



Ministerie van Defensie

Toezichtjaarplan 2024

Functionaris voor
Gegevensbescherming

Colofon

Functionaris voor Gegevensbescherming

Adres

Majoor Jan Linzel Complex
Brasserskade 227a
2497 NX Den Haag

Postadres

Ministerie van Defensie - Bestuursstaf
Postbus 20701
2500 ES Den Haag

Datum

November 2023

Voorwoord

De Functionaris voor Gegevensbescherming (FG) is een interne toezichthouder van het Ministerie van Defensie en houdt toezicht op de naleving van de wet- en regelgeving rond de bescherming van de privacy en de verwerking van persoonsgegevens. De Algemene verordening gegevensbescherming (Avg) en de Wet politiegegevens (Wpg) zijn de wettelijke basis voor het toezicht van de FG. De FG wordt ook wel aangeduid als *Data Protection Officer* (DPO). De FG controleert of betrokkenen hun privacyrechten kunnen uitoefenen en ziet toe op een correcte afhandeling van klachten over en incidenten bij het verwerken van persoonsgegevens, waaronder datalekken.

In de Defensievisie 2035 ‘*Vechten voor een veilige toekomst*’¹ onderkent de minister van Defensie het belang van informatiegestuurd optreden en onderstreept dat Defensie ook toegerust moet zijn om, binnen de geldende ethische en juridische kaders, op te treden in de informatieomgeving. In lijn hiermee besteedt de FG in 2024 meer aandacht aan de verwerking van persoonsgegevens bij de technische en organisatorische ontwikkelingen en innovaties in het kader van de informatiegestuurde krijgsmacht, en het verbeteren van de informatiehuishouding van Defensie. Voorbeelden hiervan zijn het bevorderen van de cyberveiligheid, het gebruik van biometrische herkenning, de digitalisering van de inzet, de toepassing van AI en algoritmes, en het monitoren van fysieke prestaties en gezondheidsgegevens. Hierbij kiest de FG voor een balans tussen enerzijds het bevorderen van de bewustwording en anderzijds het toezicht op de naleving van wet- en regelgeving. De FG houdt toezicht op de bestaande en de nieuwe manieren waarop Defensie persoonsgegevens verwerkt. De ambtelijke top, de operationele commandanten van de krijgsmachtonderdelen en de hoofden van de defensieonderdelen krijgen als Avg- en Wpg-beheerders gevraagd en ongevraagd advies van de FG en kunnen worden aangesproken op hun verantwoordelijkheid.

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

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

¹ Zie Ministerie van Defensie. (15 oktober 2020). *Defensienota TK 2020-2021. 34919, nr. 71., bijlage 951610*

Inhoud

1	Over de Functionaris voor Gegevensbescherming	6
	1.1 Inspelen op komende ontwikkelingen binnen het toezicht	6
	1.2 Organisatorische wijzigingen	7
	1.3 Avg-/Wpg-organisatie Ministerie van Defensie	7
2	Geplande activiteiten 2024	8
	2.1 Toezichtactiviteiten	8
	2.2 Overige activiteiten	8
	2.3 Monitoren, signaleren en reflecteren	9
	2.4 Samenwerking	9
	2.5 Overzicht voorgenomen toezichtactiviteiten 2024	10
3	Bijlage	11
	3.1 Afkortingen	11

1 Over de Functionaris voor Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) is binnen Defensie de onafhankelijke toezichthouder die toeziet op de naleving van de wet- en regelgeving bij de verwerking van persoonsgegevens². De Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg (Uavg) en de Wet politiegegevens (Wpg) zijn de wettelijke basis voor het toezicht door de FG.

Binnen Defensie zijn twee functionarissen gegevensbescherming actief, die respectievelijk toezien op de naleving van de Avg en de Wpg.

De FG hanteert in haar toezicht vier vormen van onderzoek:

- **nalevingstoezicht:** regulier toezicht gericht op het bevorderen van het naleven van wet- en regelgeving;
- **systeemtoezicht:** toezicht op de opzet, het bestaan en de werking van systemen en processen, gericht op het systematisch vergroten van kwaliteit en regelnaleving;
- **signaalgestuurd toezicht:** ad hoc-toezicht naar aanleiding van incidenten, onregelmatigheden of datalekken;
- **thematisch onderzoek:** onderzoek naar een of meer specifieke aspecten bij meerdere onderdelen. Het onderzoek leidt tot een oordeel over de uitvoering bij meerdere organisatieonderdelen.

