risico Register voor meer gedetailleerde informatie en rapportages. Schermafdrukken zijn ter illustratie in **Bijlage-B** toegevoegd.
2	Niet opgenomen in het projectplan, maar wel opgeleverd: het Centrale Risico Register inclusief werkinstructies.	Er is een initiële versie van een Centraal Risico Register gemaakt en opgeleverd in Excel. Hierin staan alle Privacy risico's vanuit de opgeleverde GEBs en IB analyses. Dit register zal -na afloop van het programma- gekoppeld worden aan Vena ter ondersteuning van de implementatie

		van de mitigerende maatregelen. Werkinstructies tbv onderhoud aan het Centrale Risico Register (document wordt nog uitgebreid):  Werkinstructies Centraal Risico Regi
3	Ontwikkelde tooling en procedures: - Gedetailleerde werkprocedure - IB Quickscan (later vervangen door de BIO quickscan) - IB Light analyse - IB Werkprogramma - Gedetailleerde voortgangsplanning WPG incl. Blauwdruk- en stuurgroep rapportages	 Procesflow Informatiebeveiligin  Template IB Quickscan - Leeg.xls  Template IB-Light analyse - leeg.xlsx  WPG-IB-Risicoanaly se-Werkprogramma  WPG Centrale voortgang Privacy en
4	Niet opgenomen in het projectplan maar wel opgeleverd: Mapping van diverse normenkaders (ISO, BIO, etc.) naar politie-specifieke maatregelen	Deze set aan politie-specifieke maatregelen zijn uiterst belangrijk om mee te nemen bij de implementatie van een volwassen GRC omgeving
5	Niet opgenomen in het projectplan maar wel opgeleverd: Werkprocedure om op zeer korte termijn een start te maken met het implementeren van de mitigerende maatregelen. Invulling van de rollen wordt ten tijde van dit schrijven nog besproken.	 Swimmerlane def concept.pptx  Quick Reference Card - processtappe  RASCI.xlsx
6	Er is een Wpg GEB formulier beschikbaar voor het uitvoeren van GEB's.	Deze was in de eerste fase van het programma gereed voor het uitvoeren van de GEB's.
7	De portefeuilles en de uitvoering in de eenheden worden middels een landelijke voorziening privacy ondersteund bij hun privacytaken	Er is een houtskoolschets opgeleverd waarin een voorstel is gedaan voor een landelijke voorziening privacy, dit voorstel wordt door de Gegevensautoriteit meegenomen in hun voorstel voor wat betreft de verbetering van de privacy governance dat ze op 7 februari 2024 presenteren tijdens het KMTO. Omdat nog een aantal zaken moet worden afgerond en de portefeuillehouders hebben aangegeven langer ondersteund te willen worden bij privacy verantwoordelijkheden, wordt vanaf 1 januari 2024, onder sturing van de deelportefeuillehouder privacy, een hulpstructuur aangeboden. Doel hiervan is de producten te borgen in de organisatie en ondersteuning te verlenen aan de portefeuillehouders (GEB gerelateerd). Benodigd budget is geaccordeerd door de korpsleiding. Na 6 maanden wordt geëvalueerd of de lijn het over kan nemen. Zo niet, dan dienen de contracten nogmaals te worden verlengd.

2. Overdracht en borging

Overdracht

Nr.	Product	Ontvanger - Eindverantwoordelijke
1	SmartPIA register	Portefeuillehouder Privacy
2	GEB per hoog-risico verwerking inclusief IB analyses	Portefeuillehouder Privacy
3	Politie-specifieke maatregelenset	Sector IB
4	Coördinatie implementatie geadviseerde maatregelen	Portefeuillehouder Privacy
5	Landelijke voorziening privacy	Portefeuillehouder Privacy

Borging

Bij borging gaat het om het werkend krijgen en up-to-date houden van de producten in de praktijk.

Nr.	Product	Verantwoordelijk	Eindverantwoor-delijk	Ondersteuning	Raadpleging	Informeren
1	SmartPIA	Primus Inter Pares	Portefeuillehouder	Afdeling Privacy PDC	-	-
2	Centraal risico register	Portefeuillehouder privacy	Portefeuillehouder privacy	Portefeuillehouder privacy	-	-
3	Politie-specifieke maatregelenset	Sector IB	Sector IB	-	-	-
4	Implementatie geadviseerde maatregelen	Primus Inter Pares	Portefeuillehouder Privacy	Afdeling Privacy PDC	-	-
5	Landelijke voorziening privacy	Gegevensautoriteit	Portefeuillehouder Privacy	Hulpstructuur	-	-

RASCI-model

Ten aanzien van het borging schema is gebruikgemaakt van het RASCI-model:

RASCI	Verantwoordelijkheid	Taak
Responsible	Verantwoordelijk voor uitvoering	Uitvoerend
Accountable	Eindverantwoordelijk	Beslissend
Supportive	Ondersteuning tijdens	Ondersteunend
Consulted	Raadpleging vooraf	Adviserend
Informed	Informeren achteraf	Geïnformeerd

Responsible en accountable spreekt waarschijnlijk voor zich. Bij consulted kan bijvoorbeeld gedacht worden aan situaties waarbij de Privacyfunctionaris geraadpleegd dient te worden en bij informed bijvoorbeeld aan de Functionaris Gegevensbescherming die geïnformeerd dient te worden. Dit kan rechtstreeks voortvloeien uit wet- en regelgeving, maar ook enkel middels beleid zo zijn bepaald. Denk voor wat betreft supportive bijvoorbeeld aan het programma (uiteraard maar tot 31-12-2023) of het Expertisecentrum Privacy.

3. Restpunten en vervolgacties

Restpunten

De restpunten van dit deelproject betreffen het afronden van een aantal GEB's die nog in Externe Review zitten. Zie Bijlage-A voor een gedetailleerde uitwerking hierover per portefeuille. Daarnaast wordt er per portefeuille een memo opgesteld waarin de restpunten tot in detail zijn beschreven zodat deze GEB's kunnen worden afgerond. Deze memo's worden met de betrokken portefeuillehouder.

Geen restpunten voor IB binnen de formele scope van het programma. Wel is belangrijk dat er doorgepakt wordt op de geadviseerde maatregelen zoals samengebracht in het Centrale Risico Register. De in de achterliggende tijd verzamelde data heeft een korte houdbaarheid in verband met het snel veranderende applicatielandschap en organisatiestructuur. Wanneer er nu geen actie ondernomen wordt, kan aangenomen worden dat de politiesystemen niet veiliger geworden zijn door de achterliggende programma's en is de investering bijna voor niets geweest.

Om de implementatie van de maatregelen te faciliteren wordt er een koppeling gemaakt met Vena zodat er een workflow geïmplementeerd kan worden tussen de partijen die betrokken zijn bij de mitigatie van de risico's.

Gelijktijdig aan het oplossen van de risico's moet er gezocht worden naar een oplossing om de risico's en opvolging ervan in de toekomst centraal te registreren. Belangrijk is dat in de gekozen oplossing de bekende PDCA cyclus geborgd is.

Vervolgacties

Onderstaande tabel geeft aan welke vervolgacties nodig zijn per restpunt, en waar deze acties zijn belegd

Nr.	Restpunt	Vervolgactie	Actiehouder
1	SmartPIA	Het up-to-date houden van de Verwerkingen en GEB's zoals deze in SmartPIA zijn geregistreerd.	PIP zoals in SmartPIA gergistreerd
2	Restend GEB-werk	De nog niet afgeronde GEB's completeren. Zie Bijlage-A voor een uitwerking.	Portefeuillehouder
3	Vena implementatie (Q1-2024)	Deze tijdelijke implementatie is nodig om op korte termijn te kunnen starten met de opvolging van de geadviseerde maatregelen.	Portefeuillehouder
4	Landelijke voorziening privacy	Voorstel verbetering privacy governance.	Gegevensautoriteit

4. Aanbeveling doorontwikkeling

Onderstaande tabel beschrijft aanbevelingen voor het doorvoeren van een verdere efficiëntie- en/of kwaliteitsverbetering op basis van de behaalde resultaten

Nr.	Resultaat	Aanbeveling doorontwikkeling
1	Informatiebeveiligingsbewustwording binnen de HR processen	Iedereen heeft een verantwoordelijkheid mbt Informatiebeveiliging en met name systeem eigenaren en product owners. Zij moeten er bijvoorbeeld op worden aangesproken als blijkt dat er nog openstaande risico's zijn voor hun systeem/applicatie. Hiervoor is uiteraard een centrale registratie nodig.
2	Het centrale risico register is een eerste aanzet naar een PDCA-cyclus maar deze cyclus moet op gang gehouden worden door o.a. passende tooling, procedures, werkafspraken en goed belegde verantwoordelijkheden.	Het registeren en mitigeren van risico's is een cyclisch proces dat zonder ondersteunende systemen zal verzanden. Een GRC-achtige oplossing helpt bij het op gang houden van deze cyclus en kan betrokken partijen actief informeren m.b.t. hun verantwoordelijkheden. Daarnaast biedt het centraal registeren van risico's de mogelijkheid om bedrijfsbreed maar ook per portefeuille rapportages op te maken met betrekking tot de risico's die de politie loopt.

1.1 Bijlage A

Per portefeuille is een gedetailleerd memo geschreven waarin de meest recente status van de GEB's is beschreven met daarbij invullende informatie die nodig is om de GEB's af te kunnen ronden.

Per 7 december 2023 is de stand van met betrekking tot de WPG GEB's als volgt:

Portefeuille	Aantal laag risico*	Aantal GEB's = hoog risico				
		Totaal	Opgeleverd	In externe review	Nog onder handen****	Teruggegeven aan portefeuille
Arrestantentaken	1	1	1			
Crisisbeheersing	2	1		1		
CTER	0	1	1			
Executie	2	0				
Dienstverlening	0	2	2			
Generieke Opsporing	9	6	3	1	1	1
GGP	18	8	2	1	2	3
Intelligence	15	11	2	2	5	2
LMS	10**	0				
Operationeel Centrum	8	1	1			
Specialistische Opsporing	3	7	2	3		2
Thematische Opsporing	2	3		3		
VIK	1	4	4			
Vreemdelingenzaken	0	5	5			
Zorg & Veiligheid	0	3	1	2		
Overig	0	1	1			
TOTAAL	**71**	54 = **52*****	25 = **23*****	**13**	**8**	**8**

* Dit betreft zowel geclusterde laag risico hoofdverwerkingen, als losse laag risico processen die niet geclusterd konden worden.
** De verwerkingen van LMS betreffen zowel laag risico als hoog risico verwerkingen. Het programma voert echter geen GEB's uit voor LMS. De bevindingen van het programma worden na afloop overgedragen aan de portefeuille.
*** 2 GEB's zijn dubbel vermeld in deze tabel, omdat deze GEB's onder 2 portefeuilles zijn uitgevoerd.
**** Voor de nog onder handen zijnde GEB's is de verwachting dat deze voor 31-dec-2023 zullen worden opgeleverd.

Een overzicht van de WPG GEB's staat hieronder met de status per 7 december 2023:

Status GEB's 07-12-2023.xlsx

1.2 Bijlage B

Schermafdrukken centraal risicoregister

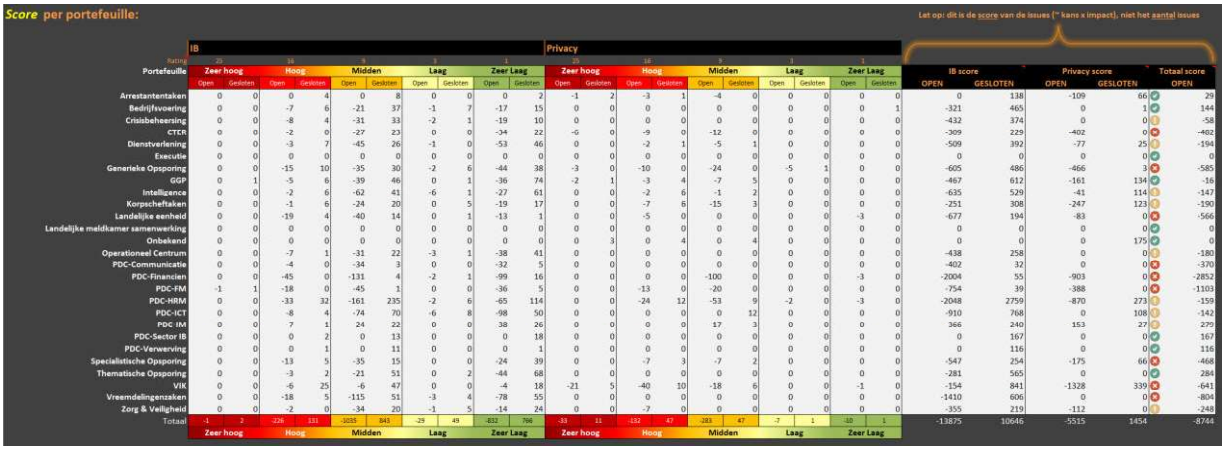
Deeloverzicht risico's

CRR - Centraal Risico Register - Privacy en IB

IB analyse / GEB			Service Manager		Programma Info		Koppeling Waardeleiten			IB Risico Analyse / GEB		MCS	NCSC						
Beer	Risico analyse / GEB (documentnaam)	Applicatienaam	CI Identifier	Portefeuille	Portefeuille wijzen Prio. Prg.	Verwerking wijzen Prio. Prg.	Productelijn / Aandachtsgebied	Contactpersoon binnen IB/Privacy	Waardeketen	Hoofdonderwerp	Thema	Mission Critical System	Top-5 risico	BIV Aspect B	BIV Aspect I	BIV Aspect V	Risicoscore K	Risicoscore E	Risicoscore R	Risicoclassificatie
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Mens	Rolbeschrijving	Mission Critical System	NCSC top-5 item			x	2	3	6	Midden
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Mens	Geheimhoudings- en verklaringsplicht	Mission Critical System	NCSC top-5 item			x	1	5	5	Midden
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Mens	Bevoegdheid	Mission Critical System					1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Mens	Huisvesting	Mission Critical System					1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Procedures	Procedure beschrijvingen	Mission Critical System					1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Procedures	Naleving	Mission Critical System					1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma Catch & Havenk.xlsx	Havenk	01008626	Specialistische Opsporing	Specialistische Opsporing	Gelaatsvergelijking	Opsporing	5.1.2.e	Opsporing	Procedures	Incident management	Mission Critical System					1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma OMS.xlsx	OMS	01749909	Thematische Opsporing	Thematische Opsporing	Onbekend	Opsporing	5.1.2.e	Opsporing	Apparatuur	Geschikte middelen		NCSC top-5 item				1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma OMS.xlsx	OMS	01749909	Thematische Opsporing	Thematische Opsporing	Onbekend	Opsporing	5.1.2.e	Opsporing	Apparatuur	Beheer						1	1	1	Zeer laag
IB	WPG-IB-Risicoanalyse-Werkprogramma OMS.xlsx	OMS	01749909	Thematische Opsporing	Thematische Opsporing	Onbekend	Opsporing	5.1.2.e	Opsporing	Apparatuur	Levenscyclusmanagement						1	1	1	Zeer laag

Algemene rapportages

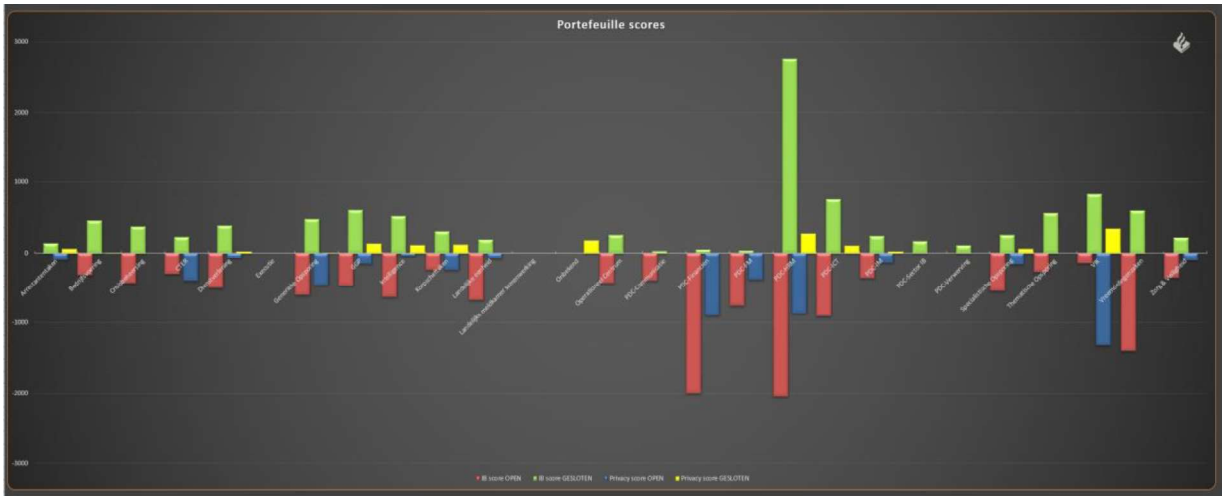
Overzichten portefeuilles



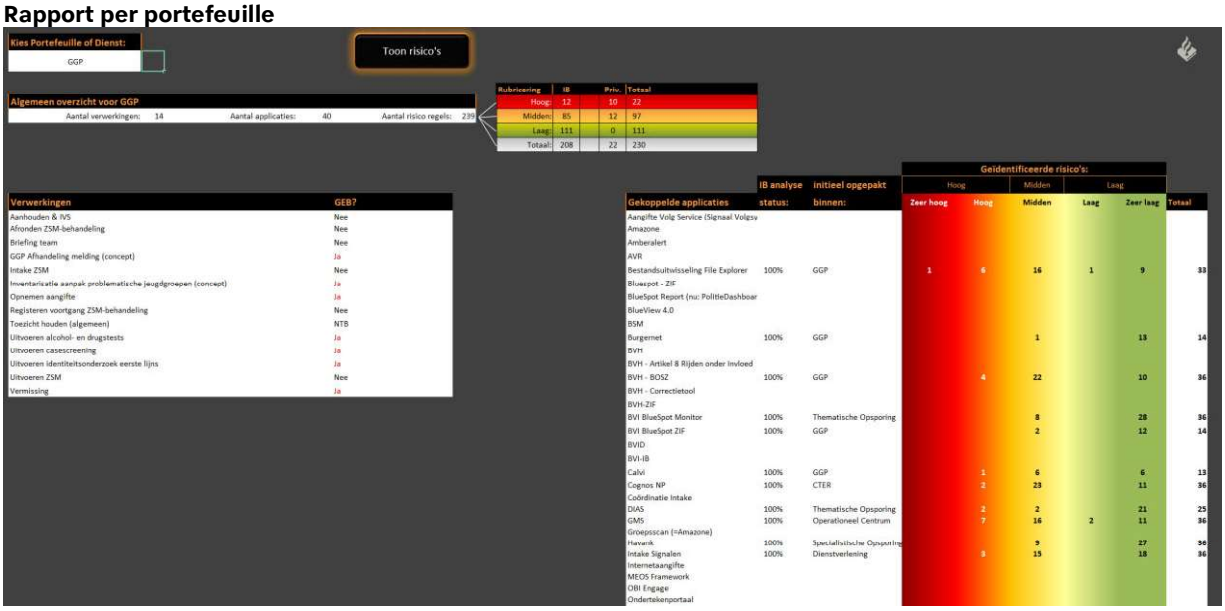
Score per portefeuille:

