Verbeterrapport na Wpg audit Douane december 2022

***Aanleiding***
De Wet politiegegevens (Wpg) schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels gesteld in de Wpg doet controleren door middel van een audit. Conform artikel 6:5 van het Besluit politiegegevens (Bpg) dient deze privacy audit eenmaal in de vier jaar te worden uitgevoerd. Deze audit heeft betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn, de controle en toezicht en de werking van deze maatregelen en procedures.

Door de Douane is aan de Auditdienst Rijk (ADR) gevraagd deze audit over het jaar 2021 uit te voeren. Op 22 december 2022 is het definitieve rapport1 door de ADR opgeleverd. De ADR heeft vastgesteld dat de Douane in 2021 in belangrijke mate niet voldeed aan de Wpg. Het daadwerkelijk bestendigen en borgen van geconstateerde verbeteringen vraagt om structurele aandacht en inzet.

De verwerkingsverantwoordelijke, bij de Douane de Directeur Generaal Douane, is, op grond van artikel 4, lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht om binnen drie maanden na datering van het auditrapport een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Met dit verbeterrapport wordt uitvoering gegeven aan deze verplichting.

***Doel verbeterrapport***
Het verbeterrapport heeft als doel om de door de ADR geconstateerde tekortkomingen over het jaar 2021 te verbeteren door het uitvoeren van acties en het inzetten van activiteiten door de Douane, en deze structureel in te bedden in de organisatie. De activiteiten worden geborgd door ze op te nemen in onze control cyclus en onze controleprocessen.

***Hercontrole***
De wijze waarop de tekortkomingen zijn afgehandeld, wordt vervolgens in een hercontrole getoetst door een externe auditor, de Auditdienst Rijk (ADR). Hierbij zal worden nagegaan of de tekortkomingen aantoonbaar door maatregelen zijn verbeterd. Het opvolgen van de tekortkomingen zal uiterlijk december 2023 zijn getoetst.

***Context en relevante ontwikkelingen***
*Algemeen*
Ontwikkeling implementatie Wpg
De Douane valt sinds maart 2019 met haar buitengewoon opsporingsambtenaren (BOA's)2 onder de Wet politiegegevens (Wpg). De implementatie van de Wpg leek in eerste instantie alleen te gaan om het aanpassen van de automatiseringssystemen. Om die reden is er ook geen uitvoeringstoets gedaan. Toen duidelijker werd dat er meer nodig was heeft de Douane een nulmeting aangevraagd bij de ADR. De Douane heeft vanaf dat moment de implementatie vormgegeven door de uitleg van de wet te toetsen aan normgevende referentiekaders (oa Noreakader), zoals ook de ADR die gebruikt, die in de loop der tijd beschikbaar zijn gekomen, maar ook door in nauw contact te staan met de FIOD en Belastingdienst over hoe zij de implementatie hebben aangepakt.

Prioriteit
De ADR benoemt in het auditrapport enkele belangrijke zaken, die door de Douane met voorrang worden opgepakt. Hierbij gaat het bijvoorbeeld om de inrichting van logging en monitoring op alle systemen die zijn opgezet voor 6 mei 2016 en die gereed moet zijn voor 6 mei 2023, maar ook de autorisatie en toegang tot politiegegevens.

Risico's en afhankelijkheden
De implementatie van de Wpg kan niet los gezien worden van enkele risico's en afhankelijkheden die voor de gehele Douane gelden. De ingebruikname van het systeem DON is bepalend voor een

1 https://www.rijksoverheid.nl/documenten/kamerstukken/2023/01/18/bijlage-adr-wpg-audit-douane-2021
2 Onder BOA's wordt ook verstaan medewerkers met een aanwijzing obv artikel 3 BpgBOA.

groot deel van de verbeterpunten en acties die in het verbeterrapport staan opgenomen. De Douane heeft een vol IV-portfolio, waardoor continu druk staat op de planning als er bijvoorbeeld weinig ruimte is om incidenten op te vangen als systemen uitvallen. De beschreven termijnen bij de aanbevelingen op dit vlak kunnen dan ook slechts als indicatie van de geplande einddatum worden gezien.

Daarnaast bestaat nog niet overal binnen de Douane een uniforme werkwijze. Nu de Douane procesbeschrijvingen, werkinstructies en eind 2023 het nieuwe systeem DON geheel klaar heeft wordt een uniforme werkwijze voorgeschreven. Het uitvoerende proces moet daarbij doorgang blijven vinden. Gezien de personele tekorten op de werkvloer kan er verminderde aandacht zijn voor de implementatie van de Wpg.

