Ministerie van Defensie

Toezichtjaarplan 2026

Functionaris voor Gegevensbescherming

2026

Voorwoord

De Functionaris voor Gegevensbescherming (FG) is de interne toezichthouder van het Ministerie van Defensie en houdt toezicht op de naleving van de wet- en regelgeving rondom de verwerking van persoonsgegevens, de bescherming van de persoonlijke levenssfeer en de verantwoorde inzet van *Artificial Intelligence* (AI) en algoritmes.

In een tijdperk van vergaande digitalisering, de snelle opkomst van kunstmatige intelligentie (AI) en toenemende en steeds complexer wordende dreiging, staat Defensie voor grote ontwikkelingen en veranderingen. De voornaamste thema's in deze veranderingen zijn de verhoging van de NAVO-norm, de versterking van de gereedheid met de focus op hoofdtaak 1, het multidomein optreden, weerstand bieden aan hybride dreiging en het verhogen van de weerbaarheid van de samenleving.

Deze ontwikkelingen zorgen ervoor dat de personele, materiële en digitale capaciteit en middelen van de krijgsmacht in hoog tempo worden uitgebreid. Hierdoor ligt vanuit het (militaire) veiligheidsbelang de nadruk op vereenvoudiging van procedures, snelle groei en benutten van innovatieve ontwikkeling. Adequate naleving en toezicht op het gebied van gegevensbeschermingsrecht benadrukt de verantwoordingsplicht en vraagt juist om een zorgvuldig proces, waarin vooraf de relevante risico's in kaart worden gebracht en de noodzakelijke mitigerende maatregelen worden getroffen.

Voorbeelden van actuele vraagstukken zijn de privacyaspecten rondom het oefenen met onbemenste surveillancesystemen of het gebruik van geavanceerde elektromagnetische sensoren die digitale sabotage of ongewenste drones detecteren. Andere vraagstukken gaan over de rechtmatige en proportionele verzameling van informatie uit openbare bronnen voor defensiedoeleinden, de zorgvuldige omgang met personeelsgegevens in verband met verplichte registratie en keuring van militairen of het monitoren van vitale lichaamsfuncties en gezondheidsrisico's.

Het belang van de landsverdediging en de nationale veiligheid enerzijds en de bescherming van de persoonlijke levenssfeer en het gegevensbeschermingsrecht anderzijds worden soms als tegenovergestelde belangen beschouwd. Vaak is dit echter een valse tegenstelling. Beschermen wat ons dierbaar is betekent immers ook dat we staan voor individuele rechten en vrijheden van burgers, ook of zelfs juist wanneer deze bedreigd worden. En een rechtmatige en zorgvuldige omgang met persoonsgegevens van onze eigen defensiemedewerkers draagt juist bij aan de bescherming van de (militaire) veiligheidsbelangen. Met name wanneer de digitale en hybride dreiging toeneemt.

Het is aan de FG om het belang van naleving en een juiste toepassing van het gegevensbeschermingsrecht te benadrukken. Door middel van toezicht en advies zorgt de FG dat er tijdig een juiste en zorgvuldige belangenafweging en beoordeling wordt gemaakt ten aanzien van verwerkingen die een hoog risico voor de bescherming van de persoonlijke levenssfeer met zich meebrengen.

De FG werkt als interne toezichthouder aan een evenwichtige benadering. Bij voorkeur gelden snelle groei enerzijds en het belang van een zorgvuldige afweging en beoordeling van voorgenomen gegevensverwerkingen in het licht van het gegevensbeschermingsrecht anderzijds niet als tegenstellingen, maar versterken die elkaar onderling. Alleen door het toezicht en de naleving van het gegevensbeschermingsrecht zo vroeg en zo nauw mogelijk te laten aansluiten op en te integreren in de vernieuwingsprocessen kan Defensie verantwoord versnellen.