Let op: dit is de score van de issues (= kans x impact), niet het aantal issues

Portefeuille	IB Zeer hoog Open	IB Zeer hoog Gesloten	IB Hoog Open	IB Hoog Gesloten	IB Midden Open	IB Midden Gesloten	IB Laag Open	IB Laag Gesloten	IB Zeer Laag Open	IB Zeer Laag Gesloten	Privacy Zeer hoog Open	Privacy Zeer hoog Gesloten	Privacy Hoog Open	Privacy Hoog Gesloten	Privacy Midden Open	Privacy Midden Gesloten	Privacy Laag Open	Privacy Laag Gesloten	Privacy Zeer Laag Open	Privacy Zeer Laag Gesloten	IB score OPEN	IB score GESLOTEN	Privacy score OPEN	Privacy score GESLOTEN	Totaal score OPEN
Arrestantentaken	0	0	0	4	0	8	0	0	0	2	-1	2	-3	1	-4	0	0	0	0	0	0	138	-109	66	29
Bedrijfsvoering	0	0	-7	6	-21	37	-1	7	-17	15	0	0	0	0	0	0	0	0	0	1	-321	465	0	1	144
Crisisbeheersing	0	0	-8	4	-31	33	-2	1	-19	10	0	0	0	0	0	0	0	0	0	0	-432	374	0	0	-58
CTER	0	0	-2	0	-27	23	0	0	-34	22	-6	0	-9	0	-12	0	0	0	0	0	-309	229	-402	0	-482
Dienstverlening	0	0	-3	7	-45	26	-1	0	-53	46	0	0	-2	1	-5	1	0	0	0	0	-509	392	-77	25	-194
Executie	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Generieke Opsporing	0	0	-15	10	-35	30	-2	6	-44	38	-3	0	-10	0	-24	0	-5	1	0	0	-605	486	-466	3	-585
GGP	0	1	-5	6	-39	46	0	1	-36	74	-2	1	-3	4	-7	5	0	0	0	0	-467	612	-161	134	-19
Intelligence	0	0	-2	6	-62	41	-6	1	-27	61	0	0	-2	6	-1	2	0	0	0	0	-635	529	-41	114	-147
Korpstaken	0	0	-1	6	-24	20	0	5	-19	17	0	0	-7	6	-15	3	0	0	0	0	-251	308	-247	123	-190
Landelijke eenheid	0	0	-19	4	-40	14	0	1	-13	1	0	0	-5	0	0	0	0	0	-3	0	-677	194	-83	0	-566
Landelijke meldkamer samenwerking	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Onbekend	0	0	0	0	0	0	0	0	0	0	0	3	0	4	0	4	0	0	0	0	0	0	0	175	0
Operationeel Centrum	0	0	-7	1	-31	22	-3	1	-38	41	0	0	0	0	0	0	0	0	0	0	-438	258	0	0	-180
PDC-Communicatie	0	0	-4	0	-34	3	0	0	-32	5	0	0	0	0	0	0	0	0	0	0	-402	32	0	0	-370
PDC-Financien	0	0	-45	0	-131	4	-2	1	-99	16	0	0	0	0	-100	0	0	0	-3	0	-2004	55	-903	0	-2852
PDC-FM	-1	1	-18	0	-45	1	0	0	-36	5	0	0	-13	0	-20	0	0	0	0	0	-754	39	-388	0	-1103
PDC-HRM	0	0	-33	32	-161	235	-2	6	-65	114	0	0	-24	12	-53	9	-2	0	-3	0	-2048	2759	-870	273	-159
PDC-ICT	0	0	-8	4	-74	70	-6	8	-98	50	0	0	0	0	0	12	0	0	0	0	-910	768	0	108	-142
PDC IM	0	0	7	1	24	22	0	0	38	26	0	0	0	0	17	3	0	0	0	0	366	240	153	27	299
PDC-Sector IB	0	0	0	2	0	13	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	167	0	0	167
PDC-Verwerving	0	0	0	1	0	11	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	116	0	0	116
Specialistische Opsporing	0	0	-13	5	-35	15	0	0	-24	39	0	0	-7	3	-7	2	0	0	0	0	-547	254	-175	66	-468
Thematische Opsporing	0	0	-3	2	-21	51	0	2	-44	68	0	0	0	0	0	0	0	0	0	0	-281	565	0	0	284
VIK	0	0	-6	25	-6	47	0	0	-4	18	-21	5	-40	10	-18	6	0	0	-1	0	-154	841	-1328	339	-641
Vreemdelingenzaken	0	0	-18	5	-115	51	-3	4	-78	55	0	0	0	0	0	0	0	0	0	0	-1410	606	0	0	-804
Zorg & Veiligheid	0	0	-2	0	-34	20	-1	5	-14	24	0	0	-7	0	0	0	0	0	0	0	-355	219	-112	0	-248
Totaal	-1	2	-226	133	-1035	843	-29	49	-832	786	-33	11	-132	47	-283	47	-7	1	-10	1	-13875	10646	-5515	1454	-8744



Rapport per portefeuille



Kies Portefeuille of Dienst: GGP

Toon risico's

Algemeen overzicht voor GGP

Aantal verwerkingen: 14 Aantal applicaties: 40 Aantal risico regels: 239

Rubricering	IB	Priv.	Totaal
Hoog:	12	10	22
Midden:	85	12	97
Laag:	111	0	111
Totaal:	208	22	230

Verwerkingen	GEB?
Aanhouden & IVS	Nee
Afronden ZSM-behandeling	Nee
Briefing team	Nee
GGP Afhandeling melding (concept)	Ja
Intake ZSM	Nee
Inventarisatie aanpak problematische jeugdgroepen (concept)	Ja
Opnemen aangifte	Ja
Registeren voortgang ZSM-behandeling	Nee
Toezicht houden (algemeen)	NTB
Uitvoeren alcohol- en drugstests	Ja
Uitvoeren casescreening	Ja
Uitvoeren identiteitsonderzoek eerste lijns	Ja
Uitvoeren ZSM	Nee
Vermissing	Ja

Gekoppelde applicaties	IB analyse status:	Initieel opgepakt binnen:	Geïdentificeerde risico's: Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Aangifte Volg Service (Signaal Volgsy								
Amazone								
Amberalert								
AVR								
Bestandsuitwisseling File Explorer	100%	GGP	1	6	16	1	9	33
Bluespot - ZIF								
BlueSpot Report (nu: PolitieDashboar								
BlueView 4.0								
BSM								
Burgernet	100%	GGP			1		13	14
BVH								
BVH - Artikel 8 Rijden onder Invloed								
BVH - BOSZ	100%	GGP		4	22		10	36
BVH - Correctietool								
BVH-ZIF								
BVI BlueSpot Monitor	100%	Thematische Opsporing			8		28	36
BVI BlueSpot ZIF	100%	GGP			2		12	14
BVID								
BVI-IB								
Calvi	100%	GGP		1	6		6	13
Cognos NP	100%	CTER		2	23		11	36
Coördinatie Intake								
DIAS	100%	Thematische Opsporing		2	2		21	25
GMS	100%	Operationeel Centrum		7	16	2	11	36
Groepsscan (=Amazone)								
Havank	100%	Specialistische Opsporing			9		27	36
Intake Signalen	100%	Dienstverlening		3	15		18	36
Internetaangifte								
MEOS Framework								
OBI Engage								
Ondertekenportaal								

De privacygovernance

Voorstel tot verbetering

Door	mr. 5.1.2.e
Afdeling	Gegevensautoriteit
Versienummer	1.0
Datum	29 januari 2024
Kenmerk	2024-0006312
Status	Concept
Rubricering	Politie INTERN - Bedrijfsvoering

1 Inleiding

1.1 Aanleiding

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

De hier voorgestelde privacygovernance sluit aan bij de korpsgovernance, die volop in ontwikkeling is. In de voorgestelde privacygovernance blijft de verantwoordelijkheid bij de lijn belegd. Daarom speelt hierbij ook de (door)ontwikkeling van de korpsgovernance een rol. Met de start van de Strategische Boards en de herziening van de portefeuilles daaronder, zou sturing op naleving van de Wpg minder complex moeten worden. De I-Tafel gaat daar een belangrijke rol bij spelen. Met de voorgestelde verbetering van de privacygoverance krijgt ook de ondersteuning van de portefeuillehouders op het gebied van privacy meer continuiteit.

1.2 Geconstateerde knelpunten

Op basis van de hiervoor genoemde onderzoeken zijn de volgende knelpunten in de huidige privacygovernance vastgesteld.

a. Diffuse governancestructuur
- Er bestaat veel vrijheid in de eenheden waardoor er uiteenlopende opvattingen ontstaan.
- Onduidelijke belegging van verantwoordelijkheid waardoor ‘eigenaarschap’ voor verwerkingen niet wordt opgepakt en mitigerende maatregelen niet worden genomen.
- Er bestaat overlap van verantwoordelijkheden.

b. Three-lines-of defence (3LoD) model
- De tweede lijn is niet of slechts beperkt ingevuld.
- Daarnaast ontbreekt de verbindende laag tussen beleid en uitvoering.

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.

2 Verbeteringen

2.1 ‘De lijn’ en een vangnet

De verbeterde privacygovernance gaat uit van het 3LoD-model voor het managen van de privacyrisico’s. Hierbij kunnen de 2e en 3e lijn worden gezien als een ‘vangnet’ voor de eerste lijn.

1e lijn: Eigenaar van risico’s: identificeert en beoordeelt risico’s. De 1e lijn neemt mitigerende maatregelen of accepteert de risico’s en is daarop ook aanspreekbaar.

2e lijn: Stelt kaders en richtlijnen op, ondersteunt en adviseert de 1e lijn in het toepassen van de kaders. Bewaakt of de 1e 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 externe toezichthouders op de naleving van de privacy wet- en regelgeving toezien.

2.2 De eerste lijn

De korpschef is de verwerkingsverantwoordelijke en daarmee formeel eindverantwoordelijk voor het naleven van de privacy wet- en regelgeving bij de politie. Elke medewerker bij de politie moet zorgdragen voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens bij de uitvoering van zijn werkzaamheden, daarbij maakt hij waar mogelijk gebruik van specifiek beleid, procedures, uitvoeringskaders en werkinstructies.

De eerste lijn in deze privacygovernance wordt gevormd door de politiechefs, directeuren van een ondersteunende dienst en portefeuillehouders.

De **politiechefs** van de eenheden en de **directeuren van de ondersteunende diensten** (SKL, PDC ODPA en LMS) zijn als lijnverantwoordelijke ook verantwoordelijk voor het zorgdragen voor de naleving van de privacyregels binnen het eigen organisatieonderdeel. Zij nemen zo nodig mitigerende maatregelen en accepteren (zowel hoge als lage) risico’s. Zij zijn daarop ook aanspreekbaar.

Voorbeeld: *In een gemeente bestaat een lokaal initiatief waarbij de politie samenwerkt met een gemeente en enkele scholen om tot een betere aanpak van jeugdcriminaliteit te komen. Hierbij kan het nodig zijn bepaalde politiegegevens te verstrekken aan de deelnemende partijen. Er wordt in dit kader een lokaal samenwerkingsconvenant afgesloten.*

De verantwoordelijkheid om bij het sluiten van dit convenant en om bij het daadwerkelijk verstrekken van politiegegevens de privacyregels na te leven, ligt in dit geval bij de politiechef (1e lijn). Hij kan hierbij zo nodig ondersteund worden door een privacyadviseur van de eenheid (2e lijn) en gebruik maken van een modelconvenant dat is opgesteld door de PF-office (2e lijn).

De **portefeuillehouder** heeft deze zelfde verantwoordelijkheid (naleving, mitigatie, risicoacceptatie, aanspreekbaarheid) voor alle privacy aangelegenheden die het onderwerp van de portefeuille betreffen. Hierbij gaat het dus niet alleen om (nieuwe) ontwikkelingen maar ook om de bestaande situatie.

Voorbeeld: *Vanuit het oogpunt van verkeersveiligheid en het toezicht daarop ontwikkelt de politie een camera die kan detecteren of iemand achter het stuur zit te bellen.*

Dit project (Thema verkeer) valt onder de hoofdportefeuille GGP. De portefeuillehouder (1e lijn) is hierbij verantwoordelijk voor het (laten) uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB). Hij wordt hierbij ondersteund door een centraal bij de PF-office ondergebrachte privacyadviseur (2e lijn). Vanwege deze nieuwe technologische toepassing is een voorafgaande raadpleging wettelijk verplicht. Deze raadpleging bij de Autoriteit persoonsgegevens (AP) loopt via de CPO (2e lijn).
Na ingebruikname van de camera wordt de toepassing doorontwikkeld. De portefeuillehouder (1e lijn) is er verantwoordelijk voor dat bij aanpassingen van de technologie wordt beoordeeld of deze nieuwe risico's voor de rechten en vrijheden van personen met zich meebrengen. Zo ja, dan neemt hij mitigerende maatregelen. Hij wordt daarbij ondersteund door een centraal bij de PF-office ondergebrachte privacyadviseur (2e lijn).

Ten behoeve van het kunnen uitvoeren van de rechten van de betrokkene, beschikken eenheden en de ondersteunende diensten in de eerste lijn (al dan niet gecombineerd) over een **privacydesk.**

Momenteel zijn er binnen de eenheden zogenaamde portefeuilleondersteuners actief. Zij ondersteunen binnen de eenheid ten aanzien van de werkzaamheden die vanuit de (deel)portefeuille privacy komen. Deze medewerkers hebben een belangrijke procesmatige en beheersmatige rol en onderscheiden zich van privacyadviseurs in werkzaamheden, expertise en vaardigheden. Ze vormen onderdeel van de 1e lijn. Deze functie wordt in de verbeterde privacygovernance geborgd. Hoewel de deelportefeuille privacy met de verbeterde privacygovernance wordt opgeheven, blijven de werkzaamheden van deze ondersteuners bestaan. Daarom wordt deze functie in de privacygovernance geborgd maar verandert de aanduiding in **privacymanagement ondersteuners**.

Het is mogelijk dat binnen sommige onderdelen van de politie mensen worden aangenomen of ingehuurd, die zich met een specifiek aspect van privacy binnen dat onderdeel bezighouden. Deze vormen dan eveneens onderdeel van de 1e lijn en moeten worden onderscheiden van de privacyadviseurs in de tweede lijn. Een goed voorbeeld is het Expertisecentrum Privacy (ECP) dat onderdeel is van de Dienst IV van het PDC. De experts bij het ECP adviseren binnen de dienst over het op juiste wijze implementeren van privacy, security en duurzame toegankelijkheid by design (PSDbD) en voeren regie op het uitvoeren van GEB's op IV-systemen waarin persoonsgegevens worden verwerkt.

Voorbeeld*: De politie wil overgaan tot aanschaf van nieuwe kantoorautomatisering. Hierbij spelen veel privacyvraagstukken.*

De verantwoordelijkheid voor het naleven van de privacyregels ligt hier bij de directeur PDC (1e lijn). Het Expertisecentrum Privacy (ECP) van de dienst IV (1e lijn) adviseert vanuit zijn specialistische kennis binnen de Dienst IV op de privacyaspecten van deze kantoorautomatisering. Zo nodig ondersteunt de privacyadviseur van het PDC (2e lijn) hierbij. De keuze voor bepaalde kantoorautomatisering kan politiek-bestuurlijke gevolgen hebben, zoals de gang naar de *cloud*, waardoor er vanuit de rijksoverheid en externe toezichthouders extra aandacht voor is. In dat geval lopen de externe contacten op dit punt primair via de CPO (2e lijn).

2.3 De tweede lijn

De tweede lijn is op drie niveaus opgebouwd:
1. Privacyadviseurs ter advisering van de lijn en de portefeuilles.

2. Een centrale voorziening (PF-office) onder leiding van de Privacyfunctionaris ondergebracht bij het PDC. Deze is belast met het opstellen van uitvoeringsbeleid, werkinstructies, modellen en is verantwoordelijk voor het verwerkingenregister en het monitoren van de naleving.
3. Een CPO-office onder leiding van een Chief Privacy Officer (CPO), rechtstreeks rapporterend aan de CIO bij de Staf Korpsleiding. De CPO stelt kaders, adviseert en is primair verantwoordelijk voor de privacyvisie, privacystrategie, privacygovernance en het privacybeleid. De CPO onderhoudt tevens de (inter)departementale contacten op het gebied van privacy.

2.3.1 Privacyadviseurs

De huidige diffuse structuur met privacyfunctionarissen en privacyadviseurs wordt verlaten. De in de Wpg verplichte privacyfunctionaris bestaat alleen nog maar als hoofd van een centrale voorziening (zie onder 2.3.2). Ter vervanging van de bestaande functionarissen komt er één nieuwe functie: **privacyadviseur**. Deze adviseur, die zowel kan adviseren over Wpg als AVG, zal mede vanuit het oogpunt van kennisborging bestaan uit een junior, medior en senior variant (S10-S12). De privacyadviseur is niet (meer) belast met toezichtswerkzaamheden of het maken van een jaarverslag.

De privacyadviseur adviseert en ondersteunt de 1e lijn bij het uitvoeren van de verantwoordelijkheden op het privacygebied. Het fungeert als 'vangnet' voor de 1e lijn bij vraagstukken op het gebied van privacy waar deze zelf niet meer uitkomt. Hiertoe moet de 1e lijn zo nodig wel nog zorgdragen voor de inhoudelijke expertise om een privacyvraagstuk te kunnen aanpakken.

Binnen de twaalf eenheden en de ondersteunende diensten zullen - naar behoefte - meerdere privacyadviseurs werkzaam zijn ter ondersteuning van de reguliere taken van de betreffende eenheid of dienst.
Specifiek ter advisering van de portefeuilles of speciale onderwerpen zijn centraal ondergebrachte 'dedicated' privacyadviseurs aanwezig bij de PF-office. Hierbij moet opgemerkt worden dat de aard en omvang van de portefeuilles onderling nogal verschillen en momenteel op verschillende wijzen zijn ingevuld.

De PF heeft een functionele aansturingslijn naar alle privacyadviseurs. De privacyadviseurs in de eenheden blijven hiërarchisch onder de politiechef vallen.

***Voorbeeld**: in een eenheid moet ten aanzien van een regionale verwerking een GEB worden uitgevoerd.*

De politiechef (1e lijn) is daarvoor verantwoordelijk. Deze kan hierbij ondersteund worden door een privacyadviseur in zijn eenheid (2e lijn). De benodigde inhoudelijke inbreng over de concrete verwerking moet uit de 1e lijn komen. Bij het opstellen van een GEB wordt gebruik gemaakt van een door de PF (2e lijn) vastgesteld model. De functionele aansturing van de privacyadviseur in de eenheid door de PF borgt dat een model ook uniform binnen de politie wordt toegepast.

