Ministerie van Defensie

# Toezichtjaarverslag 2023

## Functionaris voor Gegevensbescherming

# Colofon

## Functionaris voor Gegevensbescherming

***Adres***
Majoor Jan Linzel Complex
Brasserskade 227a
2497 NX  Den Haag

***Postadres***
Postbus 20701
2500 ES  Den Haag
MPC 85B

***Datum***
Maart 2024

# Voorwoord

De Functionaris voor Gegevensbescherming (FG) ziet als onafhankelijke interne toezichthouder bij het Ministerie van Defensie toe op de naleving van de wet- en regelgeving rond de bescherming van persoonsgegevens. De FG wordt ook wel aangeduid als *Data Protection Officer* (DPO). De Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG (UAvg) en de Wet politiegegevens (WPG) vormen de wettelijke basis voor het toezicht. Defensie heeft twee functionarissen voor gegevensbescherming, die respectievelijk toezien op de naleving van de AVG en de WPG.

Volgens de wet informeert, adviseert en controleert de FG of verwerkingen van persoonsgegevens bij Defensie rechtmatig, behoorlijk en transparant zijn. De FG controleert ook of betrokkenen van binnen en van buiten Defensie hun *privacy*-rechten kunnen uitoefenen en ziet toe op een correcte afhandeling van datalekken en klachten over het verwerken van persoonsgegevens. De FG maakt zich iedere dag sterk voor een zorgvuldige omgang met de persoonsgegevens die Defensie verwerkt en het optimaal waarborgen van het recht op gegevensbescherming en *privacy*. Tot slot werkt de FG samen met de externe toezichthouder, de Autoriteit Persoonsgegevens (AP).

2023 was een jaar van afwegingen; een afweging tussen kansen en mogelijke risico's voor Defensie en betrokkenen, maar ook tussen vrijheid en veiligheid. Technische innovaties en organisatorische ontwikkelingen bij Defensie leiden tot veel vragen over gegevensbescherming en *privacy*. Defensie maakt een digitale en technologische transitie door met nieuwe concepten en inrichtingsprincipes voor Informatiegestuurd Optreden (IGO), multidomein en geïntegreerd optreden (MDO) en de inzet bij hybride dreigingen en conflicten. De complexiteit van deze ontwikkelingen leidt tot diverse juridische vraagstukken en in zekere mate tot een heroriëntatie op de taken en bevoegdheden van de krijgsmacht. Een moderne krijgsmacht richt zich niet enkel op het 'gewapend conflict' in het fysieke domein, maar krijgt in het virtuele domein ook te maken met invloeden en effecten op de informatieomgeving.

Veel van deze ontwikkelingen spelen zich af op het snijvlak tussen burgerlijke rechten en vrijheden, en veiligheid. Veelbelovende technologieën en maatregelen om de veiligheid te bevorderen hebben tegelijkertijd, zowel binnen als buiten de defensieorganisatie, effect op de *privacy* en andere burgerlijke rechten en vrijheden van betrokkenen. Defensie moet onder zeer uiteenlopende omstandigheden het belang van veiligheid en privacy tegen elkaar afwegen. Het vooraf inzichtelijk kunnen maken en tegen elkaar afwegen van die belangen, in het licht van de relevante juridische kaders, is noodzakelijk om te komen tot adequate risicobeheersing en risicoacceptatie op het juiste niveau. De defensieonderdelen ondervinden bijvoorbeeld knelpunten in het kader van de gereedstellingstaak. De actuele dreiging van (hybride) gewapende conflicten en crisissituaties verplichten Defensie ertoe om vanuit haar grondwettelijke doelstellingen eenheden gereed te stellen, die in voldoende mate getraind en geoefend zijn om zowel in de fysieke dimensie als in de digitale informatie-omgeving te kunnen optreden. Daarbij heeft Defensie altijd de verantwoordelijkheid en de verplichting om de grondrechten van burgers en haar eigen medewerkers te respecteren en te beschermen en zich te houden aan de overige van toepassing zijnde wet- en regelgeving. De balans tussen veiligheid en privacy kan onder operationele omstandigheden en juridische kaders anders worden afgewogen dan tijdens oefening en trainingssituaties. Maar elk overheidshandelen dat ingrijpt in de (grond)rechten en vrijheden dient altijd te berusten op een wettelijke grondslag.

mevr. mr. O.L. Stenhuis-Kok
*De Functionaris voor Gegevensbescherming Algemene verordening gegevensbescherming*

mr. K.M.M. Weijers
*De Functionaris voor Gegevensbescherming Wet politiegegevens*

# Inhoud

# 1 Toezicht 2023

Bij Defensie werken ruim 69.000 beroepsmilitairen, burgers en reservisten. Defensie is in alle opzichten aan het bouwen, steeds vaker met nationale en internationale partners. De defensieorganisatie richt zich op de ontwikkeling en toepassing van nieuwe en innovatieve werkwijzen en op het optimaliseren van de bestaande processen. Defensie werkt aan verdergaande digitalisering IGO. Technologische en organisatorische ontwikkelingen doen zich organisatiebreed voor. Het gaat om uiteenlopende producten, diensten en applicaties waarbij nieuwe technologieën worden gebruikt, zoals kunstmatige intelligentie (AI), algoritmes, slim cameratoezicht, gezondheidsmonitoring, biometrische sensoren en slimme sensoren, en ICT-toepassingen aan boord van schepen, vliegtuigen en voertuigen. Ook komen er in het kader van IGO steeds meer tools beschikbaar die informatie en datastromen verwerken en inzichtelijk maken. Deze ontwikkelingen leiden tot het verwerken van persoonsgegevens van de defensiemedewerkers, maar ook in toenemende mate van betrokkenen buiten Defensie, zowel nationaal als internationaal.

De FG had in 2023 aandacht voor verwerkingen van persoonsgegevens die een hoog risico inhouden voor de rechten en vrijheden van personen, bijvoorbeeld door het gebruik van (nieuwe) technologieën. De FG genereert door middel van toezichtbezoeken, documentanalyse en waarnemingen een beeld van de naleving van wet- en regelgeving rond de bescherming van persoonsgegevens. Behalve gepland toezicht conform het Toezichtjaarplan 2023, legde de FG ook ad hoc-toezichtbezoeken af naar aanleiding van incidenten of adviesvragen. De FG besteedde gedurende het jaar aandacht aan en gaf advies over de prioritaire thema's uit het Toezichtjaarplan FG 2023, zoals IGO, *drone*-detectie, Defensie Open op Orde (DOO) en andere (technologische) ontwikkelingen. 2023 was ook een zoektocht naar de balans in de samenwerking met de *Chief Privacy Office* (CPO) om zo effectief mogelijk te zijn.

## 1.1 Uitgevoerd Toezicht

***Naleving AVG en RGMO DOPS***: De FG voerde in 2023 een toezichtbezoek uit bij de Directie Operaties (DOPS). Het betrof een onderzoek naar de naleving van de wet- en regelgeving rondom de AVG en de Regeling Gegevensbescherming Militaire Operaties (RGMO). Voor de borging van de naleving van de AVG, UAvg en de RGMO en daarmee de bescherming van persoonsgegevens is van belang dat er voldoende capaciteit, kennis en kunde beschikbaar is binnen de DOPS en ook breder binnen de defensiestaf. Ontwikkelingen, zoals IGO, brengen een aanvullende complexiteit en risico voor de naleving van de wet- en regelgeving rondom *privacy* en een toenemende kans met zich mee op een niet-rechtmatige en/of niet-proportionele inbreuk op de persoonlijke levenssfeer van betrokkenen. Uit het toezichtbezoek blijkt dat bij de DOPS meer structurele aandacht nodig is voor de naleving van de richtlijnen. Om een professionaliseringsslag te kunnen maken is versteviging van de AVG-coördinatorrol Militaire Operaties nodig. De FG adviseert zorg te dragen voor voldoende en toereikende *privacy*-kennis en -deskundigheid, in relatie tot operationele defensieprocessen, door de invulling van de AVG-coördinatorrol bij de defensiestaf beter te borgen. Tevens is meer aandacht bij de defensiestaf nodig voor bewustwording, *onboarding* en opleidingen met betrekking tot de AVG en de RGMO.

***Verantwoordingsplicht Register van verwerkingsactiviteiten***: De FG voerde in 2023 een themaonderzoek uit naar de opbouw en kwaliteit (volledigheid, juistheid en actualiteit) van het register van verwerkings-activiteiten van Defensie[1]. Om de naleving van de AVG en de WPG aan te kunnen tonen, dient de verwerkingsverantwoordelijke van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden een register op te stellen en bij te houden. Deze registerplicht is een van de belangrijkste maatregelen om de verantwoordingsplicht te waarborgen. Naast verantwoording draagt een goed register ook bij aan transparantie, het beheersen van risico's en ondersteunt het bij toezicht. Het Ministerie van

[1] FG-onderzoek naar de naleving van de registerplicht en de kwaliteit van het Register van Verwerkingsactiviteiten. BS2023034055. 8 november 2023.

Defensie maakt gebruikt van een rijksbrede applicatie voor het Register van Verwerkingsactiviteiten (voor zowel de AVG als de WPG). Sinds de ingebruikname in 2018 is veel informatie over de verwerkingsactiviteiten bij elkaar gebracht en zijn meerdere acties uitgevoerd om de juistheid en volledigheid te verbeteren. De FG constateerde dat er echter een aantal factoren zijn die veroorzaken dat het register minder bruikbaar is om aan de doelen van de registerplicht te voldoen; bijvoorbeeld dat er te beperkt richtlijnen of instructies beschikbaar zijn voor het op uniforme wijze opbouwen en indelen van het register. Er is ook geen duidelijke keuze gemaakt in uitgangspunten voor het abstractieniveau, de opbouw en de invulling van het register. Tijdens het toezichtonderzoek zijn tekortkomingen geconstateerd in de inhoudelijke kwaliteit van de registraties en tevens dat er maatregelen ontbreken om de kwaliteit te borgen, zoals de juistheid en actualiteit. Verbeterslagen leidden tot goede herzieningen, maar door ontbrekende richtlijnen en beheersingsmaatregelen is de kwaliteit nog onvoldoende geborgd. Deels is dit veroorzaakt door de beperkte beschikbare capaciteit van de *privacy*-organisatie. De FG deed aanbevelingen met betrekking tot het opstellen van intern beleid en aanvullende handreikingen. Tevens gaf de FG adviezen over het vaststellen van nadere richtlijnen voor de interpretatie en harmonisatie van de toepassing van verwerkingsgrondslagen en het opstellen van een procedure voor het periodiek *reviewen* van registraties in het register om de kwaliteit te verbeteren.