De FG streeft naar een goede balans tussen bewustwording en naleving van het gegevensbeschermingsrecht en het belang van de noodzakelijke gereedstelling en uitvoering van de grondwettelijke taken van Defensie.

Functionaris voor Gegevensbescherming
mevr. mr. O.L. Stenhuis-Kok

Colofon

Functionaris voor Gegevensbescherming

Bezoekadres
Brassersplein 1
2612 CT Delft

Postadres
Ministerie van Defensie - Bestuursstaf
Postbus 20701
2500 ES Den Haag

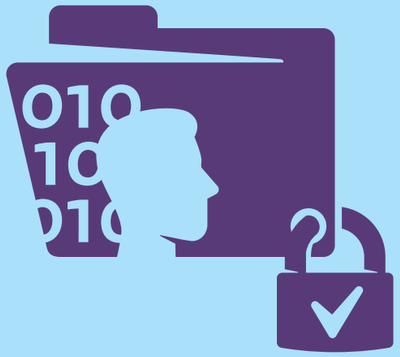
Datum
November 2025

Inhoud

1

Over de Functionaris voor Gegevens-bescherming

De Functionaris voor Gegevensbescherming (FG) ziet als onafhankelijke interne toezichthouder bij Defensie toe op de naleving van de wet- en regelgeving rond de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer. De Algemene verordening gegevens-bescherming (AVG), de Uitvoeringswet AVG (UAVG), de Wet politiegegevens (Wpg) en de AI-verordening vormen de wettelijke basis voor het toezicht. De FG is aangewezen om de verwerkingsverantwoordelijke te voorzien van advies over en toezicht te houden op de naleving van de wetgeving rond de verwerking van persoonsgegevens, de bescherming van de persoonlijke levenssfeer en de verantwoorde inzet van AI en algoritmes.



Defensie heeft twee Functionarissen voor Gegevensbescherming die respectievelijk toezien op de naleving van de AVG en de Wpg. Daarnaast heeft de FG een functionaris die, in verband met de implementatie van Europese AI-verordening, het toezicht op algoritmes en kunstmatige intelligentie coördineert. De FG wordt ondersteund door een team van inspecteurs.

1.1 Wat doet de Functionaris voor Gegevensbescherming?

De FG maakt zich iedere dag sterk voor een zorgvuldige omgang met persoonsgegevens die Defensie verwerkt en de naleving van en het toezicht op het gegevensbeschermingsrecht en de bescherming van de persoonlijke levenssfeer. De FG informeert, adviseert en controleert of verwerkingen van persoonsgegevens bij Defensie rechtmatig, behoorlijk en transparant zijn. De FG controleert ook of betrokkenen van binnen en buiten Defensie hun privacyrechten, zoals het recht op inzage en correctie, goed kunnen uitoefenen. Verder ziet de FG toe op een correcte afhandeling van datalekken en klachten over het verwerken van persoonsgegevens. Tevens is de FG het aanspreekpunt voor de externe toezichthouder, de Autoriteit Persoonsgegevens (AP).

De FG adviseert gevraagd en ongevraagd de ambtelijke top, de operationele commandanten van de krijgsmachtonderdelen en de hoofden van de defensieonderdelen die aangewezen zijn als AVG- en Wpg-beheerders.

Naast het uitoefenen van toezicht in het kader van de AVG en de Wpg, ziet de FG ook toe op het verantwoord gebruik van AI (binnen de kaders van de AI-verordening) en andere nationale en internationale principes.