*Toelichting bij termen in de aanbevelingen*
Geautomatiseerde systemen DFB, DON en ATD
In de audit van de ADR wordt regelmatig naar de geautomatiseerde systemen DFB, DON en ATD verwezen. Het geautomatiseerde systeem DFB (Douane Fraude Bestrijding) bevat strafrechtelijke dossiers van de Douane. DFB is gebouwd op een platform dat zijn einde levensduur nadert. Daarom werkt de Douane nu aan een vervangend geautomatiseerd systeem DON (Douane Onregelmatigheden), waarin de eisen en waarborgen van de Wpg ingebouwd worden.
Daarnaast werkt de Douane met het systeem ATD (Applicatie Toezicht Douane), waarin dossiers worden opgeslagen van onderzoeken in verband met de handhaving in bepaalde gevallen. Deze vorm van gegevensverwerking is bijvoorbeeld aan de orde bij een meer omvangrijk opsporingsonderzoek of bij een verkennend onderzoek.
Naar verwachting kan DON eind dit jaar volledig in gebruik genomen worden en is ATD aangepast aan de vereisten en waarborgen vanuit de Wpg.

Compliancerapportage en Wpg kwaliteitshandboek
In de rapportage van de ADR wordt meerdere malen gesproken over zowel het Wpg kwaliteitshandboek als de compliancerapportage. De compliancerapportage is de term die de Douane gebruikt voor de bundeling in de vorm van een rapportage van verwerkingen die de Douane uitvoert met de daarbij horende risicoanalyse, het beveiligingsadvies voor DON op basis van de Baselinetoets Informatiebeveiliging Overheid (BIO) en procedurebeschrijvingen. De BIO maakt dan ook onderdeel uit van het implementatietraject. De term Wpg kwaliteitshandboek geeft eenzelfde bundeling van informatie aan over hoe gewerkt moet worden in het licht van de Wpg als de compliancerapportage. Daarmee hebben deze termen dezelfde betekenis en zijn zij door elkaar te vervangen.

Verwerkingsregister
Net als bij de Algemene Verordening Gegevensbescherming (AVG) dient de Douane voor de Wpg haar verwerkingen in een register bij te houden.
De Douane heeft deze verwerkingen en met positief advies van de Functionaris Gegevensbescherming vastgelegd. Dit jaar vindt de periodieke update van het Wpg-register plaats.

Vormgeving procesbeschrijvingen en werkinstructies
Douane gaat, ter uitvoering van de Wpg, alle interne procedures beschrijven, voorwaar dat nog niet is gedaan, middels een procesbeschrijving met waar nodig een procesrisicoregister en een werkinstructie. Tevens zal de interne controle worden ingericht om te toetsen of de getroffen beheersmaatregelen in het proces hebben gewerkt om zodoende te kunnen aantonen of het proces van de Wpg wordt beheerst.
De Douane heeft de procesbeschrijving, werkinstructie en het procesrisicoregister van het meest omvangrijke proces 'Afhandelen Onregelmatigheid' inmiddels afgerond en de fase van implementatie binnen de organisatie gestart.

Bewustwordingscampagne

Bij de Douane komt de verwerking van Wpg-gegevens in alle uitvoeringsprocessen voor. Immers, het toezicht dat de Douane uitvoert kan in alle gevallen leiden tot een vermoeden van een strafbaar feit en daarmee de overgang van toezicht, AVG, naar strafrecht, Wpg. De Douane is daarom in 2022 gestart met een trapsgewijze bewustwordingscampagne met algemene brede communicatie via de organisatiebrede kanalen richting de gehele organisatie. Er is een gerichte aanpak gemaakt met interne communicatie via presentaties in overleggen, berichten op het intranet, flyers en beschikbare informatie op de mobiele werktelefoon. Ook is een landelijk netwerk van Wpg-contactpersonen in de verschillende Douaneregio's opgezet. In 2023 wordt deze campagne verder uitgebreid en meer gedetailleerd uitgevoerd met specifieke en gerichte communicatie richting de regio's en de verschillende, specialistische teams.

