



Ministerie van Defensie

Toezichtjaarplan 2023 Functionaris voor Gegevensbescherming

Colofon

Functionaris voor Gegevensbescherming

Adres

Plein-Kalvermarktcomplex
Kalvermarkt 32
2511 CB Den Haag

Postadres

Postbus 20701
2500 ES Den Haag
MPC 85B

https://intranet.mindef.nl/bs_2021/Defensiebreed/Functionaris_Gegevensbescherming

Datum

November 2022

Inhoudsopgave

Voorwoord	4
1 Over de FG	5
1.1 <i>Inspelen op komende ontwikkelingen binnen het toezicht</i>	5
1.2 <i>Organisatorische wijzigingen</i>	5
2 Geplande activiteiten 2023	7
2.1 <i>Toezichtactiviteiten</i>	7
2.2 <i>Overige activiteiten</i>	7
2.3 <i>Monitoren, signaleren en reflecteren</i>	8
2.4 <i>Samenwerking</i>	8
2.5 <i>Overzicht voorgenomen toezichtonderzoeken 2023</i>	9
3 Bijlage	10
3.1 <i>Afkortingen</i>	10

Voorwoord

De Functionaris voor Gegevensbescherming (FG) ziet als interne toezichthouder bij het Ministerie van Defensie toe op de naleving van de wet- en regelgeving rond de bescherming 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 van binnen en van buiten Defensie hun privacyrechten kunnen uitoefenen en zien ook toe op een correcte afhandeling van klachten en incidenten rond het verwerken van persoonsgegevens, waaronder datalekken.

De Defensievisie 2035, '*Vechten voor een veilige toekomst*', onderkent 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 met de ontwikkelingen die uit deze visie voortvloeien, besteedt de FG in 2023 speciale aandacht aan de verwerking van persoonsgegevens bij (innovaties in het kader van) een informatiegestuurde krijgsmacht, cyberveiligheid, biometrische herkenning, digitalisering, de inzet van algoritmes en het monitoren van prestaties. Hierbij kiest de FG voor een balans tussen het bevorderen van de bewustwording en het bewaken van de naleving van wet- en regelgeving. Hiervoor houden wij toezicht op de manieren waarop Defensie persoonsgegevens verwerkt, spreken we Avg- en Wpg-beheerders (de operationele commandanten van de krijgsmachtonderdelen en de hoofden van de andere defensieonderdelen) aan op hun verantwoordelijkheid en geven wij gevraagd en ongevraagd advies.

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 Over de FG

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 persoonsgegevens¹. 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;
- Systeem(gericht)toezicht: toezicht op de opzet, het bestaan en de werking van systemen en processen gericht op het systematisch vergroten van kwaliteit en op regelnaleving;
- Signaalgestuurd toezicht: ad hoc-toezicht naar aanleiding van incidenten, onregelmatigheden of datalekken;
- Thematisch onderzoek: onderzoek naar één of meer specifieke aspecten bij meerdere onderdelen. Dit 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 publiek toegankelijke bronnen. Defensie beschikt hierdoor over steeds grotere hoeveelheden data en daar zitten vaak gevoelige en bijzondere persoonsgegevens bij.

De FG richt zich naast de reguliere toezichtwerkzaamheden in 2023 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) en het voorbereiden op de EU-verordening *Artificial Intelligence (AI)*², 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, het gegevensbeschermingsbewustzijn en de melding, afhandeling en registratie van inbreuken op de beveiliging van persoonsgegevens (procedure meldplicht datalekken).

1.2 Organisatorische wijzigingen

Goed toezicht is onafhankelijk, transparant, effectief en professioneel. Dit betekent dat de toezichthouder zonder beïnvloeding van de onder toezicht staande partij, de verantwoordelijke bestuurder of anderen, objectief feitenonderzoek moet kunnen uitvoeren om tot een oordeel te

¹ 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).

² Zie ook: BS2022014990, ADR *deelonderzoek beheersing algoritme* (2022, 8 juli).

komen. Ter versterking van het toezicht op gegevensbescherming en ter borging van de onafhankelijke positie van de FG is de onafhankelijke toezichtscapaciteit (FG-unit) eind 2022 administratief ondergebracht bij de Inspectie Veiligheid Defensie (IVD). Begin 2023 zal de FG-unit worden versterkt met personele capaciteit. De FG-unit zal bestaan uit de FG's Avg en Wpg en inspecteurs belast met toezichtactiviteiten op het gebied van gegevensbescherming.

De beleidstaak voor gegevensbescherming blijft belegd bij het Directoraat-Generaal Beleid (DGB) en wordt versterkt met extra personele capaciteit, waaronder een *Chief Privacy Officer* (CPO).