***Onderzoek privacy-organisatie***[2]: De FG voerde in 2023 een onderzoek uit naar de positionering, kennis, capaciteit (formatie) en middelen van de AVG-coördinatoren en de WPG-privacyfunctionaris. De mate waarin deze zaken goed zijn ingeregeld, draagt bij aan in hoeverre de AVG-coördinatoren en WPG-privacyfunctionaris effectief kunnen bijgedragen aan de naleving van de AVG en WPG. Gelet op de ontwikkelingen bij Defensie nemen de werkzaamheden van de AVG-coördinator en WPG-privacyfunctionaris toe en worden ze complexer. De belangrijkste bevindingen zijn dat er geen eenduidige lijn is met betrekking tot de organisatorische plaatsing van de AVG-coördinatoren, de personele capaciteit (nog) niet passend is bij de taken/verantwoordelijkheden en dat het bij een aantal defensieonderdelen geen voltijdfunctie is. Een aantal defensieonderdelen investeerde de afgelopen jaren in de personele capaciteit. Desondanks wordt in bijna alle gevallen aangegeven dat de capaciteit niet aansluit bij alle taken en verantwoordelijken van de AVG-coördinator en WPG-privacyfunctionaris. De aanbevelingen van de FG zien dan ook toe op het uitbreiden van de personele capaciteit, het omzetten van het AVG-coördinatorschap in voltijdfuncties/ *dedicated* functies waar dit nog niet het geval is en het kritisch bekijken van de organisatorische plaatsing van de AVG-coördinator en WPG-privacyfunctionaris.

***KMar & Bestuursstaf Gegevensuitwisseling CARIB-NL***: De FG verzocht begin 2023 C-KMar[3] aan te geven welke interne verbetermaatregelen zijn genomen om een aantal eerder gesignaleerde knelpunten op te lossen, met betrekking tot het ontbreken van het benodigde inzicht in de wettelijke kaders, gezagsrelaties en relevante informatiesystemen rond de activiteiten van de KMar in het Caribisch gebied. Dit inzicht is essentieel voor de naleving van de gegevensbeschermingswetgeving en voor adequate inrichting en het beheer van de organisatie. De FG ontving in augustus 2023 de visie van de KMar[4] op het wettelijke kader. De nota beschrijft onder andere de wettelijke basis, het doel en de focus van de inzet van de KMar in Caribisch Nederland. Daarnaast stelde de KMar een nota[5] op die inzicht biedt in welke politietaken en daaraan gerelateerde gewelds- en opsporingsbevoegdheden en geweldsmiddelen de KMar heeft op de eigenstandige eilanden Curaçao, Aruba en Sint Maarten, en de eilanden Bonaire, Sint Eustatius en Saba en wie het gezag toekomt. De activiteiten om het inzicht op de naleving van de gegevensbeschermingswetgeving in het Caribisch gebeid te verbeteren worden in 2024 voortgezet.

[2] FG-Onderzoek *privacy*-organisatie; positionering van de AVG-coördinator en WPG-privacyfunctionaris binnen de organisatie delen van het Ministerie van Defensie. BS2024004414. 14 februari 2024.
[3] Nota Gegevensverwerkingen KMar Carib. 8 december 2022. BS2022031914.
[4] Visie Koninklijke Marechaussee in het Caribisch deel van het Koninkrijk. 7 augustus 2023. Definitief.
[5] Nota Overzicht Politietaken, bevoegdheden en gezet in de Carib. 11 juli 2023. KMar2023004496.

***Stand van zaken naleving WPG***: De Auditdienst Rijk (ADR) voerde in 2022 bij de KMar de vierjaarlijkse wettelijk verplichte externe *(privacy) audit* uit over de periode 2015-2018. Deze externe *audit* diende uiterlijk 2020 afgerond te zijn, maar heeft door omstandigheden vertraging opgelopen. De AP is hierover geïnformeerd en ontving een afschrift van het *audit*-rapport[6]. De verwerkingsverantwoordelijke diende binnen drie maanden na ontvangst van het rapport van de ADR een verbeterrapport op te stellen, waarin de maatregelen staan die getroffen zijn of worden, ter verbetering van de geconstateerde tekortkomingen. De FG vroeg eind 2023 een *update* aan[7] van de stand van zaken van de verbetermaatregelen. De KMar heeft wegens capaciteitsgebrek geen verbeterrapport opgesteld. De hoeveelheid WPG-werkzaamheden bij de KMar is groter dan door de huidige privacyfunctionaris kon worden uitgevoerd in 2023. De KMar nam al wel enkele maatregelen die moeten leiden tot verbetering van de naleving van de WPG. Aan de KMar is budget toegekend voor additionele capaciteit om structurele monitoring op de naleving van de WPG te verbeteren, verbetermaatregelen te implementeren en aan de verplichting van het uitvoeren van jaarlijkse interne audits te voldoen. Wegens verplichtingen gekoppeld aan de reorganisatietraject is het pas eind 2024 mogelijk om de additionele capaciteit te werven. Het is de verwachting dat in Q1 van 2025 deze functionarissen daadwerkelijk in dienst zijn [8].

***Programma Defensie Open op Orde (DOO)***: De FG vroeg in de loop van 2023 veelvuldig aandacht[9] voor het borgen van de naleving van de AVG/WPG binnen de ontwikkelingen van het programma DOO. In het programmaplan DOO, de actualisatie van het programmaplan en het uitvoeringsplan 2023 worden de verschillende projecten en deelprojecten en de stand van zaken ervan toegelicht. In geen van deze documenten worden echter de *privacy*-risico's en -maatregelen en de naleving van de relevante gegevensbeschermingswetgeving geadresseerd. Meerdere van de activiteiten die gedefinieerd zijn in de verschillende (sub-)projecten leiden tot het verwerken van persoonsgegevens (of politiegegevens), inclusief bijzondere en gevoelige persoonsgegevens. Voorbeelden hiervan zijn e-mailarchivering van *Messenger services*, *chat*-archivering, ontsluiten van missie-informatie met behulp van kunstmatige intelligentie, het openbaar maken van informatie en het gebruik van geautomatiseerde anonimisering- en lak-*software* hiervoor, burgerbrieven vastleggen en het inrichten van de loketfunctie hiervoor. Voor deze en andere *pilots*, ontwikkelingen en applicaties in het kader van het DOO-programma geldt dat toereikende maatregelen moeten zijn geïmplementeerd om te voorkomen dat persoonsgegevens onnodig of onrechtmatig worden verwerkt, of dat er onbedoeld toegang is tot persoonsgegevens en om er zorg voor te dragen dat persoonsgegevens tijdig worden verwijderd enzovoort. In 2023 kon de DOO-programma-directie dergelijke maatregelen echter nog niet (voldoende) concreet en aantoonbaar maken richting de FG. Ook is het niet duidelijk of de benodigde *privacy*-kennis en -capaciteit voor het in kaart brengen en implementeren van deze maatregelen binnen DOO aanwezig is. Gelet op de aard en omvang van de gegevensverwerkingen die bij de DOO-projecten zullen gaan plaatsvinden, leidt dit inmiddels tot enige zorgen bij de FG. Naast de stappen die DOO nog dient te maken, is ook verdergaand beleid en structureel toezicht op de ontwikkelingen benodigd om de keten van beleid, uitvoering en toezicht evenwichtig te benaderen. Aan de voorkant moeten afdoende maatregelen worden genomen om de naleving te kunnen waarborgen van de wet- en regelgeving rondom de bescherming van persoonsgegevens vanuit de AVG en WPG.

***Loggingplicht politiegegevens***: De WPG bevat een verplichting in artikel 32a voor de verwerkingsverantwoordelijke om logbestanden bij te houden van ten minste de verzameling, wijziging, raadpleging, verstrekking onder meer in de vorm van doorgiften, het combineren en vernietigen van politiegegevens. De logbestanden moeten het mogelijk maken de redenen, de datum en het tijdstip van die handelingen en indien mogelijk de identiteit te achterhalen van de persoon die de politiegegevens heeft geraadpleegd of heeft bekendgemaakt, en de identiteit van de ontvangers van die politiegegevens. Deze verplichting diende uiterlijk per 1 november 2023 doorgevoerd te zijn in de geautomatiseerde systemen van de KMar. De FG voor de WPG monitorde gedurende 2023 periodiek de status van de realisatie hiervan. Het project

[6] Zie BS2023005724, 23 februari 2023
[7] Nota Stand van zaken Wpg. BS2023036084. 21 november 2023.
[8] Antwoordnota Stand van zaken Wpg. 2024000506. 8 januari 2024.
[9] Nota DOO. BS2023017197. 7 juni 2023.

Monitoring op Logging is gericht op de benodigde aanpassingen aan de KMar-systemen om te voldoen aan de loggingplicht en daarnaast de geautomatiseerde monitoring van de logbestanden in te richten. De KMar heeft nog niet volledig voldaan aan de loggingplicht. De verwachting van de KMar is vooralsnog dat het project eind december 2024 is afgerond[10].

***CLAS/BIDKL***: de Bergings- en Identificatiedienst Koninklijke Landmacht (BIDKL) is verantwoordelijk voor het opsporen, bergen en identificeren van slachtoffers uit de Tweede Wereldoorlog. Het zekerstellen van de identiteit is alleen mogelijk door middel van DNA-onderzoek van potentiële verwanten. De FG voerde in 2022 een toezichtbezoek uit bij BIDKL. Het Commando Landstrijdkrachten (CLAS) zette diverse (verbeter) acties in gang naar aanleiding hiervan, zoals het opstellen van een DPIA. Door de complexiteit van het dossier konden de verbeteracties in 2023 niet afgerond worden. Een vervolgonderzoek naar de realisatie van de acties zal plaatsvinden in 2024.