1.1 Inspelen op komende ontwikkelingen binnen het toezicht

Defensie werkt aan verdergaande digitalisering en doorloopt een transitie naar informatiegestuurd optreden. Het gaat om uiteenlopende producten, diensten en applicaties waarbij (nieuwe) technologieën gebruikt worden. Voorbeelden hiervan zijn het ontwikkelen van *business intelligence dashboards*, kunstmatige intelligentie (AI), algoritmes, slim cameratoezicht, gezondheidsmonitoring, elektromagnetische spectrumanalyse (bijvoorbeeld *wifi-tracking*) en (biometrische) sensoren. Ook komen er steeds meer tools beschikbaar die informatie en datastromen verwerken en inzichtelijk maken vanuit publiektoegankelijke bronnen. Defensie beschikt hierdoor over steeds grotere hoeveelheden data en daar zitten vaak gevoelige en bijzondere persoonsgegevens bij.

De FG richt zich in 2024 naast de reguliere toezichtwerkzaamheden ook op verwerkingen van persoonsgegevens, waarbij nieuwe technologieën worden gebruikt die door de aard, omvang of de context en de doelen ervan mogelijk een hoog risico inhouden voor de rechten en vrijheden van personen. De FG haakt al zoveel als mogelijk aan bij implementatietrajecten, zoals de doorontwikkeling beleidsvisie 'Informatiegestuurd Optreden' (IGO), het programma 'Defensie Open op Orde', en de voorbereiding op de EU-verordening *Artificial Intelligence (AI)*³, om te voorkomen dat de privacygerelateerde risico's niet of niet juist worden geadresseerd en de gemaakte keuzes niet voldoende worden onderbouwd.

Daarnaast richt de FG zich op vaker terugkerende elementen van het toezicht, zoals de Avg- en Wpg-organisatiestructuur, de naleving van de wettelijke verantwoordingsplicht, transparantieverplichting, het gegevensbeschermingsbewustzijn en de melding, afhandeling en registratie van inbreuken op de beveiliging van persoonsgegevens (datalekken).

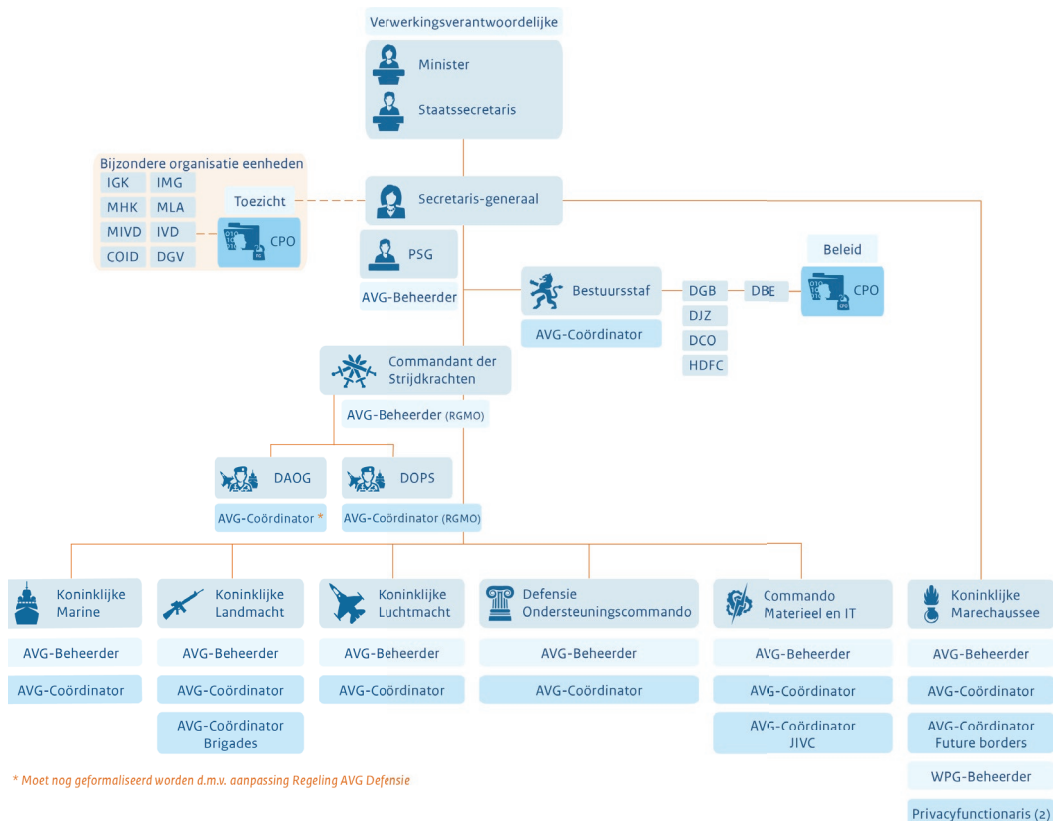
² De FG is bij Defensie niet belast met het toezicht op de naleving van de Wet op de inlichtingen en veiligheidsdiensten 2017 door de Militaire Inlichtingen en Veiligheidsdienst (MIVD).