De privacyadviseurs overleggen periodiek in het **Landelijk overleg privacy adviseurs** (Lopa) onder voorzitterschap van de PF. Dit is géén besluitvormend overleg.

2.3.2 De Privacyfunctionaris en de PF-office

Voor een goede verbinding tussen het beleid en de uitvoering komt er bij het PDC één **Privacyfunctionaris** (PF) als hoofd van een centrale voorziening. De PF, die wettelijk verplicht is en zowel een adviserende als controlerende taak heeft, draagt zorg voor het vertalen en doorontwikkelen van het beleid naar uitvoeringsbeleid (zo nodig in overleg met de direct betrokkenen, bijv. de hoofden staf). De PF is verantwoordelijk voor het bijhouden van het verwerkingenregister en coördineert

centraal de afhandeling van datalekken. Hij is eveneens belast met het monitoren op de voortgang en de kwaliteit op gemaakte privacy (management) afspraken, de voortgang en kwaliteit op de uitvoering van landelijk privacybeleid, stelt daartoe KPI's op, richt zo nodig dashboards in en signaleert trends. Hij rapporteert hier periodiek over aan de CPO. De PF zit samen met de CPO en de FG in de **privacydriehoek**.

***Voorbeeld**: Art. 31d Wpg verplicht de politie om een verwerkingenregister bij te houden.*

De 1e lijn is verantwoordelijk om de verwerkingen die onder zijn verantwoordelijkheid vallen te doen opnemen in het verwerkingenregister. De PF (2e lijn) ondersteunt en faciliteert het opnemen in het register en is tevens verantwoordelijk voor het beheer ervan.

De centrale voorziening, de **PF-office**, ondersteunt de PF in zijn taken en omvat tevens de privacyadviseurs ten behoeve van het ondersteunen van de portefeuilles. Ook kunnen met deze centrale *pool* van privacyadviseurs mogelijke piekbelastingen of 'gaten' in de eenheden of bij de ondersteunende diensten tijdelijk worden opgevangen. Ter ondersteuning van de taken van de PF zijn er naast privacyadviseurs ook privacymanagement officers bij de PF-office werkzaam. Deze laatste categorie medewerkers focust zich op de procesmatige en rapportagekant van de privacycompliance.

De PF zit het landelijk overleg van privacyadviseurs voor. De secretariële en organisatorische ondersteuning van het Lopa is bij de PF-office ondergebracht.

2.3.3 Chief Privacy Officer (CPO) en het CPO-office

In navolging van het I-stelsel Rijk en in aanvulling op de reeds bij de politie bestaande rollen van CIO, CDO en CISO wordt bij de GA van de directie Informatievoorziening (IV) een **Chief Privacy Officer** ingesteld. De CPO heeft een kaderstellende en adviserende rol. De CPO is primair verantwoordelijk voor de privacyvisie, -strategie, - governance en het privacybeleid van de politie. Daarnaast adviseert de CPO over, bewaakt en zorgt voor optimaal gebruik van kennis en middelen op het gebied van privacy. Ook onderhoudt de CPO de (inter)departementale contacten op het gebied van privacy en contacten met de Autoriteit Persoonsgegevens. De CPO heeft een doorslaggevende stem ten aanzien van privacyadvies binnen de politie. De CPO heeft een rechtstreekse verantwoordingslijn aan de CIO. Binnen de **privacydriehoek** (CPO-PF-FG) vormt de CPO ook op strategisch niveau de *linking pin* met de IV-organisatie.

***Voorbeeld:** De bewaartermijnen van de Wpg zijn in sommige gevallen te kort voor de operationele wensen ten aanzien van o.a. cold cases. Er is behoefte aan een aanpassing van de wet op dit punt.*

De CPO-office (2e lijn) onderhoudt in dit kader de directe contacten met de relevante opsporingspartners en het departement om tot een wetsvoorstel te komen om de bewaartermijnen aan te passen.

De CPO onderhoudt ook de primaire contacten met de Politieacademie en HR om in samenspraak te komen tot een betere borging, beheer en onderhoud van privacy-kennis bij de politie.

Het cluster privacy binnen de GA wordt omgevormd tot de **CPO-office** en ondersteunt de CPO in zijn taken.

2.4 De derde lijn

De **Functionaris voor Gegevensbescherming** (FG) is belast met het houden van onafhankelijk toezicht op de naleving van de Wpg en de AVG. Hij is daarmee het belangrijkste toezichtsorgaan binnen de politie. Daarnaast vormt de FG het primaire contactpunt bij de politie voor de Autoriteit Persoonsgegevens.
Nu met de verbetering van de privacygovernance de rol van de privacyfunctionarissen in feite is komen te vervallen en daarmee ook de - in de praktijk nooit adequaat uitgevoerde toezichtstaak van de PF, is een goede uitvoering van de toezichtstaak door de FG onontbeerlijk. Hiertoe zullen 2 FG's worden ondersteund door een compacte **FG-office**.

De FG heeft periodiek een gezamenlijk overleg met de CPO en de PF in de **privacydriehoek.**

Voorbeeld: *De FG heeft op basis van verschillende signalen de behoefte om een bepaald privacyonderwerp binnen de politie te adresseren.*

De FG (3e lijn) brengt dit ter sprake in de privacydriehoek waar afhankelijk van het onderwerp de PF (2e lijn) of CPO (2e lijn) dit vraagstuk op kan pakken.

Concernaudit vormt de andere van de twee interne onafhankelijke controlemechanismen. Op grond van de Wpg (art. 33) moeten periodiek controles op de naleving van deze wet worden uitgevoerd. Dit geschiedt eveneens voor de AVG.

3 Randvoorwaarden

3.1 De (deel)portefeuille privacy

Met het inrichten van een CPO in navolging van het I-stelsel Rijk leidt het handhaven van de (deel)portefeuille privacy alleen nog maar tot een diffuse verdeling van verantwoordelijkheden. Privacy is in alle werkprocessen van de politie aanwezig en in het licht van het 3LoD-model primair een aangelegenheid van de lijn, die met de verbeterde privacygovernance daarin goed wordt ondersteund. Een (deel)portefeuille privacy past niet goed in deze structuur. Deze kan daarom op termijn komen te vervallen. Echter, in de periode tot aan de volledige implementatie en operationalisering van de verbeterde privacygovernance is het wel van belang dat de portefeuille gehandhaafd blijft, mede als aanspreekpunt binnen het KMTO. De (deel)portefeuille privacy is ondergebracht bij de hoofdportefeuille Ethiek & Privacy. Deze portefeuille is ondergebracht bij de board Digitale Transformatie. De beleidsdirecteur van deze board ondersteunt en voert regie op de door de board vastgestelde prioriteiten. De IV-regisseur zorgt voor realisatie in de eigen IV-waardeketen en monitort dit.

3.2 Kennisborging, beheer en onderhoud

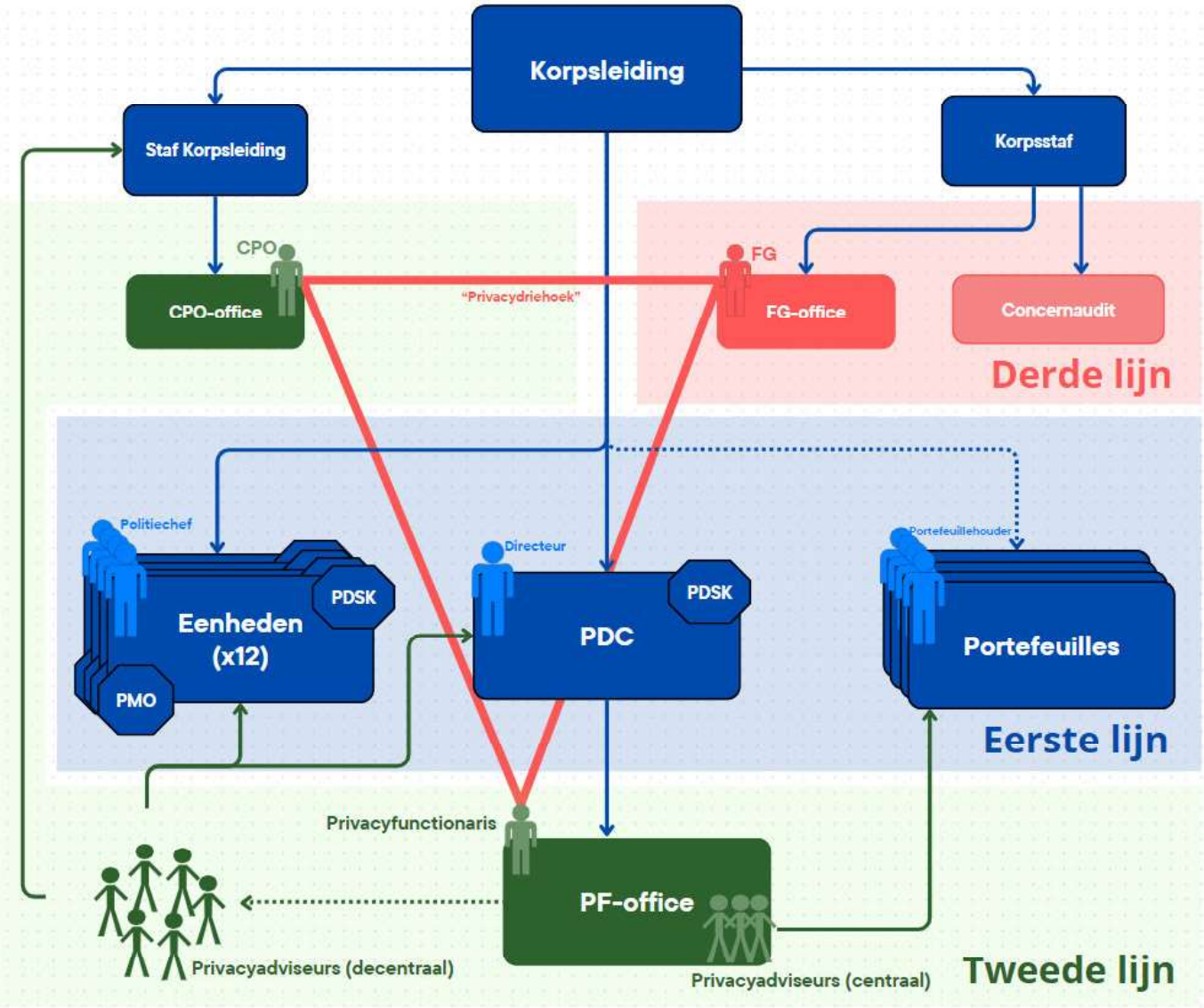
Er is in de gehele politieorganisatie behoefte aan meer en betere kennis en bewustzijn op het gebied van privacy. Hierbij zal de Politieacademie een grote(re) rol moeten spelen. Dit betekent eveneens de betrokkenheid van HR. De CPO zal hierover in overleg treden met zowel de PA als HR. Vanuit de PF-office zal ook aan awareness en voorlichting worden gewerkt. De CPO zal de kwaliteit van training en voorlichting toetsen.

Het formaliseren en actualiseren van documenten van beleid is aan de CPO en van uitvoeringsbeleid aan de PF. Vanuit de PF-office wordt de beschikbaarheid en vindbaarheid van alle beleidsdocumenten, modelformulieren, handreikingen en werkbeschrijvingen verzorgd.

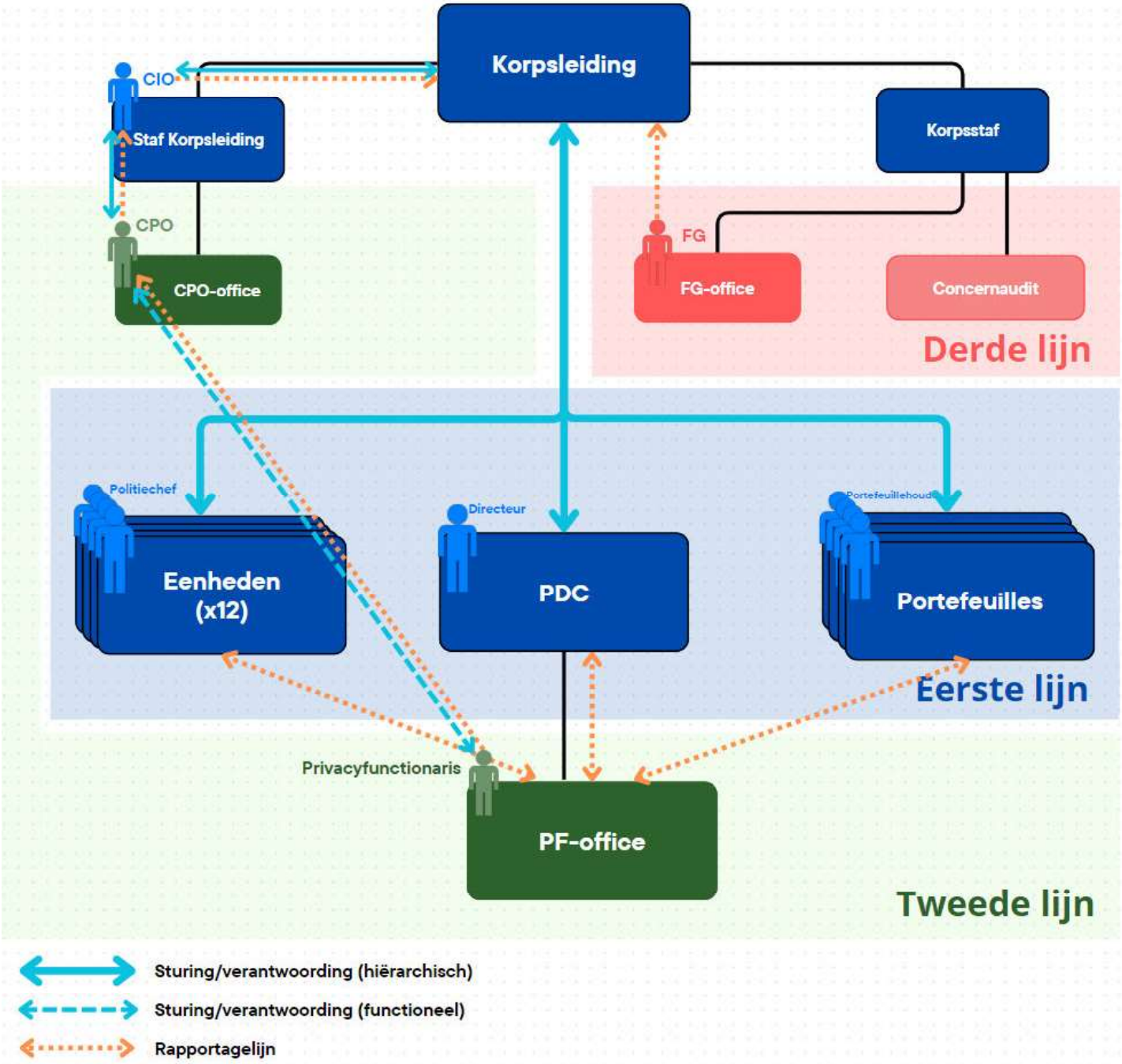
3.3 Overgangssituatie

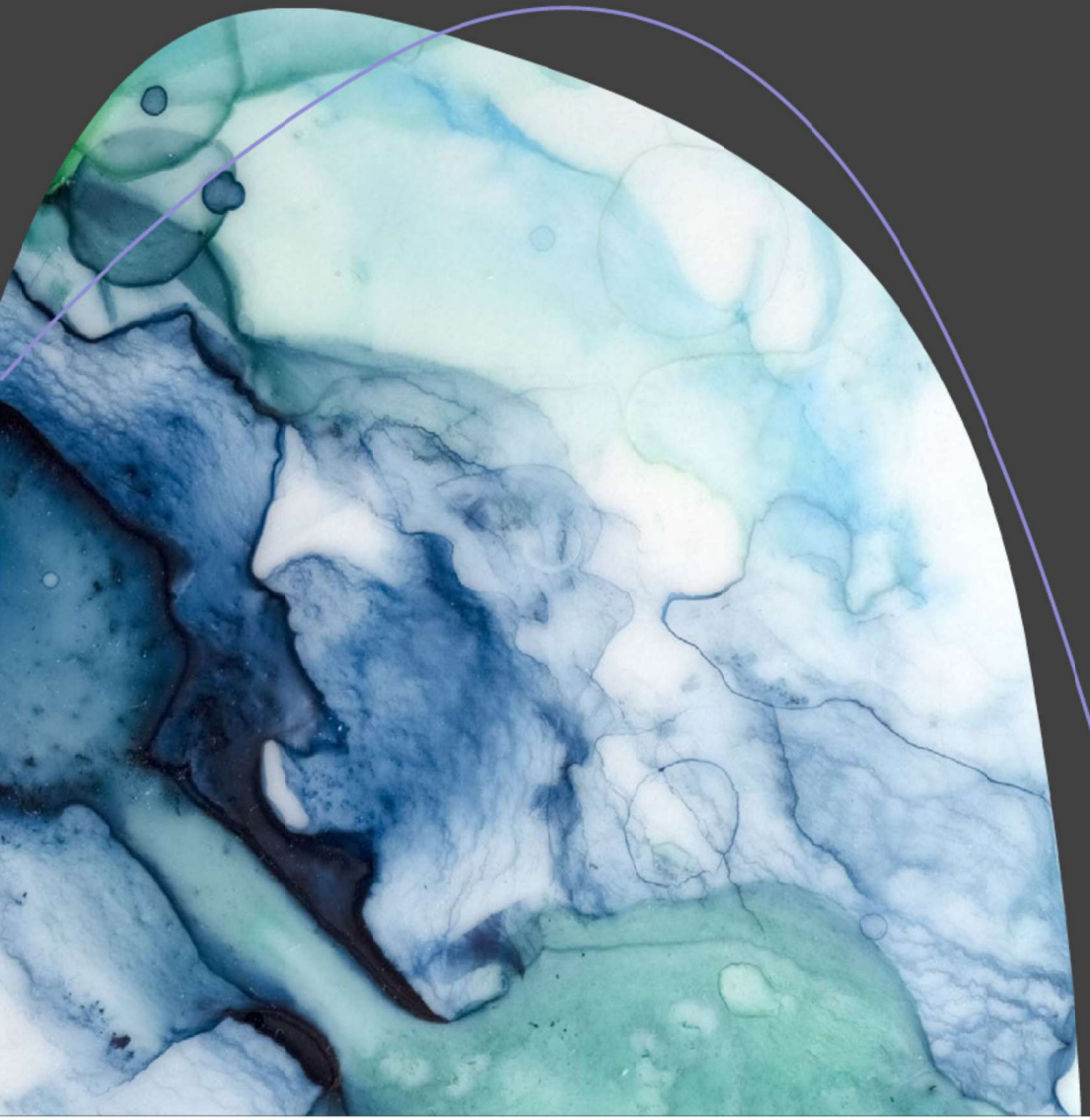
Met de omschakeling van de huidige naar de verbeterde privacygovernance gaat enige tijd gemoeid. Hiervoor zal ook een realisatiemanager moeten worden aangesteld. Tot die tijd is een portefeuillehouder en op sommige punten een hulpstructuur nog nodig. Wanneer de verbeterde privacygovernance is uitgerold en structureel geborgd, kunnen alle bestaande hulpstructuren en tijdelijke privacyfuncties definitief worden opgeheven.