***Robotics Proces Automation (RPA)***: In 2023 voerde de FG een verkennend toezichtbezoek uit bij DOSCO met betrekking tot het onderwerp *Robotics Process Automation* (RPA). RPA is een automatiseringsproces en houdt kortgezegd in dat binnen bepaalde werkprocessen de handelingen niet meer door een defensiemedewerker worden verricht, maar door een (scherm)robot. Het gaat bijvoorbeeld om het geautomatiseerd overzetten van data vanuit de ene applicatie naar de andere. Aanleiding van het bezoek is de ingebruikname van *chatbots* en de groei van het aantal defensieonderdelen dat van RPA gebruik maakt. De projectgroep herziet de DPIA. Inmiddels heeft een eerste inventarisatie plaatsgevonden van de addenda op de huidige DPIA en vindt er een vervolgtoezichtbezoek plaats in 2024.

***Toezichtbezoek MQ-9***: De MQ-9 Reaper is een onbemand vliegend wapensysteem (*Remotely Piloted Aircraft System*, RPAS), dat ingezet kan worden voor het verzamelen van informatie ten behoeve van inlichtingen. In 2023 voerde de FG ad hoc-toezicht uit om een beter beeld te krijgen van de mogelijke soort gegevens die verzameld worden tijdens de inzet van de MQ-9, en het gebruik van die gegevens. Naar aanleiding van het bezoek actualiseerde CLSK de DPIA. Bij iedere inzet van de MQ-9 zou een annex geschreven moeten worden met operatiespecifieke zaken, zoals het vigerende juridisch kader, zaken rondom communicatie en operatiespecifieke mitigerende maatregelen. Deze bijlage biedt dan – tezamen met de geactualiseerde DPIA en indien de operatie dit toelaat – een (concreet) handelingskader.

***Toezichtonderzoek melden en afhandelen inbreuk op de beveiliging/datalek***: In het laatste kwartaal van 2023 startte de FG een toezichtonderzoek naar de wijze waarop Defensie inbreuken op de beveiliging behandeld, die per ongeluk of op onrechtmatige wijze leiden tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Naar aanleiding van de voorverkenning stelde de FG een tussentijdse nota op met bevindingen[11]. De voornaamste bevindingen uit de voorverkenning betroffen verbeterpunten met betrekking tot de Peoplesoft Melden Voorvallen (PSMV)-applicatie. De FG constateerde dat er een brede, mogelijke niet noodzakelijke, toegang is tot meldingen waarbij ook persoonsgegevens van de melder inzichtelijk zijn, dat er onvoldoende dataminimalisatie is toegepast op de gegevens van de melder die verwerkt worden, dat de handleiding en aanwijzingen geactualiseerd moeten worden en dat de interne datalekregisters verbeterd moeten worden. De CPO stelde een nieuw defensiebreed *format* op voor het interne datalekregister, dat in het eerste kwartaal van 2024 in gebruik zal worden genomen. In 2024 wordt dit onderzoek voortgezet, waarbij de stand van zaken van de verbetermaatregelen wordt meegenomen.

[10] Nota niet voldoen aan loggingplicht art. 32a Wpg. KMar2023008888. 28 november 2023.
[11] Voorlopige bevindingen melden en afhandelen voorvallen (mogelijke datalekken). BS2023034031. 6 november 2023.

***Vaststellen ID naar aanleiding van klimaatactie Schiphol***: Medio 2023 ontstond uit mediaberichten het beeld dat de KMar mogelijk op onjuiste of onzorgvuldige wijze persoonsgegevens had verwerkt bij de aanhouding van klimaatdemonstranten. In de berichtgeving werd gemeld dat de KMar daarbij gebruik had gemaakt van geautomatiseerde gezichtsherkenningssoftware (CATCH). Op 5 november 2022 drongen circa 400 klimaatdemonstranten illegaal het beveiligde gedeelte (*Airside Demarcated Area*) van het luchtvaartterrein op Schiphol-Oost binnen. Omdat het onbevoegd betreden van beveiligde delen van het luchtvaartterrein een misdrijf is, werden de demonstranten door de KMar van het terrein verwijderd en aangehouden als verdachten. Meerdere personen die niet aanwezig waren bij het protest gaven in juli 2023, deels via openbare nieuwsmedia te kennen dat zij ten onrechte een waarschuwingsbrief van het Openbaar Ministerie (OM) ontvingen op hun woonadres. Enkele tientallen betrokkenen hebben hierover klachten ingediend bij het OM, het Ministerie van Defensie en de KMar, en verzochten om correctie of verwijdering van hun persoonsgegevens. Dit was voor de FG aanleiding om een onderzoek te starten naar de vraag of de KMar op Schiphol op onjuiste of onzorgvuldige wijze persoonsgegevens had verwerkt bij de ID-vaststelling van de aangehouden demonstranten. Het onderzoek van de FG richtte zich op de naleving van de WPG en het waarborgen van de kwaliteit en de rechtmatigheid van de verwerking van politiegegevens door de KMar onder beheer van het Ministerie van Defensie. Het eindrapport is begin 2024 aangeboden aan de Minister van Defensie, SG en C-KMar. Aan de AP is desgevraagd een afschrift van het rapport verstrekt. Gebleken is dat geautomatiseerde gezichtsherkenning geen rol van betekenis heeft gespeeld bij de ID-vaststelling en het strafrechtelijke onderzoek naar de klimaatacties op Schiphol. De FG stelde een aantal andere tekortkomingen vast, waarop aanbevelingen voor verbetering worden voorgesteld. Dit heeft met name betrekking op het verbeteren van de afstemming tussen het OM en de KMar, het opstellen van betere instructies rond openbronnenonderzoek en het ontbreken van instellingsprotocollen voor herkennings- en signaleringslijsten.

***Procedure melden en behandelen van (potentiële) datalekken***: Meldingen van datalekken die een (hoog) risico opleveren voor de *privacy* van de betrokkenen worden, na afstemming met de FG, door verwerkingsverantwoordelijken extern gemeld aan de AP en aan betrokkenen. De FG hield gedurende het gehele 2023 toezicht hierop. Behalve dat een datalek aanleiding kan zijn voor een toezichtbezoek, worden, mede op advies van de FG, maatregelen voorgesteld die een herhaling van een vergelijkbaar datalek in de toekomst moeten voorkomen.

***Onderzoek verwerkersovereenkomsten***: De ADR startte in opdracht van de FG in 2023 met een onderzoek bij de defensieonderdelen naar het afsluiten van verwerkersovereenkomsten. In het eerste kwartaal van 2024 wordt het rapport opgeleverd.

Toezichtonderzoeken bij het Dienstencentrum Personeelslogistiek (DCPL) en het semi-statisch archief van de KMar die gepland waren voor 2023, zijn in verband met onvoldoende capaciteit van de FG verzet naar 2024.

# 2 Hoofdlijnen uit het toezicht

## 2.1 Verantwoording

In de 'Regeling AVG Defensie' is vastgelegd dat de AVG-beheerder jaarlijks rapporteert over de naleving van de AVG binnen zijn onderdeel. De 'Regeling WPG Defensie' bevat een vergelijkbare rapportage-verplichting voor de WPG-beheerder. Alle AVG-beheerders en de WPG-beheerder leverden de jaarrapportage aan. Met betrekking tot de Bestuursstaf is er gerapporteerd over de naleving van de AVG en Defensiebrede verwerkingen. Er is niet gerapporteerd over de naleving van de RGMO.

## 2.2 AVG- en WPG-organisatie

### Organisatorische ontwikkelingen toezicht en beleid

De beoogde scheiding tussen de Beleidsfunctie belegd bij de CPO en de Toezichtfunctie belegd bij de FG-Unit komt inmiddels duidelijker naar voren in de organisatiestructuur. Ten behoeve van de onafhankelijkheid en transparantie is de toezichtcapaciteit (FG-unit) met ingang van 2023 als Bijzondere Organisatie Eenheid (BOE) onder de P-SG ingericht en administratief ondergebracht bij de Inspectie Veiligheid Defensie (IVD). Daarnaast is de FG-unit in de loop van 2023 versterkt met aanvullende personele onderzoekscapaciteit. In 2024 wordt de FG-unit verder versterkt met een 'kwartiermakers-functie' om complexe toezichtprocessen op het gebied van gegevensbescherming te coördineren en de visie en strategie te bepalen voor het toezicht op AI en algoritmes binnen Defensie. De CPO is belegd bij het Directoraat-Generaal Beleid (DGB) en is eveneens versterkt met extra personele capaciteit.

### AVG-coördinatoren en WPG-privacyfunctionaris

Conform de Regeling AVG Defensie wezen alle AVG-beheerders een AVG-coördinator aan. De DOPS wees, conform de RGMO[12], een AVG-coördinator Militaire Operaties aan. Conform artikel 34 van de WPG wees C-KMar een privacyfunctionaris aan. De AVG-coördinator en de privacyfunctionaris hebben een cruciale rol bij de naleving van de AVG en de WPG in de praktijk bij Defensie.