³ Zie ook BS2022014990, Nota managementreactie 'ADR-deelonderzoek beheersing algoritme', 8 juli 2022.

1.2 Organisatorische wijzigingen

Goed toezicht is onafhankelijk, transparant, effectief en professioneel. De toezichthouder moet zonder beïnvloeding van de onder toezicht staande partij, de verantwoordelijke bestuurder of anderen, objectief feitenonderzoek kunnen uitvoeren om tot een oordeel te komen. Het zonder belangenconflict uitoefenen van de taken en rechtstreekse rapportagelijnen naar de Secretaris-generaal, de staatssecretaris en de minister zijn een eerste vereiste⁴. Ten behoeve van de onafhankelijkheid en transparantie is de onafhankelijke toezichtcapaciteit (FG-unit) met ingang van 2023 als Bijzondere Organisatie Eenheid (BOE) onder de P-SG ingericht en administratief ondergebracht bij de Inspectie Veiligheid Defensie (IVD). Daarnaast is de FG-unit in de loop van 2023 versterkt met aanvullende personele capaciteit. In 2024 wordt de FG-unit verder versterkt met een 'kwartiermakersfunctie' om complexe toezichtprocessen op het gebied van gegevensbescherming te coördineren en de visie en strategie te bepalen voor het toezicht op AI en algoritmes binnen de defensieorganisatie. De FG-unit zal naar verwachting in 2024 bestaan uit zeven medewerkers: de twee FG's (Avg en Wpg), een kwartiermaker toezicht AI en algoritmes, drie senior inspecteurs en een junior inspecteur/secretaris. Het onderstaande organogram toont de Avg-/Wpg-organisatie van het Ministerie van Defensie. Conform de Avg- en Wpg-regelingen Defensie is de verwerkingsverantwoordelijkheid vanuit de minister van Defensie toebedeeld aan de beheerders bij de defensieonderdelen en zijn Avg-coördinatoren en Wpg-privacyfunctionarissen aangesteld. De beoogde scheiding tussen de Beleidsfunctie belegd bij de Chief Privacy Office (CPO) en de Toezichtfunctie belegd bij de FG-Unit komt inmiddels duidelijk naar voren in de organisatiestructuur.

1.3 Avg-/Wpg-organisatie Ministerie van Defensie



Figuur 1: Organogram

⁴ Zie artikel 38 lid 3 Avg 'De Functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan het hoogste leidinggevende niveau van de verwerkingsverantwoordelijke...'

2 Geplande activiteiten 2024

2.1 Toezichtactiviteiten

De FG voert onderzoeken uit naar de naleving van de Avg en de Wpg bij de defensieonderdelen en, indien van toepassing, bij verwerkers en sub-verwerkers. Ook voor gegevensverwerking bij (sub-)verwerkers is en blijft Defensie verantwoordelijk en valt de verwerking onder het nalevingstoezicht van de FG's.

De FG voert onder andere systeemtoezicht uit op de processen/systemen van de verantwoordingsplicht. De kwaliteit en borging van de verantwoordingsplicht is van belang voor een verdere inrichting van systeemtoezicht. Als een organisatieonderdeel over een goed werkend intern borgingssysteem (*compliance-management*) beschikt, dan is het waarschijnlijker dat de organisatie de kwaliteit- en gegevensbeschermingsdoelstellingen behaalt.