1.2 Missie

In een digitaliserende samenleving, waar de democratische rechtsorde door geopolitieke ontwikkelingen vaker onder druk staat, bevordert en bewaakt de FG binnen Defensie de bescherming van natuurlijke personen met het oog op de rechtmatige verwerking van persoonsgegevens. Daarmee levert de FG een belangrijke bijdrage aan de bescherming van de persoonlijke levenssfeer.[1]

In haar missie focust de FG op twee belangrijke thema's:

- het bevorderen van het draagvlak voor en bewustzijn van de bescherming van persoonsgegevens;
- het toezien op de naleving van relevante wet- en regelgeving en daarmee bijdragen aan het versterken van de *compliance.*

1.3 Werkwijze

Goed toezicht is onafhankelijk, transparant, effectief en professioneel. De toezichthouder moet zonder beïnvloeding van de onder toezicht staande, de verantwoordelijke bestuurder of anderen, objectief onderzoek kunnen uitvoeren om tot een oordeel te komen. Het uitoefenen van de taken en rechtstreeks kunnen rapporteren naar de ambtelijke en militaire leiding zonder belangenconflict, zijn hiervoor een vereiste.[2] De FG dient, conform art. 38 lid 1 AVG, te worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en krijgt indien nodig toegang tot persoonsgegevens en verwerkingsactiviteiten.

De FG kan verschillende toezichtactiviteiten uitvoeren, in de vorm van toezichtbezoeken, systeemgericht toezicht, thematisch onderzoek en de beoordeling van risicoanalyses. Ook kan de FG, naar aanleiding van incidenten of onregelmatigheden, ad hoc (signaalgestuurd) toezicht uitvoeren.

De FG anticipeert hierbij op de enorme toename van gegevensverwerkingen (onder andere het verzamelen, opslaan, opvragen, verstrekken van persoonsgegevens) en de toename van technologische toepassingen in alle domeinen, om zo bij te dragen aan de voor de gehele defensieorganisatie noodzakelijke versnelling.

1 Zie ook blz.88 Regeerprogramma (2024) Rijksoverheid.

2 Zie artikel 38 lid 3 AVG 'De Functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan het hoogste leidinggevende niveau van de verwerkingsverantwoordelijke…'

1.4 Samenwerking Toezicht Defensie

Gezamenlijke inzet Toezichtnetwerk Defensie
De toezichthouders en -autoriteiten binnen Defensie werken samen in het Toezichtberaad, dat we komende jaren willen uitbreiden met een Toezichtnetwerk. Deelnemers zijn de Beveiligingsautoriteit (BA), de Functionaris voor Gegevensbescherming (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) heeft een centrale rol als coördinerend en adviserend bureau. Het voorzitterstrio bestaande uit de MLA, IMG en IVD, heeft het jaarlijks roulerend voorzitterschap. Tot juli 2026 is de MLA de voorzitter, daarna neemt de IVD het over.

Met elkaar zetten we strategische lijnen uit, stemmen gezamenlijke thema's af en borgen we de verbinding met beleid en uitvoering. We werken aan de ontwikkeling van gedeelde toezichtinstrumenten, onze positionering en onze effectiviteit. Het BTD organiseert de Leergang Toezicht Defensie (LTD): een leertraject voor alle toezichtcollega's gericht op verdieping, uitwisseling en versterking van het gezamenlijke toezichtvak.

Komend jaar focussen we ons op thema's die aansluiten bij de (versnelde) gereedstelling voor hoofdtaak 1 en de groei van de organisatie. Dit zijn onder andere: bewuste en effectieve toepassing van integraal risicomanagement (IRM) en het voorkomen van *normalisation of deviance*. Om effectief toezicht te houden zetten we ook in op het ontwikkelen van effectievere toezichtmethoden, het verbeteren van onze informatiepositie en onze relatie met de organisatie.