Bijlage 1: Schematische weergave privacygovernance



Bijlage 2: Sturing/verantwoording en rapportages



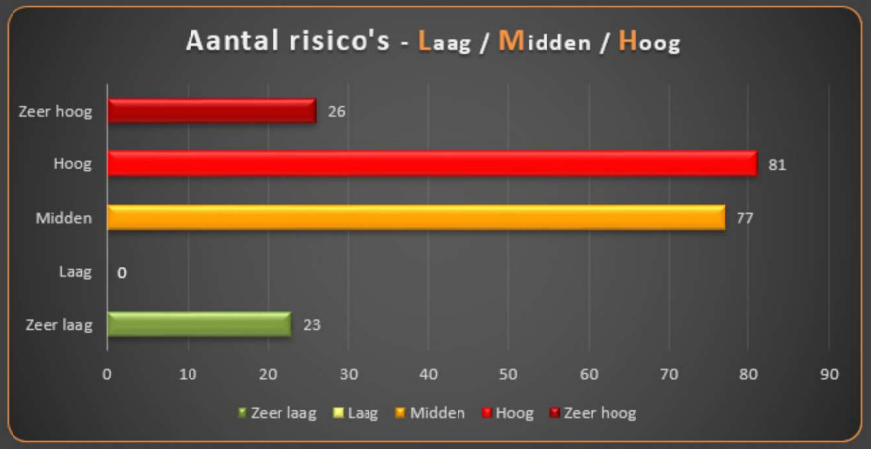


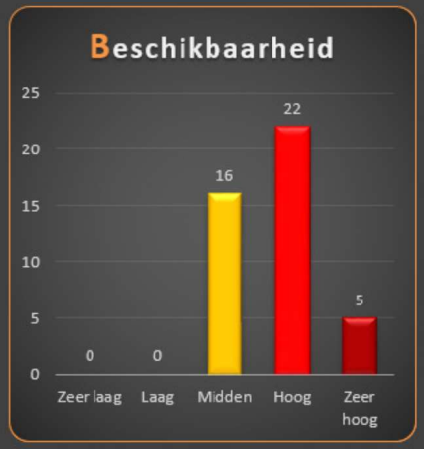
VIK

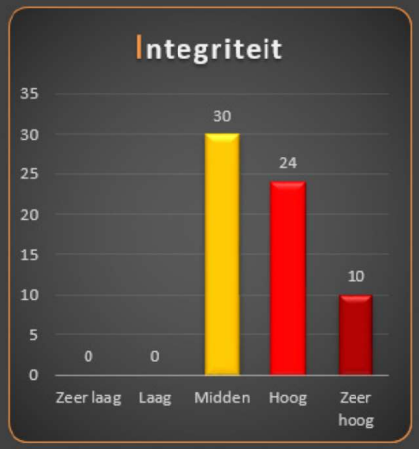
Risico overzicht per portefeuille

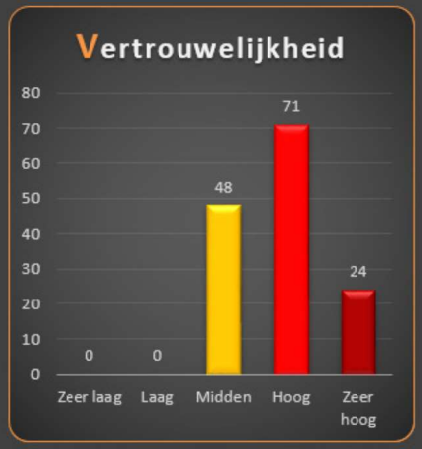
Periode: Q1-2024

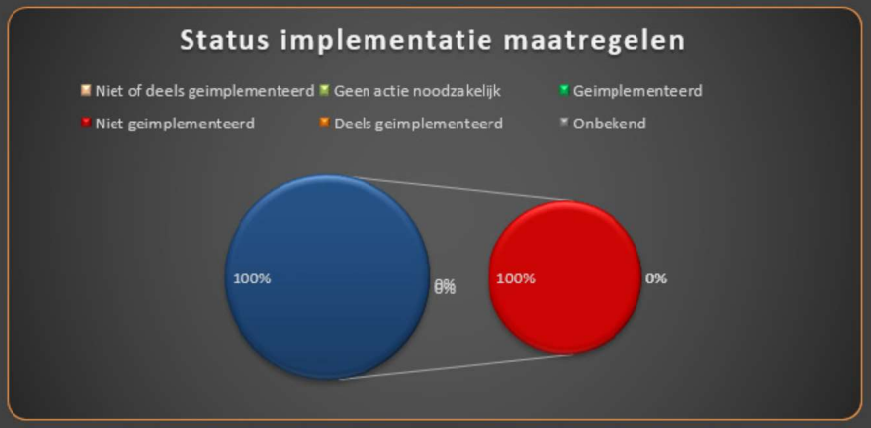
Risico classificering











Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	101	106	0	207	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

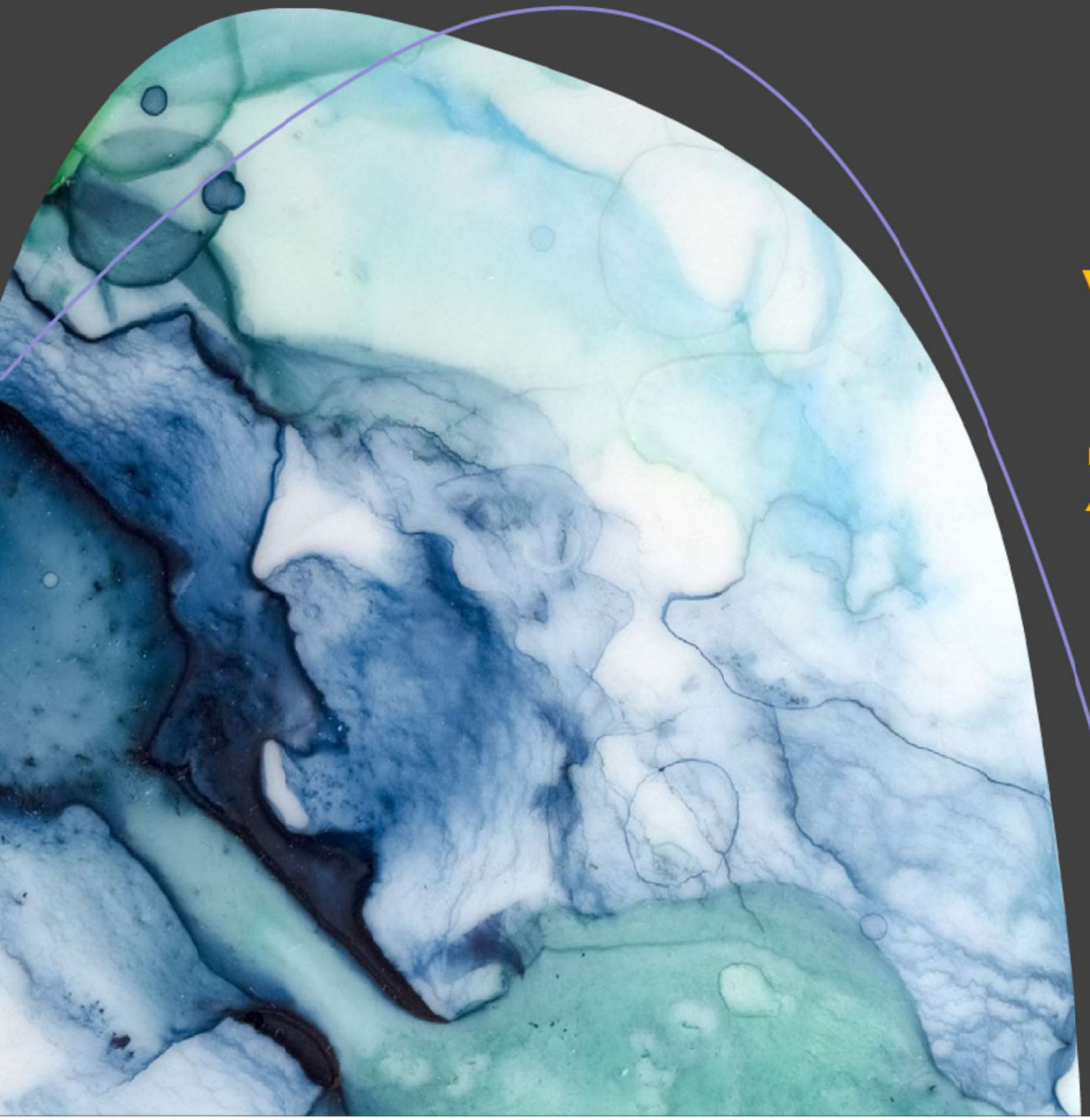
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

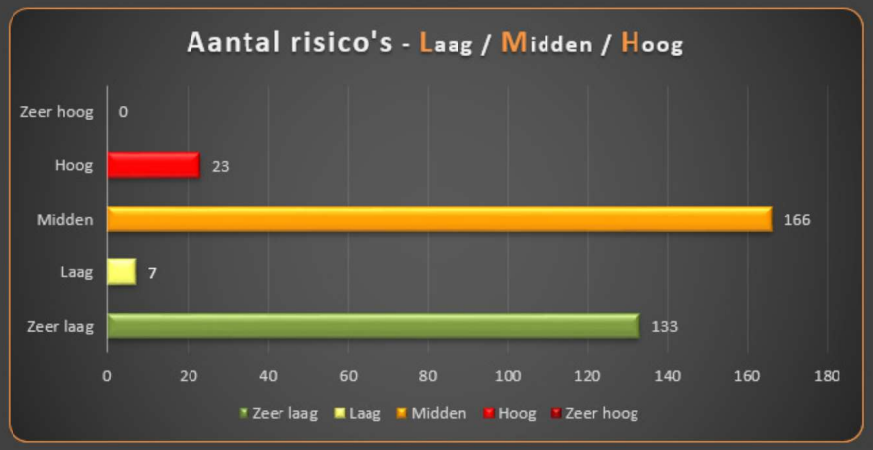


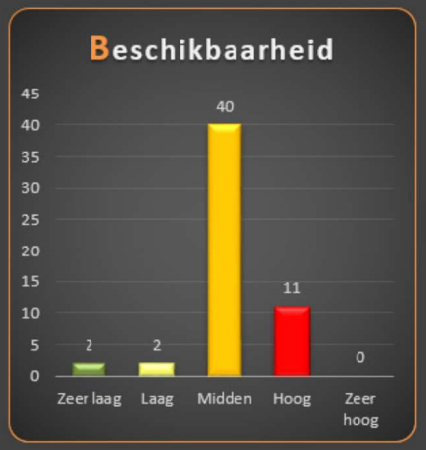
Vreemdelingen-zaken

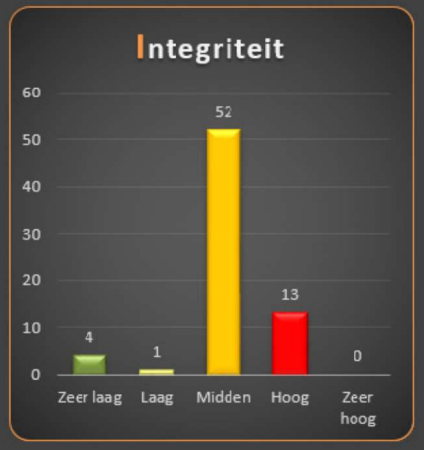
Risico overzicht per portefeuille

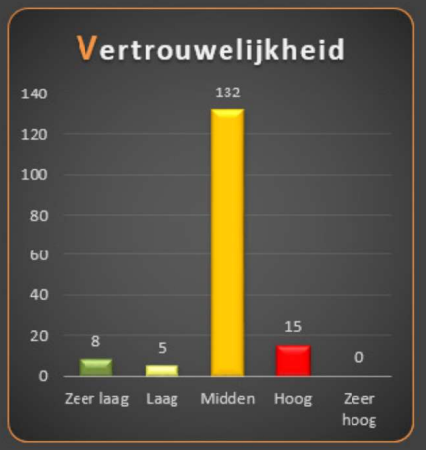
Periode: Q1-2024

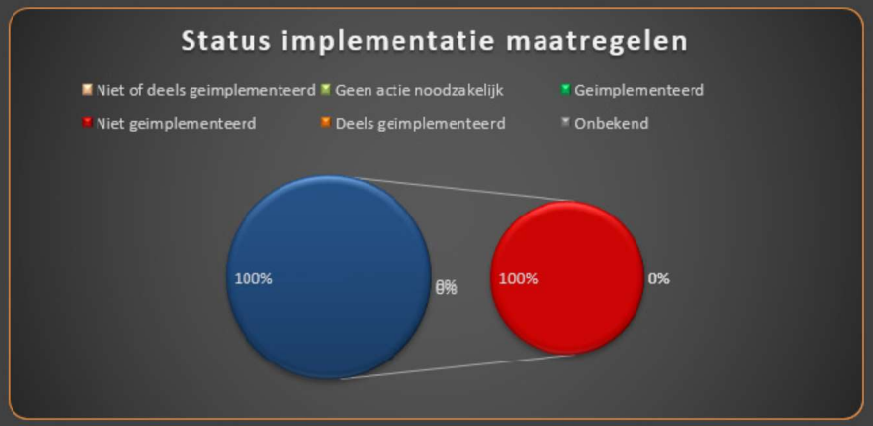
Risico classificering











Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	0	329	0	329	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

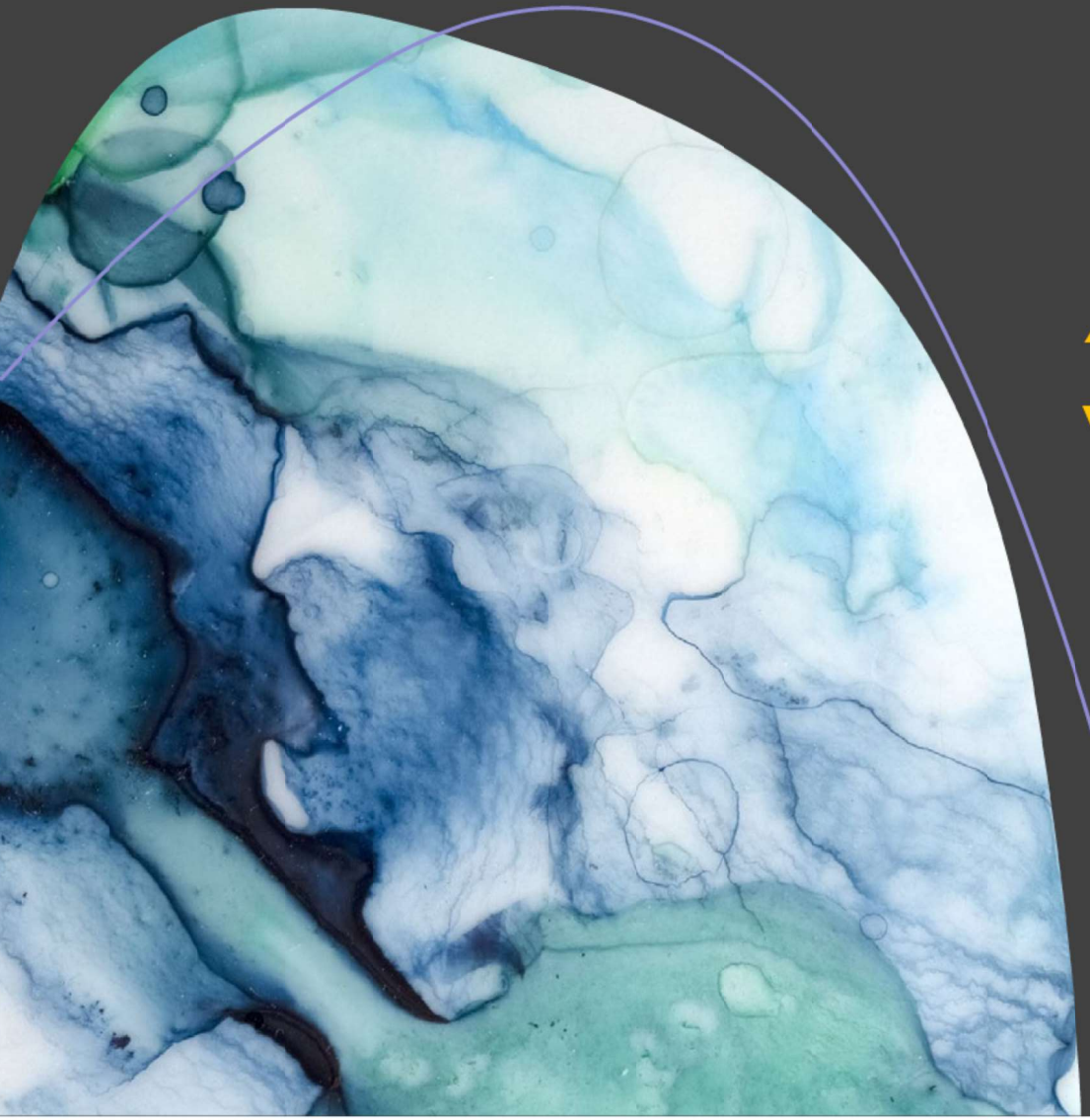
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

