Ministerie van Defensie

Toezicht-jaarverslag 2025

Functionaris voor Gegevensbescherming

Colofon

Functionaris voor Gegevensbescherming

Adres
Kantoorgebouw Koningskade 4
te Den Haag

Postadres
Kalvermarkt 38
2511 CB ‘s-Gravenhage
MPC 58B

Datum
Maart 2026

Voorwoord

De Functionaris voor Gegevensbescherming (FG) houdt intern Defensie geïntegreerd toezicht op de naleving van het gegevensbeschermingsrecht vanuit de Algemene Verordening Gegevensbescherming (AVG), de Wet Politiegegevens (Wpg) en de verantwoorde inzet van *Artificial Intelligence* (AI) en algoritmes (AI-verordening). In 2025 bracht de FG de naleving en juiste toepassing van het gegevensbeschermingsrecht veelvuldig onder de aandacht en is zowel toezicht gehouden als advies geboden.

Op het Ministerie van Defensie rust enerzijds een grote verantwoordelijkheid ten aanzien van verwerking van persoonsgegevens in het kader van intern beheer en personeelszaken. Anderzijds breidt de verwerkingsverantwoordelijkheid van Defensie zich in het licht van de technologische en geopolitieke (veiligheids)ontwikkelingen in de maatschappij en de samenleving verder uit, ook internationaal.

In lijn met de Defensievisie 2035 'Vechten voor een veilige toekomst' besteedde de FG in 2025 meer aandacht aan de verwerking van persoonsgegevens bij ontwikkelingen en innovaties in het kader van een informatiegestuurde krijgsmacht. Tevens leverde de FG een substantiële bijdrage aan de totstandkoming van het wetsvoorstel Wet op de defensiegereedheid (Wodg), onder meer door het appreciëren van de wetgevings *Data Protection Impact Assessment* (DPIA) en de herijking van de juridische kaders voor Defensie.

Als interne toezichthouder zocht de FG voortdurend naar een goede balans tussen bewustwording en naleving van het gegevensbeschermingsrecht enerzijds en een goede, veilige, efficiënte en wettelijke verantwoorde uitvoering van de defensietaken anderzijds.

De veiligheidssituatie in de wereld verslechtert en dat vraagt om een krijgsmacht die gereed is voor alle hoofdtaken, met een toenemende druk op hoofdtaak 1: de bescherming van ons eigen grondgebied en dat van de NAVO-bondgenoten. De defensieorganisatie gaat door een diepgaande transitie. De actuele dreiging van hybride en/of gewapende conflicten en crisissituaties verplichten Defensie om voor haar grondwettelijke doelstellingen toereikend eenheden gereed te stellen. Deze eenheden dienen in voldoende mate getraind en geoefend te 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.

Het toezicht richt zich in toenemende mate op het gegevensbeschermingsrecht in de maatschappelijke context van het defensieoptreden en de bescherming van fundamentele rechten en vrijheden van personen in de samenleving wiens persoonsgegevens mogelijk door Defensie verwerkt worden. Hierbij gaat het niet alleen om structurele of incidentele taken onder gezag van civiele autoriteiten bij de handhaving van de openbare orde of rechtshandhaving, zoals de Koninklijke Marechaussee (KMar) politietaken, de Kustwacht of bijstandsverlening. Het gaat ook om het verwerken van persoonsgegevens tijdens operationele taakuitvoering, zoals het bewaken en beveiligen van militaire objecten en gegevensbeschermingsvraagstukken rond gereedstellingsactiviteiten, zoals trainingen en oefeningen met drones en sensoren.

De balans tussen veiligheid en privacy kan onder operationele omstandigheden en wijzigende juridische kaders anders worden opgemaakt dan tijdens oefeningen en trainingssituaties. Overheidshandelen dat ingrijpt in (grond)rechten en vrijheden dient altijd te berusten op een wettelijke grondslag. Alleen door privacy- en gegevensbeschermingsrecht tijdig en naar behoren te betrekken en beter in innovatie- en moderniseringsprocessen te integreren, kan Defensie verantwoord versnellen.

Inhoud

1 Toezicht 2025 6
1.1 Uitgevoerde toezicht taken en werkzaamheden 7

2 Hoofdlijnen uit het toezicht 14
2.1 Verantwoording 15
2.2 Privacyorganisatie 15
2.3 Beleid 16
2.4 Volwassenheid 17
2.5 Bewustwording 17
2.6 Verwerkersovereenkomsten 18
2.7 Data Protection Impact Assessments 18
2.8 Inbreuken op de beveiliging (datalekken) 19
2.9 Rechten van betrokkenen 20
2.10 Systeem ter borging realisatie verbetermaatregelen 22
2.11 Samenwerking Toezichtberaad Defensie 23
2.12 Samenwerking buiten Defensie 23

3 Conclusies en aanbevelingen 24

4 Bijlagen 28
4.1 Afkortingen 29

1 Toezicht 2025

De Functionaris voor Gegevensbescherming (FG), ook wel *Data Protection Officer* (DPO), is binnen het Ministerie van Defensie de interne toezichthouder op de naleving van de wet- en regelgeving rond gegevensbescherming en privacy.

Het toezicht staat in het teken van de bescherming van de persoonlijke levenssfeer, de rechtmatige verwerking van persoonsgegevens en de in dat verband verantwoorde inzet van AI en algoritmes.

De AVG, de uitvoeringswet AVG (UAVG), de Wpg en de AI-verordening vormen de wettelijke basis voor het FG-toezicht.

De FG maakt zich iedere dag, binnen de gehele privacyketen, sterk voor een zorgvuldige omgang met alle persoonsgegevens die Defensie verwerkt en het optimaal waarborgen van het recht op gegevensbescherming en privacy. Desgevraagd doet de FG dat in samenwerking met de externe toezichthouder, de Autoriteit Persoonsgegevens (AP).

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 privacyrechten kunnen uitoefenen en ziet toe op een correcte afhandeling van datalekken en klachten over het verwerken van persoonsgegevens.

Defensie bevond zich in 2025 binnen een steeds complexere dreigingsomgeving in een reeks van ontwikkelingen: de versnellende gereedstelling voor hoofdtaak 1, de verdergaande digitalisering van de krijgsmacht en de samenleving, en een toenemende groei van toepassingen met AI. Dit leidt noodzakelijkerwijs tot personele, materiele en digitale versterking van capaciteiten, waarbij Defensie in een hoog tempo uitbreidt en tegelijkertijd procedures vereenvoudigd worden.

In 2025 zetten de FG en de gehele privacyorganisatie zich in om aansluiting te behouden bij de dynamische ontwikkelingen en het toezicht en de naleving op het gegevensbeschermingsrecht effectief en constructief in te richten.

Dit toezichtjaarverslag behandelt een selectie van relevante ontwikkelingen en toezichtonderwerpen en sluit af met conclusies een aanbevelingen. Het arbeidsintensieve karakter van de eerder genoemde FG-bijdrage aan de Wodg en een aantal ad hoc activiteiten naar aanleiding van incidenten was van invloed op de (niet uitputtende) uitvoering van het FG-toezichtjaarplan 2025.

1.1 Uitgevoerde toezicht taken en werkzaamheden

Toezichtwerkzaamheden FG

Toezichtbezoeken Dienstencentrum Personeelslogistiek (DCPL): In 2024 startte de FG een reeks toezichtbezoeken bij een aantal onderdelen van DCPL (*Defensity College*, *Employability*, Dienjaar, Veiligheid & Vakmanschap en de afdeling Selectie & Keuringen). In 2025 zijn de onderzoeken afgerond en stelde de FG per bezocht DPCL-onderdeel een deelrapport op. Over het algemeen genomen is de aandacht voor de bescherming van persoonsgegevens het afgelopen jaar bij alle bezochte DCPL-onderdelen toegenomen. Toch constateerde de FG bij alle onderdelen nog een aantal aandachtspunten, waarop de FG aanbevelingen deed in de deelrapporten. Algemene aandachtspunten zijn het registeren van alle specifieke DCPL-verwerkingen van persoonsgegevens in het register van verwerkingsactiviteiten, het (verder) toepassen van dataminimalisatie, het afsluiten en/of actualiseren van verwerkersovereenkomsten, het verbeteren van de informatievoorziening (transparantie) richting de betrokkenen en het adequaat afhandelen van verzoeken van betrokkenen (bijvoorbeeld inzageverzoeken). De FG deed per bezocht DCPL-onderdeel ook een aantal specifieke bevindingen en aanbevelingen. Zo is bij *Defensity College* aandacht gevraagd voor de realisatie

van al eerder onderkende verbetermaatregelen[1] over onder andere het verder toepassen van dataminimalisatie en het opstellen en toepassen van bewaartermijnen. Bij meerdere eenheden vroeg de FG aandacht voor de beveiliging van persoonsgegevens en voor naleving van wet- en regelgeving bij het gebruik van sociale media (bijvoorbeeld over het plaatsen van foto's waarop defensiemedewerkers herkenbaar staan). Bij Selectie & Keuringen is aandacht gevraagd voor het opstellen van een DPIA voor het proces van de (medische) aanstellingskeuring, voor de rechtmatigheid van het verwerken van bijzondere persoonsgegevens bij de psychologische selectie en voor het voldoen aan in de wet gestelde voorwaarden en beperkingen bij geautomatiseerde besluitvorming. Commandant DCPL gaf eind 2025 aan de FG een update van de stand van zaken van de verbetermaatregelen.[2]