1.5 Inspelen op ontwikkelingen binnen Defensie

Vanuit de destijds voorziene dreigingen en probleemanalyse werd in 2020 de Defensievisie 2035 'Vechten voor een veilige toekomst' gepresenteerd. Hierin wordt de focus nadrukkelijker dan voorheen gelegd op hoofdtaak 1: de bescherming van het eigen en het bondgenootschappelijk grondgebied, het versterken van de gevechtskracht en het verhogen van de gereedheid. Om adequaat toegerust te zijn voor actuele en toekomstige dreigingen, moet Defensie een krachtige en technologisch hoogwaardige organisatie zijn. Defensie moet flexibel, schaalbaar en informatiegestuurd kunnen opereren in een complexe, hybride omgeving; in het fysieke domein, maar vooral in het digitale domein en het informatiedomein. Hiervoor is niet alleen meer mankracht en meer geavanceerd materieel noodzakelijk, maar moeten ook militaire luchthavens, kazernes, munitieopslag en trainings- en oefenmogelijkheden uitgebreid kunnen worden. In 2023 werd in dit verband het Nationaal Programma Ruimte voor Defensie opgestart en in 2024 het wetgevingsproces voor de Wet op de defensiegereedheid (WODG).

In de Defensie Cyberstrategie 2025 staat beschreven dat verhoging van de digitale weerbaarheid en van de defensieve en offensieve cybercapaciteiten noodzakelijk is om te kunnen uitbreiden. Dit dient beter te worden geïntegreerd in de onderdelen van de krijgsmacht. Voorts wordt in de Defensie Strategie voor Industrie en Innovatie 2025-2029 benadrukt dat samenwerking, innovatiesnelheid, strategische autonomie en snellere inkoopprocedures cruciaal zijn.

In de Digitale Transformatie Strategie 'Gevechtskracht door Rekenkracht' staat beschreven dat er een versnelling is van digitale innovatie in het militaire domein. Data, AI en autonome systemen spelen hierin een dominante rol.[3] Het realiseren van de ambitie van Defensie en het geven van invulling aan de hoofdtaken vereist dat Defensie digitale technologie sneller dan de tegenstander weet om te zetten in gevechtskracht.

Technologie en informatie komen meer en meer centraal te staan in het militaire optreden. Hiervoor is de beschikking over grote hoeveelheden data onontbeerlijk, maar tegelijkertijd bestaan deze data ook vaak uit persoonsgegevens. De verwerking van persoonsgegevens kan alleen wanneer hiervoor een wettelijke grondslag bestaat. Wanneer wet- en regelgeving niet wordt nageleefd, kan dit leiden tot onrechtmatige privacyschendingen en (hoge) risico's voor de rechten en vrijheden van defensiemedewerkers en burgers.

De FG is zich bewust van de grote opgave waar Defensie voor staat en dat er een spanningsveld kan ontstaan tussen naleving van wet- en regelgeving ten aanzien van *privacy* en de belangen in het kader van de nationale veiligheid. Het is echter ook belangrijk niet uit het oog te verliezen dat een belangrijk onderdeel van deze wet- en regelgeving bedoeld is om de *privacy* van defensiepersoneel en burgers te beschermen. Datalekken zoals bij de Politie[4] of het Bevolkingsonderzoek Nederland[5] tonen aan wat de consequenties kunnen zijn wanneer dit onvoldoende gebeurt.

De activiteiten van Defensie in het cyber- en informatiedomein groeien niet alleen exponentieel, maar worden ook complexer. In alle lagen van de organisatie en binnen elke eenheid worden vaker activiteiten ontplooid in het informatiedomein. Hierom is het belangrijk te blijven investeren in organisatorische waarborgen, zoals het verder uitbouwen van de privacyorganisatie. Ook is het van belang om in te blijven inzetten op het vergroten van bewustzijn en datageletterdheid, door middel van opleidingen, trainingen en bewustwordingscampagnes.

De FG is nauw betrokken bij de totstandkoming en de nadere uitwerking van de WODG en het programma Defensie Open op Orde (DOO). Door het interne toezicht tijdig en naar behoren te betrekken, kunnen risico's voor de rechten en vrijheden van betrokkenen op het gebied van gegevensbescherming en *privacy* beter worden geïnventariseerd en kunnen beleidskeuzes beter worden afgewogen en onderbouwd. Dit zijn complexe trajecten, maar ze zijn essentieel voor de ontwikkelingen bij Defensie en in het belang van de gereedstelling voor hoofdtaak 1.