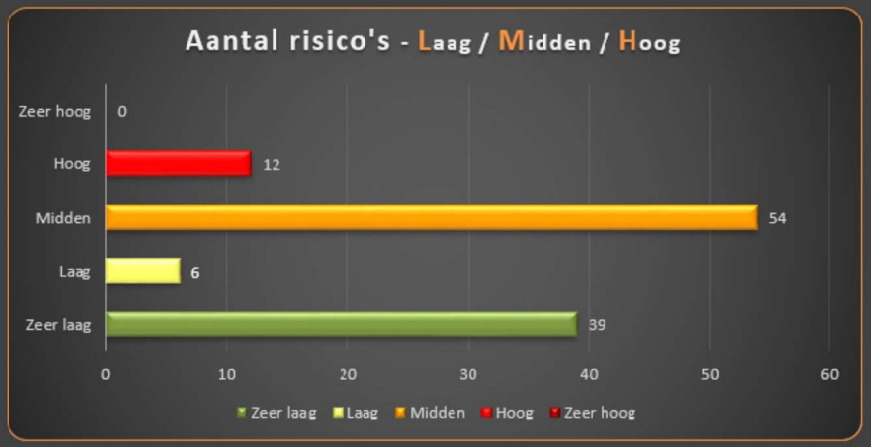


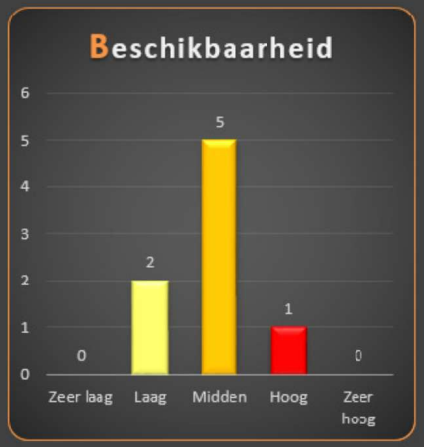
Zorg & Veiligheid

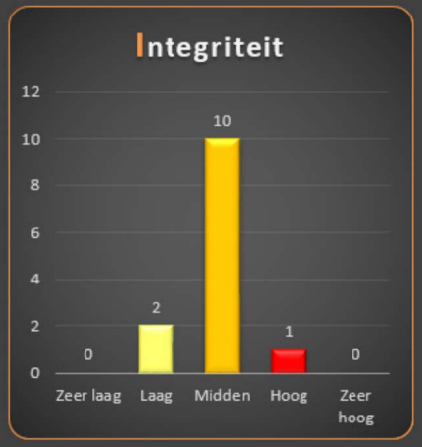
Risico overzicht per portefeuille

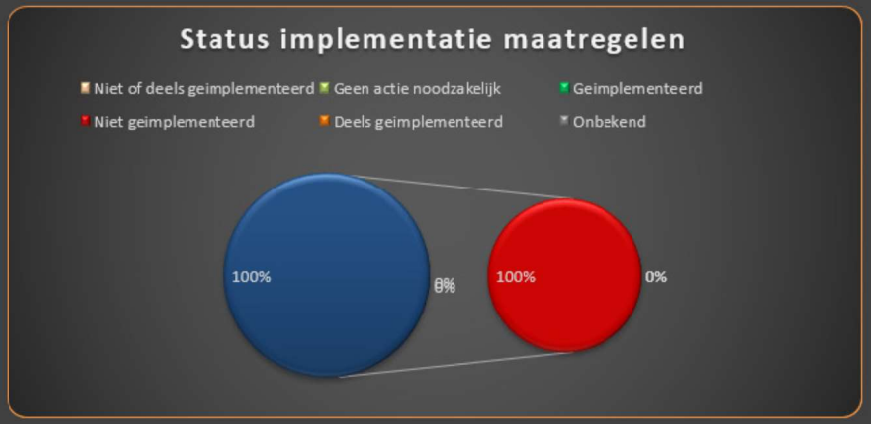
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	11	100	0	111	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

Oplegnota KLO / KMTO / BBVO / BOO

Ingebracht door / Akkoord van:
Henk Geveke

Onderwerp
Verbetering privacygovernance

Let op: de inbrenger moet alle stukken geaccordeerd hebben

Rubricering
Politie INTERN - Bedrijfsvoering

Datum overleg In te vullen door secretaris

Agendapunt In te vullen door secretaris

Behandeld door 5.1.2.e
(Staf KL/Dir IV/Gegevensautoriteit)
5.1.2.e @politie.nl
06-5.1.2.e

Bijlage(n) 1

Doel ter besluitvorming

Het KMTO wordt gevraagd

1. In te stemmen om de hier voorgestelde richting van de privacygovernance vorm te geven.
2. De directeur Staf KL de opdracht te geven deze privacygovernance nader uit te werken en een realisatieplan op te stellen waarbij rekening wordt gehouden met de (andere) governanceontwikkelingen binnen de politie.
3. De directeur Staf KL de opdracht te geven een realisatiemanager aan te stellen om de verbeterde privacygovernance te operationaliseren

** Bij een voorgenomen besluit moet het advies- of instemmingsverzoek bij de stukken worden gevoegd.*

Samenvatting
Deze notitie bevat een voorstel op hoofdlijnen om de privacygovernance bij de politie te verbeteren. Een gedetailleerde beschrijving van functieprofielen en de specifieke processen die hieruit voortvloeien, worden na instemming nader uitgewerkt. De voorgestelde governance gaat uit van een three-lines-of-defence (3LoD) benadering, waarbij de verantwoordelijkheid is belegd in de eerste lijn met een gedifferentieerde tweede lijn die hierbij ondersteunt en als 'vangnet' dient. Met dit voorstel worden de rollen en verantwoordelijkheden duidelijk belegd. De hier voorgestelde privacygovernance sluit aan bij de nieuwe korpsgovernance.

Aanleiding voor bespreking
De politie scoort al jaren slecht op het naleven van de privacyregels. Naar aanleiding van een onderzoek van Capgemini in 2022 en de uitkomsten van de recent opgeleverde externe en interne Wpg-audits is besloten te komen tot een verbetering van de privacygovernance.

Voortraject
Afstemming op individueel niveau met relevante stakeholders.

-

Typ Adres
-

Toelichting

Naar aanleiding van het onderzoek van Capgemini in 2022 naar de privacygovernance bij de politie en gezien de uitkomsten van de recent opgeleverde externe (KPMG) en interne (concernaudit) Wpg-audits is besloten te komen tot een verbetering van de privacygovernance. Deze notitie bevat dit voorstel op hoofdlijnen. Een gedetailleerde beschrijving van functieprofielen en de specifieke processen die hieruit voortvloeien (GEB, verwerkingenregister, etc.) zullen, als ingestemd wordt met deze verbeterde governance, nader worden uitgewerkt.
De voorgestelde verbeterde privacygovernance gaat uit van een three-lines-of-defence (3LoD) model.

Eerste lijn

De verantwoordelijkheid voor de naleving, mitigatie, risicoacceptatie en aanspreekbaarheid ten aanzien van de naleving van de privacyregels ligt bij de eerste lijn. Deze wordt gevormd door de politiechefs/directeuren ondersteunende diensten voor privacyvraagstukken binnen de eigen organisatie-eenheid. De portefeuillehouders hebben deze verantwoordelijkheid ten aanzien van onderwerpen die onder de portefeuille vallen (dus niet alleen ontwikkelingen maar ook reguliere situatie). In de nieuwe korpsgovernance komen deze twee aspecten ook samen in de Strategische Boards.
De eerste lijn beschikt over privacydesks en privacymanagement ondersteuners. In sommige gevallen heeft de eerste lijn nog extra privacycapaciteit georganiseerd.

Tweede lijn

De tweede lijn ondersteunt de eerste lijn hierbij en dient als een ‘vangnet’. Hiertoe is de tweede lijn op drie niveau’s ingericht.

Eerste niveau

Allereerst zijn er privacyadviseurs die de eerste lijn adviseren. Voor de lijnverantwoordelijkheid zijn deze adviseurs in de eenheden/diensten ondergebracht. Voor de portefeuilles zijn deze adviseurs centraal ondergebracht bij het PDC.

Tweede niveau

Daarnaast komt er een Privacy Functionaris (PF) aan het hoofd van een centrale PF-office. Deze PF-office wordt ondergebracht bij het PDC. De adviseurs van de portefeuilles zijn ook ondergebracht in deze PF-office. De PF is belast met het opstellen van uitvoeringsbeleid, werkinstructies en modellen. Daarnaast is de PF verantwoordelijk voor het bijhouden van het verwerkingenregister en het monitoren van de naleving doormiddel van rapportages en dashboards. De PF rapporteert hierover periodiek aan de CPO. De PF stuurt de decentraal geplaatste privacyadviseurs functioneel (maar niet hiërarchisch) aan.

Derde niveau

Bij de Staf KL komt een Chief Privacy Officer (CPO) aan het hoofd van een CPO-office. De CPO heeft een kaderstellende en adviserende rol en is verantwoordelijk voor de privacyvisie, privacystrategie, privacygovernance en het privacybeleid. De CPO adviseert en waakt over het zo optimaal gebruik van kennis en middelen op het gebied van privacy. Hij houdt hierover dan ook primair de contacten met de Politieacademie en HR. Tevens onderhoudt de CPO de (inter)departementale contacten en de contacten met de Autoriteit Persoonsgegevens. Ten aanzien van privacyadvies binnen de politie heeft de CPO een doorslaggevende stem. De CPO heeft een rechtstreekse verantwoordingslijn naar de CIO bij de Staf KL.

Derde lijn

De derde lijn wordt gevormd door onafhankelijk intern toezicht bestaande uit twee Functionarissen Gegevensbescherming (FG) ondersteund door een FG-office en concernaudit.

‘Privacydriehoek’

De CPO, FG en PF overleggen periodiek over privacyaangelegenheden binnen de politie. De CPO vormt binnen deze driehoek de *linking pin* met de IV-organisatie.

Ontwikkeling korpsgovernance en privacygovernance
De hier voorgestelde privacygovernance past binnen de (door)ontwikkeling van de korpsgovernance. Met de start van de Strategische Boards en de herziening van de portefeuilles daaronder, zou sturing op naleving van de Wpg minder complex moeten worden. De I-Tafel gaat daar een belangrijke rol bij spelen. Met deze verbetering van de privacygoverance krijgt ook de ondersteuning van de portefeuillehouders op het gebied van privacy meer continuiteit.

Realisatie / consequenties

Het voorstel moet voorafgaand aan behandeling zijn afgestemd zijn met de relevante directeuren (integrale afstemming). Geef hieronder aan wat de consequenties zijn van de realisatie van dit voorstel en wat daarover besproken is.

Consequenties	Toelichting (sta o.a. stil bij de volgende punten, indien relevant)	Akkoord van directeur:
☑ Personeel/ HRM:	Zijn er consequenties t.a.v. rechtspositie medewerkers, personeelscapaciteit van het korps, raakt het voorstel het huidige HRM-beleid of is er bijv. werving nodig? Na nadere uitwerking van de governance, zal vermoedelijk extra geworven worden. Dit zal conform regulier beleid plaatsvinden.	n.v.t.
☑ Financieel:	Hoe wordt het voorstel financieel gedekt en zijn er evt. fiscale consequenties? Afstemming heeft plaatsgevonden met Directeur F&C. Er zal structureel meer geld nodig zijn om de ophoging van de NOS capaciteit te verhogen. Op dit moment zijn de exacte kosten nog niet bekend. Daarnaast zijn er (nog) geen structurele financiële middelen beschikbaar voor de uitbreiding van capaciteit. In de begrotingsbrief 2024 is een haakje gecreëerd voor een toekomstige financiële claim richting J&V. Dit biedt echter geen garantie op structureel extra financiering. Pas na de nadere uitwerking van het plan kan besluitvorming plaatsvinden over de structurele uitbreiding van capaciteit en de bijbehorende financiering.	Akkoord op het nader uitwerken van het plan incl. financiële paragraaf
☐ Informatievoorziening:	Vraagt het voorstel om wijzigingen op IV-gebied en hoe past het voorstel dan in het portfolio IV?	nee
☐ Facility Management:	Zijn er consequenties t.a.v. huisvesting, uniformen of uitrusting?	n.v.t.
☑ Communicatie:	Vraagt het voorstel om in- of externe communicatie? Wordt opgepakt in overleg met de portefeuille privacy	nee
☐ Juridisch:	Wat zijn de uitkomsten van de juridische toets van het voorstel? (denk bijvoorbeeld aan gegevensbescherming of geweldstoepassing)	n.v.t.
☐ Politiek-bestuurlijk:	Wat is de uitstraling van het voorstel op politiek en bestuur (Tweede Kamer, burgemeesters, etc)?	nee
☐ Operatie:	Wat is de impact van het voorstel op de taakuitvoering van de politie?	n.v.t.
☑ PDC:	Is het voorstel uitvoerbaar (uitvoeringstoets)? Er is geen concrete uitvoeringstoets gedaan. De voorgestelde maatregelen zijn wel afgestemd met relevante stakeholders binnen het PDC.	nee
☐ Anders …..		

Risico's en maatregelen
De daadwerkelijke realisatie van deze privacygovernance vereist een aantal medewerkers met de juiste vaardigheden en expertise. Deze zijn zowel binnen als buiten de politieorganisatie schaars. Het binnenhalen en -houden van deze medewerkers moet vanaf het begin van de realisatie van de verbeteringen van de governance worden opgepakt.

Om te voorkomen dat met het dechargeren van het Intensiveringsprogramma privacy eind 2023 en de volledige implementatie van de voorgestelde privacygovernance (niet voor 2025) een 'gat' in de uitvoering en naleving van de privacyregels ontstaat, blijft de deelportefeuille privacy gehandhaafd en wordt vanuit die portefeuille in tijdelijke ondersteuning voor de eerste lijn voorzien.

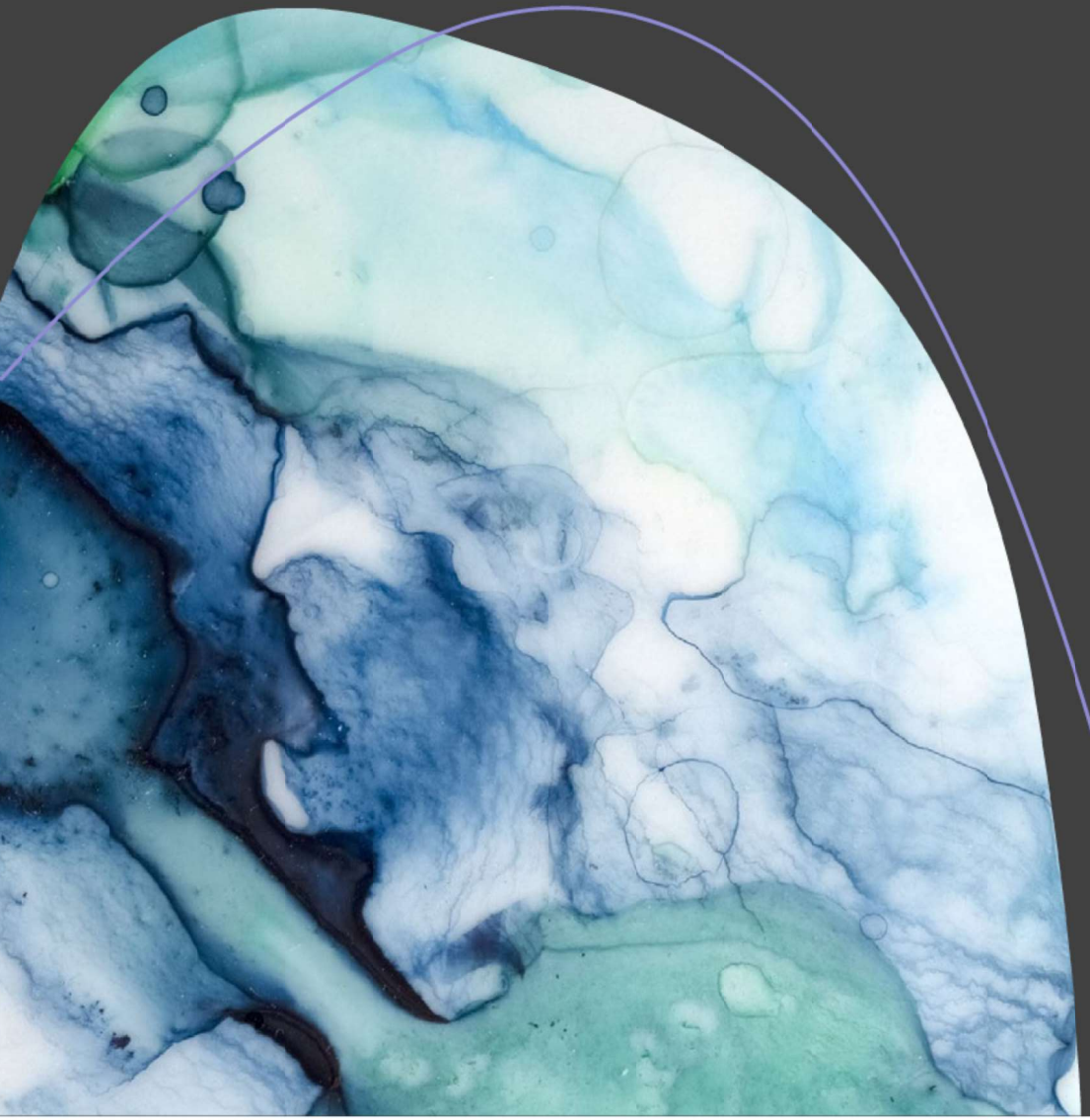
Implementatie en monitoring
Als het KMTO ermee instemt wordt de opdracht tot het nader uitwerken van deze verbeterde privacygovernance aan de directeur Staf KL gegeven. Deze zal ook zorgdragen voor het aanstellen van een realisatiemanager om de uitvoering ervan te borgen. Tot die tijd blijf de deelportefeuille privacy bestaan en zal de portefeuillehouder samen de korpsleiding de implementatie ervan monitoren.

Bijlagen
1. Voorstel verbetering privacygovernance politie

Vervolgtraject
Aankruisen wat van toepassing is.