Enquête Dienjaar: Een van de instrumenten die Defensie toepast om het dienmodel te ondersteunen en versneld te groeien naar een inzetbare en schaalbare krijgsmacht, is de invoering van een Defensie-enquête.[3] Deze enquête is bedoeld om beter en directer zicht te krijgen op de doelgroepen die willen werken voor Defensie en om de instroom te verhogen. De enquête wordt vanaf eind 2025 meegezonden met de dienstplichtbrief die alle 17-jarigen ontvangen van Defensie, waarbij verzocht wordt deze enquête vrijwillig in te vullen. Dit gebeurde vooruitlopend op aankomende specifieke regelgeving om de volledige doelgroep (17-27-jarigen) aan te schrijven. In het belang van een zorgvuldige inzet van dit instrument en de tijdige start van de verzending van de enquêtes, werd onder andere een geactualiseerde versie van de DPIA op het instroomproces ter appreciatie aangeboden aan de FG Defensie. Met het oog op het voldoende mitigeren van de onderkende risico's en het treffen van maatregelen om mogelijke hoge risico's te vermijden, vonden meerdere adviesgesprekken en afstemmomenten met de projectgroep plaats, in samenwerking met het *Chief Privacy Office* (CPO) en de Beveiligingsautoriteit (BA).

Toezichtbezoek TrainingsGeneeskunde & TrainingsFysiologie (TGTF): De FG bracht in 2025 een bezoek aan TGTF. Tijdens dit bezoek gaf TGTF uitleg over hun werkzaamheden en de problemen waar ze tegenaan lopen met het verwerken van persoonsgegevens. Vooral bij onderzoek op het gebied van gezondheid met betrekking tot beschermende maatregelen tegen extreme (weers)omstandigheden loopt TGTF tegen het vraagstuk van een ontbrekende grondslag voor de gegevensverwerking aan. Het zonder duidelijke grondslag verwerken van (bijzondere) persoonsgegevens met betrekking tot gezondheid levert extra risico's op voor betrokkenen en de organisatie. Tegelijkertijd wil TGTF zorgdragen voor de veiligheid en gezondheid van militairen. Er is vanuit TGTF een grote behoefte aan duidelijkheid en eenduidigheid van beleid binnen Defensie op dit gebied. Voor een heldere grondslag voor het onderzoek van TGTF is een wetswijziging benodigd. Er is afgesproken dat er vanuit de AVG-coördinatoren een werkgroep wordt opgezet om mee te denken over deze vraagstukken. De FG sluit hierbij aan.

Defensie Open op Orde (DOO): De toeslagenaffaire leidde ertoe dat het kabinet besloot een verandering van de informatiehuishouding van het Rijk in gang te zetten. Binnen Defensie heeft dit geleid tot de start van DOO, om de informatiehuishouding op orde te brengen en een gezaghebbende informatiepositie te verkrijgen en behouden. Aandacht voor een zorgvuldige omgang met en beveiliging van persoonsgegevens binnen het DOO-programma is voor de FG een belangrijk onderwerp.[4] In 2025 is binnen het DOO-programma een *dedicated* AVG-coördinator aangesteld. Tevens is bij de FG een inspecteur aangesteld die de focus heeft op DOO en de informatiehuishouding. In 2025 is door de *Chief Information Office* (CIO) de DPIA DefDoc aangeboden voor advies van de FG. DPIA's met betrekking tot het archiveren van e-mails en chatberichten zijn nog niet aangereikt voor advies. De FG besteedt, samen met de AVG-coördinator DOO en het CPO, ook in 2026 aandacht aan het creëren van *awareness* voor gegevensbescherming binnen DOO.

1 Verbeterplan AVG Compliancy Defensity College, versie 0.3, 20241108.
2 Nota Update n.a.v. FG Toezichtbezoek DCPL, kenmerk DOSCO2025038450. 19 december 2025.
3 Zie Kamerstukken II, 2024-2025, 36592 nr.45, 22 september 2025, Brief van de Staatssecretaris van Defensie: Start Defensie-enquête.
4 Zie ook FG Toezichtjaarplan 2025. BS20260000044

Algemene Beveiligingseisen Rijksbrede Opdrachten (ABRO): Defensie stelt eisen ten aanzien van cyberveiligheid en bestuurlijke, organisatorische, personele en fysieke veiligheid van bedrijven, voordat zij in aanraking mogen komen met bijzondere informatie en/of te beschermen belangen. Deze eisen staan beschreven in de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). Binnen Defensie wordt reeds geruime tijd gewerkt met de ABDO-procedure, om zo de nationale veiligheid bij inkoopopdrachten te waarborgen. Binnen het Rijk wordt gewerkt aan het uitrollen van de Algemene Beveiligingseisen Rijksbrede Opdrachten (ABRO). Voor ABRO is een DPIA ter appreciatie aangeboden aan het Rijksplatform van Functionarissen voor de Gegevensbescherming (RPFG), waar ook de FG Defensie in participeert. Het RPFG signaleerde in haar advies een tiental risico's en benoemde een aantal zorgpunten. Met name de (wederzijdse) overgang van verwerkingen tussen de werkingssfeer van AVG en de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) kan ervoor zorgen dat betrokkenen hun rechten niet of niet voldoende kunnen uitoefenen, doordat niet duidelijk is onder welk regime en onder wiens verantwoordelijkheid persoonsgegevens op welk moment worden verwerkt.

Verbetermaatregelen Wet Politiegegevens (Wpg): De FG constateerde in het toezichtjaarverslag 2024 dat er nog beperkte voortgang is op het daadwerkelijk nemen van verbetermaatregelen ten opzichte van 2022-2023 met betrekking tot de naleving van de Wpg. Specifiek gaat het om verwerkingen in de Caribische gebiedsdelen en de implementatie van de Wpg loggingsplicht.

De Wpg legt een auditverplichting op grond van artikel 33 Wpg op. 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 moeten worden beoordeeld.[5] 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. In 2025 heeft de Auditdienst Rijk (ADR) de *audit* bij de KMar uitgevoerd over de periode 2019-2022. Aan de hand hiervan stelde de KMar een verbeterrapport op, met de te nemen maatregelen om te voldoen aan de Wpg-normen. Om beter richting te kunnen geven aan de uitvoering van het Wpg-verbeterplan belegde Commandant KMar (C-KMar) in 2025 het Wpg-onderbeheer bij de Directeur Informatie &Technologie/dCIO. Hiermee is de centrale coördinatierol binnen de KMar eenduidig vastgelegd. In 2025 vonden er verscheidene verbeteracties plaats, die met name gericht waren op de structurele borging van de taken en verantwoordelijkheden binnen de Wpg-organisatie. Daarnaast zijn verbetermaatregelen uitgevoerd, gericht op normen uit de Wpg op het gebied van autorisatie(beheer) en doelbinding. Ook is er in 2025 een auditcoördinator aangewezen voor de periodieke interne Wpg-*audits* en de begeleiding van externe *audits*.

De FG verzocht eind 2022 C-KMar[6] om aan te geven welke interne verbetermaatregelen zijn genomen om een aantal eerder gesignaleerde knelpunten op te lossen. Deze knelpunten hadden betrekking op 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. In 2025 vonden er beperkte ontwikkelingen plaats ten aanzien van dit onderwerp. Er is een verwerkersovereenkomst en dienstverleningsovereenkomst afgesloten om *compliance* met de Wpg beter te kunnen borgen. Volgens de KMar is dit een eerste stap om Wpg *compliance* binnen een deel van Caribisch Nederland beter te kunnen waarborgen. In 2026 wordt er door Cluster Juridische Zaken (CJZ) KMar, CIO en het CPO een werkbezoek ingepland.

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 het vernietigen van politiegegevens. De logbestanden moeten het mogelijk maken de redenen, de datum en het tijdstip van die handelingen te achterhalen en indien noodzakelijk de rechtmatigheid te beoordelen. Tevens wordt, indien mogelijk, de identiteit vastgelegd van de persoon die de politiegegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die

5 Regeling periodieke audit politiegegevens.
6 Nota Gegevensverwerkingen KMar CARIB. 8 december 2022. BS2022031914.

politiegegevens. Artikel 32a Wpg is na een overgangsperiode sinds eind 2023 van kracht. De inrichting van de *logging* was in 2025 nog niet voldoende technisch ingericht. De verwachting is dat de eerste systemen begin 2026 technisch voldoen aan de loggingsplicht.