De FG heeft ook een toezichttaak als het gaat om de AI-verordening. Het verantwoord gebruik van AI biedt Defensie vele kansen in de procesdomeinen, terwijl onverantwoord gebruik juist grote risico's met zich meebrengt.

3 Digitale Transformatie Strategie, p. 6.

4 *'Datalek politie, hackers bemachtigen contactgegevens alle politiemedewerkers 27 september 2024 www.nos.nl/artikel/2538710...*

5 Datalek medisch laboratorium blijkt opnieuw veel groter, zeker 850 duizend gedupeerden 29 augustus 2025 www.volkskrant.nl/binnenland/datalek-bevolkingsonderzoek/-.....~bec92c68/

2

Geplande toezicht-activiteiten 2026

De FG focust haar toezicht vooral op de volgende onderwerpen:

- verwerking persoonsgegevens van defensiemedewerkers en de informatiehuishouding;
- innovatieve middelen en gegevensverwerking in het kader van groei, (de voorbereiding op) operationele activiteiten en hoofdtaak 1;
- gegevensuitwisseling;
- verantwoord gebruik van AI en algoritmes.

De FG houdt hierbij rekening met de prioritaire thema's, doelen en werkwijzen van de externe toezichthouder, de AP. Naar aanleiding van de uitgevoerde AP-evaluatie richt de AP haar aandacht de komende jaren op vijf grote thema's: Datahandel, Big Tech, Algoritmes & AI, Vrijheid en veiligheid en Digitale overheid.[1] Daarvan zijn met name de laatste drie ook nadrukkelijk relevant binnen Defensie.

6 https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/ap-jaarplan-2025

2.1 Verwerking persoonsgegevens van defensiemedewerkers en de informatiehuishouding

Defensie heeft via de dagorder van de Commandant der Strijdkrachten (CDS) de opdracht gekregen binnen twee jaar gereed te zijn voor hoofdtaak 1. Defensie werkt aan het versterken van de militaire paraatheid en het inrichten van een oorlogsorganisatie. Er worden grote inspanningen verricht om te komen tot een moderne, wendbare krijgsmacht. Daarnaast groeit de organisatie; binnen alle eenheden neemt de instroom van regulier personeel en reservisten toe. Maar Defensie moet nog veel verder groeien.

Defensie beschikt zodoende over een groot aantal (bijzondere) persoonsgegevens van defensie-medewerkers en potentiële belangstellenden. Dit aantal neemt alleen maar toe. Deze gegevens kunnen worden gebruikt voor verschillende doeleinden, zoals strategische personeelsplanning, gezondheidsmonitoring, training of gereedstelling. Het gebruik van persoonsgegevens moet wel altijd rechtmatig, zorgvuldig en transparant plaatsvinden. Defensie heeft hiertoe, ook in het kader van de beveiliging van gegevens en de veiligheid van personeel, een grote verantwoordelijkheid naar het defensiepersoneel. De huidige geopolitieke ontwikkelingen vormen een aanvullend risico voor defensiemedewerkers indien hun persoonsgegevens (onbedoeld) openbaar worden gemaakt. Door bijvoorbeeld gegevensuitwisseling zonder passend beschermingsniveau met (sub-)verwerkers, derde landen of internationale organisaties, kunnen er risico's ten aanzien van persoonsgegevens ontstaan.

De uitdaging voor Defensie is om zo te opereren dat persoonsgegevens zo effectief mogelijk beschermd worden binnen een organisatie waarin ontwikkelingen elkaar snel opvolgen. Dit beschermt niet alleen individuele defensiemedewerkers, maar is ook in het belang van de gereedstelling en de organisatie zelf.

