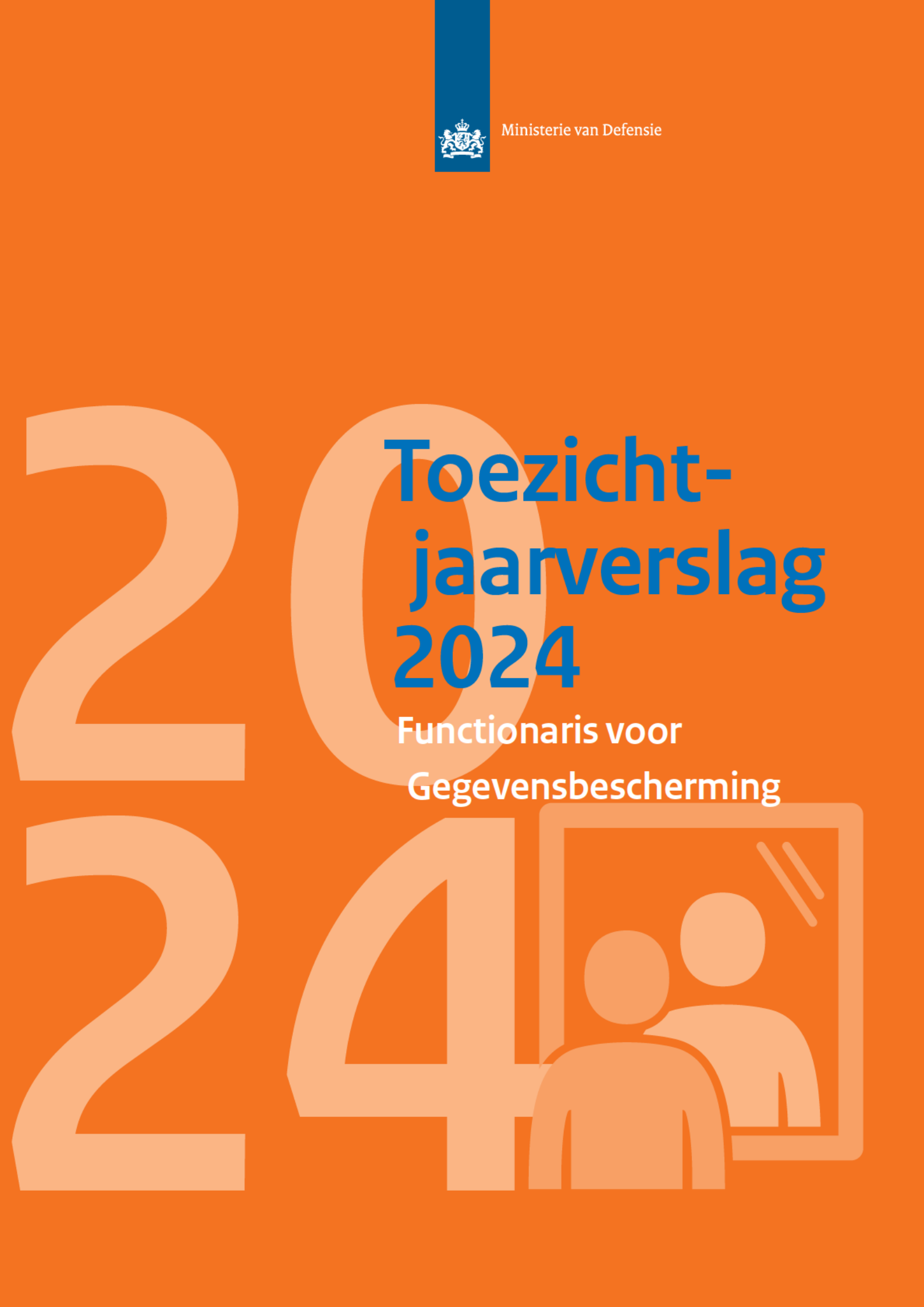
Ministerie van Defensie

Toezicht-jaarverslag 2024

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 58H

Datum
Maart 2025

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*. 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. De toezichttaken worden gecoördineerd en uitgevoerd met een team van inspecteurs die expertise hebben op het gebied van zowel de AVG, de Wpg als de Europese AI-verordening (hierna AI Act). Hierdoor is de effectiviteit van het toezicht gewaarborgd.

De FG informeert, adviseert en controleert of verwerkingen van persoonsgegevens bij Defensie rechtmatig, behoorlijk en transparant zijn. De FG controleert 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 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).

De veiligheidssituatie in de wereld verslechtert en dat vraagt om een krijgsmacht die gereed is voor alle hoofdtaken, met een toenemende druk op de hoofdtaak 1: de bescherming van ons eigen grondgebied en dat van de NAVO-bondgenoten. De defensieorganisatie maakt daarom een ingrijpende transitie door. De actuele dreiging van hybride en/of gewapende conflicten en crisissituaties verplichten Defensie ertoe om vanuit haar grondwettelijke doelstellingen eenheden gereed te stellen. Deze eenheden dienen in voldoende mate getraind en geoefend zijn, om zowel fysiek als in de digitale informatieomgeving te kunnen optreden. Daarbij heeft Defensie de verantwoordelijkheid en de verplichting om de grondrechten van burgers en van haar eigen medewerkers te respecteren en te beschermen en zich te houden aan de van toepassing zijnde wet- en regelgeving. De balans tussen veiligheid en privacy kan onder operationele omstandigheden en juridische kaders anders worden afgewogen dan tijdens oefeningen en trainingssituaties. Maar elk overheidshandelen dat ingrijpt in (grond)rechten en vrijheden dient altijd te berusten op een wettelijke grondslag.

In lijn met de Defensievisie 2035 ‘Vechten voor een veilige toekomst’ en de in 2024 uitgebrachte Weerbaarheidsopgave ‘Versterken van weerbaarheid in het licht van militaire en hybride dreigingen’ besteedde de FG in 2024 meer aandacht aan de verwerking van persoonsgegevens bij ontwikkelingen en innovaties in het kader van een informatiegestuurde krijgsmacht. Tevens droeg de FG bij aan de herijking van de juridische kaders voor Defensie en implementatie hiervan.

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 2024

Bij Defensie werken circa 74.000 beroepsmilitairen, burgers en reservisten. Defensie is in alle opzichten aan het opbouwen, steeds vaker met nationale en internationale partners.

De defensieorganisatie richt zich hierbij op de ontwikkeling en toepassing van nieuwe en innovatieve werkwijzen en op het optimaliseren van bestaande processen. Technologische en organisatorische ontwikkelingen doen zich organisatiebreed voor. Het gaat om uiteenlopende producten, diensten en applicaties waarbij nieuwe technologieën worden gebruikt. Voorbeelden hiervan zijn kunstmatige intelligentie (AI), algoritmes, slim cameratoezicht, gezondheidsmonitoring, biometrische technologie en slimme sensoren, en ICT-toepassingen aan boord van schepen, vliegtuigen en voertuigen. Ook komen er steeds meer *tools* beschikbaar die informatie verzamelen en datastromen verwerken en inzichtelijk maken. Deze ontwikkelingen leiden tot het verwerken van persoonsgegevens van defensiemedewerkers, maar ook in toenemende mate van betrokkenen in de samenleving buiten Defensie, zowel nationaal als internationaal.

De FG had in 2024 aandacht voor verwerkingen van persoonsgegevens die mogelijk een hoog risico inhouden voor de rechten en vrijheden van personen. De FG genereert door middel van toezichtbezoeken, documentanalyse en waarnemingen een beeld van de naleving van wet- en regelgeving rond de bescherming van persoonsgegevens binnen Defensie. Behalve gepland toezicht conform het Toezichtjaarplan 2024, voerde de FG ook ad hoc-toezicht uit naar aanleiding van incidenten of adviesvragen.

Naast het toezicht op de naleving van de AVG en Wpg, nam de FG in 2024 ook het toezicht op de naleving van de AI Act in haar toezichttaken op. Deze nieuwe taak vereist aandacht voor de razendsnel evoluerende ontwikkelingen in het veld van AI, evenals voor de gefaseerde implementatie van de AI Act en de interne ontwikkelingen binnen de organisatie.

1.1 Uitgevoerd toezicht AVG en Wpg

***Robotic Process Automation* (RPA):** In 2024 gaf de FG vervolg aan het verkennende toezichtbezoek in 2023 bij Defensie Ondersteuningscommando (DOSCO)[1]. RPA is een automatiseringsproces en houdt in dat binnen bepaalde werkprocessen de handelingen niet meer door een defensiemedewerker worden verricht, maar door een (scherm)robot. De belangrijkste bevinding is dat DOSCO een overzichtelijke *governance* en werkwijze heeft ingericht voor het robotiseren van processen, waarbij het rekening houdt met het belang van gegevensbescherming. Doordat deze werkwijze echter (nog) niet defensiebreed wordt toegepast, zijn tussen defensieonderdelen verschillen in werkwijzen door de FG waargenomen, bijvoorbeeld bij het al dan niet opstellen van addenda op de *Data Protection Impact Assessment* RPA (DPIA RPA) bij nieuwe inzet van robots. Daarbij ontbrak ook een centraal overzicht van alle uitgevoerde addenda. De aanbevelingen vanuit de FG richten zich daarom vooral op het formaliseren van het beleidskader van RPA (door toedoen van het *Chief Privacy Office* (CPO)) en het inventariseren, uitvoeren en documenteren van addenda door de defensieonderdelen. De DPIA RPA is inmiddels herzien en voorzien van advies van de FG.