☐ KMTO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming	☐ KLO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming
☐ BBVO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming	☐ BOO	☐ ter informatie ☐ ter opinievorming ☐ ter advisering ☐ ter besluitvorming
☐ COR (WOR)	☐ ter informatie ☐ voor instemming ☐ voor advies	☐ Vakbonden	☐ formeel, via CGOP ☐ informeel via overleg KL-vakbonden
☐ Combi MT	☐ ter besluitvorming ☐ ter bespreking/opinievorming ☐ ter kennisgeving	☐ LOVP	☐ ter informatie ☐ ter opinievorming ☐ ter besluitvorming

Archivering
DIV Staf KL

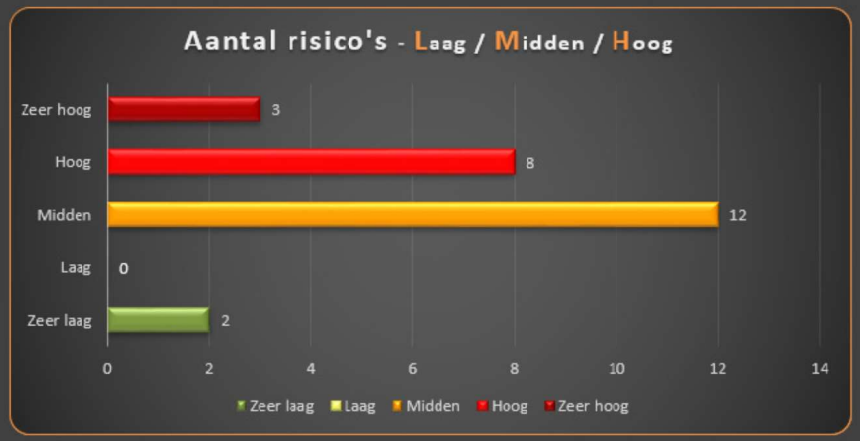


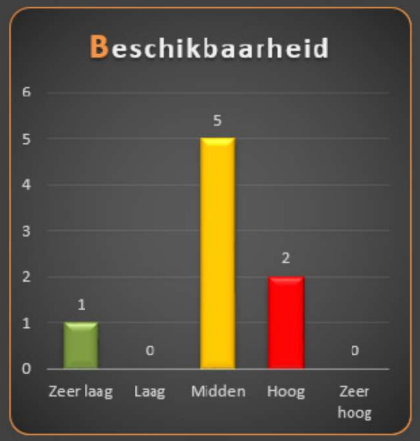
Arrestanten-taken

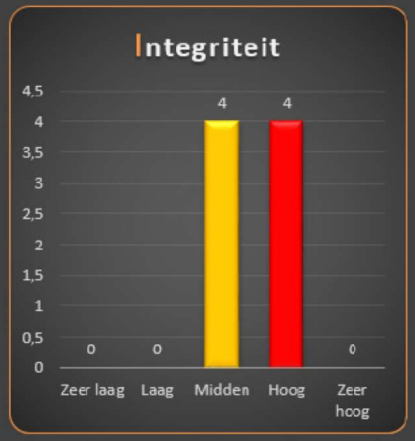
Risico overzicht per portefeuille

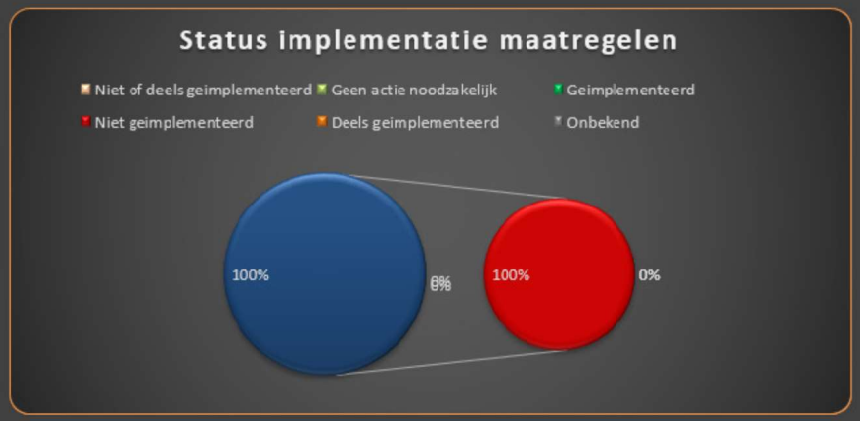
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	11	14	0	25	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

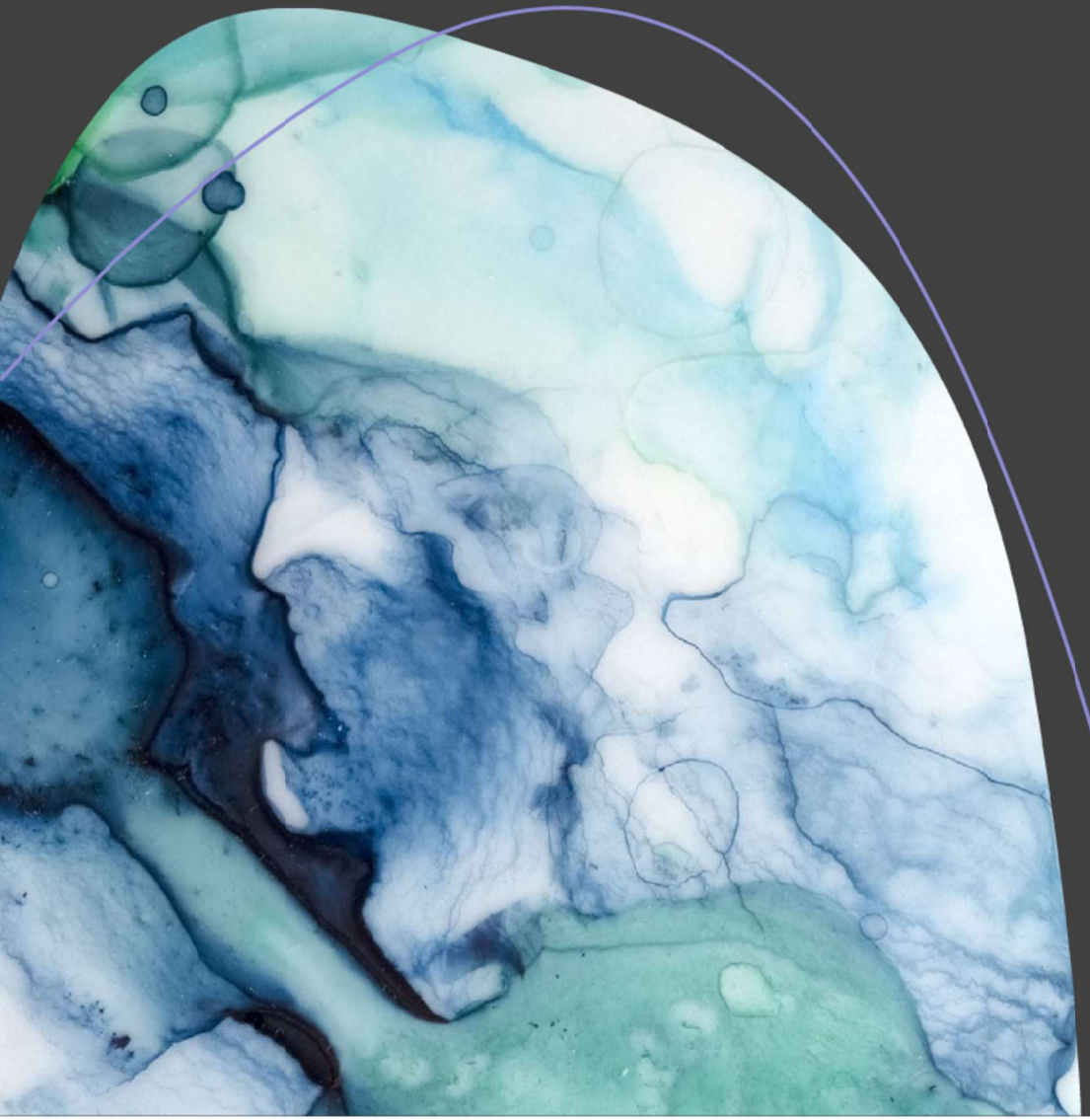
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

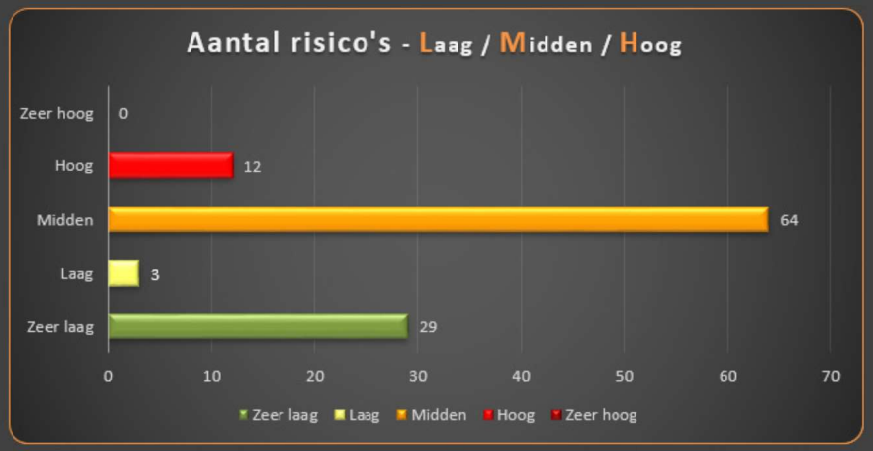


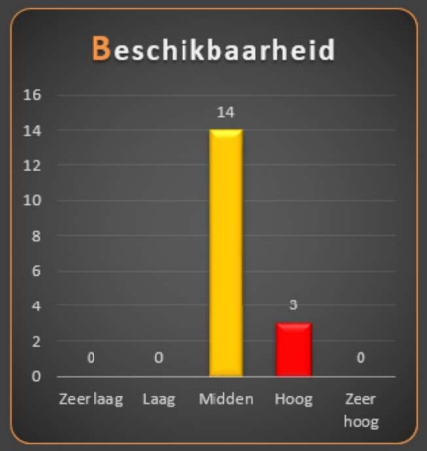
Crisis-beheersing

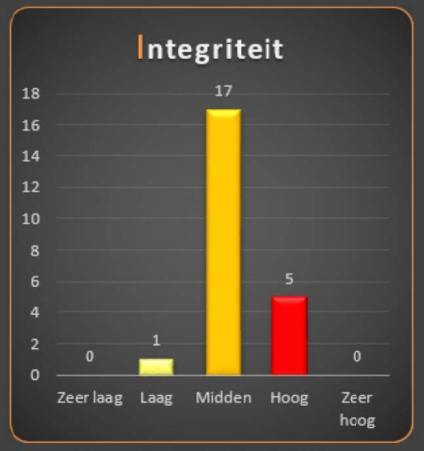
Risico overzicht per portefeuille

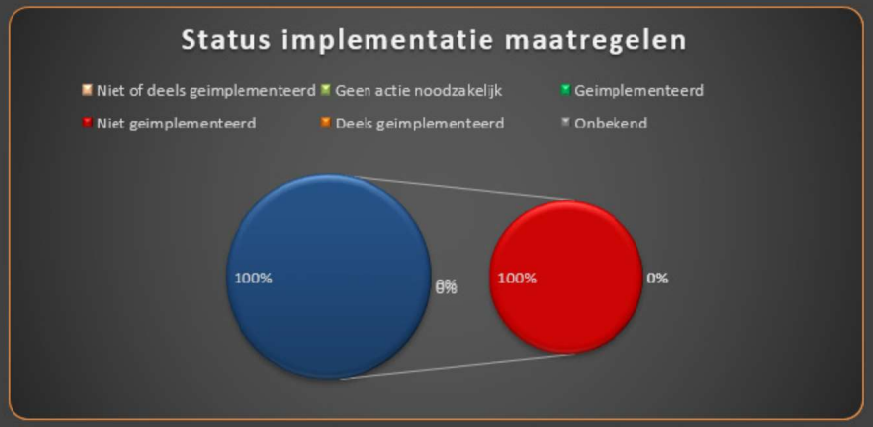
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	0	108	0	108	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

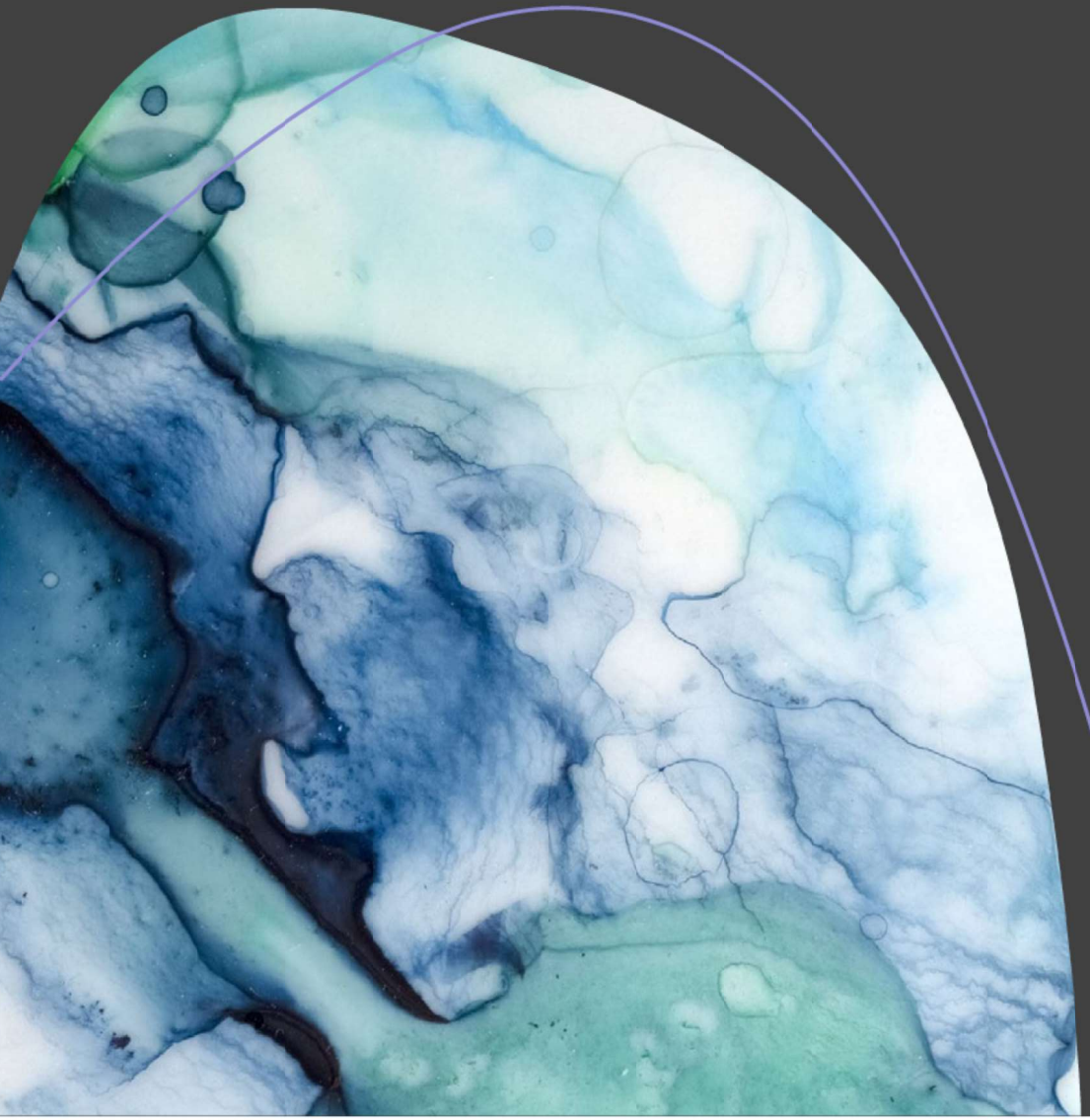
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

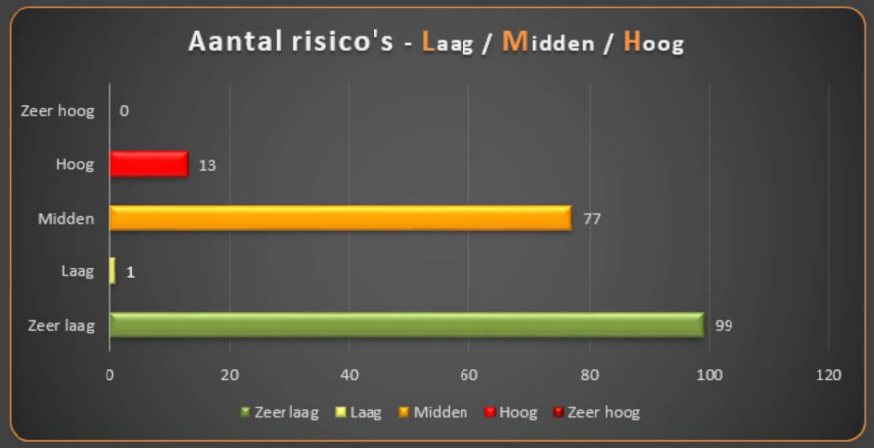


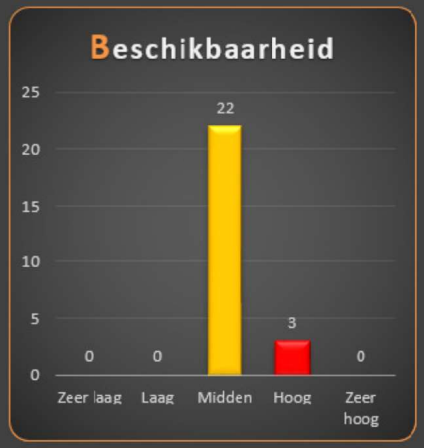
Dienst-verlening

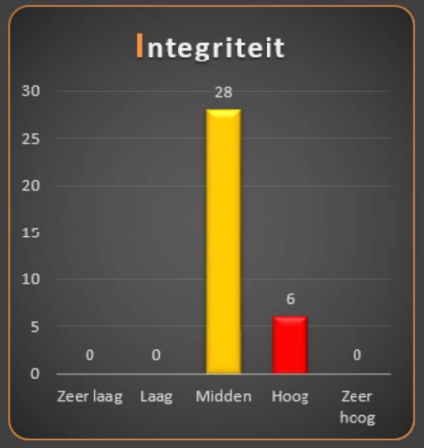
Risico overzicht per portefeuille

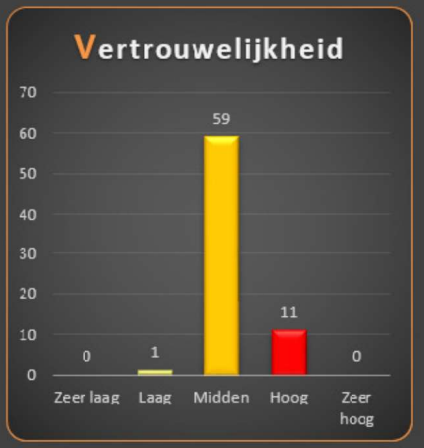
Periode: Q1-2024

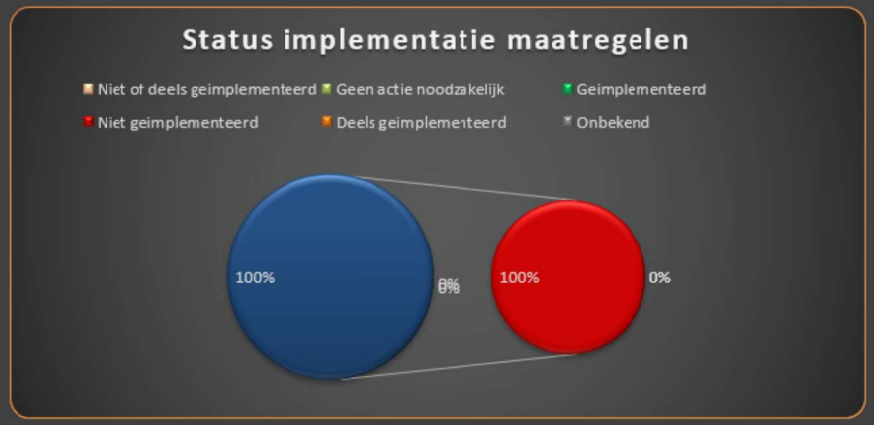
Risico classificering











Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	9	181	0	190	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