Defensie Open op Orde

In 2026 blijft de FG nauw betrokken bij de initiatieven rondom het verbeteren van de informatievoorziening en –huishouding, onder andere binnen het programma DOO. Als overheidsorganisatie heeft Defensie een zorgplicht op het gebied van informatievoorziening. Een belangrijk onderdeel hiervan is een ordentelijke informatiehuishouding. Het versnellen van de trajecten rondom de informatiehuishouding is noodzakelijk, maar biedt ook vele kansen voor Defensie. Een informatiehuishouding op orde betekent ook een deugdelijke bescherming van en zorgvuldige omgang met persoonsgegevens. Dit vraagt continue aandacht van de organisatie en dus ook van haar toezichthouders, zoals de FG.

2.2 Gegevensverwerkingen operationele activiteiten en hoofdtaak 1

In het kader van de versnelde gereedstelling werkt Defensie aan de WODG. Een belangrijk onderdeel van deze wet zijn de bepalingen aangaande de informatieomgeving, waarin enkele grondslagen voor gegevensverwerkingen worden gecreëerd en aangescherpt. Uit deze wet vloeien aanvullende taken voor de FG voort, zoals een verruiming van de toezichttaak en een adviestaak ten aanzien van lagere regelgeving op grond van de WODG.

Het gebruik van hoogtechnologische toepassingen in alle defensiedomeinen neemt een vlucht en autonome onbemenste systemen ontwikkelen in snel tempo. Bovendien versterkt de nationale en internationale samenwerking door de toenemende dreigingen. De *whole of society*-benadering vraagt om een weerbare en adaptieve samenleving die in gezamenlijkheid met Defensie dreigingen het hoofd moet gaan bieden. Deze samenwerking vraagt om een intensievere vorm van gegevensverwerking en van gegevensuitwisseling tussen militaire en civiele organisaties die belast zijn met rechtshandhaving, beveiliging en toezicht. Dit biedt veel kansen, maar brengt ook risico's met zich mee.

In 2026 blijft de FG focussen op de ontwikkeling en de inzet van sensoren die voorzienbaar of onvoorzienbaar, directe of indirect herleidbare persoonsgegevens verzamelen en voor diverse doeleinden kunnen verwerken en combineren. Voorbeelden zijn beeld-verwerking met camera's en elektromagnetische sensoren die informatie- en communicatiesystemen of drones kunnen detecteren en onderscheppen.

De privacywetgeving vereist dat een toezichthouder zich extra richt op verwerkingen van persoonsgegevens waarbij nieuwe technologieën worden gebruikt die door de aard, de omvang of de context en de doelen ervan mogelijk een hoog risico inhouden voor de rechten en vrijheden van personen. Bewust of onbewust misbruik of onverantwoordelijk gebruik van deze technologieën kan bijvoorbeeld leiden tot onjuiste besluitvorming, discriminatie en uitsluiting of veiligheidsrisico's, zoals datalekken. Het toezicht van de FG richt zich in 2026 nadrukkelijk op innovatieve en technologische thema's om de bescherming van persoonsgegevens binnen Defensie te waarborgen.

2.3 Gegevensuitwisseling

Door het complexe en meer hybride karakter van de nationale en internationale veiligheidsomgeving, werkt Defensie intensiever samen met publieke en private partijen. Hierbij worden samenwerkingsverbanden en informatieknooppunten ingericht waarbinnen militaire en civiele diensten gegevens uitwisselen, bijvoorbeeld op het gebied van bewaken en beveiligen, crisismanagement en dreigingsbeeldanalyse. Dit betreft samenwerkingsverbanden waarin de KMar participeert vanuit de militaire taken en (grens)politietaken of waarin sprake is van militaire bijstand en samenwerking door andere defensieonderdelen. Hierbij is het van belang dat de gegevensuitwisseling wordt ingericht binnen de kaders van de AVG, de Wpg en specifieke wetgeving zoals de Wet gegevensuitwisseling in samenwerkingsverbanden (WGS). Deze vormen van gegevensuitwisseling vormen voor de FG ook in 2026 een punt van aandacht.