Melden en afhandelen inbreuk op de beveiliging (datalek): 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 in bepaalde gevallen ook aan betrokkenen.

In 2024 voerde de FG toezichtonderzoek[2] uit naar de wijze waarop Defensie handelt bij datalekken c.q. inbreuken op de beveiliging, die per ongeluk of op onrechtmatige wijze leiden tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Defensie heeft een procedure voor het melden van verschillende typen voorvallen met gebruik van de applicatie *PeopleSoft* Melden Voorvallen (PSMV). De voornaamste verbeterpunten uit het onderzoek hebben betrekking op de inrichting en het gebruik van de PSMV-applicatie en

1 *Functionaris voor Gegevensbescherming. 16 juli 2024. Rapport FG-toezichtbezoeken DOSCO RPA. BS2024024034.*

2 *Functionaris voor Gegevensbescherming. 28 oktober 2024. Toezichtonderzoek afhandelen datalekken. BS2024037730.*

de tijdigheid van afhandelen van meldingen.
Daarnaast is meer voorlichting nodig over het melden van voorvallen en het gebruik van PSMV. Ook is er onvoldoende dataminimalisatie toegepast op de gegevens van de melder. Door CPO wordt een appreciatie van het toezichtrapport opgesteld waarbij te nemen acties en actiehouders worden afgestemd.

De CPO introduceerde in 2024 een nieuw defensiebreed format voor het intern datalekregister, ter verbetering van het afhandelen van datalekken.
Dit format is begin 2025 in gebruik genomen.
Hiermee werkt de gehele defensieorganisatie met een uniform datalekregister. Ook is een concept procedure opgesteld en in gebruik genomen voor het intern melden, beoordelen en afhandelen van datalekken.

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 van een onbekend slachtoffer is alleen mogelijk door middel van DNA-onderzoek van potentiële verwanten. De FG voerde in 2022 een toezichtbezoek uit bij BIDKL. Naar aanleiding hiervan nam het Commando Landstrijdkrachten (CLAS) diverse verbetermaatregelen, zoals het opstellen van een *Data Protection Impact Assessment* (DPIA) en het actualiseren van convenantafspraken met ketenpartners zoals de Politie en het Nederlands Forensisch Instituut. Uit het vervolgonderzoek en de appreciatie op de DPIA[3] in 2024 blijkt dat de CLAS de meeste verbetermaatregelen onderhanden of gerealiseerd heeft.

Verantwoordingsplicht Register van verwerkingsactiviteiten: De FG voerde in 2023 een themaonderzoek uit naar de opbouw en de kwaliteit van het register van verwerkingsactiviteiten van Defensie. 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. In 2024 startte de CPO een project voor een nieuwe opzet van het register. Onderdeel van het project is het ontwikkelen van een helder raamwerk om de opzet en uniformiteit van het register te verbeteren.
Dit raamwerk wordt afgestemd met de FG en de defensieonderdelen. De CPO heeft daarnaast een standaardformulier opgesteld voor het aanmelden van (nieuwe) verwerkingen, een concept instructie voor het beheren en onderhouden van het register en een concept handleiding voor het uniform en consistent invullen van de informatievelden in het register. Deze documenten worden in 2025 opgeleverd.

Verwerkersovereenkomsten: De Auditdienst Rijk (ADR) voerde, in opdracht van de FG, in 2023-2024 een onderzoek uit naar de genomen maatregelen voor het opstellen, vaststellen, registeren en beheren van verwerkersovereenkomsten bij inkopen door Defensie[4].
De ADR constateert dat maatregelen zijn genomen voor het sluiten van verwerkersovereenkomsten, maar dat aanvullende maatregelen nodig zijn op het gebied van beleid, organisatie en permanente educatie. Heldere, eenvoudige en praktische richtlijnen, meer inzicht en overzicht in het geheel van verwerkersovereenkomsten in de privacy-organisatie en betere inrichting van de adviesfunctie ten behoeve van de inkoopfunctie zijn enkele aanbevelingen uit het rapport.
De CPO en de Coördinerend Directeur Inkoop werken aan het ontwikkelen van specifiek beleid op het gebied van inkoop en privacy, met een nadruk op het afsluiten en beheren van verwerkersovereenkomsten en op heldere, eenvoudige kaders en vereisten voor leveranciers. Een AVG-klankbordgroep Inkoop moet gaan zorgdragen voor advies en meer contact tussen de AVG-coördinatoren, inkoopfunctionarissen en andere betrokken partijen. Tot slot zal er meer inzicht en overzicht worden gecreëerd over de afgesloten verwerkersovereenkomsten en moeten er gerichte trainingen en bewustzijnsactiviteiten voor de inkoop en privacy *community* worden georganiseerd.

Defensie Open op Orde (DOO): In het Toezichtjaarverslag 2023 uitte de FG bij verschillende projecten van het programma DOO haar zorgen over de tot nu toe genomen maatregelen die moeten voorkomen dat persoonsgegevens onnodig, onjuist of onrechtmatig worden verwerkt, te lang worden bewaard of onbedoeld worden ingezien. Het gaat hierbij om projecten waarbij er via bepaalde systemen op grote schaal persoonsgegevens (waaronder bijzondere persoonsgegevens) worden verwerkt, zoals het

3 *Functionaris voor Gegevensbescherming. 18 juni 2024. FG-Appreciatie DPIA CLAS/BIDKL. BS2024022887*

4 *Auditdienst Rijk. 25 juni 2024. Evaluatie van de maatregelen voor de verwerkersovereenkomsten bij inkoop van Defensie. 2024-0000262902.*

documentmanagementsysteem DefDoc, het archiveren van chat- en e-mailberichten, het openbaar maken van bestuurlijke informatie en het gebruik van geautomatiseerde anonimiserings- en laksoftware. Daarnaast leefde de vraag of er genoeg kennis en capaciteit binnen de DOO-projectorganisatie aanwezig was om deze maatregelen in kaart te brengen en te implementeren. De FG haalde in 2024 de contacten met DOO aan. Zo zijn er met tussenkomst van de *Chief Information Office*/afdeling Documentaire Informatievoorziening (CIO/DI) meerdere sessies en presentaties georganiseerd waarin de stand van zaken en aanpak omtrent de DOO-projecten en de daaraan gekoppelde DPIA's zijn toegelicht. Ook is een AVG-coördinator geworven die zich vanaf 2025 specifiek bezig gaat houden met het coördineren van de uitvoerende werkzaamheden met betrekking tot gegevensbescherming bij de DOO-projecten.
Hoewel er nog genoeg uitdagingen zijn, tonen deze ontwikkelingen aan dat DOO het afgelopen jaar meer aandacht had voor gegevensbescherming. Ook voor 2025 geldt dat er vanuit de FG speciale aandacht zal zijn voor de ontwikkelingen binnen DOO. Vanaf medio 2025 is hiervoor een inspecteursfunctie toegevoegd aan het FG-team.

MQ9: De FG was nauw betrokken bij het, binnen de kaders van de AVG, beoordelen van voorgenomen activiteiten en processen van het Commando Luchtstrijdkrachten (CLSK) rond de operationele gereedstelling en getraindheid van de MQ-9 in Nederland. Het was de eerste keer dat een dergelijk proces onder tijdsdruk doorlopen moest worden.
De evaluatie van dit proces leidde tot interessante inzichten en verbetermaatregelen.
Belangrijk aandachtspunt betreft de onderlinge communicatie tussen CLSK, de CPO en de FG en het elkaar proactief aan de voorkant betrekken bij voorgenomen gegevensverwerkingen. Daar staat tegenover dat juist de wijze waarop alle partijen met elkaar hebben samengewerkt er ook toe leidde dat in 2024 de eerste vluchten van de MQ-9 boven Nederland op een afgewogen manier konden plaatsvinden.

Directie Operaties (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 rond de AVG en de Regeling Gegevensbescherming Militaire Operaties (RGMO). Daarbij adviseerde de FG onder andere om 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 (DS) beter te borgen. 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 DS.
De geopolitieke ontwikkelingen, waarbij Defensie in haar taken steeds meer de nadruk legt op hoofdtaak 1, wordt het belang van capaciteit, kennis en kunde op het gebied van gegevensbescherming alleen maar groter. De DOPS heeft geen voortgang gerapporteerd ten aanzien van te nemen verbetermaatregelen.