Op grond van de wettelijke verantwoordingsplicht moeten alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen Defensie worden vastgelegd in een register van verwerkingsactiviteiten, voordat met de verwerking ervan wordt aangevangen. Dit centrale register biedt op een overzichtelijke manier inzicht in alle processen en activiteiten waarbij persoonsgegevens betrokken zijn, inclusief de verwerkingsdoelen en wettelijke grondslagen. De FG's voeren toezicht uit op de kwaliteit en de naleving van de verplichting tot het bijhouden van het register van verwerkingsactiviteiten door de verwerkingsverantwoordelijke en de beheerders.

De FG houdt tevens toezicht op de uitvoering van de *Data Protection Impact Assessments* (DPIA's). Op de binnen Defensie opgestelde DPIA's wordt een kwaliteitstoets door de *Chief Privacy Office* (CPO) uitgevoerd. De FG ziet toe op de goede uitvoering van de DPIA's en wordt uiteindelijk verzocht de DPIA te beoordelen (appreciatie) op de inhoud, de risicobeoordeling en de acceptatie van eventuele restrisico's. In sommige gevallen moet, door tussenkomst van de FG, het traject van voorafgaande raadpleging bij de Autoriteit Persoonsgegevens (AP) worden doorlopen.

Daarnaast selecteert de FG (innovatieve en technologische) thema's om te onderzoeken. Een themagericht onderzoek richt zich op een of meer specifieke aspecten bij meerdere defensieonderdelen.

Behalve gepland toezicht worden ook ad hoc-toezichtbezoeken uitgevoerd naar aanleiding van incidenten, onregelmatigheden of datalekken. Meldingen van datalekken die een hoog risico opleveren voor de privacy van de betrokkenen, worden in afstemming met de FG ook extern gemeld aan de AP. Een datalek kan aanleiding zijn voor een onderzoek.

2.2 Overige activiteiten

De FG Defensie heeft, naast de toezichtactiviteiten, in ieder geval tot taak:

- het jaarlijks rapporteren aan de minister over de naleving van de Avg en de Wpg;
- het adviseren van de minister en de beheerders over de toepassing en uitvoering van de Avg en Wpg;
- het begeleiden en verzorgen van contacten tussen het ministerie en de AP, en interdepartementaal;
- het toezien op de juiste afwikkeling van klachten rond het verwerken van persoonsgegevens;
- het toezien op het evalueren van (risicovolle) incidenten met betrekking tot het verwerken van persoonsgegevens of politiegegevens;
- het adviseren over de naleving van de Avg en Wpg in het kader van (beleids)ontwikkelingen en implementatietrajecten.

De FG heeft een belangrijke signalerende en adviserende rol ten aanzien van (voorgenomen) risicovolle verwerkingen van persoonsgegevens. De FG dient door de defensieorganisatie tijdig en naar behoren te worden betrokken bij nieuwe ontwikkelingen.

Klachtbehandeling is geen wettelijke toezichtstaak van de FG. Het kan echter wel voorkomen dat een klacht of incident aanleiding is om een onderzoek uit te voeren. Dit hangt af van de aard van de klacht of het incident en de ernst van de gevolgen ervan. Daarnaast kan een datalek melding, een adviesvraag over een bestaand verwerkingsproces of een nieuwe werkwijze aanleiding zijn om te bezien in hoeverre toezicht vooraf zal plaatsvinden. Ook kan er aanleiding zijn om achteraf toezicht te houden op het verlopen proces.

De FG neemt deel aan het Rijksplatform van Functionarissen voor Gegevensbescherming (RPFPG), het overleg van de FG's van de ministeries en enkele rijksbrede organisaties, en aan het platform van Functionarissen voor Gegevensbescherming op grond van de Wpg en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze samenwerkingsverbanden zorgen voor meer samenhang in het toezicht op de bescherming van persoonsgegevens binnen de Rijksoverheid.