2.4 Verantwoord gebruik van AI en algoritmes

Data, AI en autonomie zijn speerpunten in de Digitale Transformatie Strategie Defensie. Dat is niet verwonderlijk, want de introductie van AI in het militaire domein heeft een grote impact en een juist gebruik kan leiden tot een belangrijke voorsprong in het militaire domein. Denk hierbij aan de enorme toename van autonome onbemenste systemen of het versnellen van besluitvormingsprocessen.

De ontwikkeling van een data ecosysteem, bestaande uit kenniscentra, een centraal datalab en decentrale datateams, is een specifieke strategische doelstelling gerelateerd aan AI. Daarnaast moet AI breed worden toegepast in zowel militaire als bedrijfsmatige processen en moet Defensie met behulp van AI internationaal koploper worden op het vlak van adoptie en continue verbetering van autonome systemen.[2]

Het gebruik van AI en algoritmes brengt naast vele kansen echter ook risico's met zich mee. Om deze kansen zo optimaal mogelijk te benutten en de risico's zo veel als mogelijk te mitigeren, is sinds 1 augustus 2024 de Europese AI-verordening van kracht. Samen met de AVG, de Wpg en de principes van diverse internationaalrechtelijke organisaties geeft de AI-verordening de kaders voor een verantwoorde inzet van AI en algoritmes binnen Defensie.

De AI-verordening bevat een uitzondering voor AI-systemen die uitsluitend dienen voor militaire, defensie- of nationale veiligheidsdoeleinden. Hoewel dit voor een deel van de AI-systemen binnen Defensie geldt, vallen er vermoedelijk ook AI-systemen onder het *dual use*-principe. De toepassing en naleving van de AI-verordening is voor Defensie daarom onverminderd relevant, onder andere met het oog op de rechten en vrijheden van individuele betrokkenen. Daarnaast is de toepassing en naleving relevant bij geautomatiseerde besluitvorming voor interne bedrijfsvoering, zoals fraudedetectie, preventieve militaire gezondheidszorg, of de uitvoering van grenscontroles met behulp van AI door de KMar. In het verlengde hiervan geldt dat — ook in het militaire domein — veelal persoonsgegevens zullen worden gebruikt, zowel bij de ontwikkeling als bij de toepassing van AI. Dit alles moet op een verantwoorde wijze binnen de kaders van wet- en regelgeving plaatsvinden.

In deze fase van de inzet van AI en algoritmes binnen de defensieorganisatie richt de FG in 2026 haar aandacht op de volgende onderwerpen:

- het verkrijgen van inzicht in en overzicht over het gebruik van AI en algoritmes binnen Defensie, onder andere op basis van registers;
- het verder uitbouwen van een intern en extern netwerk;
- de naleving van de AI-verordening, met de nadruk op de hoogrisico toepassingen;
- het proactief adviseren over het verantwoord gebruik van AI en algoritmes, in gezamenlijkheid met de *Chief Information Office* (CIO) en de CPO;
- het bijdragen aan de AI-geletterdheid binnen de defensieorganisatie;
- het uitwerken van een concreet toepasbaar toetsingskader.

2.5 Vaste toezichtonderwerpen

Register van verwerkingsactiviteiten AVG en Wpg
Op grond van de wettelijke verantwoordingsverplichting moeten alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen Defensie worden vastgelegd in een register van verwerkingsactiviteiten. Het register draagt bij aan transparantie, het beheersen van risico's en het voorkomen van onrechtmatige verwerking van persoonsgegevens.