Defensie Cyber Security Centrum (**DCSC**): In het rapport 'Onderzoek naar *social media monitoring* bij het Ministerie van Defensie'[5] deed de FG een aantal aanbevelingen. Een van de aanbevelingen was zorg te dragen voor aanvullend beleid en aanvullende richtlijnen voor het gebruik van *social media monitoring* en *–scraping tools*. Dit leidde bij het DCSC tot het opstellen van een concept DPIA die aan de FG is voorgelegd voor advies. Momenteel werkt het DCSC in samenwerking met Directie Juridische Zaken en CPO het juridisch kader hiervoor verder uit. Een Richtlijn voor *Cyber Threat Intelligence* (CTI) wordt ook uitgewerkt. Naar verwachting kunnen begin 2025 zowel de geactualiseerde DPIA, het uitgewerkt juridisch kader als de aangepaste Richtlijn CTI voor advies aan de FG worden voorgelegd.

Bureau Justitiële Administratie en Archieven Koninklijke Marechaussee (KMar): In het kader van het interne toezicht op de naleving van de Wpg heeft de FG in 2024 een toezichtbezoek uitgevoerd bij het Bureau Justitiële Administratie en Archieven (BJAA) van de KMar. Wegens verenigde belangen en om de toezichtdruk te verlagen, is ervoor gekozen om naast de FG Wpg ook andere expertisegebieden te betrekken bij het toezichtbezoek. Dit onderzoek is uitgevoerd samen met de Beveiligingsautoriteit (DGB/DBE/BA) voor de (informatie)beveiligingsaspecten en met de CIO/DI voor het toezicht op documentbeheer en de archivering.
De nadruk lag op de naleving van de bij en krachtens de Wpg gestelde wet- en regelgeving voor het op juiste gronden bewaren en vernietigen van politiegegevens. De FG deed aanbevelingen gericht op het opstellen en toepassen van selectielijsten, intensivering van de samenwerking met andere archieven binnen de

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

defensieorganisatie en opleiding en training voor medewerkers BJAA om de kwaliteit van het proces te verbeteren en te borgen.

Wet politiegegevens: 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 periodiek worden beoordeeld[6]. 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 externe *audit*, door de ADR uitgevoerd over de periode 2019-2022 werd in augustus 2024 afgerond. De voorafgaande interne *audits* over de jaren 2021-2023 voerde de KMar niet uit wegens capaciteitsproblemen. Om de kwaliteit en continuïteit van de interne controle op de naleving van de Wpg te waarborgen, is in het lopende reorganisatietraject bij de KMar een functie opgenomen voor een interne *auditor*. Deze *auditor* is verantwoordelijk voor de uitvoering en coördinatie van de jaarlijkse interne *audit*. De KMar stelde na het ADR-rapport 2019-2022 een verbeterrapport op, met de te nemen maatregelen om te voldoen aan de Wpg-normen. Het verbeterrapport heeft vijf speerpunten gedefinieerd. Dit betreft onder andere het oplossen van het capaciteitstekort van de privacyfunctionarissen, de actualisatie van interne instructies, registers, documentatie en procesbeschrijvingen en het ontbreken van interne *audit* capaciteit. Een hercontrole vindt plaats in 2025.

Loggingsplicht Wpg: 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 te achterhalen. Tevens indien mogelijk wordt de identiteit vastgelegd van de persoon die de politiegegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die politiegegevens. Artikel 32a Wpg is na een overgangsperiode sinds eind 2023 van kracht. De KMar heeft nog niet volledig voldaan aan de loggingsplicht. De door de KMar eerder aangegeven realisatiedatum van eind december 2024 is niet gehaald. Een zorgpunt van de FG is dat realisatie niet voor eind 2025 wordt verwacht. De reden hiervoor is dat er plannings- en capaciteitsproblemen zijn bij het invoeren van nieuwe ICT-systemen en het verbeteren van oudere systemen. Andere opsporingsorganisaties lopen tegen vergelijkbare vertragingen en problemen aan.[7]

Gegevensbescherming in het Caribisch gebied: De FG verzocht C-KMar[8] eind 2022 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. In 2024 deed de KMar een eerste inventarisatie naar de openstaande vragen vanuit de FG. Verder constateerde de FG dat er slechts beperkt voortgang is voor wat betreft het daadwerkelijk nemen van verbetermaatregelen ten opzichte van 2022-2023. Mede door het voorgaande bevat het toepasselijk normenkader nog altijd veel onduidelijkheden en was in 2024 een toezichtbezoek nog niet opportuun.

Dienstencentrum Personeelslogistiek (DCPL): De FG startte in 2024 met een onderzoek bij onderdelen van het DCPL, namelijk: Defensity College, Employability, Dienjaar, Veiligheid & Vakmanschap en de afdeling Selectie & Keuringen. In het eerste kwartaal van 2025 worden de rapportages opgeleverd.

6 *Regeling periodieke audit politiegegevens.*

7 *Kamerbrief over voortgang loggingsverplichting gegevensverwerking in het politiedomein en justitiedomein, 17 januari 2024, 498915.*

8 *Nota Gegevensverwerkingen KMar CARIB. 8 december 2022. BS2022031914.*

1.2 Uitgevoerd Toezicht AI & Algoritmes

Op 2 augustus 2024 werd de AI Act van kracht en per 2 februari 2025 werden de eerste AI-systemen verboden. Het doel van de AI Act is om het verantwoord gebruik van AI te stimuleren en om risico's op bijvoorbeeld discriminatie en misleiding te verkleinen.
Deze verordening is ook van toepassing op het Ministerie van Defensie. Er is slechts een uitzonderingsgrond indien sprake is van militaire, defensie- of nationale veiligheidsdoeleinden. Om toe te zien op een juiste implementatie en naleving van de AI Act is de FG in 2024 versterkt met twee functionarissen. Omdat de eerste verplichtingen die voortvloeien uit de AI Act pas vanaf 2 februari 2025 van kracht zijn geworden, vonden in 2024 nog geen toezichtbezoeken plaats. Daadwerkelijk toezicht op naleving van de AI Act zal plaatsvinden in 2025. De FG ziet toe op toepassingen die binnen het bereik van de AI Act vallen én toepassingen die buiten het bereik van de AI Act vallen maar waar persoonsgegevens in worden verwerkt. AI-toepassingen die zijn uitgesloten van het toepassingsgebied van de AI Act en waarin geen persoonsgegevens worden verwerkt, vallen buiten het toezichtdomein van de FG. Een zorgpunt van de FG is de druk die benodigde activiteiten in het kader van de naleving van de AI Act op de capaciteit en kennis van de privacy- en dataorganisatie legt.

Interne kaders AI en algoritmes: De FG dacht in 2024 actief mee bij het opstellen van interne kaders voor het gebruik van AI en algoritmes. Deze kaders worden in het eerste kwartaal van 2025 vastgesteld. Het is hierbij van belang dat de kaders handhaafbaar en uitvoerbaar zijn. De FG constateert ook dat binnen Defensie diverse organisatorische en personele ontwikkelingen in gang zijn gezet om op verantwoorde wijze gebruik te gaan maken van alle mogelijkheden die AI te bieden heeft. De verplichting om AI- of algoritmische toepassingen op (de)centrale wijze te registreren moet de komende twee jaar geeffectueerd worden. Mede hierdoor ontbreekt op dit moment nog een sluitend overzicht en is het zeer complex inzichtelijk te krijgen welke vormen van AI of algoritmische toepassingen worden gebruikt en wat de effecten en de risico's zijn.

***Responsible artificial intelligence in the military domain* (REAIM):** De FG heeft de afgelopen jaren deelgenomen aan de REAIM-Conferentie. Hier wordt in internationaal verband - ook door de Nederlandse minister van Defensie - het belang van verantwoord gebruik van AI in het militaire domein benadrukt. De FG adviseert Defensie om na te denken over een verdere uitwerking van de verschillende nationale en internationale principes zodat ook in het militaire domein duidelijke kaders voor het gebruik van AI en algoritmes worden gecreëerd.

Ontwikkeling van een toezichtkader voor AI: De FG nam in 2024 het initiatief om een specifiek toezichtkader voor AI en algoritmes te ontwikkelen. Dit kader wordt begin 2025 voltooid en gaat als leidraad dienen voor toekomstige toezichtactiviteiten op het gebied van AI. Het hebben van een dergelijk toezichtkader is van toegevoegde waarde voor de organisatie, aangezien het zorgt voor een consistente en transparante toetsing van AI-toepassingen. Bovendien helpt dit kader Defensie om te voldoen aan de verder ontwikkelende regelgeving op het gebied van AI.

Interdepartementale samenwerking: De AI Act heeft ertoe geleid dat er op interdepartementaal vlak wordt nagedacht over een uitvoeringswet en hoe het toezicht op naleving op nationaal niveau moet worden ingericht. De FG is aangesloten bij deze samenwerking om de belangen van Defensie te behartigen.

1.3 Toezichtactiviteiten hoofdtaak 1

De afgelopen jaren is door de geopolitieke ontwikkelingen de nadruk steeds meer komen te liggen op de hoofdtaak 1 van Defensie: het verdedigen van het eigen en bondgenootschappelijk grondgebied.
Een groot gedeelte van de dreiging speelt zich af in het informatiedomein, waardoor defensieactiviteiten in dat domein toenemen. Ook in het fysieke domein zijn hoogtechnologische ontwikkelingen niet meer weg te denken. Het grootschalig gebruik van data met behulp van onder andere *data science* en AI vergroot het vermogen van Defensie om de tegenstanders een stap voor te blijven. Zoals ook uit de Defensiestrategie *Data Science* en AI blijkt, moet Defensie informatie snel en slim verzamelen, structureren, verstrekken enzovoort, om goed te kunnen reageren op activiteiten van de tegenstander. Hiervoor is de beschikking over grote hoeveelheden data onontbeerlijk, maar tegelijkertijd bevat deze data ook vaak persoonsgegevens.
Defensie is bij de verwerking van deze persoonsgegevens gebonden aan de relevante privacywetgeving en moet ervoor zorgen dat gegevens altijd zorgvuldig en rechtmatig worden verwerkt.