2.3 Monitoren, signaleren en reflecteren

Om risico's in te schatten en de toezichtactiviteiten van de FG te plannen en voor te bereiden, maakt de FG onder andere gebruik van het register van verwerkingsactiviteiten en uitgevoerde DPIA's. De FG krijgt de benodigde toegang tot persoonsgegevens en verwerkingsactiviteiten voor het houden van toezicht. In het kader van haar toezichthoudende taak onderhoudt de FG binnen Defensie nauw contact met de Avg-coördinatoren en Wpg-privacyfunctionarissen als eerste contactpersoon bij de diverse defensieonderdelen. De Avg-coördinatoren en Wpg-privacyfunctionarissen hebben, naast de CPO, ook een belangrijke signalerende en adviserende rol ten aanzien van (voorgenomen) risicovolle verwerkingen van persoonsgegevens. De FG ontvangt intern Defensie de benodigde ondersteuning en middelen om de taken naar behoren uit te kunnen voeren.

2.4 Samenwerking

Samen met de andere interne toezichthouders van Defensie, verenigd in het Toezichtberaad, werkt de FG aan een sterkere positie van het toezicht bij Defensie en daarmee aan een betere balans tussen de driehoek 'Beleid, Uitvoering en Toezicht'. Om de kwaliteit, zichtbaarheid en effectiviteit van het toezicht te vergroten, zoekt de FG ook in 2024 aansluiting bij andere toezichthouders binnen Defensie, zoals de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD) en de Beveiligingsautoriteit (BA). Indien mogelijk proberen de interne toezichthouders hun toezichtbezoeken gecombineerd af te leggen.

2.5 Overzicht voorgenomen toezichtactiviteiten 2024

Onderzoek	Toelichting
Nalevingstoezicht Avg en Wpg	Regulier toezicht gericht op het bevorderen van het naleven van de Avg en de Wpg. Toezichtonderzoeken bij verschillende defensieonderdelen. Een selectie van onderdelen/verwerkingen vindt plaats op basis van een risicoafweging, ontwikkelingen binnen Defensie en DPIA's. Toezichtbezoeken kunnen plaatsvinden ten behoeve van het opstellen van advies op een DPIA.
Follow-up-onderzoeken	Toezichtonderzoeken (naleving- of systeemtoezicht) kunnen worden uitgevoerd naar de realisatie van aanbevelingen uit eigen onderzoeken of onderzoeken van derden.
Systeemtoezicht Avg en Wpg	Toezicht gericht op de kwaliteit (opzet, bestaan en werking) van de processen en van de (kwaliteit)systemen waarmee die processen bewaakt worden. Onderzoeken kunnen plaatsvinden op onder andere de procedure 'Meldplicht datalekken', onderdelen van de verantwoordingsplicht en rechten van betrokkenen.
Signaalgestuurd toezicht	Ad hoc-toezicht wordt uitgevoerd naar aanleiding van incidenten, onregelmatigheden of datalekken.
Thematisch onderzoek	Onderzoek wordt uitgevoerd naar een of meer specifieke aspecten bij meerdere organisatieonderdelen. Een selectie van thema's en onderdelen/verwerkingen vindt plaats op basis van een risicoafweging, innovaties en ontwikkelingen binnen Defensie.

Een indicatief overzicht toezichtbezoeken 2024 wordt na afstemming met de Avg-coördinatoren en -beheerders nagezonden.

3 Bijlage

3.1 Afkortingen

AP	Autoriteit Persoonsgegevens
Avg	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
CPO	<i>Chief Privacy Office</i>
DPO	Defensie Gezondheidsorganisatie
DI	Documentaire Informatievoorziening
DPIA	<i>Data Protection Impact Assessment</i> (Engelse term voor GEB)
DPO	<i>Data Protection Officer</i> (Engelse term voor FG)
FG	Functionaris voor Gegevensbescherming (Nederlandse term voor DPO)
GEB	Gegevensbeschermingseffectbeoordeling (Nederlandse term voor DPIA)
IMG	Inspectie Militaire Gezondheidszorg
IVD	Inspectie Veiligheid Defensie
MGZ	Militaire Gezondheidszorg
RPFPG	Rijksplatform van Functionarissen voor Gegevensbescherming
UAvg	Uitvoeringswet Avg
Wjsg	Wet justitiële- en strafvorderlijke gegevens
Wpg	Wet politiegegevens