DPIA-evaluatie: De FG voerde in 2025 in gezamenlijkheid met het CPO een evaluatie uit van de procedure voor het uitvoeren van DPIA's die toentertijd een jaar in gebruik was. Het doel van deze evaluatie was om inzicht te krijgen in de inrichting van en ervaringen met het huidige DPIA-proces om de doeltreffendheid van het DPIA-proces te verbeteren. Een passend werkproces voor de uitvoering van DPIA's en een adequate uitvoering daarvan bevordert de kwaliteit van de DPIA's en stelt de organisatie in staat om de risico's voor betrokkenen te identificeren en te mitigeren. Uit de evaluatie zijn verscheidene verbetermaatregelen voortgekomen die in de komende maanden worden doorgevoerd. Bijvoorbeeld het aanpassen van formats ten behoeve van verwerkingen in het kader van de Wpg, het ondersteunen bij risicoworkshops en het creëren van helderheid over de definitie van defensiebrede verwerkingen. Een scherpe definitie ontbreekt, waardoor (te) veel verwerkingen als defensiebreed worden aangemerkt. In de praktijk leidt dit ertoe dat veel verwerkingen centraal onder de Defensiestaf vallen, terwijl de privacycapaciteit daar beperkt is en de uitvoeringsverantwoordelijkheid bij een defensieonderdeel is belegd. Dit resulteert in vertraging bij de uitvoering en herziening van DPIA's.

Wet op de defensiegereedheid (Wodg): Het Ministerie van Defensie bereidt sinds augustus 2024 een wetsvoorstel voor de Wodg voor. De FG levert door middel van gevraagd en ongevraagd advies een bijdrage aan het wetgevingstraject. Op grond van de motie Franken[7] zijn rijksorganisaties verplicht een Gegevensbeschermingstoets/wetgevingsDPIA uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien en waarbij mogelijk het grondrecht op bescherming van de persoonlijke levenssfeer wordt beperkt. Het doel is om de bescherming van persoonsgegevens mee te nemen in de belangenafweging en besluitvorming rond de ontwikkeling van nieuwe wet- en regelgeving. Zodoende kan het wetsvoorstel worden verbeterd en kunnen de gemaakte keuzes en afwegingen worden toegelicht in de memorie van toelichting. De wetgevingsDPIA Wodg is aan de FG voorgelegd ter advies. De FG-appreciatie is in maart 2025 afgegeven. Tevens is de FG verzocht om een uitvoerbaarheids- en handhaafbaarheidstoets uit te voeren op het concept wetsvoorstel. Deze leverde de FG in juli 2025 aan bij de Directie Juridische Zaken (DJZ). Eind 2025 is in de ministerraad besloten het wetsvoorstel voor advies voor te leggen aan de Raad van State. Daarna volgt behandeling in de Tweede en Eerste Kamer.

Inventarisatie Innovatieprojecten: In 2025 startte de FG een verkennend onderzoek om te achterhalen of het rechtmatig en zorgvuldig verwerken van persoonsgegevens inclusief verantwoord toepassen van AI en Algoritmes bij Defensie-innovatieprojecten (vroegtijdig) wordt onderkend. Ook wil de FG achterhalen of er in innovatieprojecten voldoende kennis en bewustzijn is over de geldende eisen uit de AVG, Wpg en/of AI-verordening. Defensie heeft een platform dat innovaties samenbrengt en collega's de kans biedt om eenvoudig samen te werken. De FG heeft ongeveer 350 innovatieprojecten aangeschreven om een beeld te krijgen van de mate van kennis omtrent de AVG, Wpg en/of de AI-verordening. Op basis van de antwoorden vond er een analyse plaats en het streven is om in 2026 hieraan opvolging te geven. Enerzijds is het de bedoeling om het platform verder te optimaliseren op het gebied van privacy en AI-*compliance*, zodat collega's die een project starten weten wat er op dat gebied van ze wordt verwacht. Anderzijds zullen projecten waar potentieel hoge risico's aan vastzitten nader worden beoordeeld om, indien nodig, met *guidance* en advies tijdig bij te sturen.

Schadevergoedingsregeling Indonesië: De Minister van Buitenlandse Zaken (BZ) en de Minister van Defensie hebben de opdracht gekregen om een bestaand overzicht bekend te stellen van personen die tijdens militaire acties in Indonesië zijn omgekomen of anderszins slachtoffer zijn geworden van geweld door Nederlandse militairen die actief waren in (post)koloniale tijd in Indonesië. Deze opdracht volgt uit de aangenomen motie van het lid Sjoerdsma c.s. van 14 juni 2023[8], inzake het lokaal bekendstellen van het samengestelde overzicht door het Nederlands Instituut

7 Motie-Franken (CDA) c.s, aangenomen 18 mei 2011, Kamerstukken I 2011, 31.051, nr. D.
8 Kamerstukken II 2022-2023, 26 049, nr. 101 (motie) en Handelingen TK 2022-2023, 95/18 (stemming over de motie).

voor Militaire Historie (NIMH) en het in behandeling nemen van claims (van nabestaanden) van slachtoffers van standrechtelijke executies, martelingen en verkrachtingen in het voormalige Nederlands-Indië. Het voornemen is om de bestaande overzichten te verstrekken aan een bestaande Indonesische stichting, die nabestaanden reeds ondersteunt bij de aanvraag van schadevergoedingen. Deze verstrekking van persoonsgegevens geldt als internationale doorgifte, waarvoor de AVG aanvullende eisen en waarborgen stelt. In 2024 is reeds een *Data Transfer Impact Assessment* (DTIA) door de FG's van BZ en Defensie van een advies voorzien. Vanwege de gevoelige aard van de gegevens en de situatie, is op advies van de FG's BZ en Defensie een DPIA opgesteld. Op 28 augustus 2025 is een gezamenlijk FG-advies op de DPIA uitgebracht. Momenteel wordt de DPIA aangepast naar aanleiding van het gezamenlijk advies. De FG verwacht dat de DPIA in 2026 wordt vastgesteld.

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 de (eenduidige) opbouw/invulling van het register, het verbeteren van de kwaliteit van de registraties, en richtlijnen voor de interpretatie en harmonisatie van de toepassing van verwerkingsgrondslagen. In 2024 startte het CPO een project voor het onder andere ontwikkelen van een helder raamwerk om de opzet en uniformiteit van het register te verbeteren. In samenwerking met de FG leidde dit in 2025 tot een hernieuwde opzet van het register, die de uniformiteit moet verbeteren. De instructie voor het beheren en onderhouden van het register en een handleiding ten behoeve van het uniform en consistent invullen van de informatievelden levert het CPO begin 2026 op.
Daarnaast besteedde de FG in 2025 veel tijd aan de totstandkoming van een passend raamwerk voor het register, door onder andere te ondersteunen en adviseren bij het actualiseren van de generieke selectielijst voor archiefbescheiden van Defensie. Beoogd is om de opbouw en de indeling van het register van verwerkingsactiviteiten voor de AVG en de Wpg te verbeteren en in de basis te harmoniseren met het beschrijvingsniveau, met processen en met handelingen van de generieke selectielijst. In 2026 wordt een analyse gedaan op het vernieuwde register om te bezien welke processen (en daarmee eventuele DPIA's) er ontbreken.

Algoritmeregister: Defensie kent de interne verplichting algoritmes te inventariseren en te registreren. Deze registratie dient meerdere doelen. Allereerst verbetert registratie de risicobeheersing van algoritmische toepassingen. Daarnaast creëert het een intern inzicht en overzicht. Dit inzicht en overzicht versterkt de transparantie van het gebruik en biedt behoeftestellers en ontwikkelaars van algoritmische toepassingen en AI de mogelijkheid om te kijken of een gewenste toepassing al niet reeds voorhanden is.

De FG constateert dat in 2025 alle defensieonderdelen concrete stappen hebben gezet in de inventarisatie en de registratie van algoritmes. Wat echter ook blijkt is dat de registratie en inventarisatie niet compleet zijn en dat een gestructureerde eenduidige werkwijze met instructies en een gestandaardiseerde registratietool ontbreekt. Het is bovendien belangrijk te realiseren dat deze registratie niet een eenmalige exercitie is. De inventarisatie en registratie van algoritmes moet een voortdurend proces zijn, waarbij het van belang is dat het gecreëerde overzicht actueel is. De AP biedt in de recent verschenen handreiking 'Aan de slag met algoritmeregistratie'[9] acht waardevolle handvatten aan die ook voor Defensie waardevol kunnen zijn.

***Robotic Proces Automation* (RPA):** In 2023 en 2024 vonden een tweetal toezichtbezoeken van de FG plaats bij het *Robotic Control Centrum* van Defensie Ondersteuningscommando (DOSCO) (inmiddels de afdeling *DevOps* binnen de nieuwe Directie IT & Innovatie), waarover is gerapporteerd in het FG toezichtjaarverslag 2024. RPA is een automatiseringsproces en houdt in dat binnen bepaalde werkprocessen (repetitieve) taken en handelingen geautomatiseerd worden en dus niet meer door een defensiemedewerker worden verricht, maar door een schermrobot. De belangrijkste aanbevelingen zagen toe op het formaliseren van het RPA-beleidskader door het CPO en het inventariseren, uitvoeren en documenteren van alle addenda op de DPIA RPA bij de inzet van nieuwe robots. Op dit moment lijken er op deze vlakken nog geen volledige en concrete verbetermaatregelen te zijn gerealiseerd.