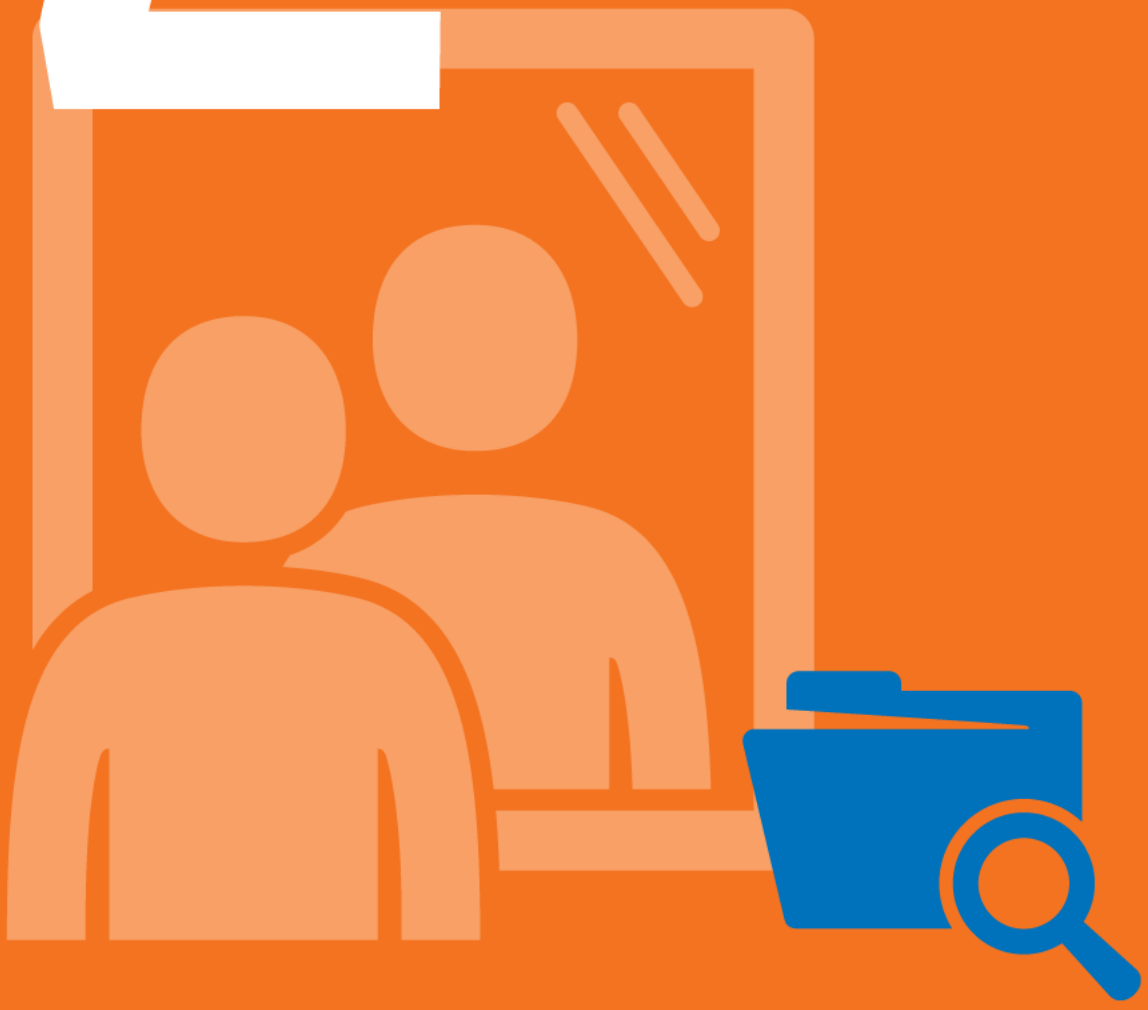
De verschillende defensieonderdelen investeren fors in materieel, technologische ontwikkelingen en personeel om zo te komen tot een technologisch hoogwaardige krijgsmacht. Veel nieuwe technologieën en systemen bevatten sensoren die op grote schaal (persoons)gegevens verwerken en die ook interoperabel moeten zijn. Deze verregaande digitalisering van de operationele activiteiten en prioritering van taken binnen Defensie had in 2024 ook effect op de toezicht- en adviesrol van de FG, onder andere door een toename van complexe DPIA's van gegevensverwerkingen in operationele context en het met spoed adviseren op urgente dossiers. De FG is nauw betrokken bij trajecten zoals wetgevingstrajecten met betrekking tot gereedstelling en inzet van Defensie. Door aan de voorkant bij dergelijke trajecten proactief mee te denken en hierbij met de CPO gezamenlijk op te trekken, wordt voorkomen dat privacygerelateerde risico's niet of onjuist worden geadresseerd en de gemaakte keuzes onvoldoende worden onderbouwd.

Verwacht wordt dat in 2025 de ontwikkelingen in het kader van hoofdtaak 1 ook een sterk effect zullen hebben op de prioritering van het toezicht en de daarvoor benodigde capaciteit. Een zorgpunt van de FG is het effect dat deze ontwikkelingen zullen hebben op de toch al beperkte capaciteit van de AVG-coördinatoren, ook door het ontbreken van AVG-capaciteit en kennis bij de DS.

Gereedheid van Defensie: De huidige wet- en regelgeving is niet toereikend voor de benodigde voorbereiding op het beschermen en verdedigen van het eigen grondgebied en dat van bondgenoten. Defensie werkt daarom aan passende wet- en regelgeving voor de uitvoering van haar taken, vooral voor urgente gereedstelling en de inzet en de randvoorwaarden daarvoor. De FG-unit adviseert proactief in dit traject, alsmede op de bijbehorende wetgevings-DPIA. De wetgeving moet, indien er bijvoorbeeld sprake is van inbreuk op de persoonlijke levenssfeer van burgers, specifieke voorwaarden stellen om een rechtmatige en behoorlijke verwerking van persoonsgegevens door de overheid te waarborgen.

Toezichtstrategie: Gezamenlijk met andere toezichthouders is de (wijziging in) toezichtstrategie in relatie tot ontwikkelingen in het kader van hoofdtaak 1 uitgewerkt. Bij wetgevingstrajecten, die mogelijk leiden tot uitbreiding van activiteiten van de krijgsmacht ten behoeve van gereedstelling en inzet van Defensie waarbij het recht op privacy- en gegevensbescherming mogelijk in het geding komt, is van groot belang dat ook het uitvoeren van onafhankelijk toezicht wordt geborgd. Belangrijke aandachtspunten bij het wetgevingstraject zijn het inrichten van toereikende waarborgen met betrekking tot gegevensbescherming bij het verkrijgen en verwerken van persoonsgegevens inclusief het toezicht daarop en aandacht voor de toetsbaarheid van de naleving.

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 rapportageverplichting voor de Wpg-beheerder.
De AVG-beheerders en Wpg-beheerder leverden een (concept) jaarrapportage aan. De rapportage van de DOPS (naleving Regeling Gegevensbescherming Militaire Operaties) is niet ontvangen[9].

2.2 Privacy-organisatie

Organisatorische ontwikkelingen toezicht en beleid

De ontvlechting van beleid (CPO) en toezicht (FG), die in 2022 in gang is gezet, is bestendigd. Hierbij is de samenwerking tussen toezicht en beleid verder geprofessionaliseerd en versterkt. Sinds de ontvlechting hebben zowel het CPO als de FG zich als eigen organisatieonderdelen verder ontwikkeld. De FG heeft gewerkt aan een eigen missie en visie en trof voorbereidingen om tot een zelfstandige Bijzondere Organisatorische Eenheid te komen (administratieve ontvlechting van de Inspectie Veiligheid Defensie).

De FG-unit is in de loop van 2024 versterkt met aanvullende personele onderzoekscapaciteit. Het gaat om een 'kwartiermakersfunctie' om de visie en strategie te bepalen voor het toezicht op AI en algoritmes binnen Defensie en om een tijdelijke functie voor toezicht op AI en algoritmes. Ook bij het CPO vond personele uitbreiding plaats, want daar begon in 2024 een coördinerend beleidsadviseur privacy en AI. Ook voor 2025 zijn er personele uitbreidingen voorzien voor het CPO en de FG.