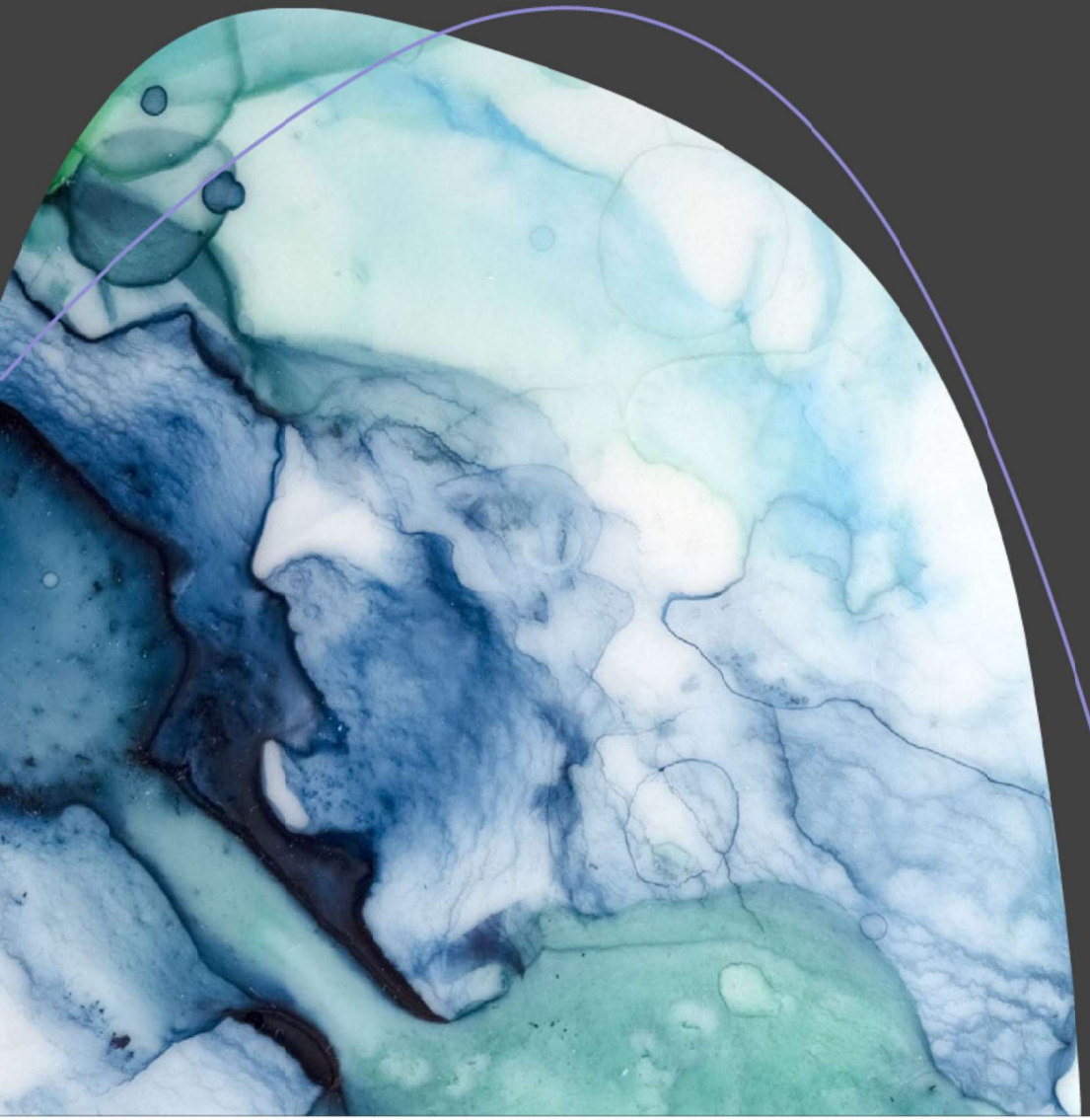
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

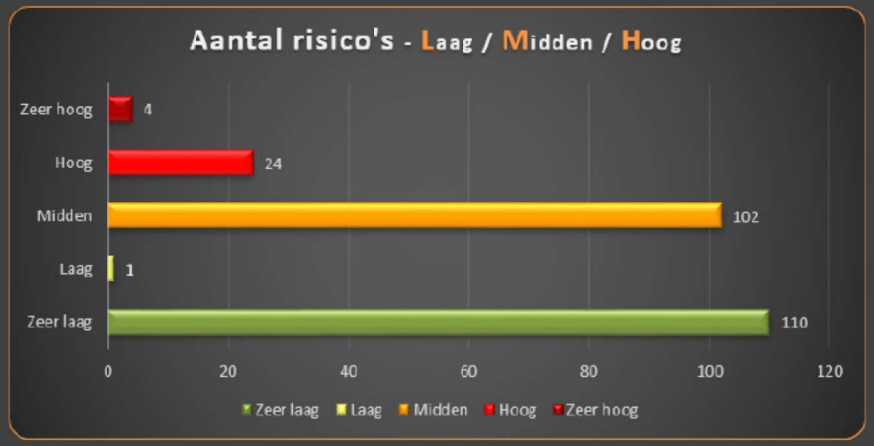


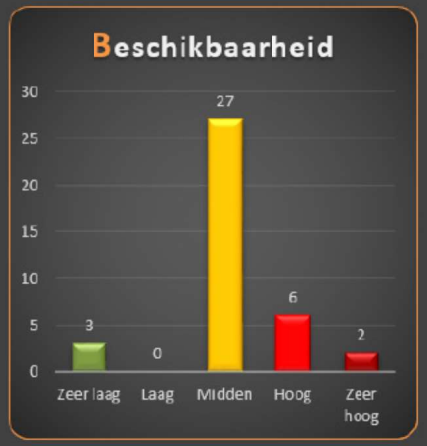
GGP

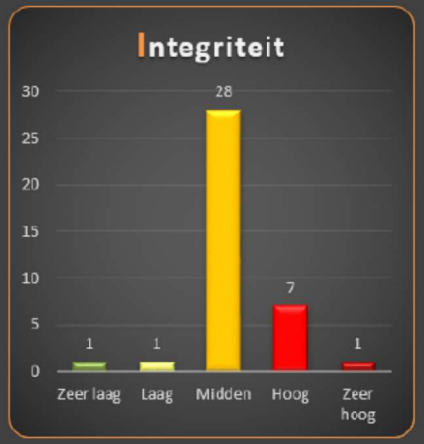
Risico overzicht per portefeuille

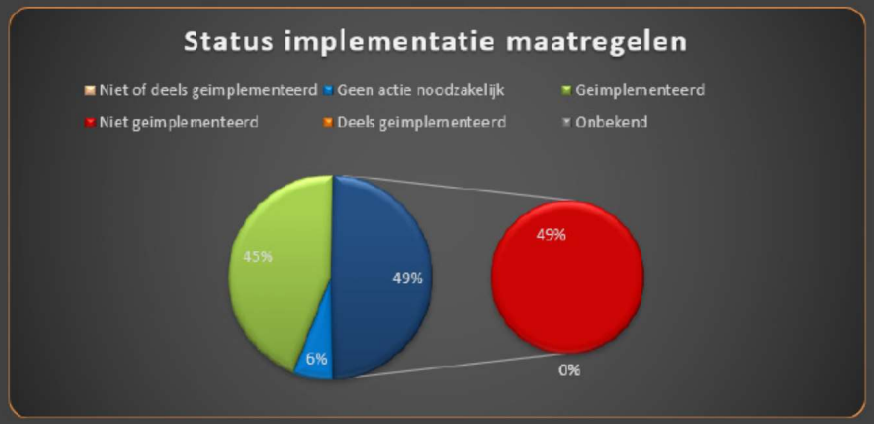
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	33	217	0	250	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

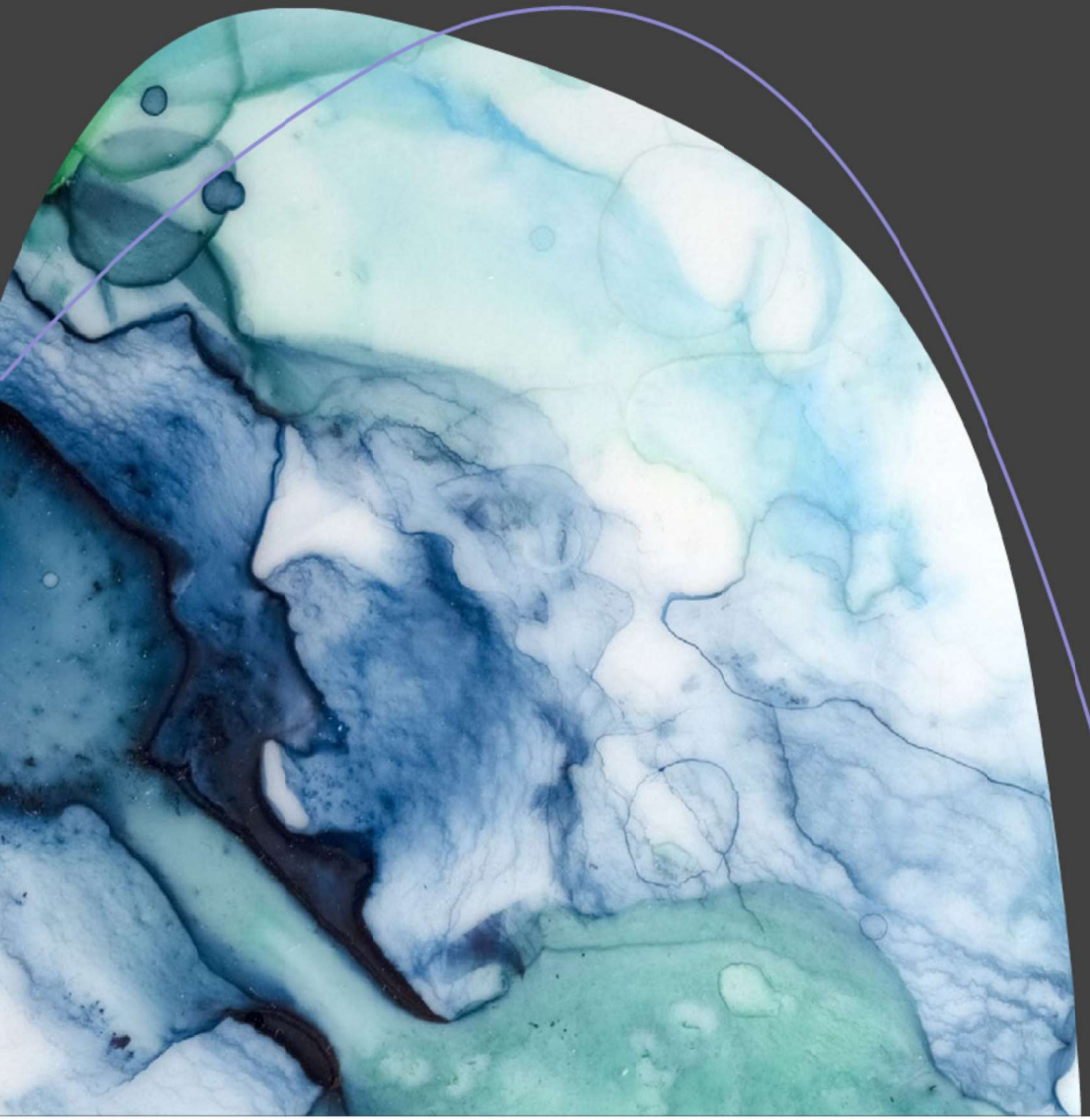
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

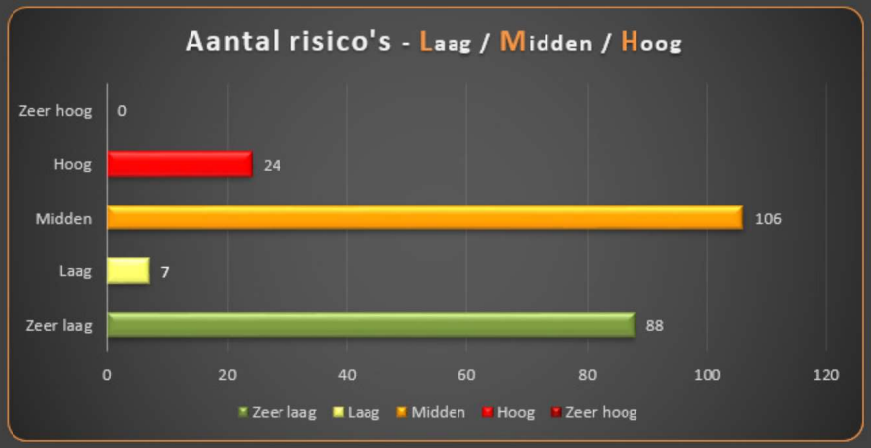


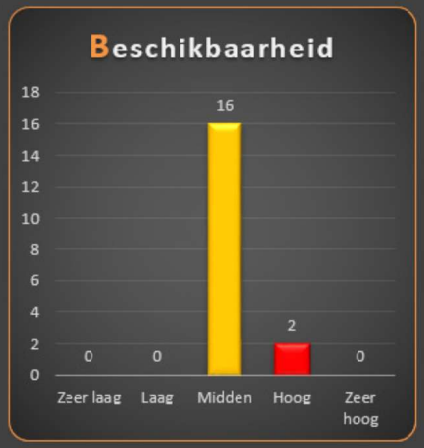
Intelligence

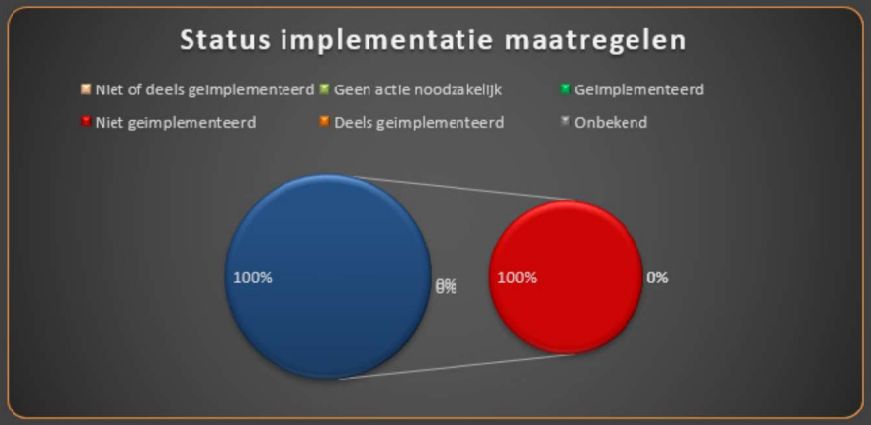
Risico overzicht per portefeuille

Periode: Q1-2024

Risico classificering







Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	19	234	0	253	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

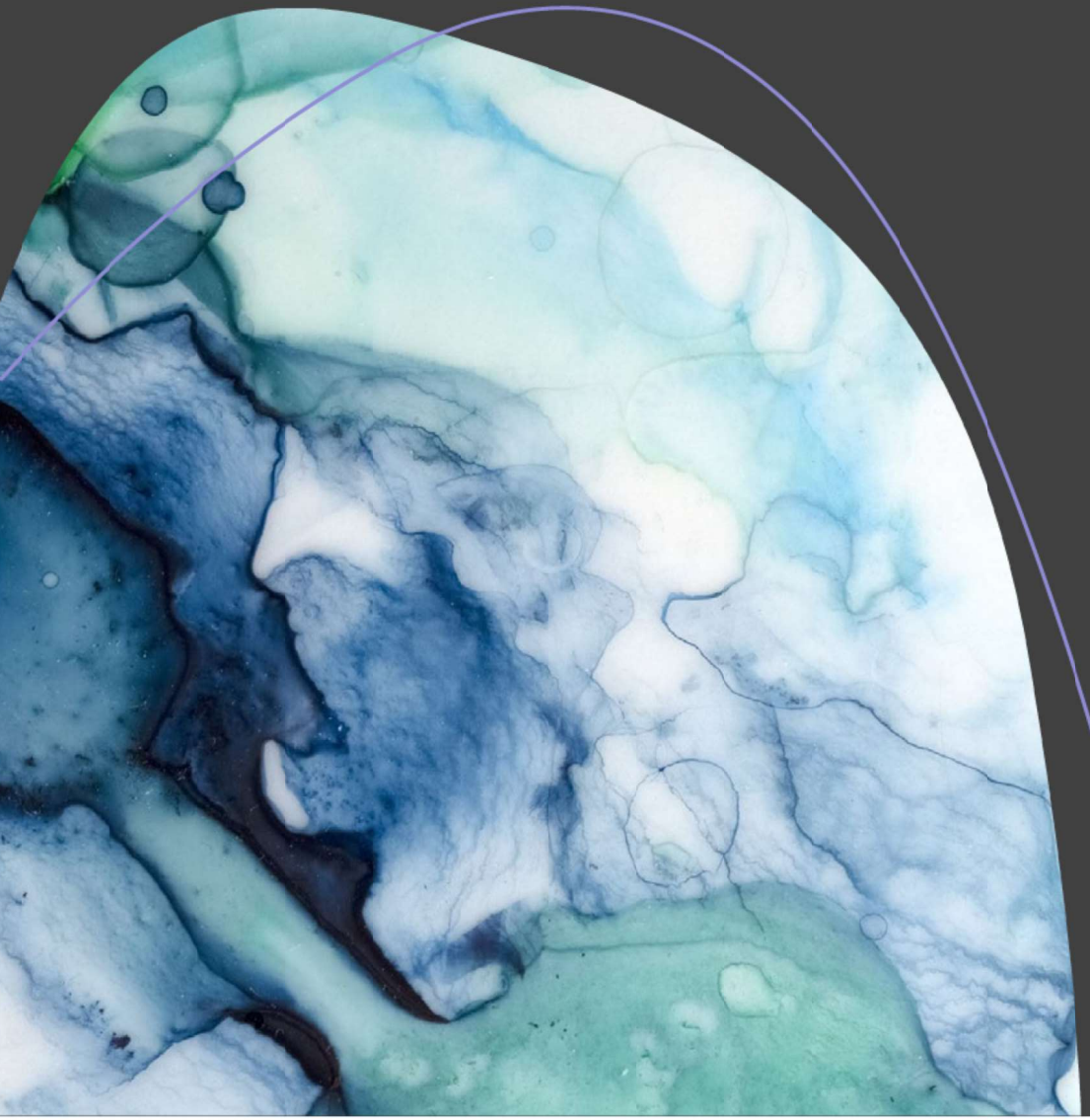
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