9 Autoriteit Persoonsgegevens, Juli 2025:https://autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-algoritmeregistratie-handvatten-voor-organisaties

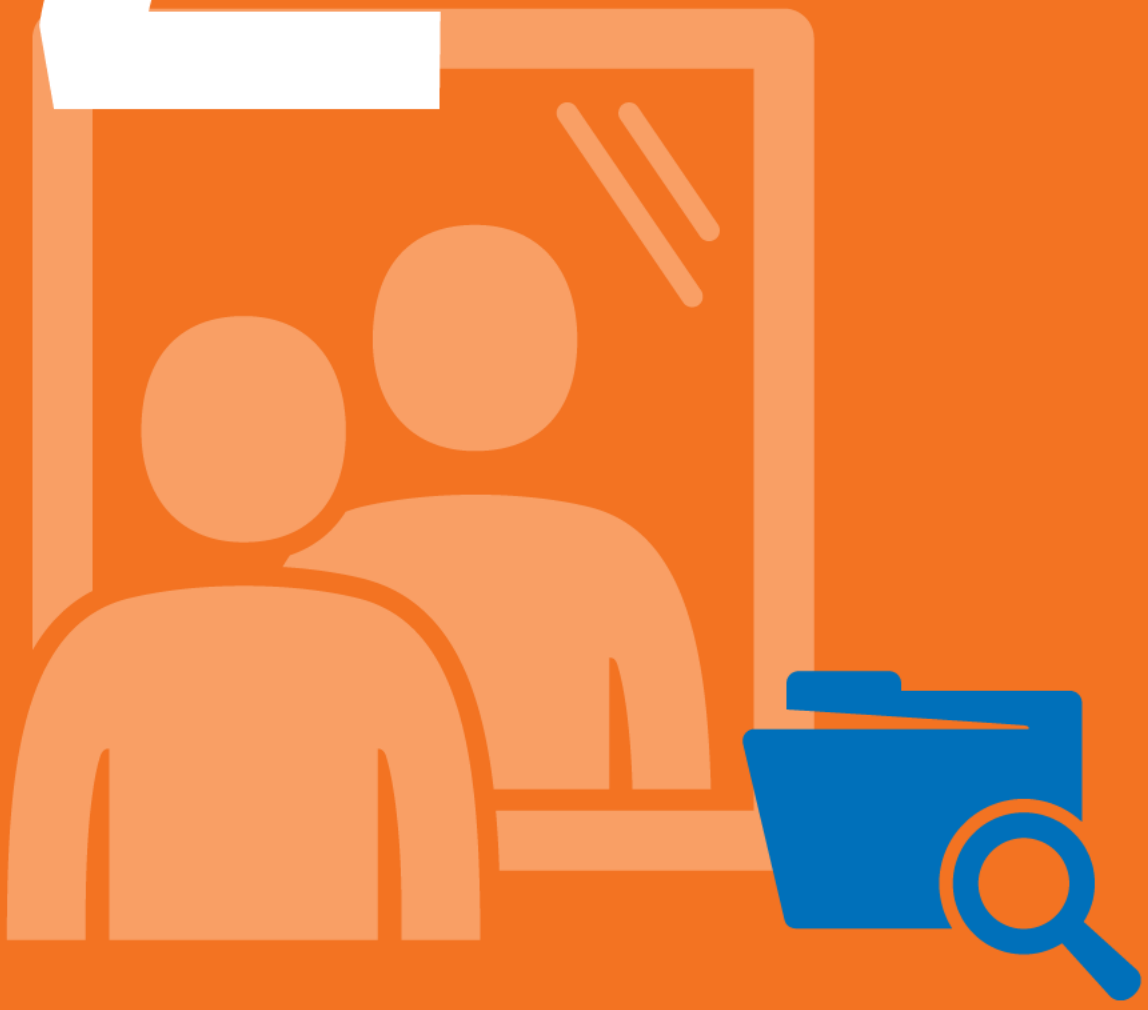
Lopende onderzoeken

Rechten betrokkenen: De FG startte eind 2025 met een themaonderzoek naar de procedure bij Defensie voor het afhandelen van verzoeken op basis van de rechten die de AVG toekent aan personen van wie persoonsgegevens worden verwerkt. Zo hebben deze betrokkenen onder andere het recht op inzage, correctie, verwijdering en overdraagbaarheid van hun persoonsgegevens en het recht om bezwaar te maken tegen de verwerking ervan. Met name het recht op inzage is een belangrijk onderdeel voor het gehele systeem van gegevensbescherming, omdat betrokkenen zich via het inzagerecht op de hoogte kunnen stellen van de verwerking van hun persoonsgegevens en de rechtmatigheid en nauwkeurigheid daarvan. Het inzagerecht vormt daarmee tevens een basis voor het uitoefenen van de overige AVG-rechten. Het is daarom van belang dat Defensie de verzoeken van betrokkenen op basis van hun AVG-rechten tijdig en juist afhandelt. De procedure die hiervoor is ingericht, is onderwerp van het FG-onderzoek. Dit onderzoek wordt in de eerste helft van 2026 afgerond.

***Red teaming*:** De FG voert een onderzoek uit naar de naleving van het gegevensbeschermingsrecht en de privacyaspecten in relatie tot het uitvoeren van *red teaming* activiteiten. *Red teaming* is een geavanceerde securitytest, waarbij een realistische cyberaanval wordt gesimuleerd op een of meerdere kritieke functies van een organisatie. Dit onderzoek wordt in het eerste kwartaal van 2026 afgerond.

Onderzoek Sensoren *Unmanned Aircraft Systems* (UAS): Eind 2025 is een onderzoek begonnen naar gegevensbescherming en privacyrechtelijke aspecten van waarnemingen door sensoren op UAS. Dit onderzoek verschilt van andere (toezicht)onderzoeken in de zin dat het niet tot doel heeft om de mate van naleving van wet- en regelgeving vast te stellen. Het onderzoek heeft tot doel om te komen tot algemene *guidance* en richtsnoeren voor Defensie die voor een aantal relevante scenario's handvatten en richtlijnen bieden voor een adequate en gestructureerde inventarisatie en beoordeling van de risico's voor de rechten en vrijheden van personen die het gebruik van UAS (met bijvoorbeeld camerasensoren) met zich meebrengen. Op deze wijze draagt het onderzoek bij aan een betere risicobeheersing, mitigerende maatregelen, betere naleving van wet- en regelgeving en daarmee aan de versnelde gereedstelling. De FG streeft ernaar om aan het begin van het tweede kwartaal van 2026 de vastgestelde *guidance* op te leveren.

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 allemaal een jaarrapportage aan. Tevens is door NLD *Joint Force Command* (JFC) een AVG-jaarrapportage aangeleverd.

2.2 Privacyorganisatie

Organisatorische ontwikkelingen toezichthouderschap

De FG is in opbouw om haar rol en positie verder te ontwikkelen en te versterken. Sinds 2022 is de FG administratief ondergebracht bij de Inspectie Veiligheid Defensie (IVD) en wordt in 2026 organisatorisch ontvlochten en formatief versterkt, om in 2027 als toezichthouder met de naam *Data Protection Office (DPO)* als volledig zelfstandige eenheid rechtstreeks onder de plaatsvervangend secretaris-generaal te worden geplaatst.

Uitbreiding toezicht op AI & Algoritmes

De FG houdt naast toezicht op de naleving van de AVG en Wpg, waarin geautomatiseerde besluitvorming en profilering gereguleerd zijn, toezicht op een verantwoorde naleving van de AI-verordening. De verordening werd op 2 augustus 2024 van kracht en treedt stapsgewijs in werking.

Sinds 2 februari 2025 zijn bepaalde AI-toepassingen verboden en moeten bedrijven en instellingen AI-geletterd personeel hebben. Vanaf 2 augustus 2025 gelden de basisregels voor nieuwe algemene AI-modellen, *governance*, vertrouwelijkheid, boetes en toezicht. Bestaande modellen hebben tot 2 augustus 2027 om te voldoen aan de basisregels. Vanaf 2 augustus 2026 treden de overige bepalingen, met name strengere verplichtingen voor hoog-risico AI, in werking.

De AI-verordening kent militaire of nationale veiligheidsdoeleinden als uitzonderingsgrond. Dit betekent echter niet dat daarmee een groot deel van de AI-activiteiten binnen het Ministerie van Defensie buiten de reikwijdte van deze verordening vallen. Alleen de puur militaire operationele AI-toepassingen zijn uitgesloten van de werkingssfeer van de AI-verordening. Wanneer bij deze toepassingen persoonsgegevens en/of politiegegevens worden verwerkt, blijven de AVG, UAVG en Wpg overigens ook van toepassing.

De FG bouwde in 2025 de capaciteit voor het toezicht op AI & Algoritmes uit en gebruikte het afgelopen jaar vooral om het opgebouwde netwerk te bestendigen, inzichtelijk te krijgen welke organisatieonderdelen zich bezighouden met de ontwikkeling en het gebruik van AI, en om over gebruik van AI te adviseren. Er zijn diverse informele bezoeken afgelegd met de verschillende *data-units* binnen de defensieorganisatie, om zo een beter zicht te krijgen op de stand van zaken.

Eind 2025 is gewerkt aan de ontwikkeling van een zoveel als mogelijk geïntegreerde strategische visie voor effectief intern toezicht op de naleving van de AVG, de Wpg en de verantwoorde inzet van AI & Algoritmes bij Defensie. Deze geïntegreerde toezichtvisie wordt naar verwachting in het voorjaar van 2026 afgerond.