Samenwerkingsafspraken met de Belastingdienst

De Douane heeft op het gebied van haar automatiseringssystemen samenwerkingsafspraken gemaakt met de Belastingdienst over hoe er samengewerkt wordt aan systemen die bij de Belastingdienst draaien. De ADR adviseert om deze samenwerkingsafspraken inzake het verwerken van Wpg-gegevens verder uit te breiden met concrete afspraken inzake het verwerken van politiegegevens. De Douane zal gevolg geven aan dit advies, waarbij wordt voorzien dat gezamenlijk wordt opgetrokken met een aantal organisatieonderdelen binnen de Belastingdienst. Verwachting is dit traject uiterlijk in december 2023 af te ronden.

***Korte versie van te nemen acties:***

| ADR: Aanbevelingen | Acties door Douane | Gereed |
|---|---|---|
| | | |
| Doelbinding<br><br>**Aanbeveling:** stel de verwerkingen vast in het register van verwerkingsactiviteiten en beschrijf een proces dat erop toeziet dat het doel wordt vastgelegd in de gehanteerde systemen evenals dat er vanuit bestaan controle op wordt uitgevoerd.<br>Neem dit ook op in een Wpg kwaliteits-handboek. | 1. Actualiseren Wpg-verwerkingen<br>2. Vaststellen geactualiseerd Wpg-register<br>3. Wpg kwaliteitshandboek aanvullen met verwijzingen naar Wpg-register<br>4. Procedurebeschrijving en werkinstructie aanpassen aan vastlegging doel in gehanteerde systemen<br>5. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>6. Inrichten controle op bestaan vastlegging doel<br>7. Inrichten control op bestaan vast-legging doel | Q4 2023 |
| Noodzakelijkheid en rechtmatigheid<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin de noodzakelijkheid en rechtmatigheid van de verwerking van politiegegevens is opgenomen.<br>Beschrijf tevens een werkinstructie betreffende een controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen. | 1. Wpg kwaliteitshandboek aanvullen op noodzakelijkheid en rechtmatig-heid<br>2. Wpg-register actualiseren<br>3. Procedurebeschrijving en werk instructie aanpassen<br>4. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>5. Inrichten controle op bestaan tech-nische en organisatorische maatregelen<br>6. Inrichten control op bestaan tech-nische en organisatorische maatregelen | Q4 2023 |
| Juistheid en volledigheid<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin de juistheid en volledigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen. | 1. Wpg kwaliteitshandboek aanvullen op juistheid en volledigheid<br>2. Inrichten controle op juistheid en volledigheid van de verwerking van politiegegevens<br>3. Procedurebeschrijving en werk-instructie aanpassen<br>4. Procedurebeschrijving en werk-instructie laten landen en borgen in primair proces<br>5. Inrichten controle op bestaan tech-nische en organisatorische maatregelen<br>6. Inrichten control op bestaan tech-nische en organisatorische maatregelen | Q4 2023 |
| Bijzondere categorieën van persoonsgegevens<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin het verwerken van bijzondere persoonsgegevens is opgenomen en de manier waarop de Douane hiermee omgaat.<br>Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen. | 1. Wpg kwaliteitshandboek aanvullen op bijzondere categorieën van persoonsgegevens<br>2. Procedurebeschrijving en werkinstructie aanpassen<br>3. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>4. Inrichten controle op verwerken van bijzondere persoonsgegevens | Q3 2023 |

| | | |
|---|---|---|
| | 5. Inrichten control op verwerken van bijzondere persoonsgegevens | |
| Geautomatiseerde individuele besluitvorming<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin geautomatiseerde individuele besluitvorming dan wel profilering is opgenomen. | 1. Het niet toestaan van geautomatiseerde individuele besluitvorming en het niet gebruik daarvan in profilering opnemen in Wpg kwaliteitshandboek<br>2. Opnemen van deze beleidsregel in de technische eisen waaraan geautomatiseerde systemen minimaal moeten voldoen | Q4 2023 |
| Onderscheid feiten en oordeel<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin het onderscheid tussen feiten en oordeel is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen. | 1. Wpg kwaliteitshandboek aanvullen op onderscheid feiten en oordeel<br>2. Procedurebeschrijving en werkinstructie aanpassen<br>3. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>4. Inrichten technische en organisatorische maatregelen | Q4 2023 |
| Aanwijzen bevoegd functionarissen<br><br>**Aanbeveling:** houd de lijst van de verantwoordelijke aangewezen bevoegde functionarissen actueel. | 1. Inrichten controlecyclus om aanwijzingen actueel te houden<br>2. Inrichten interne control op uitvoering | Q4 2023 |
| Onderscheid tussen verschillende categorieën van betrokkenen<br><br>**Aanbeveling:** beschrijf in opzet een Wpg kwaliteitshandboek waarin het onderscheid tussen verschillende categorieën van betrokkenen is opgenomen. | 1. Wpg kwaliteitshandboek aanvullen op onderscheid categorieën van betrokkenen<br>2. Opnemen in de geautomatiseerde systemen | Q3 2023 |
| Reikwijdte<br><br>**Aanbeveling:** realiseer het voornemen om de Wpg verwerkingen verder in kaart te brengen. Maak de medewerkers bewust van de informatie die beschikbaar is om hen in de praktijk te helpen met de sfeerovergang en de daarbij behorende aandachtspunten. | 1. Actualiseren van Wpg verwerkingen in het Wpg-register<br>2. Bewustwording medewerkers vergroten onder meer via de bewustwordingscampagne<br>3. Borging structurele aandacht via privacyorganisatie Douane | Q4 2023 |
| Gegevensbescherming door beveiliging en ontwerp<br><br>**Aanbeveling:** Continueer het voornemen om de compliance rapportage Wpg verder uit te werken om de risico's inzichtelijk te krijgen. Besteed hierbij tevens aandacht voor de benodigde maatregelen om deze risico's te mitigeren evenals het toepassen van privacy by design bij het verder ontwikkelen van DON. | 1. Risico’s uitwerken in compliance rapportage Wpg (Wpg kwaliteitshandboek)<br>2. Implementeren privacy by design in automatiseringssystemen waar Wpg-informatie in verwerkt wordt | Q4 2023 |
| Verwerkers en verwerkersovereenkomsten<br><br>**Aanbeveling:** breid de samenwerkingsafspraken met de Belastingdienst verder uit met concrete | 1. Uitbreiden samenwerkingsafspraken met de Belastingdienst op het gebied van privacy-gerelateerde onderwerpen | Q4 2023 |

| | | |
|---|---|---|
| afspraken inzake het verwerken van politiegegevens. | | |
| Geheimhouding<br><br>**Aanbeveling:** Kristalliseer de discussie uit over aanvullende screening voor boa's. | 1. Innemen standpunt over aanvullende screening voor boa's en daaraan opvolging geven | Gereed |
| Gegevensbeschermingseffectbeoordeling / DPIA<br><br>**Aanbeveling:** Realiseer het voornemen om de compliance rapportage verder uit te werken en af te ronden. | 1. Afronden compliance rapportage | Q4 2023 |
| Melding datalekken<br><br>**Aanbeveling:** zorg dat binnen de Douane meer aandacht wordt gegeven aan wat een datalek is, niet alleen gegevens maar ook de devices waarop de gegevens zijn vastgelegd. Zorg hierbij dat: de procedure meldplicht datalekken breder bekend wordt hoe wordt gemeld; hoe de betrokkenen in kennis worden gesteld van inbreuken op hun gegevens; op juiste wijze de meldingen worden geregistreerd en aan de AP worden gemeld. | 1. Bewustwording vergroten binnen de Douaneorganisatie<br>2. Melding datalekken verbijzonderen op AVG en Wpg-gegevens | Q4 2023 |
| Gegevensbescherming door standaardinstellingen<br><br>**Aanbeveling:** Regel alsnog dat een risicoanalyse wordt opgesteld voor de applicatie DFB waarin de gegevens inzake de WPG worden vastgelegd ais de implementatie van DON de opvolger van DFB meer tijd vergt. De uitkomsten van deze risicoanalyse zijn de input voor Autorisaties en Toegang tot politiegegevens. | 1. Indien de implementatie van opvolger DON later plaatsvindt dan beoogd: opstellen risicoanalyse op het te vervangen systeem DFB | Q2 2023 |
| Autorisaties en Toegang tot politiegegevens<br><br>**Aanbeveling:** Richt de logische toegangsbeveiliging waarvoor een proces is ingericht zodanig in dat ook voldaan wordt aan de eisen van de WPG:<br>- Pas de autorisatiematrix/ functiescheidingsmatrix voor DFB Douane Fraude Bestrijding of de opvolger DON aan dat voldaan wordt aan de eisen uit de WPG eisen. Hierbij wordt onderscheid gemaakt tussen artikel 8 en artikel 9 verwerkingen en wordt onderscheid gemaakt naar ouderdom van gegevens die op grond van de WPG dient te worden gemaakt.<br>- Borg dat ook het dossiersysteem ATD Caseware voldoet aan de WPG eisen.<br>- Pas het Jaarlijks uitgevoerde controleprogramma Beveiliging aan zodat de controles ook zijn gericht op de eisen die de Wpg stelt aan de logische toegangsbeveiliging van de systemen. | 1. Inrichten logische toegangsbeveiliging<br>2. Aanpassen autorisatiematrix DFB/DON<br>3. ATD Caseware Wpg-proof maken<br>4. Aanpassen jaarlijkse controleprogramma Beveiliging | 1,4: Q1 2024<br>2,3: Q4 2023 |