2 Geplande activiteiten 2023

2.1 Toezichtactiviteiten

De FG voert onderzoeken uit op de naleving bij de onderdelen van Defensie en, waar van toepassing, bij verwerkers en subverwerkers. 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 systeemgericht toezicht uit op de processen/systemen rond, onder andere, de verantwoordingsplicht. De kwaliteit en borging van de verantwoordingsplicht is van belang voor een verdere inrichting van systeemgericht toezicht. Als een organisatieonderdeel over een goed werkend intern borgingsstelsel (*compliance management*) beschikt, dan is het waarschijnlijker dat de organisatie de doelstellingen behaalt op het terrein van kwaliteit en gegevensbescherming.

Op grond van de wettelijke verantwoordingsplicht moeten alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens worden vastgelegd in een register van verwerkingsactiviteiten, voordat met de verwerking ervan wordt aangevangen. Dit centrale register toont inzichtelijk en overzichtelijk welke processen en activiteiten er met persoonsgegevens plaatsvinden, inclusief de verwerkingsdoelen en wettelijke grondslagen. De FG's houden toezicht 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 daarnaast toezicht op de uitvoering van de *Data Protection Impact Assessments* (DPIA's). Bij het opstellen van de DPIA wordt verplicht het advies (consultatie) ingewonnen van de FG, waarbij uiteindelijk ook een oordeel (appreciatie) wordt gevormd over de kwaliteit van de DPIA en de acceptatie van eventuele risico's.

Daarnaast selecteert de FG (innovatieve en technologische) thema's om te onderzoeken. Bij een themagericht onderzoek wordt onderzoek gedaan naar één of meer specifieke aspecten bij meerdere onderdelen.

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 Autoriteit Persoonsgegevens (AP). Een datalek kan aanleiding vormen 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 interdepartementale contacten;
- 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 tijdig 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 vraag om advies of goedkeuring voor een bepaald verwerkingsproces of een nieuwe werkwijze, aanleiding zijn om te bezien in hoeverre toezicht vooraf plaats zal vinden. 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 fora 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, wordt onder andere gebruik gemaakt 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 heeft de FG binnen Defensie nauw contact met de Avg-coördinatoren en de Wpg-privacyfunctionaris als eerste contactpersoon bij de diverse defensieonderdelen. De Avg-coördinatoren en Wpg-privacyfunctionaris hebben ook een belangrijke signalerende en adviserende rol ten aanzien van (voorgenomen) risicovolle verwerkingen van persoonsgegevens. De FG ontvangt de benodigde ondersteuning en middelen om de taken naar behoren uit te kunnen voeren.

2.4 Samenwerking

Samen met andere interne toezichthouders 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 wordt ook in 2023 aansluiting gezocht bij andere toezichthouders binnen Defensie, zoals de Inspectie Militaire Gezondheidszorg (IMG), Documentaire Informatievoorziening (DI), de Inspectie Veiligheid Defensie (IVD) en de Beveiligingsautoriteit (BA). Ook kunnen toezichtbezoeken gecombineerd worden afgelegd met andere interne toezichthouders. De interne toezichthouders vormen samen het Toezichtberaad Defensie.

2.5 Overzicht voorgenomen toezichtonderzoeken 2023

Onderzoek	Toelichting
Nalevingstoezicht Avg en Wpg	Regulier toezicht gericht op het bevorderen van het naleven van de Avg en de Wpg. Toezichtonderzoeken bij verschillende onderdelen van Defensie. 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 onderzoek, of onderzoek van derden.
Systeemtoezicht Avg en Wpg	Toezicht gericht op de kwaliteit (opzet, bestaan en werking) van de processen en van de (kwaliteits)systemen waarmee die processen bewaakt worden. Onderzoeken kunnen plaatsvinden op, onder andere: de procedure meldplicht datalekken, onderdelen van de verantwoordingsplicht en rechten betrokkenen.
Signaalgestuurd toezicht	Ad hoc-toezicht wordt uitgevoerd naar aanleiding van incidenten, onregelmatigheden of datalekken.
Thematisch onderzoek	Onderzoek wordt uitgevoerd naar één 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 2023 wordt na afstemming met de Avg- en Wpg-beheerders door tussenkomst van de Avg-coördinatoren en Wpg-privacyfunctionaris nagezonden.

3 Bijlage

3.1 Afkortingen

AP	Autoriteit Persoonsgegevens
Avg	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
DPO	Defensie Gezondheidsorganisatie
DI	Documentaire Informatievoorziening
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
FG	Functionaris voor Gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
IMG	Inspectie Militaire Gezondheidszorg
IVD	Inspectie Veiligheid Defensie
MGZ	Militaire Gezondheidszorg
RPFG	Rijksplatform van Functionarissen voor Gegevensbescherming
UAvG	Uitvoeringswet Avg
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens