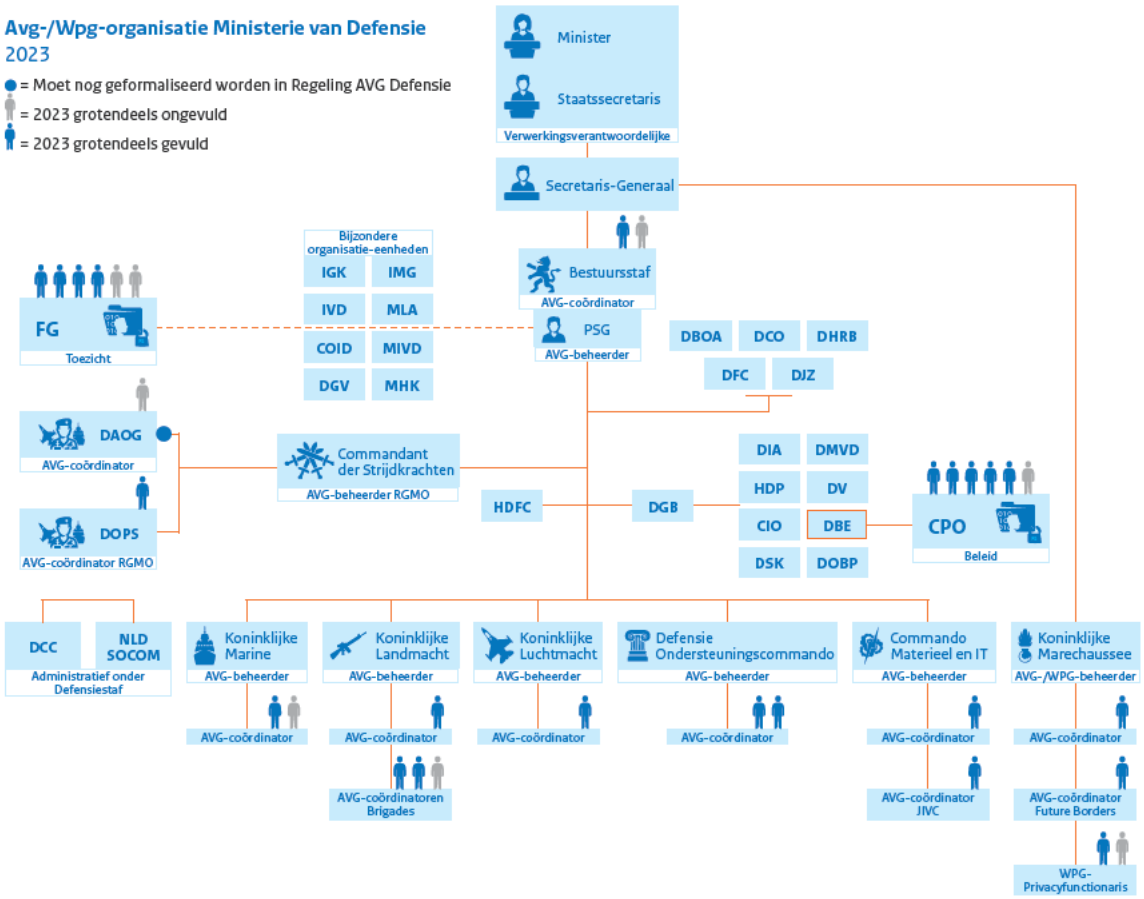
In het Toezichtjaarverslag FG 2021 en 2022 staat de aanbeveling om de *privacy*-organisatie te versterken en te professionaliseren. Dit betreft naast het kennisniveau en de samenwerking met de operationele en juridische lijn ook het zorgdragen voor een duidelijk(e) *privacy*-beleid en -kaders, en het zorgdragen voor *tools* ter ondersteuning van de werkzaamheden. In 2023 voerde de FG een toezichtonderzoek uit naar de positionering, kennis, capaciteit en middelen van de AVG-coördinatoren en de WPG-privacyfunctionaris (zie ook onder hoofdstuk 1). Op het vlak van personeel is een aantal ontwikkelingen zichtbaar, ter versterking van de *privacy*-organisatie. Zo startte bijvoorbeeld een tweede AVG-coördinator bij het CZSK en kwamen er extra AVG-brigadecoördinatoren bij het CLAS[13]. Ook is aandacht besteed aan het vergroten van kennis van de *privacy*-organisatie; zo is er in 2023 wederom een CIPP/E en een DPIA-training georganiseerd en is er een CIPM-training georganiseerd. Zoals al eerder vermeld wordt er echter nog steeds door de defensieonderdelen over het algemeen gesteld dat de personele capaciteit nog niet passend is, gelet op alle taken/verantwoordelijkheden. Dit, terwijl de organisatie meer behoefte heeft aan diepgaandere kennis en kunde op het gebied van *privacy* en gegevensbescherming. Onder andere omdat de vraagstukken complexer worden en ontwikkelingen zich in een spanningsveld bevinden ten opzichte van de wetgeving. De behoefte van het CLSK aan een tweede AVG-coördinator wordt in 2024 gerealiseerd. De tweede WPG-privacyfunctionaris bij de KMar is een groot gedeelte van 2023 vacant geweest, maar wordt in het eerste kwartaal 2024 gevuld. Ook bij de DOPS is er met het coördinatorschap als neventaak onvoldoende capaciteit om de taken vakkundig uit te voeren. Ten behoeve van de Bestuursstaf (apparaat) en voor defensiebrede verwerkingen (BS-breed) wordt uitbreiding verwacht in 2024.

[12] Artikel 6, Regeling Gegevensbescherming Militaire Operaties.
[13] Naar verwachting bestaat de AVG-organisatie bij de CLAS in 2024 uit een AVG-coördinator en vier AVG-brigadecoördinatoren.

Daarnaast geven AVG-coördinatoren aan dat de opleidingen meer toegespitst zouden kunnen worden op de toepassing bij Defensie en dat er voor de WPG weinig opleidingsaanbod beschikbaar is. In 2023 ontwikkelde de CPO hiertoe een opleidingsprogramma voor de *privacy*-organisatie.

Een van de aanbevelingen uit het Toezichtjaarverslag FG 2021 is zorgen voor intensivering van de samenwerking met de operationele en juridisch lijn. De inrichting van een decentraal *Chief information Office*-stelsel (CIO) vraagt eveneens aandacht voor raakvlakken en versterking op het gebied van gegevensbescherming. De organisatorische plaatsing van de AVG-coördinator kan van invloed zijn op de samenwerking en invloed hebben op de slagkracht van de AVG-coördinator. De organisatorische plaatsing dient een goede samenwerking met de operationele-, beveiligings- en juridische lijn te faciliteren. Daarnaast is het belangrijk dat de afstand en communicatielijnen tot de AVG-beheerder kort zijn, zodat de AVG-beheerder betrokken blijft bij het zorgdragen van de AVG-naleving van het defensieonderdeel. Op dit moment is er geen eenduidige lijn te herkennen in de organisatorische plaatsing van de AVG-coördinator en WPG-privacyfunctionaris. De verschillende posities brengen specifieke voor- en nadelen met zich mee. Zo kan een plaatsing binnen HR/P&O-afdelingen ervoor zorgen dat de focus vooral op de verwerking van personeelsgegevens ligt en kan een decentrale plek binnen een onderdeel zorgen voor een (te) grote afstand tot de AVG-(onder)beheerder. Het risico van een grotere afstand tot de AVG-beheerder is dat de AVG-naleving in de praktijk de verantwoordelijkheid van de AVG-coördinator wordt.

***Zie verder Bijlage A.***




Figuur 1: Organogram met indicatief beeld van de vulling van de privacy-organisatie in 2023

## 2.3 Bewustwording

Alle defensieonderdelen, met uitzondering van de DOPS, voerden in 2023 diverse bewustwordingsactiviteiten uit, zoals voorlichting, presentaties en colleges. Daarnaast is er voor alle defensiemedewerkers een intranetsite over beveiliging en *privacy* beschikbaar. Enkele onderdelen verzorgden onlinetrainingen. In 2023 organiseerde de privacy- en beveiligingsorganisatie ook een *Privacy & Security week*.

Een aandachtspunt is het structureel borgen van bewustwordingsactiviteiten, bijvoorbeeld met een *awareness*-programma, en het meten van de effectiviteit van de bewustwordingsactiviteiten. Er is geen doorlopend *privacy awareness*-programma binnen Defensie. De CPO startte in 2023, in samenspraak met de FG, met een plan hiervoor. Een tweede aandachtspunt is het structureel inrichten van het bevorderen van bewustwording door aandacht bij het *onboardings*-proces en voorlichting aan nieuwe medewerkers.

Er is vanuit de organisatie (voornamelijk vanuit opleidingen) een groeiende vraag naar het gebruik van *smart devices*. Hoewel het bewustzijn is gegroeid dat hierbij rekening moet worden gehouden met de AVG, lijkt er ook een neiging te zijn om wegen te bedenken om buiten de kaders van de AVG te opereren.

## 2.4 Verwerkersovereenkomsten

Wanneer Defensie gebruik maakt van een verwerker, dient een verwerkersovereenkomst (of andere rechtshandeling, zoals een convenant of een verwerkersafspraak) opgesteld te worden. Er is geen actueel en volledig overzicht beschikbaar voor de FG of verwerkersovereenkomsten zijn afgesloten voor alle verwerkingen waarbij er sprake is van een verwerker. Dit vormt een risico met betrekking tot de naleving van de AVG en voor de bescherming van persoonsgegevens, bijvoorbeeld doordat de beveiliging niet voldoet aan de eisen van Defensie. De gevolgen bij een datalek kunnen groter zijn indien er geen adequate afspraken zijn over de afhandeling.

Verwervers/inkopers zijn verplicht om een verwerkersovereenkomst te registeren in het contractenregister van SAP M&F. In het contractregister van SAP M&F staan 44 verwerkersovereenkomsten geregistreerd, waarvan een deel voor dezelfde verwerking. Voor de meeste van deze overeenkomsten kan geen koppeling gemaakt worden met de verwerkingen in het register van verwerkingsactiviteiten.

Ook dient, conform de Regelingen AVG en WPG Defensie, een verwerkersovereenkomst in het register van verwerkingsactiviteiten te worden opgenomen. In de praktijk worden bijna geen verwerkers-overeenkomsten opgenomen in het AVG-register. Aangegeven is dat deze richtlijn niet wordt toegepast, omdat de overeenkomsten in het contractenregister SAP M&F worden opgenomen. Deze afwijking van de formele Regelingen is niet vastgelegd en bekrachtigd. Ook gaven een aantal AVG-coördinatoren aan dat ze weinig tot geen zicht hebben op het inkoopproces en de totstandkoming van de bijbehorende verwerkersovereenkomsten.

| Register van verwerkingsactiviteiten | 2023 |
|---|---|
| Aantal vastgestelde verwerkingen waarbij is aangegeven dat er sprake is van een verwerker | 130 |
| Aantal verwerkingen waarbij de verwerkersovereenkomst is toegevoegd in het register | 26 |
| In het contractregister SAP M&F opgenomen verwerkersovereenkomsten | 44 |

Een deel van het verschil in aantallen wordt veroorzaakt doordat het register van verwerkingsactiviteiten op dit element nog onjuistheden bevat, omdat er bijvoorbeeld ten onrechte wordt aangegeven dat er sprake is van een verwerker.

## 2.5 Register van verwerkingsactiviteiten

De verwerkersverantwoordelijke dient in het kader van zijn verantwoordingsplicht een register bij te houden van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. De registerplicht is een vereiste volgens zowel de AVG als de WPG. Het register van verwerkingsactiviteiten bevat basisinformatie over door 'wie', 'waar', 'waarom' en 'waarmee' persoonsgegevens worden verwerkt binnen organisaties. Zie paragraaf 1.1 voor de uitkomsten van het door de FG uitgevoerde themaonderzoek naar de opbouw en kwaliteit van het register van verwerkingsactiviteiten.

## 2.6 Data Protection Impact Assessment

De FG houdt toezicht op de uitvoering van de *Data Protection Impact Assessments* (DPIA's). Een DPIA is een wettelijk verplicht instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen en om de maatregelen om deze risico's te verkleinen te bepalen. Bij het opstellen van een DPIA, alvorens met een hoog risicoverwerking wordt aangevangen, wint Defensie verplicht advies in bij de FG. In 2023 ontving de FG 33 DPIA's of addenda op DPIA's ter advies, waarvan een beleids-DPIA. Als er ondanks de voorgenomen maatregelen onvoldoende zekerheid kan worden geboden dat de verwerking in overeenstemming is met de AVG of de WPG, kan de verwerking niet aanvangen (of worden voortgezet).

| | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 |
|---|---|---|---|---|---|---|
| Voorgelegd aan FG ter appreciatie of consultatie (incl. addenda) | 33 | 23 | 17 | 17 | 11 | 4 |
| Vastgesteld/Gereed voor vaststelling | 9 | 19 | 13 | 9 | 9 | 12 |
| Actualisering/wijziging bestaande DPIA | 6 | | | | | |
| Lopend | 34 | | | | | |

Het verplichte karakter van de DPIA, de complexiteit en de benodigde kwaliteit en zekerheid waarmee de technische- en juridische kaders van het proces beschreven dienen te zijn, leiden soms tot een lange doorlooptijd. Lange doorlooptijden van de DPIA's doen afbreuk aan de naleving van de geldende gegevensbescherming wetgeving. Dit onderstreept de noodzaak om het DPIA-proces tijdig op te starten, het in teamverband op te stellen en de risico's voor de *privacy* goed te analyseren. Uit door de FG uitgevoerde appreciaties blijkt nog een ontoereikende kwaliteit van de DPIA's, waardoor DPIA's soms meerdere keren voor appreciatie moeten worden aangeboden.

De CPO was in 2023 bezig met het opstellen van een DPIA-procedure ter verbetering van het proces en tevens zijn DPIA-trainingen georganiseerd. Tevens heeft de CPO een pre-DPIA *scan model* geïntroduceerd om te bepalen of voor een verwerking een DPIA moet worden opgesteld. Aanvullend hieraan werkte de FG-unit de kwaliteitseisen uit waarop ze de DPIA's beoordelen, en deze beschikbaar gesteld. Naar verwachting stelt de CPO in 2024 de DPIA-procedure vast.

Naast het realiseren van de DPIA's is het van belang dat onder andere de adviezen en maatregelen uit DPIA's ook daadwerkelijk door de organisatie worden opgepakt, zodat zij niet enkel een papieren werkelijkheid blijven. Dit blijft een aandachtspunt.

Een DPIA uitvoeren is niet een eenmalige opdracht, maar een continu proces. Er moet blijvend gemonitord worden of er veranderingen zijn in de gegevensverwerking, de risico's van de verwerking en de context van de verwerking, die aanpassing van de DPIA nodig maken. Het is een goede praktijk om een DPIA continu te herzien en regelmatig opnieuw te beoordelen. Deze periodieke herziening is nog een aandachtspunt.

## 2.7 Inbreuken/datalekken

Defensiemedewerkers melden inbreuken in verband met persoonsgegevens (potentiële datalekken) in het systeem 'PeopleSoft Melden Voorvallen'(PSMV-systeem) als 'privacy-voorval'. Dit kunnen meldingen zijn met betrekking tot een hack, verkeerd gestuurde persoonsgegevens, openstaande SharePoint-sites, verloren of gestolen gegevensdragers, datalekken bij verwerkers enzovoorts. De FG ontvangt een afschrift van de in het PSMV-systeem gemelde voorvallen die aangevinkt zijn als een 'privacy-voorval'. In 2023 ontving de FG 294 meldingen. Dit is een toename ten opzichte van voorgaande jaren. Het vergroten van de bewustwording over privacy en het belang van het melden van datalekken hebben hier mogelijk aan bijgedragen. In enkele van de gevallen leidde de melding tot het instellen van nader toezicht en is met defensieonderdelen contact geweest over het treffen van maatregelen ter verbetering van de processen.

| | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 |
|---|---|---|---|---|---|---|
| AVG-gerelateerde (PSMV-)meldingen | 290 | 197 | 154 | 156 | 95 | 75 |
| WPG-gerelateerde (PSMV-)meldingen | 4 | 0 | 1 | 5 | 9 | n.v.t. |

(Potentiële) datalekken dienen geregistreerd te worden in de interne datalekregisters van de defensieonderdelen. Omdat niet alle meldingen ook daadwerkelijk datalekken betreffen, beoordelen de AVG-coördinator of WPG-privacyfunctionaris eerst de meldingen en wordt, indien nodig, de FG geconsulteerd. Het aantal (285) datalekken in de registers is daarom ook lager dan het aantal ontvangen '*privacy*-voorval' meldingen.

| | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 |
|---|---|---|---|---|---|---|
| Intern geregistreerde inbreuken | 285 | 248 | 169 | 109 | - | - |

In 2023 meldde Defensie in totaal 29 datalekken bij de AP.

| | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 |
|---|---|---|---|---|---|---|
| Bij AP (extern) AVG gemelde datalekken | 29 | 19 | 16 | 15 | 14 | 16 |
| Bij AP (extern) WPG gemelde datalekken | 0 | 0 | 1 | 0 | 1 | n.v.t. |

De vaakst voorkomende datalekken bij Defensie zijn SharePoint-sites waarvan de autorisaties niet toereikend zijn ingericht, verkeerd/te breed verstuurde e-mails en datalekken verband houdend met het medisch dossier. In het geval van een datalek van medische gegevens doet de behandelende zorgmedewerker altijd een melding aan de betrokkene(n). In 2023 zijn er ook meerdere datalekken geweest van persoonsgegevens van defensiemedewerkers door *hacks* bij andere organisaties. Doordat dit vaak e-mail en telefoonnummers van defensiemedewerkers betreft, brengt dit een verhoogd risico van *phishing* en ongewenste benadering met zich mee.

Naar aanleiding van signalen dat het PSMV-systeem en het proces van melden voorvallen/datalekken verbetering behoeft, startte de FG in 2023 een onderzoek naar de procedure voor afhandeling. Zie ook paragraaf 1.1. Signalen zijn bijvoorbeeld dat AVG-voorvallen ten onrechte als beveiligingsincident of als integriteitskwestie worden aangemerkt in het PSMV-systeem, of dat de afhandeling door de leidinggevende te lang duurt. Dit kan problemen opleveren voor de naleving van de wettelijke termijn van melden binnen 72 uur aan de AP.

Ter verbetering van het afhandelen van datalekken wordt, zoals eerder aangegeven, in het eerste kwartaal van 2024 een nieuw centraal format van het interne datalek register in gebruik genomen en een instructie voor de afhandeling van datalekken vastgesteld.

## 2.8 Rechten van betrokkenen

De AVG en WPG kennen *privacy*-rechten toe aan betrokkenen. Daartoe is een proces 'rechten betrokkenen' ingericht voor zowel de AVG als de WPG. Externe verzoeken van betrokkenen kunnen via een daartoe ingerichte internetsite van Defensie worden ingediend. Voor medewerkers in werkelijke dienst geldt een vergelijkbaar proces via een intranetpagina van Defensie. Binnen Defensie bestaat een procedure ingericht voor de afhandeling van de verzoeken.

In 2023 kwamen er 2179 verzoeken binnen middels het online beschikbare formulier. De meeste betrokkenen doen informatie- of inzageverzoeken. Van de 2197 verzoeken leidden slechts enkele tot vragen bij de FG over het niet nakomen van de termijn van afhandeling. De organisatie handelde deze vragen af. De vertraging in afhandeling is met name veroorzaakt door een tekort aan personele capaciteit bij de afhandelende eenheid. Eind 2023 is de personele capaciteit voor het afhandelen aan verzoeken verhoogd.

Naast de verzoeken op grond van de AVG is er stijging te zien in het aantal informatieverzoeken dat door betrokkenen wordt gedaan op grond van de WPG. In 2023 kwamen 125 verzoeken binnen, ten opzichte van +/- 90 in 2022. Er zijn in het jaar 2023 geen informatieverzoeken volledig afgewezen op een van de in artikel 27 WPG genoemde gronden. Wel is in enkele gevallen een beroep gedaan op een uitzonderingsgrond uit dit artikel om specifieke informatie niet te delen met een betrokkene, zoals een actieve signalering met betrekking tot CTER.

In 2023 is zes keer beroep ingesteld en vier keer hoger beroep. De beroepen zien veelal op besluiten die zijn gemaakt naar aanleiding van informatieverzoeken. Gronden van beroep variëren tussen het idee van betrokkenen dat er informatie zou ontbreken in het besluit, tot het niet eens zijn met de formulering ervan.

Bij de FG kwamen in 2023 22 klachten binnen. Twaalf van deze klachten zijn naar aanleiding van de klimaatdemonstraties op 5 november 2022 op het terrein van luchthaven Schiphol (zie ook paragraaf 1.1). Deze klachten zijn nog in behandeling bij de klachtencommissie van de KMar. De overige klachten zijn behandeld en waar nodig verzocht de FG de organisatie om verbetermaatregelen te nemen.

Er lopen nog twee AVG-klachten waarvan de afwikkeling in 2024 wordt verwacht. Een klacht is in behandeling bij de bezwaarschriftencommissie van Defensie. De andere klacht is in behandeling bij de AP.

### Verder

In geval van overlijden van een medewerker of een ander zwaarwegend belang (bijvoorbeeld bij langdurige ziekte van een medewerker) kan het voorkomen dat het noodzakelijk is om, met ondersteuning van JIVC, toegang te verschaffen tot het digitale account van betrokkene. Hiervoor moet dan door de betreffende beveiligingscoördinator (BC) toestemming worden verleend. De daadwerkelijke vrijgave vindt vertrouwelijk plaats met gebruikmaking van een *two person concept*. Van een dergelijke toestemming wordt melding gemaakt bij de FG. In 2023 ontving de FG zes van dergelijke meldingen.

## 2.9 Verbetermaatregelen

In verschillende interne en externe onderzoeken deed de FG aanbevelingen ter verbetering van de naleving van de AVG en de WPG. Tevens staan in verschillende DPIA's op moment van vaststelling meerdere openstaande maatregelen aangegeven. Dit betreft maatregelen die nodig zijn om de aangegeven risico's van de verwerking te mitigeren. De defensieonderdelen zijn bezig met het realiseren van verbetermaatregelen. Het is onvoldoende inzichtelijk of alle onderdelen het overzicht en inzicht hebben in alle openstaande verbetermaatregelen, alsmede de status van de realisatie van verbetermaatregelen. Een ondersteunend systeem dat ervoor zorgt dat de realisatie van verbetermaatregelen wordt geborgd en bewaakt, ontbreekt. Hierna wordt ingegaan op de stand van zaken van een aantal verbetertrajecten.

De Commissie Brouwer (en eerdere rapporten van de FG, Eiffel en het JEKOI) wijst op toenemende spanning tussen nieuwe dreigingen en bestaande kaders en deed aanbevelingen voor tijdelijke en structurele oplossingen van knelpunten. Een van de door Defensie ingezette lijnen is de zogenaamde 'IGO-wasstraat'. Defensie onderzoekt de mogelijkheden en beperkingen van oefenen en gereedstelling in de informatieomgeving en hoe zij daarbij de ruimte binnen de bestaande juridische kaders zo goed mogelijk kan gebruiken. Onderdelen gaven aan welke activiteiten in de informatieomgeving niet binnen de bestaande wet- en regelgeving kunnen worden uitgevoerd. De defensieonderdelen hebben casussen aangereikt die geclusterd zijn naar thema en door een Expertisetafel worden geanalyseerd met als doel een adviesrapport inclusief oplossingsrichtingen. De experttafel bestaat uit een multidisciplinair team. De casus medische gegevens/medische inzetbaarheid is door de IGO-wasstraat afgerond met een adviesrapport inclusief oplossingsrichtingen. De afronding van de thema's staat gepland voor de eerste helft van 2024.

Eind 2022 bood de FG het rapport "Onderzoek naar *social media monitoring* bij het Ministerie van Defensie[14]" aan bewindspersonen aan, waarin een aantal aanbevelingen zijn gedaan. Een van de aanbevelingen was om zorg te dragen voor aanvullend beleid en richtlijnen voor het gebruik van *social media monitoring* en -*scraping tools*. Aan deze aanbeveling is nog geen uitvoering gegeven. Hoewel het ministerie van Binnenlandse Zaken wel een handreiking met juridisch kader heeft gepubliceerd om gemeenten meer duidelijkheid te geven over het gebruik van *social monitoring tools* en wat wel en niet is toegestaan bij het verrichten van onderzoek, zijn er nog geen richtlijnen voor de Rijksoverheid. In de loop van 2023 zijn wel door defensieonderdelen een beperkt aantal stappen genomen om verbeteringen te treffen. DPIA's voor communicatiebeleid/(sociale) mediamonitoring, beveiliging van de IT-Infrastructuur door de Defensie Cyber Security Center (DCSC) en de beleidsvisie IGO zijn uitgevoerd, maar nog niet vastgesteld. De DCSC heeft een externe partij gevraagd voor advies over de juridische onderbouwing van de wettelijke grondslag voor het verzamelen van informatie over cyberkwetsbaarheden in openbare bronnen. Bij het verzamelen van dergelijke informatie kunnen namelijk persoonsgegevens worden verwerkt en inbreuk worden gemaakt op de privacy (persoonlijke levenssfeer) van betrokkenen. De uitkomst hiervan ontving Defensie eind 2023.

Het toezicht op AI en algoritmes is in ontwikkeling. In 2023 werkte Defensie aan het uitbreiden en versterken van de monitoring op de ontwikkeling en de inzet van algoritmes die persoonsgegevens gebruiken.

[14] FG-onderzoek naar het gebruik van *social monitoring* en –*scraping tools*. BS20220020402. 29 augustus 2022.

In 2023 is uitvoering gegeven aan de aanbeveling in het FG-Toezichtjaarverslag 2022 om de positie en functie van de AVG-coördinator te versterken en te professionaliseren. Hiernaast is de aanstelling van een *Chief Privacy Officer* een belangrijke stap in het versterken en professionaliseren van de *privacy*-organisatie. Tevens kon de *privacy*-organisatie meerdere *privacy*-gerelateerde opleidingen volgen, is een DPIA-training georganiseerd, is een week van de *Privacy & Security* georganiseerd en is een kennisbank ingericht. Voor enkele onderdelen blijft echter de capaciteit ontoereikend en een aandachtspunt, wat zorgt voor een kwetsbaarheid binnen de *privacy*-organisatie.

De FG ontving de laatste jaren van meerdere onderdelen signalen over de behoefte aan meer *privacy*-beleid, duidelijke richtlijnen en defensiebrede standpunten, en de FG beval in het jaarverslag van 2022 aan om *privacy*-beleid en *privacy*- en juridische kaders op te stellen. Door de nieuw ingerichte CPO is in samenwerking met een aantal AVG-coördinatoren in 2023 een start gemaakt met het opstellen van een Defensie *privacy*- en gegevensbeschermingsbeleid. Tevens worden instructies opgesteld voor onder andere het opstellen van DPIA's en het behandelen van datalekken. Zoals eerder is aangegeven is tevens een kennisbank voor de *privacy*-organisatie opgesteld. Op de kennisbank zijn onder andere FAQ's opgenomen.

In 2021 en 2022 beval de FG aan om het volwassenheidsniveau van de gehele privacy-organisatie te verhogen. De *privacy*-organisatie bij de defensieonderdelen implementeerde de AVG met beperkte centrale sturing. Onvoldoende centrale sturing, de relatief lange doorlooptijd van de implementatie en de beperkingen van de beschikbare capaciteit hebben geleid tot een laag volwassenheidsniveau. Het *privacy*-volwassenheidsniveau nam in 2023 geleidelijk maar duidelijk toe, bijvoorbeeld door investeringen in capaciteit en opleidingen. De organisatie is bezig om dit uit te bouwen en vast te houden in 2024. Het instellen van een volwassenheidsmodel wordt meegenomen in Defensie *privacy*-beleid dat opgesteld wordt. Ook wordt in het *privacy*-beleid aandacht besteed aan het beter inrichten van de *privacy governance*.

In 2021 voerde de AP bij de KMar een *audit* uit op het Schengeninformatiesysteem (SIS II)[15]. Het onderzoek betrof een inventarisatie en *review* van de opzet en het bestaan van het stelsel van maatregelen en procedures (interne beheersing) gericht op de bescherming van persoonsgegevens in het SIS II. In dit onderzoek zijn meerdere aandachtspunten geconstateerd, zoals beleid voor bewaartermijnen, het tijdig verwijderen van het verstrijken van de bewaartermijnen, het zorgdragen van een jaarlijkse *privacy*-training voor medewerkers en het in kaart brengen van de rollen en verantwoordelijkheden in de keten. In de loop van 2022 en 2023 nam de KMar verbetermaatregelen. Op basis van dit vervolgtraject constateerde de AP[16] dat de voorgestelde en doorgevoerde verbeteringen voldoende zijn.

## Internationaal verband

De CPO zorgde in 2023 voor een *Memorandum of Understanding* (MoU) Gegevensbescherming Nederland-Duitsland. In de Duits-Nederlandse samenwerking wordt een veelvoud aan persoonsgegevens verwerkt, waarvoor nadere afspraken vastgelegd dienen te worden. Doelstelling van de MoU is het bieden van een raamwerk voor het maken van afspraken over de gezamenlijke verwerking van persoonsgegevens. De overeengekomen MoU is de basis voor deze afspraken. In 2024 wordt een NLD-DUI *Data Protection Committee* opgestart. Het comité heeft tot taak het geven van advies, opstellen van beleid, monitoren van (strategische) ontwikkelingen en het toezien op de naleving van de implementatie van de maatregelen in het kader van de MOU en vervolgafspraken. In 2024 richt het comité zich voornamelijk op het advies en de monitoringstaak.

[15] Onderzoek naar Schengen Informatiesysteem II, KMar. 14 september 2021. Wdn/nda/8394.
[16] Eindbrief verbetertraject Schengen Informatie Systeem (SIS). 14 september 2023. 2023-211679.

## 2.10 Wet politiegegevens

De hoeveelheid WPG-werkzaamheden bij de KMar was in 2023 groter dan de privacyfunctionaris kon uitvoeren. Vanwege onvoldoende capaciteit bij het cluster Juridische Zaken en een openstaande vacature kon de privacyfunctionaris in 2023 minder prioriteit geven aan een aantal taken. Een van deze taken betrof het uitvoeren van toezichtwerkzaamheden op de naleving van de WPG.

Bij de privacyfunctionaris komen vanuit de Staf, het LTC, het OTC en alle brigades vrijwel dagelijks meerdere vragen binnen over de WPG en daaraan gerelateerde onderwerpen. Daarnaast is er een stijging te zien in het aantal inzageverzoeken (125 in 2023) op basis van de WPG. Het beantwoorden van de advies vragen en inzage verzoeken vergt veel tijd van de privacyfunctionaris. Het aanbod aan werkzaamheden is groter dan de privacyfunctionarissen (waarvan 1 vacant in de tweede helft van 2023) kon worden afgehandeld.

De WPG kent een *audit*-verplichting op grond van artikel 33 WPG. Deze verplichting houdt in dat door middel van interne- en externe *audits* de opzet, het bestaan en de werking van de genomen maatregelen en procedures rond de naleving van de WPG worden beoordeeld. Deze *audits* dienen jaarlijks intern uitgevoerd te worden op deelaspecten van de WPG en eenmaal per vier jaar dient een volledige en onafhankelijke externe audit uitgevoerd te worden. De ADR voerde in 2022 de verplichte externe *(privacy) audit* van 2019 over de periode 2014-2018 uit. De ADR startte eind 2023 met de externe *audit* over de periode 2019-2022. Deze loopt door in 2024.

De interne *audits* over de jaren 2021-2023 voerde de KMar niet uit. Oorzaak hiervan is dat de interne *audit*-capaciteit in 2012 met de bezuinigingen is weggesneden. Zoals aangegeven in paragraaf 1.1 investeert de KMar in 2024 in het terugbrengen van interne *audit*-capaciteit.

De KMar stelde na het ADR-rapport 2015 - 2018, geen verbeterrapport op. Er is in 2023 wel gewerkt aan een aantal verbeteringen:

- In 2022 hanteerde de DPIA-werkgroep een hernieuwde aanpak voor het verder aanvullen van het verwerkingenregister. Hierbij wordt een toepassingslijst gebruikt, waarin de verschillende systemen van de KMar staan. Deze lijst wordt als aanknopingspunt gebruikt om de verwerkingsactiviteiten in het register verder toe te voegen. De verdere afstemming hiervan met de FG is begin 2023 afgerond, waarna op basis van deze nieuwe structuur een begin is gemaakt met het invullen van het register van verwerkingsactiviteiten.

- De privacyfunctionaris neemt deel aan een interdepartementaal overleg over het verstrekken van politiegegevens aan derde landen. In deze werkgroep wordt gewerkt aan een eenduidig toetsingskader voor verwerkingsverantwoordelijken, zodat zij kunnen beoordelen of een derde land passende waarborgen heeft voor de bescherming van de rechten van betrokkenen in juridisch bindende instrumenten.

- Er is een start gemaakt met het verbeteren van de tekortkomingen op de onderdelen zoals gerapporteerd in het ADR-externe audit-rapport 2025-2019. De KMar verbetert de elementen kennis & kunde, het verwijderen en vernietigen van politiegegevens, het archiveren van gegevens bij cultureel en historisch belang en het vastleggen van ondersteunende taken (art 13 WPG).

## 2.11 Samenwerking

Bij Defensie zijn verschillende toezichthouders actief. Samen controleren zij op thema's zoals gezondheidszorg, (vlieg)veiligheid, beveiliging, voedselveiligheid, stralingsbescherming en de bescherming van persoonsgegevens. De toezichthouders zijn: de Inspectie Veiligheid Defensie (IVD), de Inspectie Militaire Gezondheidszorg (IMG), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS), de Militaire Luchtvaart Autoriteit (MLA), de Directeur Bedrijfsvoering en Evaluatie in zijn rol als Beveiligingsautoriteit (BA) en de Functionarissen voor Gegevensbescherming (FG). Alle toezichthouders zijn onafhankelijk in hun oordeelsvorming en beschikken voor hun taakuitvoering over bijzondere bevoegdheden.

De interne toezichthouders bij Defensie overleggen periodiek met elkaar onder leiding van de Inspecteur-Generaal Veiligheid in het zogenaamde Toezichtberaad. Vanaf eind 2021 is de secretarisrol van dit overleg belegd bij het Ondersteuningsteam Toezicht.

Om de effectiviteit van het toezicht te vergroten, wordt nadrukkelijker en vaker onderling aansluiting gezocht tussen de interne toezichthouders. Voor de FG's zijn dit met name de IMG, de IVD en de BA. Binnen het Toezichtberaad is afgesproken dat de samenwerking wordt geïntensiveerd en dat ook de samenwerking met andere interne toezichthouders wordt gezocht. Dit zal vooral zichtbaar zijn in gezamenlijk toezichtbezoeken afleggen en combineren. Vanuit de FG-taken bezien is er veel belang bij het in samenwerking met de BA ontwikkelen van een gezamenlijk onderzoeks- en toetsingskader.

### Samenwerking binnen Defensie

In het kader van haar toezichthoudende taak heeft de FG binnen Defensie nauw contact met de AVG-coördinatoren en WPG-privacyfunctionaris als eerste contactpersoon bij de diverse defensieonderdelen. Hierbij geeft de FG ook incidenteel advies, zolang de toezichthoudende rol hiermee niet in het gedrang komt.

De Directie Juridische Zaken (DJZ) is belast met de tweedelijns juridische advisering rond defensiebrede beleidsvorming en juridische advisering omtrent vraagstukken van (politiek) principiële aard, ook ten aanzien van onderwerpen die raken aan de bescherming van persoonsgegevens. Intensivering van de samenwerking met de juridische en operationele lijn is van groot belang. In 2023 had de FG herhaaldelijk contact met DJZ, bijvoorbeeld aangaande de voorgenomen wijziging van de Ministeriële Regelingen AVG, WPG en RGMO en adviezen ten aanzien van internationale gegevensuitwisseling.

Enkele malen werkte de FG samen met de WOO-coördinator van het Ministerie van Defensie, toen in concrete situaties de bescherming van de persoonsgegevens en de openbaarheid van bestuur elkaar raakten.

Aangezien het toezichtdomein op het gebied van de AVG veel raakvlakken heeft met andere (toezicht) domeinen, zoals integriteit, documentaire informatievoorziening & beveiliging, zijn het afgelopen jaar de samenwerkingsverbanden ook op die vlakken geïntensiveerd. Tevens is aansluiting en ondersteuning gevonden bij de IVD als coördinerend toezichthouder en het Ondersteuningsteam Toezicht (OTT) van het Toezichtberaad. Dit betrof zowel organisatorische, juridische als facilitaire ondersteuning.

### Samenwerking buiten Defensie

Om haar taak goed uit te kunnen voeren, werkt de FG ook samen met personen en instanties buiten de defensieorganisatie. In 2023 had de FG meermaals contact met medewerkers van de AP.

## Het RPFG

De voor de FG AVG belangrijkste externe samenwerking vindt plaats in het Rijksplatform van Functionarissen voor de Gegevensbescherming (RPFG). Dit is het overleg van de FG's van de ministeries. Het belang van het RPFG is aanzienlijk toegenomen, gezien het toenemende aantal rijksbrede initiatieven en *shared service*-voorzieningen, waarbij ook persoonsgegevens worden verwerkt. Het RPFG wordt steeds meer een gesprekspartner in allerlei rijksbrede trajecten. Naar verwachting zal in 2024 het RPFG door middel van een Besluit als gremium worden geformaliseerd.

## Platform FG voor WPG en Wjsg

Sinds 2020 is ook een platform actief voor de Functionarissen voor Gegevensbescherming die, krachtens de Europese Richtlijn voor de verwerking van persoonsgegevens door bevoegde autoriteiten voor opsporing, vervolging van strafbare feiten en tenuitvoerlegging van straffen[17], zijn aangesteld op grond van de WPG en de Wet justitiële en strafvorderlijke gegevens (Wjsg). In 2023 is het platform verder vormgegeven en ingericht onder de naam LED-Werk.

[17] EU 2016/680 *Law Enforcement Directive*

# 3 Conclusies en aanbevelingen

In de FG-Toezichtjaarverslagen van de afgelopen jaren en in verschillende toezichtrapporten deed de FG-aanbevelingen ter verbetering van de naleving van de AVG en de WPG. De defensieorganisatie verzette het afgelopen jaar veel werk wat betreft *privacy compliance*. Dit is niet altijd direct zichtbaar, omdat niet alle activiteiten al hebben geleid tot afgeronde producten of een aantoonbaar effect.

In 2023 was, door de ontwikkelingen, een verhoging en een verschuiving van de werk- en toezichtdruk zichtbaar in het werkveld van *privacy*- en gegevensbescherming. De ontwikkelingen en de transitie naar IGO leidden tot complexere en een grotere hoeveelheid van *privacy*-vraagstukken. De ontwikkelingen leidden ook tot een toename van de complexiteit van de *privacy*-vraagstukken en het aantal uit te voeren DPIA's. De *privacy*- en juridische organisatie wordt in het kader van een adviesrol in toenemende mate betrokken. In 2023 versterkte een aantal personele ontwikkelingen de *privacy*-organisatie, bijvoorbeeld door de inrichting van een CPO. Wel blijkt uit onderzoeken dat bij een aantal defensieonderdelen de AVG- of WPG-capaciteit ontoereikend is om uitvoering aan de AVG, WPG en de feitelijke handelingen die daarvoor nodig zijn, voldoende te coördineren.

De voor de uitvoering benodigde kennis en ervaring is zeer gespecialiseerd en kwetsbaar. In 2023 besteedde de *privacy*-organisatie veel aandacht aan het vergroten van de kennis van de AVG en de bewustwording binnen de organisatie. Aandachtspunten zijn de structurele borging van bewustwordingsactiviteiten, de structurele inbedding van *governance* rond gegevensbescherming, de naleving van verschillende elementen van de AVG en de WPG, de verhoging van de kwaliteit van de DPIA's en van de registraties in het register van verwerkingsactiviteiten en de realisatie van verbetermaatregelen omtrent gegevensbescherming.

## 3.1 Aanbevelingen

De ontwikkelingen vragen om vaardige AVG-coördinatoren, die multidisciplinair inzetbaar zijn. Het vraagt ook om een structurele samenwerking met de operationele- en de juridische lijn, en om een duidelijk privacy-beleid met en kaders en tools ter ondersteuning van de werkzaamheden.

***Aanbeveling 1:***
*Versterk de privacy-organisatie bij CLSK, KMar (WPG), JIVC, Defensiestaf en BS.*

Bij deze organisatieonderdelen is de capaciteit nog ontoereikend om voldoende uitvoering te kunnen geven aan de taken.

***Aanbeveling 2:***
*Verhoog het volwassenheidsniveau van de gehele privacy-organisatie*[18].

Stel periodiek in samenspraak de geambieerde volwassenheidsniveaus vast. Maak 'SMART'-afspraken over hoe dit te bereiken dan wel te behouden.

[18] Zie ook TK 2022-2023 32761 nr.258 Kamerbrief 13 januari 2023, Rapport en beleidsreactie Onderzoekscommissie Brouwer naar het LIMC inclusief bijlage: Rapport Grondslag gezocht, Onderzoekscommissie Land Information Manoeuvre Centre (LIMC).

***Aanbeveling 3:***
*Borg dat de organisatie in staat is kwalitatief goede DPIA's uit te voeren.*

Zorg dat de nieuwe werkinstructie met betrekking tot het uitvoeren van DPIA's wordt toegepast en zorg voor workshops om hierbij te ondersteunen.

***Aanbeveling 4:***
*Richt een systeem in ter borging van de realisatie van verbetermaatregelen.*

Breng de vanuit diverse bronnen afkomstige aanbevolen verbetermaatregelen met betrekking tot de naleving van gegevensbescherming in kaart en borg de realisatie hiervan beter.

***Aanbeveling 5:***
*Maak gegevensbescherming en privacy voldoende kenbaar, begrijpelijk en praktisch toepasbaar.*

Zorg voor het verder ontwikkelen van het gegevensbeschermingsbeleid en duidelijke privacy- en juridische kaders.

# 4 Bijlagen

## 4.1 Bevindingen per defensieonderdelen

| | Avg- en Wpg-organisatie | CZSK | CLAS | CLSK | KMar Avg | KMar Wpg | BS | BS DOPS | Defensie breed | Commit | Dosco |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | AVG-beheerders hebben een AVG-coördinator aangewezen. De WPG-beheerder heeft een privacyfunctionaris aangewezen. | | | | | 1 | | 2 | | | |
| B | De AVG-coördinatoren en PF zijn aangemeld bij de FG. | 3 | | | | 4 | | | 5 | | |
| C | De AVG-coördinatoren en de PF zijn formeel bekend gesteld binnen de organisatie. | | | | | | | 6 | | | |
| D | De taak van AVG-coördinator en PF is opgenomen in de functieomschrijving van de aanwezen medewerkers. | | | | | | 7 | 7 | 7 | 8 | |
| E | Geborgd is dat de AVG-coördinatoren en de PF de benodigde tijd, middelen en ruimte krijgt om de taak naar behoren uit te voeren. Tevens dat ze voldoende opleiding krijgen om de functie uit te voeren. | 9 | | 10 | | 11 | 12 | 13 | | 14 | |
| F | Het defensieonderdeel heeft activiteiten uitgevoerd in het kader van 'AVG- en WPG-awareness'. | | | | | | | 13 | | | |

| | |
|---|---|
| Ja/goed | |
| Verbetering nodig | |
| Onbekend/geen info | |

1. Voor een groot deel van 2023 is een van de privacyfunctionaris functies vacant geweest.
2. Eind 2023 is de functie vacant geraakt.
3. CZSK heeft in 2023 een tweede AVG-coördinator aangewezen. De nieuwe AVG-coördinator die eind 2023 is gestart is nog niet aangemeld bij de FG.
4. De AVG-coördinator is aangemeld bij de FG. Voor de PF is nog geen aanmelding ontvangen.
5. Tot 1 oktober 2023 zijn de taken belegd geweest binnen CPO. Formalisering van de taken van de functie bij de DAOG moet nog plaatsvinden.
6. Tijdens het FG-toezichtbezoek in 2023 is gebleken dat er te weinig bekendheid was met de functie van AVG-coördinator binnen de DOPS. Momenteel is er geen AVG-coördinator aangewezen. Het is niet duidelijk of en hoe de functie gevuld gaat worden.
7. Omdat er wordt gewerkt met generieke functiebeschrijvingen maken de AVG-taken geen onderdeel uit van de generieke functiebeschrijving.
8. In verband met wijzigingen in de werklast en de noodzakelijke scheiding tussen proces, inhoud/uitvoering van taken is de functiebeschrijving niet meer toereikend.
9. Omdat korte plaatsingsduren van AVG-coördinatoren in het verleden leidden tot een achterstand in kennis en netwerk, wordt vanaf 2023 de AVG-coördinator langer op functie geplaatst. Daarnaast heeft eind 2023 de AVG-coördinator versterking verkregen door uitbreiding met een burgerfunctie.
10. Gezien de verschillende *privacy*-gerelateerde taken en de hoeveelheid te verwerken persoonsgegevens moet worden vastgesteld dat een enkele AVG-coördinator CLSK op stafniveau niet geacht kan worden volledig in control te zijn: er blijven zaken liggen omdat er geprioriteerd moet worden. Dit geldt evenzeer voor de onderdelen, waar de lokale AVG-coördinatoren hun werkzaamheden in het beste geval als neventaak uitoefenen. Een uitbreiding met een tweede AVG-coördinator wordt in 2024 verwacht.
11. Naast de in 2023 vacant gevallen functie is er voor de WPG, de functie van privacyfunctionaris en de interne auditor WPG weinig opleidingen beschikbaar.
12. Binnen HR&BV heeft onder andere toenemende aandacht voor de AVG geleid tot het besluit om over te gaan tot het weven van een fulltime, *dedicated* AVG-coördinator voor het apparaatsdeel van de BS.
13. De functie van AVG-coördinator 'Militaire operaties' is een nevenfunctie en in 2023 was er vrijwel geen tijd beschikbaar voor de uitvoering ervan. Om de rol AVG-coördinator 'Militaire operaties' op een betere en meer verantwoorde manier in te zetten is meer expertise en capaciteit nodig.
14. Binnen COMMIT HR wordt ingestoken op een minimale borging in de reorganisatie van de D-HR met ophogen met twee VTE'n voor uitvoerende AVG-taken met onderbrengen van de functies in de stafsectie Regie Planning en Coördinatie.

## 4.2 Afkortingen

| | |
|---|---|
| ADR | Auditdienst Rijk |
| AP | Autoriteit Persoonsgegevens |
| AVG | Algemene verordening gegevensbescherming |
| | |
| BA | Beveiligingsautoriteit |
| BIDKL | Bergings- en Identificatiedienst Koninklijke Landmacht |
| BOE | Bijzondere Organisatie-eenheid |
| BS | Bestuursstaf |
| | |
| CIO | *Chief Information Office* |
| CLAS | Commando Landstrijdkrachten |
| CLSK | Commando Luchtstrijdkrachten |
| COMMIT | Commando Materieel en IT |
| CPO | *Chief Privacy Office* |
| CZSK | Commando Zeestrijdkrachten |
| | |
| DCo | Directie Communicatie |
| DCPL | Dienstencentrum Personeelslogistiek |
| DCSC | Defensie Cyber Security Center |
| DGB | Directoraat-Generaal Beleid |
| DJZ | Directie Juridische Zaken |
| DOO | Defensie Open op Orde |
| DOPS | Directie Operaties |
| DOSCO | Defensie Ondersteuningscommando |
| DPIA | *Data Protection Impact Assessment* (Gegevensbeschermingseffectbeoordeling) |
| DPO | *Data Protection Officer* |
| | |
| FG | Functionaris voor Gegevensbescherming |
| | |
| IGO | Informatiegestuurd optreden |
| IMG | Inspectie Militaire Gezondheidszorg |
| IVD | Inspectie Veiligheid Defensie |
| | |
| JIVC | Joint IV Commando |
| | |
| KMCGS | Korps Militaire Controleurs Gevaarlijke Stoffen |
| | |
| LIMC | *Land Information Manoeuvre Centre* |
| LTC | Landelijk Tactisch Commando |
| | |
| MDO | Multidomein en geïntegreerd optreden |
| MLA | Militaire Luchtvaart Autoriteit |
| MoU | *Memorandum of Understanding* |
| | |
| OM | Openbaar Ministerie |
| OTC | Opleidings-, Trainings- en Kenniscentrum |
| OTT | Ondersteuningsteam Toezicht |

| | |
|---|---|
| PF | Privacy Functionaris |
| PSMV | Peoplesoft Melden Voorvallen |
| RGMO | Regeling Gegevensbescherming Militaire Operaties |
| RPA | *Robotics Process Automation* |
| RPAS | *Remotely Piloted Aircraft System* |
| RPFG | Rijksplatform van Functionarissen voor de Gegevensbescherming |
| SG | Secretaris-Generaal |
| SIS | Schengen Informatie Systeem |
| TK | Tweede Kamer |
| UAvg | Uitvoeringswet AVG |
| Wjsg | Wet justitiële en strafvorderlijke gegevens |
| WOO | Wet Open Overheid |
| WPG | Wet politiegegevens |

## 4.3 Begrippen

| Begrippen | Toelichting |
|---|---|
| **Avg-beheerder** | Het diensthoofd dat namens de Minister van Defensie belast is met de zorg voor de naleving van de AVG en de wet ten aanzien van verwerkingen die gevoerd worden binnen het dienstonderdeel. De operationele commandanten van de krijgsmachtonderdelen, de commandant DOSCO, de directeur van de DMO en de plaatsvervangend Secretaris-generaal voor de Bestuursstaf zijn aangewezen als AVG-beheerder. |
| **Avg-coördinator** | Functionaris, aangewezen door de AVG-beheerder, die de uitvoering van de AVG en de wet, en de feitelijke handelingen die daarvoor nodig zijn, binnen het betreffende dienstonderdeel coördineert. |
| **Wpg-beheerder** | De WPG-beheerder draagt zorg voor naleving van de regelgeving omtrent verwerking van politiegegevens door de KMar. De C-KMar is WPG-beheerder namens de Minister van Defensie. |