| | | |
|---|---|---|
| Uitvoering van de dagelijkse politietaak<br><br>**Aanbeveling:**<br>Implementeer richtlijnen voor het verwerken van politiegegevens volgens Wpg. Bepaal wanneer er sprake is van verwerking en houdt hierbij rekening met de overgang van controle naar opsporing. Pas DFB aan of richt de opvolger DON zodanig in dat aan de Wpg wordt voldaan. Volgens de Wpg dienen de gegevens in een artikel 8 omgeving na een jaar te worden gearchiveerd. Deze gearchiveerde gegevens mogen volgens de Wpg alleen na verkregen toestemming benaderbaar zijn. | 1. Procedurebeschrijving en werkinstructie aanpassen<br>2. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>3. Geautomatiseerde systemen Wpg-proof maken<br>4. Bewaartermijnen Wpg toepassen<br>5. Bewustwording voor het verschil tussen AVG en Wpg vergroten. | 1,2,4,5: Q4 2023<br>3: Q4 2023 |
| Bewaartermijnen, verwijderen en vernietigen<br><br>**Aanbeveling:** Voer procedures in waarmee bewaar- /vernietigingstermijnen van de Wpg gegevens worden gemonitord en geschoond op de binnen de Douane gebruikte opslagen: de gemeenschappelijke Q-schijf, de applicatie DFB, het dossiersysteem ATD/Caseware en de tijdelijke opslag op netwerkschijven (C:, N: en Q:) en e-mail. | 1. Procedures opstellen t.b.v. geautomatiseerde monitoring van bewaar- en vernietigingstermijnen<br>2. Geautomatiseerd schonen na verlopen bewaar- en vernietigingstermijnen | Q1 2024 |
| Doorgiften aan derde landen<br><br>**Aanbeveling:** Pas het register met Wpg verwerkingen aan op het punt van doorgiften aan derde landen zodat duidelijk en eenduidig is in welk geval er sprake of geen sprake is van doorgiften aan derde landen. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor doorgiften van politiegegevens onderdeel van het periodiek toezicht door de PF en/of pFG. Het toezicht op de naleving van richtlijnen voor het verstrekken en doorgeven van politiegegevens kan ook onderdeel uitmaken van een formele interne controle door een afdeling kwaliteitsbeheer. | 1. Actualiseren Wpg-register<br>2. Inrichten en implementeren interne controle<br>3. Inrichten periodieke toetsing door PF en/of pFG. | Q4 2023 |
| Rechtstreekse verstrekking<br><br>**Aanbeveling:** pak het toezicht door de PF en pFG zo snel als mogelijk na afronding van deze audit en op basis van de resultaten op in samenhang met het nog in te richten systeem voor interne controle en audit. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor verstrekkingen onderdeel van dit toezicht. | 1. Inrichten periodieke toetsing door PF en/of pFG. | Q3 2023 |
| Informatie aan de betrokkene, Recht op inzage rectificatie en Verwijdering<br><br>**Aanbeveling:** De werking van het proces en de instructies in wording kan nog niet getoetst worden omdat er nog geen verzoeken zijn gedaan. Actualiseer en completeer het beschreven proces en de instructies en toets dit op toereikendheid zodra er verzoeken zijn | 1. Actualiseren procedurebeschrijving en werkinstructie bij de rechten van betrokkenen.<br>2. Procedurebeschrijving en werkinstructie laten landen en borgen in primair proces<br>3. Richt een controle in op de toetsing van toereikendheid voor toekomstige verzoeken | Q1 2024 |