De privacyorganisatie bij de defensieonderdelen

Uit het merendeel van de jaarrapportages van de defensieonderdelen komt naar voren dat de werkvoorraad in 2025 groter is dan met de beschikbare personele capaciteit kan worden uitgevoerd. Dit betekent dat er bij deze onderdelen werkzaamheden zijn blijven liggen en anders geprioriteerd moesten worden. De toenemende focus op hoofdtaak 1 en de gegevensverwerkingen in het operationele domein zorgen voor nieuwe vraagstukken, en daarmee ook voor een toenemende vraag naar capaciteit en kennis bij de AVG-coördinatoren. Daarbij spelen ook nog de ontwikkelingen rond de Wodg en de implementatie van de AI-verordening, waarvan het in veel gevallen nog niet duidelijk is in welke mate deze impact zullen hebben op de taken en werkzaamheden van de AVG-coördinatoren in de eerste lijn. De privacyketen moet in zijn algemeenheid in de toekomst veel meer betrokken worden bij gegevensbeschermingsvraagstukken rond gereedstellingsactiviteiten en inzet, omdat naar verwachting deze activiteiten zullen toenemen in het licht van de verhoogde en versnelde gereedstelling voor hoofdtaak 1. De rol van de AVG-coördinator in de eerste lijn dient op dit gebied bij de meeste defensieonderdelen nog afdoende ingeregeld te worden.

De privacyorganisatie is in 2025 bij een aantal defensieonderdelen uitgebreid. Zo is in de tweede helft van 2025 Privacy & Ethiek onderdeel geworden van het CIO-Commando Materieel en IT (COMMIT) en zijn

hierbinnen een (decentrale) CPO en *dedicated* AVG-coördinator aangesteld. Bij DOSCO is er een AVG-onderbeheerder aangewezen en is er een *dedicated* Adviseur Privacy & Security bij de Staf DOSCO gestart. Met betrekking tot de personele ontwikkelingen en bezetting zijn er vooral bij het Commando Landstrijdkrachten (CLAS) veel mutaties geweest, waardoor er arbeidsplaatsen binnen het team voor een deel vacant bleven in 2025.

Bij de KMar zijn er personeelswisselingen geweest, waardoor er zowel een nieuwe AVG-coördinator is als een privacyjurist bij *Future Borders*. Daarnaast is voor de Wpg een coördinerend jurist en een extra Wpg-jurist aangenomen. Dit brengt het totaal nu op drie juristen bij CJZ KMar voor advisering op de naleving van de Wpg. Ook is middels het Wpg-subtaakbesluit een Wpg-onderbeheerder aangewezen.

De FG heeft in het toezichtjaarverslag van 2024 aanbevolen de privacyorganisatie bij het Joint Informatie Voorziening Commando (JIVC), de Defensiestaf (DS) en de Bestuursstaf (BS) te versterken, omdat de capaciteit bij deze organisatieonderdelen nog ontoereikend was om voldoende uitvoering te kunnen geven aan de taken. Net als vorig jaar blijven de zorgen om de positie van de AVG-coördinator Regeling Gegevensbescherming Militaire Operaties (RGMO) bij het JFC (voorheen gepositioneerd bij de Directie Operaties). Hoewel er getracht is om te werven, is deze positie ook in het geheel van 2025 vacant geweest. Er lopen initiatieven om de privacyorganisatie bij de defensieonderdelen te versterken, waaronder capaciteit bij de Defensiestaf. Besluitvorming hierover vindt in 2026 plaats.

2.3 Beleid

In 2025 zette het CPO goede stappen in het tot stand brengen van de privacy *governance*. Bij het opstellen van het beleidskader Privacy Governance en Beleid is de Integrale Beleidscyclus van Defensie doorlopen. Ook voerde de Defensiestaf een uitvoerbaarheidstoets uit. Daaruit kwam naar voren dat het beleid uitvoerbaar wordt geacht, met inachtneming van een aantal voorwaarden voor de succesvolle implementatie ervan. Het MT DGB stelde het beleidskader Privacy Governance en Beleid op 5 december 2025 vast. In 2026 geeft het CPO de vervolgfase van implementatie van het beleid verder vorm, door onder andere een implementatiekader op te stellen. Daarnaast worden diverse onderliggende beleidskaders, voor bijvoorbeeld het opstellen van DPIA's en het afhandelen van datalekken, vastgesteld.

Daarnaast is het CIO-beleid voor de *governance* van algoritmes (waaronder AI) en data binnen de defensieorganisatie in februari 2026 vernieuwd. Het nieuwe beleid omschrijft de diverse rollen in de data- en AI-organisatie, zowel binnen de BS als bij de defensieonderdelen, en geeft kaders voor (verantwoorde) AI & Algoritmes.

Op interdepartementaal niveau is afgelopen jaar hard gewerkt aan de uitvoeringswet AI-verordening, waarin onder andere de taken en bevoegdheden in het nationale toezichtlandschap zijn vastgelegd. De FG heeft namens Defensie actief deelgenomen en bijgedragen aan de uitwerking van de uitvoeringswet.

In afwachting van bovengenoemde kaders heeft de FG het voorgenomen toetsingskader AI in 2025 niet af kunnen ronden. Het afronden van dit kader blijft voor de eerste helft van 2026 een belangrijk aandachtspunt.

2.4 Volwassenheid

Onder regie van het CPO is tussen maart en juli 2025 gezamenlijk met de defensieonderdelen een privacyvolwassenheidsmeting uitgevoerd. Het privacyvolwassenheidsmodel kent vijf niveaus. Defensie heeft bepaald dat de organisatie op volwassenheidsniveau drie moet functioneren.[10] Dit betekent dat relevante werkzaamheden organisatiebreed volgens een vastgestelde werkwijze worden uitgevoerd en dat aantoonbaar aan privacywet- en regelgeving wordt voldaan.

Op basis van het vastgestelde volwassenheidsniveau wordt van ieder defensieonderdeel verwacht dat het een ontwikkelplan voor 2026 opstelt. In dit plan maakt het defensieonderdeel concreet hoe het naar het voornoemde ambitieniveau toewerkt. Aan de hand van de input van de defensieonderdelen stelt het CPO een defensiebreed ontwikkelplan op. De FG houdt toezicht op de realisatie van de ontwikkelplannen.

Verder kan op hoofdlijnen worden geconstateerd dat de AI-*community* binnen Defensie nog grotendeels verspreid zit door de gehele organisatie en dat ook het AI-volwassenheidsniveau per defensieonderdeel behoorlijk verschilt. Er is op dit moment geen centrale *community of interest* of een AI-expertgroep die systematische kennisuitwisseling bevordert. Dergelijke initiatieven zouden het kennisniveau verhogen en de output kunnen vergroten.

2.5 Bewustwording

In 2025 heeft de FG getracht actiever bij te dragen aan de bekendheid van gegevensbescherming en privacy binnen Defensie. Hiertoe zijn voorlichtingen gegeven op de dag voor Bijzondere Organisatie Eenheden (BOE's), tijdens de Leergang Beleidsontwikkeling Defensie, voor DOO-medewerkers en tijdens de Leergang Toezicht Defensie. Ook zijn er contacten gelegd met onder meer de Koninklijke Militaire Academie (KMA). In 2026 zet de FG hier nog meer op in. Het opstellen van beleidskaders voor het borgen van privacybewustzijn binnen Defensie en het inrichten van een defensiebreed bewustzijnsprogramma zijn aandachtspunten die voortkomen uit de volwassenheidsmetingen.

Naast de AVG en de Wpg is in 2025 ook aandacht besteed aan AI-*awareness*. AI-geletterdheid, of AI-*literacy*. Dit is een verplichting die voortvloeit uit de AI-verordening en die organisaties verplicht om medewerkers die AI gebruiken of ontwikkelen naar een voldoende hoog AI-kennisniveau te tillen. Het juiste AI-kennisniveau beperkt de risico's op onverantwoord, onwenselijk of onrechtmatig gebruik van AI. Een juiste mate van AI-geletterdheid verkleint ook de risico's voor de organisatie. Het voorkomt dat men onbedoeld persoonsgegevens deelt of persoonsgegevens gebruikt bij het trainen van modellen, en dat gerubriceerde informatie onbewust in AI-modellen terechtkomt. Daarnaast creëert AI-geletterdheid extra kansen wanneer mensen de juiste kennis en kunde hebben in het gebruik van AI en wordt het innovatieve vermogen vergroot. De FG draagt door deze opleidingen en trainingen binnen Defensie bij aan verbetering van het kennisniveau rondom het verantwoord gebruik van AI. Ook zijn waardevolle contacten met de academische wereld gelegd.

In 2025 zijn er binnen Defensie op verschillende niveaus cursussen en opleidingen aangeboden waarin AI wordt behandeld. Wat echter ontbreekt is een centraal integraal plan van aanpak, of een plan van aanpak per defensieonderdeel, om de AI-geletterdheid binnen de organisatie te verbeteren.

10 1 Programmaplan Implementatie Algemene Verordening Gegevensbescherming bij Defensie, 8 juli 2017; Gegevensbescherming 2.0, BS201908597, 25 april 2019.