De privacy-organisatie bij de defensieonderdelen

Conform de 'Regeling AVG Defensie' wezen alle AVG-beheerders een AVG-coördinator aan. De functie van AVG-coördinator Militaire Operaties[10] is daarentegen niet gevuld. 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.
Bij enkele defensieonderdelen is de personele capaciteit in 2024 (tijdelijk) uitgebreid. Zo is onder andere een tweede AVG-coördinator gestart bij het CLSK en kreeg DOSCO ondersteuning van een privacy-jurist. Ondanks de personele uitbreiding blijft de werkdruk bij de AVG-coördinatoren en Wpg-privacyfunctionarissen over het algemeen genomen hoog[11]. Hierdoor moesten sommige defensieonderdelen prioriteiten stellen en kwamen ze aan bepaalde werkzaamheden niet toe. Dit geldt voor de KMar (AVG en Wpg), CLSK, COMMIT, BS en CZSK. Deels is dit mede veroorzaakt door personele wisselingen en niet-gevulde functies. Bij de KMar was in verband met omstandigheden één van de twee posities van privacyfunctionaris het merendeel van 2024 feitelijk niet gevuld.[12]

Bij de FG blijven er zorgen om de positie van de AVG-coördinator RGMO bij de DOPS. Deze positie bleef geheel 2024 vacant. Met betrekking tot de versterking van de privacy-organisatie van de DS en de BS heeft het CPO gewerkt aan een nota over de benodigde indeling van de privacy-organisatie bij deze defensieonderdelen. Met deze nota kunnen de afspraken over de verdeling van taken en verantwoordelijkheden op het gebied van gegevensbescherming tussen de DS en BS worden geformaliseerd. Deze versterking is des te meer nodig met het oog op verwerkingen van persoonsgegevens in het kader van hoofdtaak 1 en de potentiele risico's voor betrokkenen. Ook zijn in het door het CPO opgestelde concept *Privacy Governance* en Beleidskader de rollen, taken en verantwoordelijkheden verder verduidelijkt.

Verder verzorgde het CPO het afgelopen jaar een aantal interne trainingen en opleidingen om het kennisniveau van de privacy-organisatie te verhogen.
Onderwerpen betroffen onder andere AI en Algoritmes en gegevensbescherming in internationaal perspectief. Ook zijn er in 2024 wederom CIPP/E en CIPM[13] trainingen aangeboden.

9 Zie Bijlage 1

10 10 Zie RGMO.

11 Zie Bijlage 1.

12 Zie ook Bijlage 1.

13 International Association of Privacy Professionals. Certified Information Privacy Professional/Europe & Certified Information Privacy Manager.

Volwassenheid privacy-organisatie

In het toezichtjaarverslag van 2023 beval de FG aan om het volwassenheidsniveau van de gehele privacy-organisatie te verhogen. Dit was ook een aanbeveling uit het rapport van de Onderzoekscommissie Brouwer[14].

In 2024 stelde het CPO een plan van aanpak op voor een privacy-volwassenheidsmeting. De volwassenheidsmeting wordt gedurende de eerste helft van 2025 in samenwerking met de AVG-coördinatoren uitgevoerd. Het eindproduct van dit traject is een geconsolideerd rapport waarin defensiebreed inzicht wordt gegeven in de privacy-volwassenheid en op basis waarvan per defensieonderdeel concrete acties worden geformuleerd om het gewenste volwassenheidsniveau te bereiken. Bij de FG zijn er vooral zorgen om de privacy-volwassenheid en de daadkracht om deze volwassenheid te verhogen bij defensieonderdelen die geen of geen dedicated AVG-coördinatoren hebben.

Beleid

In het toezichtjaarverslag 2023 beval de FG wederom aan om zorg te dragen voor het verder ontwikkelen van het gegevensbeschermingsbeleid en duidelijke privacy- en juridische kaders. In 2024 zette het CPO stappen voor een *Privacy Governance &* Beleid. Een concept beleidsdocument is gereed en aangeboden voor stafbehandeling. In 2025 toetst de FG op de toezichtbaarheid van het beleidsdocument.
De onderliggende procesbeschrijvingen, werkinstructies en formats voor specifieke privacy- en gegevensbeschermingsonderwerpen zijn in ontwikkeling en deels in concept gereed.

Bewustwording

Voor het structureel verhogen en borgen van bewustwording voor privacy, gegevensbescherming en informatiebeveiliging wordt door CPO gewerkt aan een concept Plan van Aanpak (PvA). De planning is dat het PvA in Q1 2025 wordt opgeleverd. In 2024 ontplooiden de AVG-coördinatoren diverse activiteiten voor het verhogen van de bewustwording. Dit betreft bijvoorbeeld het geven van voorlichting op verschillende niveaus in de organisatie en een intranetsite beveiliging en privacy met algemene uitleg en links. Het CPO organiseerde in samenwerking met de BA en de FG, een *Privacy & Security*-dag, met presentaties over sensoren, *data science* en AI en Algoritmes.
Het bevorderen van bewustwording over de AVG en Wpg kreeg in 2024 bij meerdere defensieonderdelen noodgedwongen minder aandacht dan gewenst.
De voornaamste reden hiervoor is de grote hoeveelheid werk en een tekort aan capaciteit.

Samenwerking toezichthouders binnen Toezichtberaad

Gezamenlijk met de andere toezichthouders binnen Defensie maakt de FG onderdeel uit van het Toezichtberaad. Op het gebied van methodologieën en strategische toezichtontwikkelingen wordt steeds intensiever samengewerkt, vaak met ondersteuning van het Bureau Toezicht Defensie. Wanneer sprake is van overlap in een toezichtdomein wordt de inhoudelijke samenwerking opgezocht.

Samenwerking buiten Defensie

Om haar taak goed uit te kunnen voeren, werkt de FG ook samen met personen en instanties buiten de defensieorganisatie. In 2024 had de FG meermaals contact met medewerkers van de AP over bijvoorbeeld datalekken, klachten en het wetgevingstraject met betrekking tot de gereedheid van Defensie.

Rijksplatform van Functionarissen voor de Gegevensbescherming (RPFG): De voor de FG AVG belangrijkste externe samenwerking vindt plaats in het 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 brengt daar advies over uit. Het RPFG wordt zo steeds meer een gesprekspartner in allerlei rijksbrede trajecten. Daarnaast is binnen het RPFG afgestemd over een nieuw format voor een DPIA voor wetgeving. Dit format zal in 2025 worden uitgerold.

Platform FG voor Wpg en Wet justitiële en strafvorderlijke gegevens (Wjsg): Sinds 2020 is een platform actief voor de FG's die in Nederland, krachtens de Europese Richtlijn voor de verwerking van persoonsgegevens door bevoegde autoriteiten voor opsporing, vervolging van strafbare feiten en tenuitvoerlegging van straffen (EU 2016/680 *Law Enforcement Directive*), zijn aangesteld op grond van de Wpg en de Wjsg. In 2023 is het platform verder vormgegeven en ingericht onder de naam LED-Werk.

14 *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).*

2.3 Verwerkersovereenkomsten

Wanneer Defensie gebruik maakt van een verwerker, dient een verwerkersovereenkomst (of andere rechtshandeling, zoals een convenant) opgesteld te worden om te waarborgen dat de verwerker ten behoeve van Defensie persoonsgegevens volgens de regels van de AVG verwerkt en beschermt. Er is geen actueel en volledig overzicht beschikbaar voor de FG of (sub)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 daarmee voor de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Bijvoorbeeld doordat de beveiliging niet voldoet aan de eisen van Defensie of dat er persoonsgegevens onrechtmatig worden verwerkt. Ook kunnen de gevolgen bij een datalek 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. Ook dient, conform de Regelingen AVG en Wpg Defensie, een verwerkersovereenkomst in het register van verwerkingsactiviteiten te worden opgenomen. Een controle door de FG van de registratie van verwerkersovereenkomsten in SAP M&F toont aan dat de registratie niet volledig is. Ook is niet vast te stellen welke inkoopcontracten een verwerkersovereenkomst missen. Het register van verwerkingsactiviteiten biedt ook geen inzicht in en overzicht van alle verwerkersovereenkomsten. Vanwege onder andere de onvolledigheid van het contractenregister en de wijze van registratie in SAP M&F is er geen link te leggen tussen de verwerkingen in het register voor verwerkingen en verwerkersovereenkomsten in het contractenregister van SAP M&F. Deze tekortkomingen in de verantwoordingsplicht van Defensie, die de FG al meerdere jaren heeft geconstateerd, zijn ook door de ADR bevestigd in haar onderzoek (zie paragraaf 1.1). Het CPO startte in 2024 met een concept instructie inkoop en verwerkersovereenkomsten. Deze instructie wordt in 2025 verder uitgewerkt en geformaliseerd.

2.4 Data Protection Impact Assessments

De FG houdt toezicht op de uitvoering van de DPIA's. Een DPIA is een wettelijk verplicht instrument om vooraf de hoge 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. 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).

In 2024 ontving de FG 22 DPIA's of addenda op DPIA's en 1 *Data Transfer Impact Assessment* (DTIA) ter advies. Daarnaast zijn meerdere DPIA's ter tussentijds advies aangeboden aan de FG. 38 DPIA's en 1 wetgevings-DPIA zijn onderhanden bij de defensieonderdelen, dit zijn deels DPIA's waar het advies van de FG nog in verwerkt moet worden door de verwerkingsverantwoordelijke. Volledig inzicht en overzicht van uitgevoerde, lopende en nog benodigde DPIA's is nog onvoldoende beschikbaar.