Risico-assessments
De FG houdt toezicht op de uitvoering van de *Data Protection Impact Assessments* (DPIA's): de beoordeling van het effect van de beoogde verwerkingsactiviteit op de bescherming van persoonsgegevens. De FG ziet toe op een goede uitvoering van de DPIA's en appreciëert deze op onder andere inhoud, risicobeoordeling en mitigerende maatregelen. Ook kunnen andersoortige *assessments* aan de FG ter appreciatie voorgelegd worden. Bij nieuwe wetgevingstrajecten die impact hebben op de bescherming van de persoonlijke levenssfeer en het gegevensbeschermingsrecht is onder andere een advies op de wetgevings-DPIA onderdeel van het traject.

Uit de systematiek van de DPIA's komt naar voren dat er na de risico-inventarisatie en -beoordeling voldoende mitigerende maatregelen geformuleerd moeten worden om hoge risico's te beperken. De daadwerkelijke implementatie en naleving van deze maatregelen is vaak een voorwaarde voor een positief advies. In 2026 ziet de FG nauwer toe op de implementatie en naleving van de mitigerende maatregelen in de uitvoeringspraktijk.

Datalekken AVG en Wpg
De FG ziet toe op een goede afhandeling van (risicovolle) incidenten met betrekking tot het verwerken van persoons- of politiegegevens en het naleven van de datalekprocedure. Daarbij zoekt de FG afstemming met defensieonderdelen bij meldingen die een (hoog) risico opleveren voor de rechten en vrijheden van betrokkenen. De FG ziet ook toe op de volledigheid van het interne datalekkenregister.

Wet politiegegevens
De FG Wpg houdt toezicht op de naleving van de verplichtingen en waarborgen, met name op de uitvoering van de wettelijk verplichte interne en externe Wpg-audit en de realisatie van de daaruit voortgekomen verbetermaatregelen.

Rechten van betrokkenen AVG en Wpg
De FG ziet erop toe dat betrokkenen gebruik kunnen maken van hun rechten, zoals het recht op inzage en correctie. Ook ziet de FG toe op de juiste afwikkeling van klachten van betrokkenen rond de verwerking van hun persoonsgegevens.

Awareness
De FG heeft een taak in het vergroten van kennis en het bevorderen van bewustwording binnen de defensieorganisatie. Dit vindt plaats middels toezichtactiviteiten, door informatievoorziening, het geven van adviezen en aanbevelingen en, in samenwerking met de CPO, georganiseerde bewustwordingsactiviteiten. Daarnaast draagt de FG actief bij aan cursussen en opleidingen om op deze manier het kennisniveau rondom de verwerking van persoonsgegevens en de datageletterdheid te vergroten.

De FG wil in 2026 de contacten met de verschillende defensieonderdelen verder versterken. Zodoende ontstaat een grotere zichtbaarheid en meer bewustwording. Hierdoor kan beter geanticipeerd worden op eventuele risicovolle verwerkingen met een hoge urgentie. Door verder aan de voorkant en vroegtijdig betrokken te worden bij ontwikkelingen rondom gegevensverwerkingen, kan de FG op een laagdrempeliger wijze adviseren, waardoor processen versneld kunnen worden.

2 Digitale transformatie strategie, p. 15

3

Bijlage

3.1 Afkortingen

AI	*Artificial Intelligence*
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
BTD	Bureau Toezicht Defensie
CDS	Commandant der Strijdkrachten
CIO	*Chief Information Office*
CPO	*Chief Privacy Office*
DOO	Defensie Open op Orde
DPIA	*Data Protection Impact Assessment*
FG	Functionaris voor Gegevensbescherming (Nederlandse term voor DPO)
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
IVD	Inspectie Veiligheid Defensie
KMar	Koninklijke Marechaussee
KMCGS	Korps Militaire Controleurs Gevaarlijke Stoffen
MLA	Militaire Luchtvaart Autoriteit
NAVO	Noord-Atlantische Verdragsorganisatie
UAVG	Uitvoeringswet AVG
WGS	Wet gegevensuitwisseling in samenwerkingsverbanden
WODG	Wet op de defensiegereedheid
Wpg	Wet politiegegevens