2.6 Verwerkersovereenkomsten

Wanneer Defensie gebruikmaakt van een externe partij om persoonsgegevens namens Defensie te laten verwerken (een verwerker), dient een verwerkersovereenkomst (of andere rechtshandeling, zoals een convenant) opgesteld te worden. Dit is nodig om te waarborgen dat de verwerker ten behoeve van Defensie persoonsgegevens volgens de regels van de AVG verwerkt en beschermt. Conform de Regelingen AVG en Wpg Defensie moet een verwerkersovereenkomst in het register van verwerkingsactiviteiten worden opgenomen. Hiermee krijgt de privacyorganisatie inzicht in de afgesloten verwerkersovereenkomsten en de gemaakte afspraken.

Er is momenteel geen inzicht in een actueel en volledig overzicht van door Defensie afgesloten verwerkersovereenkomsten. Het register van verwerkingsactiviteiten biedt geen inzicht in en overzicht van alle verwerkersovereenkomsten. Vanwege de wijze van registratie in SAP Materieel & Financiën (M&F) is er geen link te leggen tussen de verwerkingen in het register voor verwerkingsactiviteiten en verwerkersovereenkomsten in het contractenregister van SAP M&F. Ook is niet vast te stellen welke inkoopcontracten een verwerkersovereenkomst missen. Deze tekortkomingen zijn door de FG al meerdere jaren geconstateerd, maar heeft nog niet tot verbetering geleid. Bij meerdere FG-toezichtonderzoeken blijkt dat verwerkersovereenkomsten niet (tijdig) zijn opgesteld en de werkzaamheden van de verwerker niet voldoende afdekken, of verouderd zijn. Dit vormt een risico voor de naleving van de AVG en daarmee voor de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Ook kunnen de gevolgen bij een datalek groter zijn indien er geen adequate afspraken zijn over de afhandeling.

De 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.[11] Heldere, eenvoudige en praktische richtlijnen, meer inzicht en overzicht in het geheel van verwerkersovereenkomsten in de privacyorganisatie en betere inrichting van de adviesfunctie ten behoeve van de inkoopfunctie zijn enkele aanbevelingen uit dit onderzoek. Ter verbetering van de geconstateerde risico's wordt door het CPO, in samenwerking met de Afdeling Inkoopmanagement, de conceptversie van de instructie inkoop en verwerkersovereenkomsten herzien in 2026.

2.7 *Data Protection Impact Assessments*

Een DPIA is een wettelijk instrument dat ertoe verplicht om bij een gegevensverwerking die waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen opleveren, vooraf de privacyrisico's gestructureerd in kaart te brengen en maatregelen te bepalen die deze risico's kunnen verkleinen. 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). Als uit een DPIA een hoog risico naar voren komt dat met maatregelen onvoldoende kan worden beperkt, dan dient dit ter advies te worden voorgelegd aan de AP12 en mag de voorgenomen verwerking (nog) niet starten.

De FG houdt toezicht op de uitvoering van de DPIA's bij Defensie. De FG heeft in het toezichtjaarverslag 2024 aanbevolen om te zorgen voor een beter inzicht in en overzicht van de uitgevoerde, lopende, te actualiseren en nog benodigde DPIA's. De privacy *community* stelde in 2025 een overzicht op met uitgevoerde, lopende en te actualiseren DPIA's, en ontwikkelde de *pre-scan* DPIA's, die in 2025 als hulpmiddel in gebruik is genomen. Voor volledig inzicht in en overzicht van uitgevoerde, lopende en nog benodigde DPIA's is het van belang dat het opgestelde overzicht actueel wordt gehouden. Dit is nog een aandachtspunt.

Bij het opstellen van een DPIA, alvorens met een hoog risicoverwerking wordt aangevangen, wint Defensie verplicht advies in bij de FG. Binnen Defensie is er een achterstand in het opstellen van DPIA's, waardoor de FG niet tijdig en naar behoren betrokken kan worden voor advies. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. Bij veranderingen in de gegevensverwerking, de context van de verwerking of

11 Auditdienst Rijk. 25 juni 2024. Evaluatie van de maatregelen voor de verwerkersovereenkomsten bij inkoop van Defensie. 2024-0000262902.
12 Proces van voorafgaande raadpleging cfm artikel 36 AAG en 33b Wpg.

de risico's van de verwerking is mogelijk een actualisatie van de DPIA nodig. Bijvoorbeeld doordat een nieuwe technologie in gebruik wordt genomen. Het is een goede praktijk om een DPIA regelmatig opnieuw te beoordelen op nieuwe risico's of veranderende omstandigheden en indien noodzakelijk periodiek te herzien. Vanwege mogelijke veranderingen in technische en organisatorische processen raadt de AP sowieso aan om eens per drie jaar de DPIA te updaten en indien nodig opnieuw uit te voeren. Ook met betrekking tot het actualiseren van DPIA's is een achterstand geconstateerd.

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 gegevensbeschermingswetgeving en innovaties en projecten kunnen vertraging oplopen. Dit onderstreept de noodzaak om het DPIA-proces tijdig op te starten, DPIA's in teamverband op te stellen, de risico's voor de privacy goed te analyseren en de FG tijdig te betrekken in het proces.

Voor nieuwe verwerkingen worden *pre-scans* uitgevoerd om te beoordelen of een DPIA noodzakelijk is. *Pre-scans* worden ook aangeboden aan de FG ter beoordeling. De FG wordt door een aantal defensieonderdelen nog onvoldoende betrokken bij het beoordelen van *pre-scans*. Het tijdig laten beoordelen van een *pre-scan* door de FG kan voorkomen dat op een later moment aanpassingen nodig zijn in een verwerking of *scope* van een DPIA of dat een DPIA onnodig wordt opgesteld, omdat er geen sprake is van een hoog risicoverwerking.

Naast het realiseren en vaststellen van de DPIA's is het van belang dat de defensieorganisatie inzichtelijk heeft welke maatregelen binnen welke termijn daadwerkelijk geïmplementeerd moeten zijn. Dit blijft een aandachtspunt.

2.8 Inbreuken op de beveiliging (datalekken)

Defensiemedewerkers melden inbreuken in verband met persoonsgegevens (potentiële datalekken) in het Peoplesoft Melden Voorvallen (PSMV)-systeem als privacyvoorval. Dit kunnen meldingen zijn met betrekking tot een *hack*, verkeerd gestuurde persoonsgegevens, openstaande *SharePoint-sites*, verloren of gestolen gegevensdragers of datalekken bij verwerkers. Bij deze privacyvoorvallen gaat het ook om meldingen van of signalen over het (ongewenst) publiceren van foto's van defensiemedewerkers op sociale media. In 2025 ontving de FG circa 210 intern ingediende datalekmeldingen, waarvan 16 meldingen politiegegevens (Wpg) betroffen. Ook ontving de FG 157 privacygerelateerde meldingen die geen datalek betroffen. 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. 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 2025 meldde Defensie in totaal 27 datalekken bij de AP.

De FG ontving 25 meldingen van datalekken bij externe partijen waarbij persoonsgegevens van defensiemedewerkers zijn betrokken. Dit is een toename ten opzichte van voorgaande jaren. Daarbij lijkt ook de ernst van de datalekken bij externe partijen te zijn toegenomen, zowel qua grootte als qua type persoonsgegevens. In verband met de veiligheid van defensiemedewerkers heeft de FG bij deze datalekken aandacht voor de afhandeling van het datalek door de externe partij, waaronder de melding aan betrokkenen. In enkele gevallen is door Defensie zelf een melding aan betrokkenen gedaan via interne berichtgeving.

	2025	2024	2023	2022	2021	2020
Ontvangen interne datalekmeldingen	210	213	285	248	169	109
Aantal meldingen aan AP	27	32	29	19	17	15

In *Sharepoint* kunnen medewerkers op het defensienetwerk (MULAN/intranet) gemakkelijk samenwerken door documenten te delen en gezamenlijk te beheren. Door onjuiste configuraties, zoals verkeerd ingestelde toegangsrechten, komt het regelmatig voor dat documenten met persoonsgegevens toegankelijk worden voor onbevoegden, bijvoorbeeld voor alle defensiemedewerkers in plaats van een beperkte groep. Datalekken veroorzaakt door een openstaande *SharePoint*-omgeving kwamen, net zoals in 2024, ook in 2025 regelmatig voor. Daarbij zijn ook bijzondere, strafrechtelijke en gevoelige persoonsgegevens gecompromitteerd geweest.

Ook datalekken van medische gegevens kwamen in 2025 nog regelmatig voor. Het betreft dan bijvoorbeeld medische gegevens die verstrekt zijn aan een verkeerde zorgverlener, aan personeel dat niet medisch bevoegd is of aan een verkeerde patiënt. Gegevens werden bijvoorbeeld aan de verkeerde persoon gemaild of verstuurd, of werden per ongeluk opgeslagen in het patiëntendossier van een andere patiënt.
In 2024 voerde de FG toezichtonderzoek[13] uit naar de wijze waarop Defensie handelt bij (potentiële) datalekken. De voornaamste verbeterpunten uit het onderzoek hebben betrekking op de inrichting en het gebruik van de PSMV-applicatie en de tijdigheid van het 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. In de CPO-appreciatie van het rapport worden de aanbevelingen van de FG onderschreven. De aanbevelingen zijn omgezet in concrete maatregelen en toegewezen aan actiehouders, waaronder het CPO. Een aantal maatregelen is reeds afgerond.