| | | |
|---|---|---|
| gedaan. Van belang daarbij is dat dit onderdeel wordt aangepast aan de Wpg. | | |
| Register<br><br>**Aanbeveling:** Actualiseer het register in overeenstemming met de eisen van art 31d Wpg en betrek daarbij de uitkomst van de lopende discussie over de invulling van het register. | 1. Actualiseren van het Wpg-register | Q4 2023 |
| Documentatie<br><br>**Aanbeveling:** Maak een centraal overzicht van alle verstrekkingen en doorgiften van Wpg gegevens. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor verstrekkingen onderdeel van het periodiek toezicht door de PF en of pFG. | 1. Inrichten centraal overzicht verstrekkingen en doorgiften<br>2. Inrichten periodieke toetsing door PF en/of pFG.<br>3. Inrichten interne controle op volledigheid overzicht | Q1 2024 |
| Logging:<br><br>**Aanbeveling:** Toets deze norm bij de eerstvolgende (interne) audit afhankelijk van de situatie op dat moment. Dat wil zeggen toepassen op DON als dit systeem dan operationeel is en/of op andere voor de Wpg gegevensverwerking gebruikte systemen w.o. DFB en ATD/Caseware, die nog operationeel zijn. Uiterlijk 2023 zal aan de Wpg eisen voor logging moeten worden voldaan. Uitgangspunten voor het inrichten van logging en monitoring zijn in de BIO (paragraaf 12.4) en het beleid voor Logging en monitoring van het ministerie van Financiën opgenomen. | 1. Inrichten loggen en monitoren op Wpg-systemen in 2023 | Q2 2023 |
| Audits<br><br>**Aanbeveling:** Geef prioriteit aan het daadwerkelijk inrichten en borgen van een werkend proces voor controle en audit, waarbij interne controles en audits gebruikt kunnen worden ter voorbereiding op de vierjaarlijkse externe privacy audit en ten behoeve van het toezicht door de pFG en PF. | 1. Borgen periodieke uitvoering interne en externe audits<br>2. Inrichten periodieke toetsing door PF en/of pFG | Q4 2023 |
| Privacyfunctionaris<br><br>**Aanbeveling:** Beleg het interne toezicht op de naleving van de Wpg conform art 34 formeel en met voldoende gekwalificeerde capaciteit bij de Privacyfunctionaris zodat invulling gegeven wordt aan een werkende cyclus voor intern toezicht. | 1. Beleggen van intern toezicht bij de Privacyfunctionaris | Q2 2023 |
| Functionaris voor gegevensbescherming<br><br>**Aanbeveling:** Pak het externe toezicht door de pFG zo snel als mogelijk na afronding van deze audit en op basis van de resultaten op in samenhang met het nog in te richten systeem voor interne controle en audit. | 1. Invulling geven aan extern toezicht door de pFG | Q2 2023 |

| | | |
|---|---|---|
| Cryptografie<br><br>**Aanbeveling:** Richt een aantoonbaar proces in dat periodiek toeziet op het toepassen en naleven van het gebruik van cryptografische beheersmaatregelen door verwerkers en dienstverleners. | 1. Inrichten proces cryptografische beheersmaatregelen | Q4 2023 |
| Vulnerability scans en Penetratietesten<br><br>**Aanbeveling:** Indien DFB binnen afzienbare tijd is uitgefaseerd bevelen wij aan periodiek volgens vastgesteld beleid pentesten uit te voeren op DON en ATD. Als DFB nog enige tijd operationeel blijft en/of de gegevens blijven nog beschikbaar, maak dan een aantoonbare afweging voor het alsnog uitvoeren van een penetratietest op deze omgeving. | 1. Periodiek uitvoeren penetratietesten op Wpg-systemen | Q3 2023 |
| Wijzigingenbeheer en Beheer van kwetsbaarheden<br><br>**Aanbeveling:** Borg in het verbeterrapport dat voor DON ook de WPG-vereisten voor wijzigingsbeheer en het beheer van kwetsbaarheden worden opgenomen. Als de implementatie van DON, de opvolger van DFB, meer tijd vergt, dan adviseren wij dat deze onderdelen tussentijds worden getoetst in de eerstvolgende interne audit. | 1. Inrichten wijzigingsbeheer en beheer van kwetsbaarheden.<br>2. Inrichten interne audit conform de Regeling periodiek audit politie-gegevens. Dit inclusief de genoemde opleiding genoemd in artikel 6 van deze regeling. | Q4 2023 |