Na aanleiding van aanpassing van de concept Instructie Uitvoeren DPIA worden voor nieuwe verwerkingen *pre-scans* uitgevoerd om te beoordelen of een DPIA noodzakelijk is. In 2024 zijn twaalf *pre-scans*, conform de nieuwe procedure, aangeboden aan de FG ter beoordeling. Aandachtspunten bij een beoordeling van een pre-scan zijn de weging en de *scope*.

Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. Bij veranderingen in de gegevensverwerking, de context van de verwerking of de risico's van de verwerking is een actualisatie van de DPIA mogelijk nodig. Bijvoorbeeld doordat een nieuwe technologie in gebruik wordt genomen. Het is een goede praktijk om een DPIA continu te herzien en regelmatig opnieuw te beoordelen. Vanwege mogelijke veranderingen wordt sowieso aangeraden om eens per drie jaar de DPIA uit te voeren. In 2024 zijn 19 DPIA's toe aan actualisatie, omdat ze ouder zijn dan drie jaar.

Hiervan is één gewijzigde versie van een DPIA aangeboden aan de FG ter appreciatie en zijn enkele van de DPIA's onderhanden bij de defensieonderdelen.

	2024	2023	2022	2021	2020	2019	2018
Voorgelegd aan FG ter appreciatie (incl. Addenda)	23	33	23	17	17	11	4
Vastgesteld/ gereed voor vaststelling	14	9	19	13	9	9	12
Actualisering/ wijziging bestaande DPIA	1	6					

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. In 2024 is de concept Instructie Uitvoeren DPIA met betrekking tot het uitvoeren van DPIA's door de organisatie toegepast. In 2025 wordt het effect van de nieuwe werkwijze op de kwaliteit van de DPIA's en de doorlooptijd van het opstellen ervan geëvalueerd. De *pre-scan* DPIA's die aangeboden zijn aan de FG leidden in enkele gevallen tot overleg over de *scope* en aanpak van de verwerking.

2.5 Inbreuken op de beveiliging (datalekken)

Defensiemedewerkers melden inbreuken in verband met persoonsgegevens (potentiële datalekken) in het systeem PSMV-systeem als privacy-voorval. Dit kunnen meldingen zijn met betrekking tot een *hack*, verkeerd gestuurde persoonsgegevens, openstaande *SharePoint-sites*, verloren of gestolen gegevensdragers of datalekken bij verwerkers. Omdat het om privacy-voorvallen gaat, kan het ook gaan om het (ongewenst) publiceren van foto's van defensiemedewerkers op *social media-sites* en het ontvangen van ongewenste berichten. De FG ontvangt een afschrift van de in het PSMV-systeem gemelde voorvallen die aangevinkt zijn als een privacy-voorval. In 2024 ontving de FG 362 privacy-voorval meldingen. Dit is een toename ten opzichte van voorgaande jaren. In enkele gevallen leidde een melding tot het instellen van nader toezicht door de FG en is met defensieonderdelen contact geweest over het treffen van maatregelen ter verbetering van de processen.

	2024	2023	2022	2021	2020
AVG-gerelateerde (PSMV-) meldingen	357	290	197	154	156
Wpg-gerelateerde (PSMV-) meldingen	5	4	0	1	5

(Potentiële) datalekken dienen geregistreerd te worden in de interne datalekregisters van de defensieonderdelen. Omdat niet alle meldingen ook daadwerkelijk datalekken betreffen, beoordeelt de AVG-coördinator of Wpg-privacyfunctionaris eerst de meldingen en wordt, indien nodig, de FG geconsulteerd. Daarnaast kunnen datalekken in eerste instantie als beveiligingsincident zijn gemeld of is een datalekmelding van een externe partij binnengekomen (in 2024 ging het om acht meldingen). Het aantal datalekken in de interne datalekregisters is daarom ook afwijkend van het aantal ontvangen privacy-voorvalmeldingen. In totaal zijn 213 van de privacy-voorvalmeldingen als datalek geregistreerd. Dit is een afname ten opzichte van 2023. De afname wordt voornamelijk veroorzaakt doordat verloren defensiepassen vanaf 2024 alleen als beveiligingsincident worden geregistreerd, en niet meer in het datalekregister.

	2024	2023	2022	2021	2020
Intern geregistreerde inbreuken	213	285	248	169	109
Aantal meldingen aan AP	32	29	19	17	15

In 2024 meldde Defensie in totaal 32, waarvan 2 nog voorlopig, datalekken bij de AP. Daarmee is het aantal bij de AP gemelde datalekken vergelijkbaar met het aantal in 2023, namelijk 29.

De volgende soorten datalekken kwamen het meest voor:

- Het opslaan van (bijzondere) persoonsgegevens op een openstaande *SharePoint*-omgeving. Dit betreft bijvoorbeeld paspoortgegevens en/of kopieën van paspoorten, rijbewijzen en bankpassen van (oud-) defensiemedewerkers die inzichtelijk zijn op een *SharePoint*-omgeving doordat de toegangsautorisatie niet (meer) goed was ingeregeld. Er hebben dan meer personen toegang tot de persoonsgegevens dan noodzakelijk.
- Datalekken van medische gegevens. Het betreft dan medische gegevens die verstrekt zijn aan een verkeerde zorgverlener, personeel dat niet medisch bevoegd is of aan een verkeerde patiënt. Bijvoorbeeld doordat het aan de verkeerde persoon gemaild of verstuurd is of opgeslagen is in het patiëntendossier van een andere patiënt.
- Verloren of verkeerd bezorgde poststukken.
- Verkeerde mandateringen voor het personeelssysteem, waardoor medewerkers toegang hadden tot meer persoonsgegevens van medewerkers dan noodzakelijk.
- Onbevoegd toegang tot gegevens door verkeerde autorisaties. Dit betreft vooral autorisaties in het personeelssysteem waarbij medewerkers (onbevoegd) toegang krijgen tot personeelsinformatie.

Er zijn meerdere datalekken waarbij er sprake is van een mogelijk hoog risico voor betrokkenen.
Enkele voorbeelden hiervan zijn:

- Het verstrekken van te veel persoonsgegevens in het kader van een reorganisatietraject, bijvoorbeeld een volledig beoordelingsmodel met persoonsgegevens van reorganisaties (BCO-fase 3), toegezonden aan een vakbond in het kader van de begeleidingscommissie personele implementatie. De verstrekking vond niet plaats conform de daarvoor geldende beveiligingsmaatregelen. Het tot overeenstemming komen van een voor beide partijen acceptabele werkwijze is een langlopend traject, dat nog steeds niet is afgerond. Een externe partij is om advies gevraagd.
- Documenten zoals rekesten met onderliggende documenten met gevoelige persoonsgegevens die onterecht in X-Post zijn opgeslagen.
- Een datalek van medische testresultaten dat plaatsvond omdat werd afgeweken van de in de DPIA vastgestelde maatregelen.
- Door een storing van NAFIN, waarvan Defensie de IT-dienstverlener is, zijn persoonsgegevens bij Defensie langere tijd niet beschikbaar geweest. Dit heeft bijvoorbeeld effect gehad op processen in de militaire gezondheidszorg en de afgifte van noodpaspoorten door de KMar. Door middel van *workarounds* is het effect voor betrokkenen zo laag mogelijk gehouden. De storing heeft ook effect gehad op andere aangesloten overheidsdiensten. Het volledige effect van de storing op de beschikbaarheid van persoonsgegevens is onvoldoende inzichtelijk voor de FG. Voor dergelijke grote storingen is een aanscherping van de procedure en de communicatie noodzakelijk.
- Een via de post verstuurd medisch dossier dat door een onbevoegde is geopend.
- Een afgedrukt overzicht van gezondheidsgegevens van medewerkers dat inzichtelijk was voor onbevoegden.

2.6 Rechten van betrokkenen

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

AVG

In 2024 kwamen er 2424 verzoeken binnen middels het online beschikbare formulier. Veruit de meeste van deze verzoeken betreffen informatie- of inzageverzoeken. Van de 2424 verzoeken leidde dit in ongeveer zeven gevallen tot vragen bij de FG over het niet nakomen van de termijn van afhandeling. Met tussenkomst van de FG handelde de organisatie deze vragen af.
Uit een aantal van de FG-toezichtbezoeken in 2024 bleek dat er ook buiten de centrale procedure verzoeken van rechten worden ingediend en afgehandeld, bijvoorbeeld via contactpunten binnen specifieke afdelingen van defensieonderdelen. De reacties vanuit deze afdelingen voldeden niet altijd aan de voorgeschreven vormvereisten uit de (U)AVG.
De procedure(s) voor het afhandelen van rechten van betrokkenen verzoeken zijn onderwerp van het FG-toezicht voor 2025-2026. De CPO zal op basis hiervan een instructie voor het afhandelen van rechten van betrokkenen verzoeken opstellen.