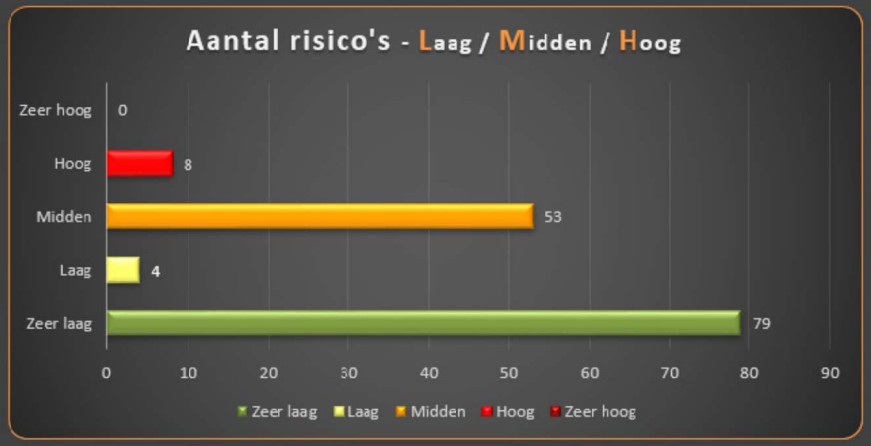


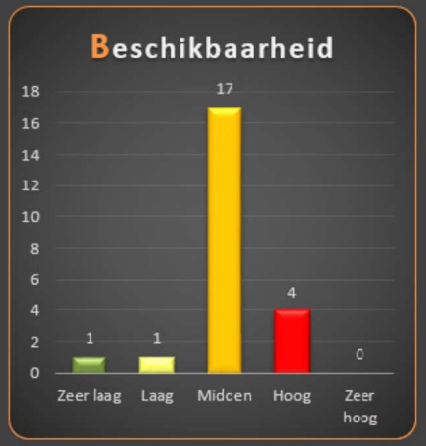
Operationeel Centrum

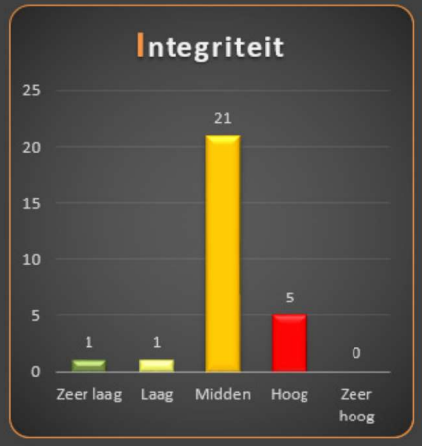
Risico overzicht per portefeuille

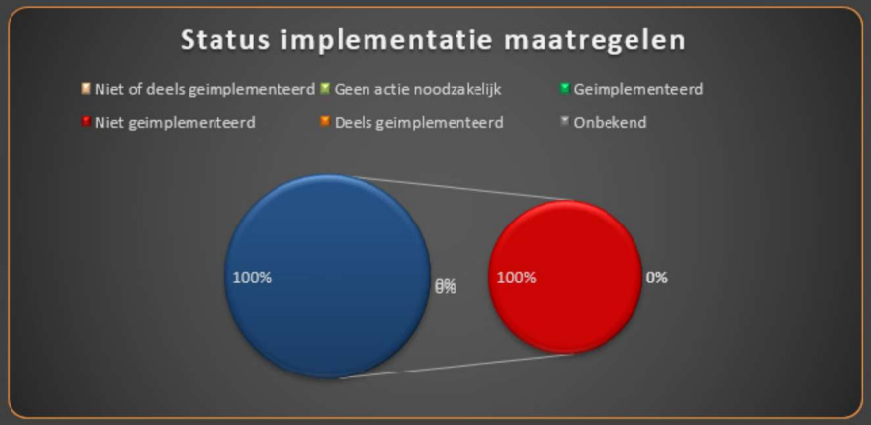
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	0	144	0	144	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

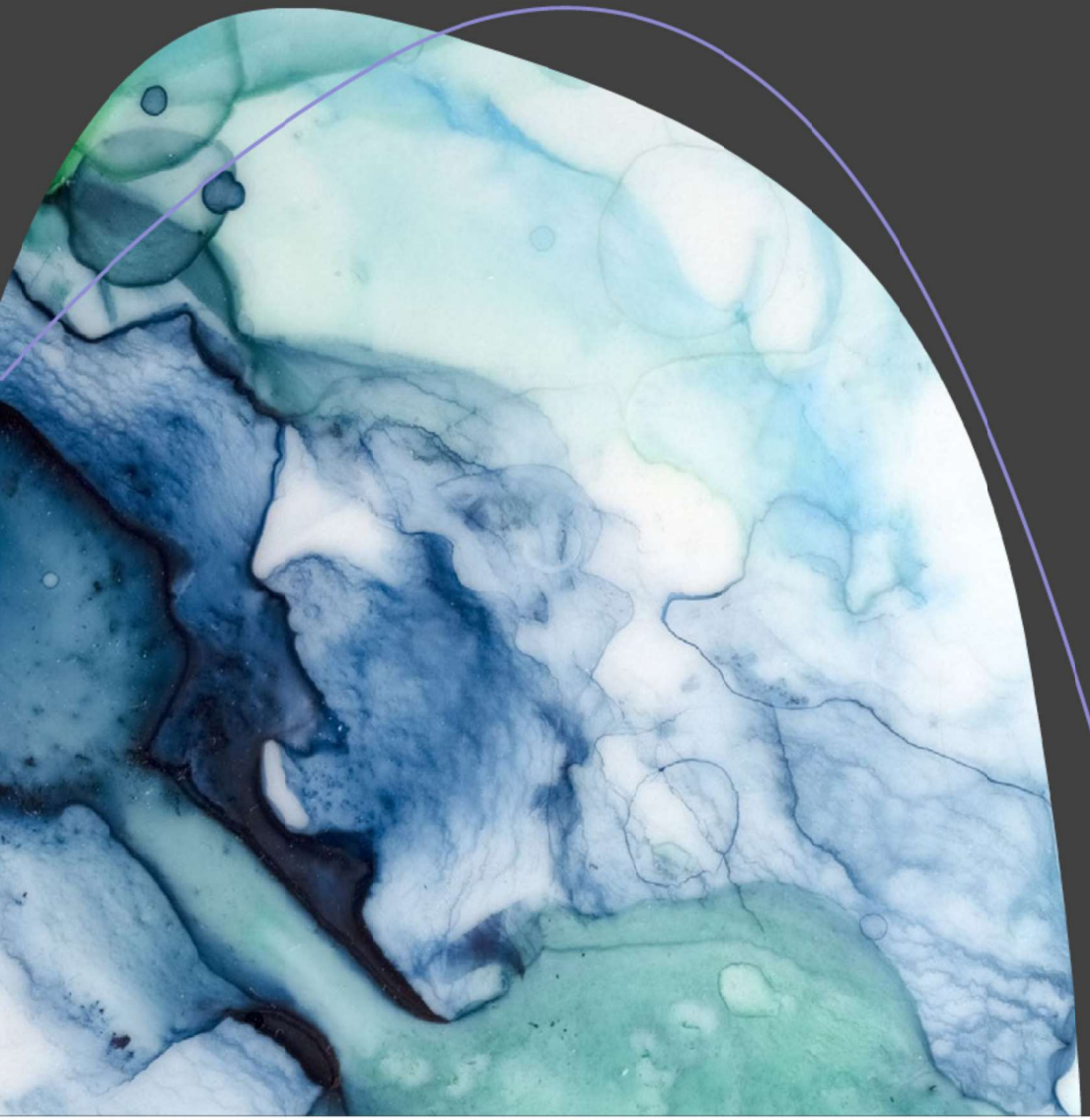
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

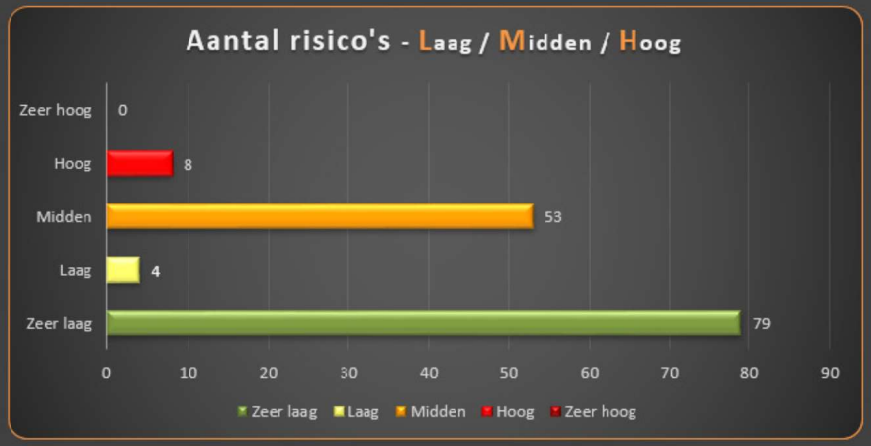


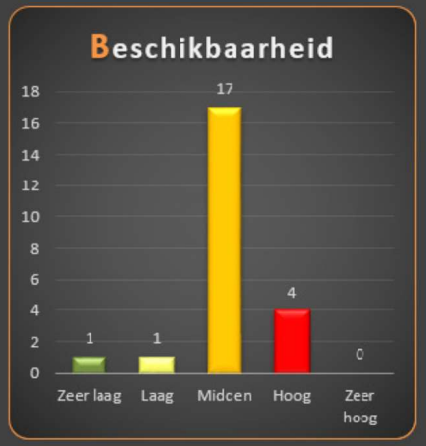
Specialistische Opsporing

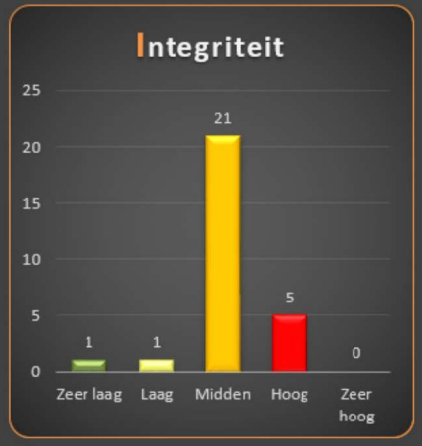
Risico overzicht per portefeuille

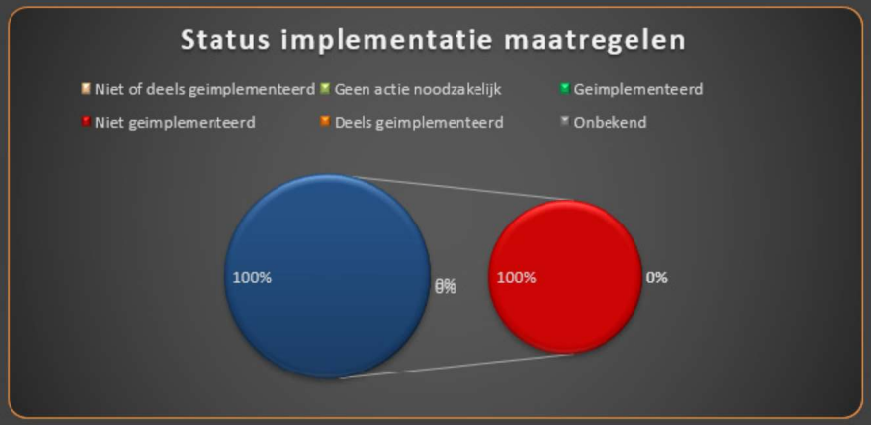
Periode: Q1-2024

Risico classificering









Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	28	131	0	159	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

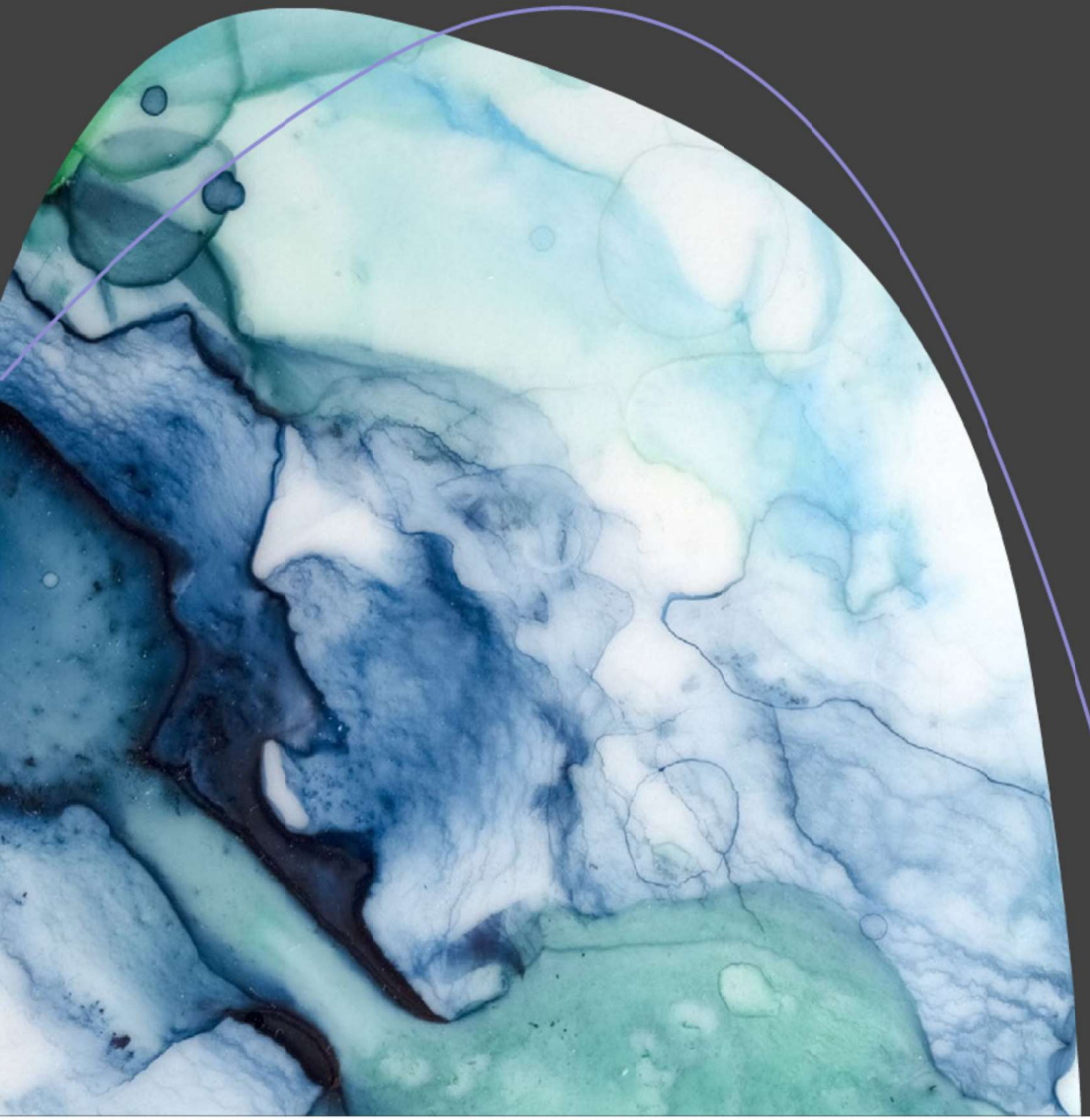
Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>

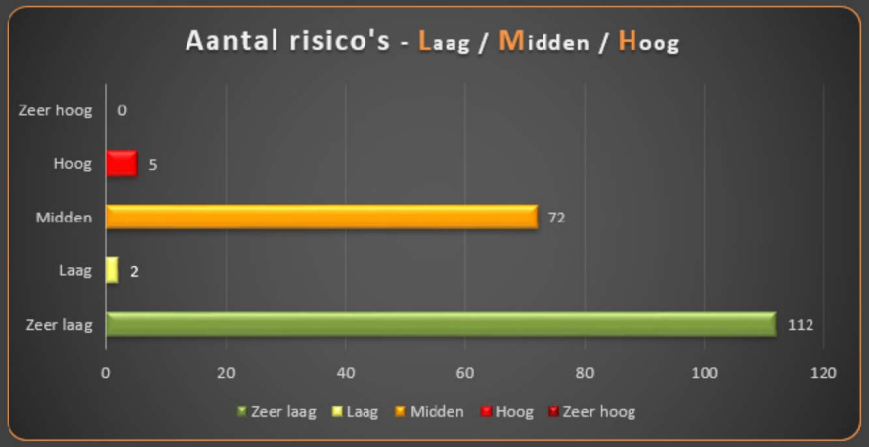


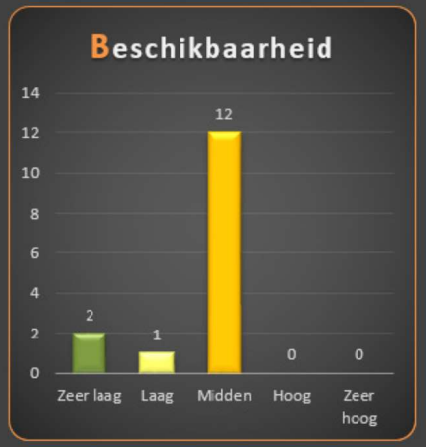
Thematische Opsporing

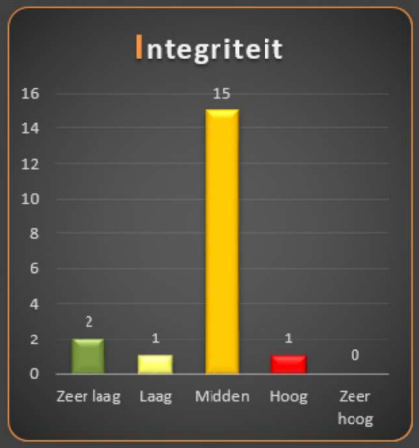
Risico overzicht per portefeuille

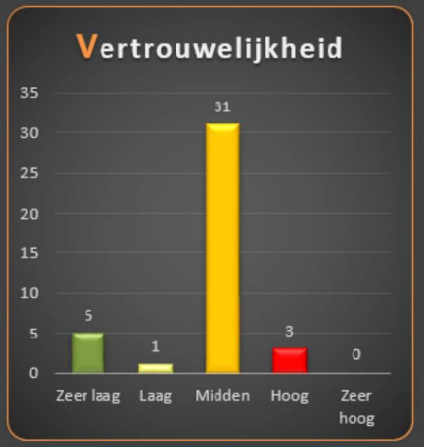
Periode: Q1-2024

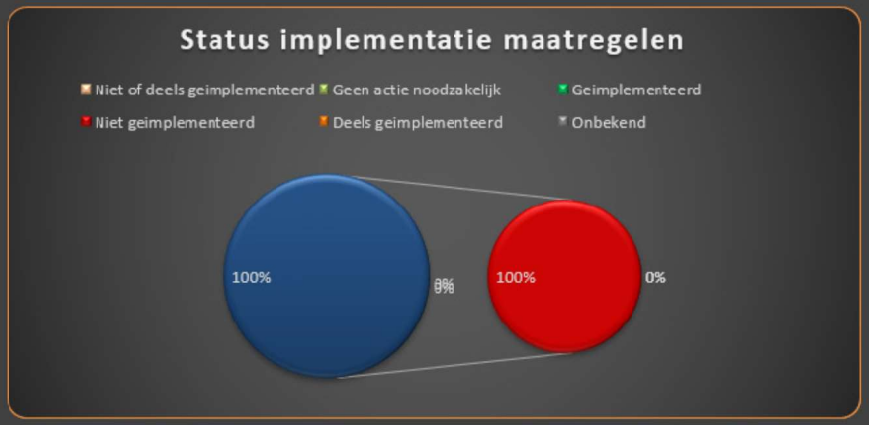
Risico classificering











Voortgang

Voortgang

Ten opzichte van vorige kwartaal is de volgende voortgang geboekt

Periode	Privacy risico's open	IB risico's open	Totaal gesloten	Totaal open	Voortgangs-percentage
Q1-2024	0	270	0	270	0%
Q2-2024					
Q3-2024					
Q4-2024					

Risico details

Overzicht
Zie bijgaand Excel overzicht voor details.

Aanwijzingen
- Het overzicht is per applicatie en/of GEB gerangschikt
- In de eerste kolom staat een link naar het dossier waar de IB analyse en/of GEB te vinden zijn

Vragen

Contact

Bij vragen, opmerkingen of meer informatie: neem contact op middels de mailbox van de hulpstructuur: <mailto: 5.1.2.i [redacted] @politie.nl>