(Potentiële) datalekken dienen geregistreerd te worden in de interne datalekregister van Defensie. In 2025 is een nieuw centraal datalekregister in gebruik genomen. Alle defensieonderdelen dienen datalekken hierin te registeren. Uitzondering zijn datalekken in verband met politiegegevens. Op basis van onderzoek door de FG blijkt dat meer aandacht nodig is voor de kwaliteit en volledigheid van de registraties.

2.9 Rechten van betrokkenen

De AVG en Wpg kennen privacyrechten toe aan betrokkenen, de personen van wie de persoonsgegevens worden verwerkt. Zo hebben betrokkenen bijvoorbeeld het recht op inzage en correctie van hun persoonsgegevens en in sommige gevallen ook verwijdering van hun persoonsgegevens. Via deze rechten kunnen betrokkenen te weten komen welke persoonsgegevens van hen worden verwerkt en of dit op rechtmatige wijze gebeurt. Om de AVG- en Wpg-rechten van betrokkenen te faciliteren, is er binnen Defensie een proces ingericht: Afhandeling verzoeken ‘rechten betrokkenen’. Betrokkenen kunnen verzoeken indienen via een hiervoor ingerichte internetsite van Defensie. Voor medewerkers in werkelijke dienst geldt een vergelijkbaar proces via een intranetpagina van Defensie.

AVG-verzoeken

In 2025 kwamen 2455 verzoeken binnen middels het online beschikbare formulier. Veruit de meeste van deze verzoeken betreffen informatie- of inzageverzoeken. Van de 2455 verzoeken leidden ongeveer zes gevallen tot berichten aan de FG over het niet nakomen van de termijn van afhandeling. Met tussenkomst van de FG handelde de defensieonderdelen deze berichten alsnog af. Daarnaast beantwoordde de FG ongeveer 35 vragen van betrokkenen over hun AVG-rechten, bijvoorbeeld over de wijze waarop zij hun verzoek kunnen indienen en welke informatie daarbij nodig is. De procedure(s) voor het afhandelen van verzoeken rondom de rechten van betrokkenen zijn onderwerp van een onderzoek dat de FG in 2025 startte en in 2026 afrondt.

Een opvallende ontwikkeling die de FG zag bij de KMar is dat er sinds de inwerkingtreding van de EES-verordening (*European Entry/Exit System*) in oktober een flinke stijging van inzageverzoeken heeft plaatsgevonden. Deze verzoeken zijn met name gericht op inzage in en informatie over de toegestane verblijfsduur in de Schengenzone en algemene vragen over het doel van EES.

13 Functionaris voor Gegevensbescherming. 28 oktober 2024. Toezichtonderzoek afhandelen datalekken. BS2024037730.

Wpg verzoeken

In 2025 kwamen 131 WPG-informatieverzoeken binnen, ten opzichte van 80 in 2024. Zowel het aantal inzageverzoeken als het aantal verzoeken gericht op rectificatie of vernietiging van politiegegevens is daarmee sterk gestegen ten opzichte van 2024. In 14 gevallen besloot de KMar om, op basis van de uitzonderingsgronden van artikel 27 Wpg, specifieke informatie niet te delen met de betrokkenen.
In 2025 liepen er meerdere (hoger) beroepszaken naar aanleiding van Wpg-besluiten. Er kwamen in 2025 zeven nieuwe beroepszaken binnen. Tevens is er gewerkt aan diverse beroepszaken die reeds in 2023 en 2024 waren gestart, mede vanwege de lange doorlooptijden van (hoger) beroepsprocedures bij rechtbanken.

Op grond van de Wpg kunnen betrokkenen wiens verzoek om inzage of correctie van politiegegevens is afgewezen, de AP vragen om te bemiddelen voordat ze in beroep gaan bij de bestuursrechter. In 2025 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 privacyrechten (artikel 38, vierde lid van de AVG). De binnengekomen berichten zijn te onderscheiden in onder andere vragen, meldingen (signalen) of klachten. Buiten de eerder genoemde berichten over de termijnoverschrijding van AVG-verzoeken, kwamen er in 2025 circa tien klachten van betrokkenen binnen bij de FG over de verwerking van hun persoonsgegevens. Dit waren bijvoorbeeld klachten over het verwerken van onjuiste persoonsgegevens (naam, e-mailadres en woonadres) en over het (vermeend) onterecht opvragen van het burgerservicenummer van betrokkenen door verschillende defensieonderdelen. De FG zag toe op een zorgvuldige afhandeling van de klachten en waar nodig verzocht de FG de defensieorganisatie om verbetermaatregelen te nemen.

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 JIVC, toegang te verkrijgen tot het digitale account van een medewerker van Defensie. Hiervoor moet de betreffende beveiligingscoördinator toestemming verlenen. De daadwerkelijke vrijgave vindt vertrouwelijk plaats met gebruikmaking van een *two person*-concept (of het vierogenprincipe). Van een dergelijke toestemming wordt melding gemaakt bij de FG. In 2025 ontving de FG zes 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[14] en het Verwerkingsregister Rijksoverheid[15]. Meerdere defensieonderdelen hebben een eigen privacyverklaring. Een aandachtspunt hierbij is eenduidigheid, juistheid en volledigheid van de verstrekte informatie.

14 https://www.defensie.nl/privacy
15 https://www.avgregisterrijksoverheid.nl/organisatie/ministerie-van-defensie

2.10 Systeem ter borging realisatie verbetermaatregelen

De FG heeft in het toezichtjaarverslag van 2024 aanbevolen om een systeem in te richten ter borging van de realisatie (en inzicht daarin) van privacygerelateerde verbetermaatregelen die voortkomen uit bijvoorbeeld DPIA's, interne en externe toezichtrapporten en datalekken. In 2025 was er nog geen voortgang op dit aspect. Hoewel werd aangegeven dat mogelijk de Integraal Risicomanagement *tooling* (IRM-*tooling*), dat al langere tijd in ontwikkeling is, hiervoor gebruikt zal worden, lijken er in 2025 nog geen specifieke maatregelen te zijn genomen.

Binnen Defensie loopt het project voor defensiebrede en domeinoverstijgende *tooling* voor IRM. Vanuit het privacydomein zijn het CPO en de Directie Aansturen Operationele Gereedheid (DAOG) hierbij aangesloten. De FG liet zich hier in 2025 over voorlichten en wil in 2026 actiever onderzoeken hoe deze methodiek of *tooling* voor gegevensbescherming kan worden ingezet. Ook vanuit de hele toezichtketen wordt hier actiever op ingezet. De verwachting is dat meer nadruk op aspecten en belangen van gegevensbescherming binnen IRM bijdraagt aan bredere bewustwording binnen Defensie op dit vlak en zo bijdraagt aan een effectievere bescherming van persoonsgegevens, ook wanneer er versneld moet worden opgetreden.

2.11 Samenwerking Toezichtberaad Defensie

De toezichthouders en -autoriteiten binnen Defensie werken samen in het Toezichtberaad, dat de komende jaren wordt uitbreid tot een Toezichtnetwerk. Deelnemers zijn de BA, de FG, de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS) en de Militaire Luchtvaart Autoriteit (MLA). De Inspecteur-Generaal der Krijgsmacht (IGK) is toehoorder. Het Bureau Toezicht Defensie (BTD) ondersteunt daarbij de deelnemers van het Toezichtberaad.

De toezichthouders en –autoriteiten hebben gezamenlijk strategische lijnen uitgezet en gewerkt aan de ontwikkeling van gedeelde toezichtinstrumenten. Om effectief toezicht te houden wordt in 2026 verder ingezet op het ontwikkelen van effectievere toezichtmethoden, het verbeteren van de informatiepositie en de relatie met de organisatie.

Het BTD organiseerde in 2025 wederom de Leergang Toezicht Defensie: een leertraject voor alle toezichtcollega's gericht op verdieping, uitwisseling en versterking van het gezamenlijke toezichtvak. In 2025 hebben alle nieuwe medewerkers van de FG hieraan deelgenomen. Ook is door de BTD een toezichtdag voor alle toezichthouders georganiseerd. Hieraan heeft ook de FG bijgedragen.

2.12 Samenwerking buiten Defensie

Om haar taak goed uit te kunnen voeren, werkt de FG ook samen met personen en instanties buiten de defensieorganisatie. In 2025 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 tussen 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.

LED-werk Platform FG's voor Wpg en Wet justitiële en strafvorderlijke gegevens (Wjsg): Sinds 2020 is het LED-werk opgericht voor en door 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.

Duits-Nederlandse *Data Protection Committee:* De samenwerking met Duitsland in de Duits-Nederlandse *Data Protection Committee* is verder versterkt. In de halfjaarlijkse bijeenkomsten van dit comité worden de ontwikkelingen in de Duits-Nederlandse samenwerking en (strategisch) relevante nationale ontwikkelingen rond het gegevensbeschermingsbeleid en -toezicht besproken.