Wpg

In 2024 kwamen 80 informatieverzoeken binnen, ten opzichte van 106 in 2023. Geen van de informatieverzoeken zijn volledig afgewezen. In enkele gevallen is wel door de KMar besloten om, op basis van een uitzonderingsgrond uit artikel 27 Wpg, specifieke informatie niet te delen met een betrokkene.
Daarnaast is er een stijging van het aantal verzoeken om toe te zien op rectificatie en vernietiging van politiegegevens; 10 in 2024 ten opzichte van 4 in 2023.

In 2024 liepen er meerdere (hoger) beroepszaken naar aanleiding van Wpg-besluiten. Er liepen vijftien zaken bij de bestuursrechter in eerste aanleg, waarvan inmiddels een aantal is afgerond en een aantal nog in behandeling is.

Op grond van de Wpg kunnen betrokkenen wiens verzoek om inzage of correctie van politiegegevens is afgewezen, eerst de AP vragen om te bemiddelen, voordat ze in beroep gaan bij de bestuursrechter.
In 2024 diende een betrokkene een bemiddelingsverzoek in bij de AP, naar aanleiding van een afgehandeld Wpg-verzoek. Het bemiddelingsverzoek handelde de privacyfunctionaris KMar in samenspraak met de FG af. Dit leidde tot intrekking van het initiële besluit en het nemen van een nieuw, nader onderbouwd en gemotiveerd besluit.

Klachten

Betrokkenen kunnen contact opnemen met de FG over de verwerking van hun persoonsgegevens en het uitoefenen van hun privacy-rechten (artikel 38, vierde lid van de AVG). De binnengekomen berichten zijn te onderscheiden in onder andere vragen, meldingen (signalen) of klachten. In 2024 kwamen 20 klachten binnen bij de FG. Enkele voorbeelden hiervan zijn klachten over datalekken (bijvoorbeeld e-mailadressen van afgewezen sollicitanten in de cc-regel in plaats van de bcc-regel van een e-mailbericht) en het onvolledig informeren van een betrokkene over de verwerking van zijn persoonsgegevens bij het aanmelden voor een Defensie Infodag. Ook kwamen er meerdere klachten en signalen binnen omtrent het publiceren van beeldmateriaal van defensiemedewerkers op het internet. De FG zag toe op een zorgvuldige afhandeling van de klachten en waar nodig verzocht de FG de organisatie om verbetermaatregelen te nemen.

Er is voor zover bekend een drietal klachten/ bemiddelingsverzoeken bij de AP ingediend in 2024. De klachten of bemiddelingsverzoeken zijn afgehandeld.

Overige zaken

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 Joint IV Commando (JIVC), toegang te verkrijgen tot het digitale account van betrokkene. Hiervoor moet de betreffende beveiligingscoördinator dan toestemming verlenen.
De daadwerkelijke vrijgave vindt vertrouwelijk plaats met gebruikmaking van een *two person*-concept. Van een dergelijke toestemming wordt melding gemaakt bij de FG. In 2024 ontving de FG 7 van dergelijke meldingen.

Defensie is verplicht om mensen duidelijk te informeren over wat de organisatie met hun persoonsgegevens doet en waarom. Deze informatieplicht moet Defensie in principe schriftelijk geven. De AVG stelt een aantal specifieke eisen aan de inhoud, de toegankelijkheid en de duidelijkheid van de informatie. Het Ministerie van Defensie gebruikt hiervoor onder andere een privacyverklaring[15] en het Verwerkingsregister Rijksoverheid[16]. Meerdere defensieonderdelen hebben een eigen privacyverklaring. Een aandachtspunt hierbij is eenduidigheid, juistheid en volledigheid van de verstrekte informatie.

2.7 Verbetermaatregelen

In verschillende 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 FG heeft in het toezichtjaarverslag van 2023 aanbevolen om een systeem in te richten ter borging van de realisatie (en inzicht daarin) van verbetermaatregelen.

De meeste defensieonderdelen hebben verbetermaatregelen gedefinieerd en zijn bezig met het realiseren ervan. Zo heeft COMMIT bijvoorbeeld een Jaarplan/Werkplan AVG 2024/2025 waarin het verbetermaatregelen en geplande activiteiten heeft opgenomen. Verder heeft CLSK een controleslag uitgevoerd om te kijken of alle RPA's van een AVG-advies zijn voorzien. De meeste onderdelen hebben maatregelen genomen om hun privacy-organisatie te versterken. Centraal zijn verbetermaatregelen opgestart met betrekking tot bijvoorbeeld het verbeteren van het register en het verhogen van het volwassenheidsniveau. Hierbij zijn de defensieonderdelen ook betrokken. Het is nog onvoldoende inzichtelijk of alle defensieonderdelen volledig overzicht hebben over en inzicht hebben in alle openstaande verbetermaatregelen, alsmede de status van de realisatie van de verbetermatregelen. Uit een controle door de FG op de realisatie van verbetermaatregelen blijkt dat maar deels centraal inzicht is in en controle is op de voortgang. Een Integraal Risico Management-*tool* wordt door een aantal deelnemers in pilotvorm beproefd. Na het doorvoeren van de feedback uit de *pilot* zal de IRM-tool ter consultatie worden aangeboden aan de privacy-community.

Naast het realiseren van de DPIA's is het van belang dat de defensieorganisatie onder andere de adviezen en maatregelen uit DPIA's ook daadwerkelijk oppakt, zodat ze niet enkel een papieren werkelijkheid blijven. Dit blijft een aandachtspunt.

15 *https://www.defensie.nl/privacy*

16 *https://www.avgregisterrijksoverheid.nl/organisatie/ministerie-van-defensie*

3 Conclusies en aanbevelingen

De afgelopen jaren heeft Defensie door de geopolitieke ontwikkelingen de nadruk steeds meer gelegd op de hoofdtaak 1 van Defensie. Grootschalig gebruik van data, met behulp van onder andere *data science* en AI, vergroot het vermogen van Defensie om de tegenstanders een stap voor te blijven. Zoals ook uit de Defensiestrategie *Data Science* en AI blijkt, moet Defensie informatie snel en slim verkrijgen, verwerken en verspreiden om zo succesvol te kunnen reageren op activiteiten van de tegenstander. Hiervoor is de beschikking over grote hoeveelheden data onontbeerlijk, maar tegelijkertijd bevat deze data ook vaak persoonsgegevens. Daarbij heeft Defensie altijd de verantwoordelijkheid en de verplichting om de grondrechten van burgers en haar eigen medewerkers te respecteren, te beschermen en zich te houden aan 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.

De afgelopen jaren deed de FG in haar toezichtrapporten en toezichtjaarverslagen aanbevelingen ter verbetering van de naleving van de AVG en de Wpg. De defensieorganisatie verzette het afgelopen jaar veel werk wat betreft de borging van de naleving van de privacywetgeving.
De defensieorganisatie besteedde aandacht aan onder andere het opstellen van gegevensbeschermingsbeleid, het versterken van de privacy-organisatie, aan het verhogen van de volwassenheid, het verbeteren van de kwaliteit van het register van verwerkingsactiviteiten, het DPIA-proces en het datalekproces. Tevens voerde zij diverse bewustwordingsactiviteiten uit. Het effect van de verbeteractiviteiten is niet altijd direct zichtbaar, omdat niet alle activiteiten al hebben geleid tot afgeronde producten of een aantoonbaar effect.
De geplande volwassenheidsmeting kan hier een bijdrage aan leveren door beter inzichtelijk te maken waar de organisatie staat.

Belangrijke aandachtspunten bij de ontwikkelingen zijn het inrichten van toereikende waarborgen met betrekking tot gegevensbescherming bij de verwerking van persoonsgegevens en de toetsbaarheid van deze waarborgen. De ontwikkelingen vragen ook om vaardige AVG-coördinatoren met brede kennis en om toereikende capaciteit. Tot slot vraagt het om structurele samenwerking met de operationele en de juridische lijn en om tools ter ondersteuning van de werkzaamheden.

Aanbeveling 1:

Versterk de privacy-organisatie bij JIVC, DS en BS.
Bij deze organisatieonderdelen is de capaciteit nog ontoereikend om voldoende uitvoering te kunnen geven aan de taken. Ook bij andere defensieonderdelen zoals CZSK en CLSK staat de realisatie van de werkvoorraad onder druk. Verwacht wordt dat in 2025 de ontwikkelingen in het kader van hoofdtaak 1 ook een sterk effect zal hebben op de toch al beperkte capaciteit van de AVG-coördinatoren, ook door het ontbreken van AVG-capaciteit en kennis bij de Defensiestaf.

Aanbeveling 2:

Richt een systeem in ter borging en verantwoording van de realisatie van verbetermaatregelen.
Breng de aanbevolen verbetermaatregelen met betrekking tot naleving van gegevensbescherming afkomstig uit diverse bronnen in kaart en borg de realisatie hiervan beter.

Aanbeveling 3:

Signaleer en analyseer risico's van AI- en algoritmes en zorg voor uitleg over de risico's van algoritmes en hoe algoritmes verantwoord zijn in te zetten.
Maatregelen zijn nodig om op verantwoorde wijze gebruik te maken van alle mogelijkheden die AI te bieden heeft. Hierbij kan gedacht worden aan het op korte termijn registreren van risicovolle AI- of algoritmische toepassingen, het vergroten van de bewustwording bij de inzet van AI en het inzichtelijk maken van de effecten en de risico's bij algoritmische toepassingen.

Aanbeveling 4:

Zorg voor realisatie van de maatregelen ter borging van de naleving van de Wpg.
FG constateert dat er nog beperkte voortgang is voor wat betreft het daadwerkelijk nemen van verbetermaatregelen ten opzichte van 2022-2023 met betrekking tot de naleving van de Wpg, het CARIB-dossier en de implementatie van de loggingplicht.

Aanbeveling 5:

Zorg voor inzicht en overzicht in de DPIA's en tijdige actualisatie van DPIA's.
Volledig inzicht in en overzicht van uitgevoerde, lopend, te actualiseren en nog benodigde DPIA's is onvoldoende beschikbaar. Daarnaast loopt de actualisatie van al langer bestaande DPIA's achter. Van de 19 DPIA's die toe zijn aan actualisatie, is één gewijzigde DPIA aangeboden aan de FG ter appreciatie.

Aanbeveling 6:

Zorg bij wetgevingstrajecten, nieuwe of gewijzigde verwerkingen en innovatietrajecten voor toereikende waarborgen voor de bescherming van persoonsgegevens.
Belangrijk aandachtspunt bij nieuwe of gewijzigde verwerkingen is het inrichten van toereikende en controleerbare waarborgen met betrekking tot gegevensbescherming bij het verkrijgen en verwerken van persoonsgegevens en aandacht voor de toezichtbaarheid ervan. Borg de toetsing van de waarborgen door de toezichthouder(s).

4 Bijlagen

4.1 Bevindingen per defensieonderdeel

	AVG- en Wpg-organisatie	CZSK	CLAS	CLSK	KMar AVG	KMar Wpg	BS	BS DOPS	Defensie breed[17]	COMMIT	DOSCO
A	AVG-beheerders hebben een AVG-coördinator aangewezen. De Wpg-beheerder heeft een privacyfunctionaris aangewezen.							A1			
B	De functie(s) zijn in 2024 gevuld geweest.	B1				B2		B3		B4	
C	De AVG-coördinatoren en PF zijn aangemeld bij de FG.	C1				C2		B3	C3		
D	De beheerder heeft een jaarrapportage aangeleverd.	D2		D2	D2	D2		D1	D2		
E	De werkvoorraad in 2024 staat in verhouding tot de capaciteit (kwantitatief en kwalitatief) bij de onderdelen.	E1		E2	E3	E4	E5		E6	E7	
F	Het defensieonderdeel heeft activiteiten uitgevoerd in het kader van 'AVG- en Wpg-*awareness*'.	F1			F1						
G	AVG-coördinator heeft inzicht in afgesloten verwerkers-overeenkomsten	G1	G1	G1		G1	G1		G2	G1	G1

Ja/goed
Verbetering nodig
Nee
Geen informatie ontvangen

A1: Er is in 2024 geen AVG-coördinator (ten behoeve van de RGMO) aangewezen.

B1: De huidige AVG-coördinator (burger) is aangesteld per 1 november 2023. Per december 2024 is de militair AVG-coördinator opgevolgd door zijn opvolger. Gedurende 2024 was de (militair) AVG-coördinator regelmatig afwezig vanwege uitzendingen en (verplichte) cursussen. De aanstelling van een nieuwe (burger) coördinator heeft een noodzakelijke overgangsperiode met zich meegebracht, waarin tijd en ruimte nodig was voor inwerken en vertrouwd raken met de organisatie, de interne processen en het complexe werkveld van gegevensbescherming binnen Defensie.

B2: Twee privacyfunctionarissen zijn geplaatst bij het cluster Juridische Zaken. Wegens omstandigheden bestond de capaciteit in 2024 de facto uit één privacyfunctionaris.

B3: De functie is geheel 2024 niet gevuld geweest.

B4: De functie van AVG-coördinator voor JIVC is voor een deel van 2024 vacant geweest. De functie is gedurende die tijd wel waargenomen door de voormalige AVG-coördinator.

C1: CZSK heeft in 2023 een tweede AVG-coördinator aangewezen. De nieuwe AVG-coördinator die eind 2024 is gestart is nog niet aangemeld bij de FG.

C2: De (nieuwe) privacyfunctionaris is nog niet formeel aangemeld bij de FG.

C3: Tot 1 oktober 2023 zijn de taken belegd geweest binnen CPO. Formalisering van de taken van de functie bij de DAOG moet nog plaatsvinden. Formalisering van de belegging van taken voor defensiebrede processen moet nog plaatsvinden.

D1: Een rapportage, conform artikel 1.3, lid 4 van de Regeling AVG Defensie is niet aangeleverd.

D2: Een concept rapportage is aangeleverd door de AVG-coördinator. Een vastgestelde rapportage dient nog aangeleverd te worden.

E1: De huidige werkvoorraad binnen CZSK staat onder aanzienlijke druk in verhouding tot de beschikbare capaciteit.

E2: De werkvoorraad staat niet in verhouding tot de capaciteit binnen CLSK, ook na de start van de tweede AVG-coördinator en de tijdelijke ondersteuning door de junior. Dat heeft enerzijds te maken met de complexiteit van de materie, de gevoeligheid en tijdsdruk. Anderzijds heeft het te maken met continue toestroom van meer behoefte aan advisering, terwijl de reeds bestaande *workload* niet afneemt.

E3: Vanwege de grote hoeveelheid aan werk en het tekort aan personeel hebben enkele taken noodgedwongen minder aandacht gekregen dan gewenst.

E4: De huidige werkvoorraad brengt uitdagingen met zich mee in verhouding tot de beschikbare capaciteit van de privacyfunctionarissen, zowel op kwantitatief als kwalitatief vlak.
Prioriteiten moesten gesteld worden waardoor in de praktijk echter weinig ruimte over blijft om invulling te geven aan interne controle en de ongevraagde adviestaak. Dit structurele gebrek aan capaciteit belemmert de mate waarin proactieve naleving en verbeteringen binnen de organisatie kunnen worden gerealiseerd.

E5: De werkvoorraad is groter dan de beschikbare tijd. Dit geldt zowel in kwalitatief als in kwantitatief opzicht. Ook is meer specialistische kennis benodigd.

E6: Werkzaamheden ten behoeve van de Wet op de Defensie Gereedheid nemen veel tijd in beslag, wat ten koste gaat van andere dossiers.

E7: Als gevolg van alle intensiveringen, investeringen en vernieuwingen in techniek op de gebieden Materieel en IT, zijn de werkzaamheden aanzienlijk toegenomen. De inrichting van een decentraal CIO- stelsel vraagt eveneens aandacht voor raakvlakken en versterkingen op het gebied van gegevensbescherming. De acties die opgezet zijn om tot de nodige capaciteitsuitbreiding c.q. herschikking te komen, zijn (nog) niet gerealiseerd.

F1: Het bevorderen van bewustwording over de AVG heeft ook in 2024 noodgedwongen minder aandacht gekregen dan gewenst.
De voornaamste reden hiervoor is de grote hoeveelheid aan werk en het tekort aan personeel.

G1: AVG-coördinatoren hebben geen doorlopende toegang tot of inzicht in de afgesloten verwerkersovereenkomsten. Dit is een defensiebrede verbeteractie. Meerdere AVG-coördinatoren hebben aangegeven betere contacten te hebben opgebouwd met Inkoop.

G2: Er wordt een overzicht ontvangen uit ERP M&F van verwerkersovereenkomsten. Het overzicht is niet volledig.

4.2 Afkortingen

ADR	Auditdienst Rijk
AI	*Artificial Intelligence* (kunstmatige intelligentie)
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
BIDKL	Bergings- en Identificatiedienst Koninklijke Landmacht
BJAA	Bureau Justitiële Administratie en Archieven
BS	Bestuursstaf
CIO	*Chief Information Office*
CLAS	Commando Landstrijdkrachten
CLSK	Commando Luchtstrijdkrachten
COMMIT	Commando Materieel en IT
CPO	*Chief Privacy Office*
CTI	*Cyber Threat Intelligence*
CZSK	Commando Zeestrijdkrachten
DCPL	Dienstencentrum Personeelslogistiek
DCSC	Defensie *Cyber Security* Centrum
DOO	Defensie Open op Orde
DOPS	Directie Operaties
DOSCO	Defensie Ondersteuningscommando
DPIA	*Data Protection Impact Assessment* (Gegevensbeschermingseffectbeoordeling)
FG	Functionaris voor Gegevensbescherming
IGO	Informatiegestuurd optreden
JIVC	Joint IV Commando
KMar	Koninklijke Marechaussee
PF	Privacyfunctionaris
PSMV	*Peoplesoft* Melden Voorvallen
PvA	Plan van Aanpak
REAIM	*Responsible artificial intelligence in the military domain*
RGMO	Regeling Gegevensbescherming Militaire Operaties
RPA	*Robotics Process Automation*
RPFG	Rijksplatform FG's
UAVG	Uitvoeringswet AVG
Wjsg	Wet justitiële en strafvorderlijke gegevens.
Wpg	Wet politiegegevens