***Memorandum of Understanding* (MOU) met België en Luxemburg:** In de samenwerking met België en Luxemburg zijn, volgend op de *letter of intent* uit 2024, door het CPO en DJZ stappen gezet om de samenwerking verder te formaliseren. Zo is er een *Memorandum of Understanding* (MOU) opgesteld, waarvan in Nederland en Luxemburg de *staffing* is afgerond. Na afronding van de *staffing* in België, kan tot ondertekening worden overgegaan. Naast een algemene MOU is er een concept *Implementing Arrangement* over het uitwisselen van personeelsgegevens opgesteld.

Internationale bijeenkomsten: In 2025 nam de FG deel aan verschillende internationale bijeenkomsten op het gebied van privacy, gegevensbescherming, AI en algoritmes. Om optimaal gebruik te kunnen maken van AI, met oog voor de uitdagingen en risico's, is het belangrijk dat AI op een verantwoorde wijze gedurende de hele *life cycle* wordt ontwikkeld en ingezet binnen de kaders van nationale en internationale wet- en regelgeving.[16] Op het internationale toneel speelt Nederland een centrale rol als aanjager om te komen tot verdere internationale kaderstelling.[17]

16 Blueprint for Action, REAIM.

17 https://www.rijksoverheid.nl/documenten/kamerstukken/2025/12/15/stand-van-zaken-internationale-inzet-voor-verantwoorde-kunstmatige-intelligentie-in-het-militaire-domein.

3 Conclusies en aanbevelingen

In 2025 besteedde de privacyorganisatie aandacht aan het vergroten van de kennis van de AVG en de bewustwording binnen de organisatie. De defensieorganisatie verzette het afgelopen jaar veel werk wat betreft *privacycompliance* en het opzetten van nieuw beleid op *data governance*, AI en algoritmes.

Defensie bevond zich in 2025 binnen een steeds complexere dreigingsomgeving in een reeks van ontwikkelingen: de versnellende gereedstelling voor hoofdtaak 1, de verdergaande digitalisering van de krijgsmacht en de samenleving, en een toenemende groei van toepassingen met AI. Dit leidt noodzakelijkerwijs tot personele, materiele en digitale versterking van capaciteiten, waarbij Defensie in een hoog tempo uitbreidt en tegelijkertijd procedures vereenvoudigd worden.

In 2025 zetten de FG en de gehele privacyorganisatie zich in om aansluiting te behouden bij de dynamische ontwikkelingen en het toezicht en de naleving op het gegevensbeschermingsrecht effectief en constructief in te richten. 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. Een geïntegreerd en breed intern toezicht op het gegevensbeschermingsrecht is en blijft essentieel. Ook ter bescherming en waarborging van grondrechten van defensiemedewerkers.

Aandachtspunten zijn:

- de structurele borging van bewustwordingsactiviteiten;
- de structurele inbedding van *governance* rond gegevensbescherming (AVG, Wpg én AI-verordening);
- de naleving van verschillende elementen van de AVG en de Wpg en een verantwoorde inzet van AI & algoritmes;
- de verhoging van de kwaliteit van de DPIA's;
- de registraties in het register van verwerkingsactiviteiten;
- de realisatie van verbetermaatregelen omtrent gegevensbescherming;
- de uitwerking en afstemming van een mogelijk bijkomende toezichttaak op de AI-verordening en de ontwikkeling en inzet van AI & Algoritmes.

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 en privacyfunctionarissen 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 organisatie rondom gegevensbescherming.

Bij JIVC, de DS en de BS is de capaciteit nog ontoereikend om voldoende uitvoering te kunnen geven aan de gegevensbeschermingstaken. Voor de gehele privacyorganisatie geldt verder dat de ontwikkelingen in het kader van hoofdtaak 1, de Wodg en de toename aan innovatieprojecten ook een sterk effect zullen hebben op de toch al beperkte capaciteit van de AVG-coördinatoren. Zorg ook binnen het AI- & algoritmedomein dat complianceprocessen en rolverdelingen in de organisatie belegd zijn, met geïntegreerde samenwerkingen tussen diverse disciplines die raken aan data, AI en algoritmes.

Aanbeveling 2:
Borg de *governance* voor AVG, Wpg en AI & Algoritmes.

Overall is er aandacht nodig voor de (verdere) structurele inbedding van *governance* rond gegevensbescherming (AVG, Wpg én AI-verordening). AVG-(governance)beleid is goed op weg, maar dit dient verder geïmplementeerd en geborgd worden. Ook voor de Wpg zijn stappen genomen om de *governance* te verbeteren, maar is aandacht nodig voor het beter in beeld brengen van de Wpg-*governance*, met inachtneming van de bijzondere, gedeelde beheer- en gezagsstructuur van de KMar. Zorg voor een defensiebrede uitwerking van het governancekader voor data, AI en algoritmes.

Aanbeveling 3:
Verhoog de bewustwording omtrent gegevensbescherming, inclusief AI-geletterdheid.

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. Ook is blijvende aandacht nodig voor bekendheid met de richtlijnen uit de AVG en de (compliance)stappen die genomen moeten worden indien er een voornemen is om persoonsgegevens te verwerken. Bij nieuwe innovaties is aandacht nodig voor het toepassen van *privacy-by-design* maatregelen.

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

Zorg voor betere bewaking en de daadwerkelijke uitvoerbaarheid van de noodzakelijke mitigerende matregelen. Breng de aanbevolen AVG- en Wpg-verbetermaatregelen met betrekking tot naleving van gegevensbescherming afkomstig uit diverse bronnen in kaart en borg de realisatie hiervan beter.

Aanbeveling 5:
Zorg voor verbetering/versnelling van DPIA-trajecten en andere risico-inventarisaties en acceptatie-instrumenten. Overweeg om te bekijken of de diverse risico-inventarisaties (DPIA's, DTIA's, IAMA's, IRM enz.) en acceptatie-instrumenten beter op elkaar kunnen aansluiten.

DPIA-trajecten zijn langdurig en er is een achterstand in de realisatie ervan. Daarnaast loopt de actualisatie van al langer bestaande DPIA's achter. Zorg voor een herijking van de verantwoordelijkheden voor het opstellen van DPIA's en andere risico-inventarisaties, ten behoeve van een betere verdeling van de belasting op de capaciteit. Zorg voor capaciteit om het opstellen van DPIA's te ondersteunen.

Aanbeveling 6:
Bestendig het succes van de registratie- en verantwoordingsplicht voor AVG en Wpg. Zorg ook voor een sluitende en transparante registratie van AI en algoritmes.

De aanpak voor de herijking van het bestaande AVG- en Wpg-register is in 2025 succesvol geweest en moet in 2026 doorgezet worden. Zorg dat de aanpak voor de registratie van AI & algoritmes deze volwassenheidsslag ook maakt en dat er heldere verwijzingen tussen beide registers gemaakt worden.

4 Bijlage

4.1 Afkortingen

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten
ABRO	Algemene Beveiligingseisen Rijksbrede Opdrachten
ADR	Auditdienst Rijk
AI	*Artificial Intelligence* (kunstmatige intelligentie)
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
BOE	Bijzondere Organisatie Eenheid
BS	Bestuursstaf
BTD	Bureau Toezicht Defensie
BZ	Buitenlandse Zaken
CIO	*Chief Information Office*
CJZ	Cluster Juridische Zaken
C-KMar	Commandant Koninklijke Marechaussee
CLAS	Commando Landstrijdkrachten
COMMIT	Commando Materieel en IT
CPO	*Chief Privacy Office*
DAOG	Directie Aansturen Operationele Gereedheid
DCPL	Dienstencentrum Personeelslogistiek
DGB	Directoraat-Generaal Beleid
DJZ	Directie Juridische Zaken
DOO	Defensie Open op Orde
DOSCO	Defensie Ondersteuningscommando
DPIA	*Data Protection Impact Assessment* (Gegevensbeschermingseffectbeoordeling)
DPO	*Data Protection Office*
DS	Defensiestaf
DTIA	*Data Transfer Impact Assessment*
FG	Functionaris voor Gegevensbescherming
IAMA	*Impact Assessment* Mensenrechten en AI
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
IRM	Integraal Risicomanagement
IVD	Inspectie Veiligheid Defensie
JFC	*Joint Force Command*
JIVC	Joint Informatie Voorziening Commando
KMA	Koninklijke Militaire Academie
KMar	Koninklijke Marechaussee
KMCGS	Korps Militaire Controleurs Gevaarlijke Stoffen
M&F	Materieel & Financiën
MLA	Militaire Luchtvaart Autoriteit
MOU	*Memorandum of Understanding*
NIMH	Nederlands Instituut voor Militaire Historie
PSMV	Peoplesoft Melden Voorvallen
RGMO	Regeling Gegevensbescherming Militaire Operaties
RPA	*Robotics Process Automation*
RPFG	Rijksplatform FG's
TGTF	Toezichtbezoek Trainings Geneeskunde & TraningsFysiologie
UAS	*Unmanned Aircraft System*
UAVG	Uitvoeringswet AVG
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wodg	Wet op de defensiegereedheid
Wpg	Wet politiegegevens