Ministerie van Defensie

Toezichtjaarverslag 2022

Functionaris voor Gegevensbescherming

Colofon

Functionaris voor Gegevensbescherming

Adres
Majoor Jan Linzel Complex
Brasserskade 227a
2497 NX Den Haag

Postadres
Postbus 20701
2500 ES Den Haag
MPC 85B

Datum
Maart 2023

Voorwoord

De Functionaris voor Gegevensbescherming (FG) ziet als onafhankelijke interne toezichthouder bij het Ministerie van Defensie toe op de naleving van de wet- en regelgeving rond de bescherming van persoonsgegevens. De FG wordt ook wel aangeduid als *Data Protection Officer* (DPO). De Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg (Uavg) en de Wet politiegegevens (Wpg) zijn de wettelijke basis voor het toezicht door de FG. Defensie heeft twee functionarissen gegevensbescherming, die respectievelijk toezien op de naleving van de Avg en de Wpg.

Volgens de wet informeert, adviseert en controleert de FG of verwerkingen van persoonsgegevens bij Defensie rechtmatig, behoorlijk en transparant zijn. De FG controleert ook 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. De FG heeft ook de taak om met de externe toezichthouder, de Autoriteit Persoonsgegevens (AP), samen te werken.

De FG zette in 2022, naast het bewaken van de naleving van wet- en regelgeving, in op het bevorderen van het privacybewustzijn. De FG hield in 2022 toezicht op de manieren waarop Defensie persoonsgegevens verwerkt, sprak met Avg- en Wpg-beheerders (de operationele commandanten van de krijgsmachtonderdelen en de hoofden van de andere defensieonderdelen) over hun verantwoordelijkheid, heeft onderzoek gedaan en heeft gevraagd en ongevraagd advies gegeven. De FG had in 2022 daarnaast aandacht voor verwerkingen van persoonsgegevens die een hoog risico inhouden voor de rechten en vrijheden van personen, bijvoorbeeld door het gebruik van (nieuwe) technologieën.

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

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

Inhoud

1 Reflectie op 2022

De defensieorganisatie richt zich continu op de ontwikkeling en toepassing van nieuwe en innovatieve werkwijzen en op het optimaliseren van de bestaande processen. Defensie werkt aan verdergaande digitalisering en doorloopt een transitie naar informatiegestuurd optreden (IGO). Technologische en organisatorische ontwikkelingen doen zich organisatiebreed voor, zowel in de bedrijfsvoeringsprocessen als in de operationele taakuitvoering. Het gaat om uiteenlopende producten, diensten en applicaties waarbij nieuwe technologieën worden gebruikt. Voorbeelden hiervan zijn het ontwikkelen van *business intelligence dashboards*, de toepassing van kunstmatige intelligentie (AI), algoritmes, slim cameratoezicht, gezondheidsmonitoring, biometrische sensoren en slimme sensoren en ICT-toepassingen aan boord van schepen, vliegtuigen en voertuigen. Ook komen er in het kader van IGO steeds meer tools beschikbaar die informatie en datastromen verwerken en inzichtelijk maken.

Bij deze ontwikkelingen is veel onduidelijkheid over de rechtmatigheid en juridische kaders, bijvoorbeeld op het vlak van inlichtingenverwerkingen en IGO. De noodzaak die de defensieorganisatie voelt om innovatieve werkwijzen en technologische middelen toe te passen om hun taak effectief uit te kunnen voeren in de informatieomgeving, wringt met de bestaande wettelijk kaders en bevoegdheden. Dit beeld wordt bevestigd in het onderzoek van de Onderzoekscommissie *Land Information Manoeuvre Centre* (LIMC)[1] (Commissie Brouwer). Dit onderzoek geeft aan dat "ondersteunende beleidsmatige en juridische kaderstelling bij de aanpak van hybride dreigingen door middel van IGO (nog) niet goed van de grond zijn gekomen"[2]. Het onderzoek van het juridisch adviesbureau EIFFEL[3] naar de naleving van de Avg bij verschillende verwerkingen binnen Defensie maakt ook knelpunten inzichtelijk met betrekking tot de toegekende taken en huidige bevoegdheden. Defensie onderzoekt de mogelijkheden en beperkingen van oefenen en gereedstelling in de informatieomgeving en hoe zij daarbij de ruimte binnen de bestaande juridische kaders zo goed mogelijk kan gebruiken.

"De noodzaak die de defensieorganisatie voelt om innovatieve werkwijzen en technologische middelen toe te passen om hun taak effectief uit te kunnen voeren in de informatie-omgeving, wringt met de bestaande wettelijke kaders en bevoegdheden."

In 2022 was, door de ontwikkelingen, een verhoging en een verschuiving van de werk- en toezichtdruk zichtbaar in het werkveld van privacy- en gegevensbescherming. De ontwikkelingen en de transitie naar IGO leiden tot complexere en een grotere hoeveelheid van privacyvraagstukken. De ontwikkelingen leiden ook tot een toename van de complexiteit van en het aantal uit te voeren *Data Protection Impact Assessments* (DPIA's). De privacy- en juridische organisatie wordt in het kader van een adviesrol in toenemende mate betrokken. Hierbij is de huidige privacy- en juridische organisatie niet altijd toereikend om hun taak naar behoren uit te voeren. In 2022 versterkte een aantal personele ontwikkelingen de privacyorganisatie.

[1] Zie TK 2022-2023 32761 nr.258 Kamerbrief 13 januari 2023, Rapport en beleidsreactie Onderzoekscommissie Brouwer naar het LIMC inclusief bijlage: Rapport 'Grondslag gezocht', Onderzoekscommissie Land Information Manoeuvre Centre (LIMC).
[2] Zie ook Rapport Grondslag gezocht, Onderzoekscommissie Land Information Manoeuvre Centre (LIMC).
[3] Zie TK 2022-2023 32761 nr.51 Kamerbrief 25 november 2022, Voortgang gegevensbescherming binnen Defensie, inclusief bijlage Eiffel-rapport 'Onderzoek Avg bij het Ministerie van Defensie'.

Tevens is aandacht besteed aan het vergroten van de kennis van de Avg en de bewustwording binnen de organisatie. Ondanks deze ontwikkelingen geven meerdere onderdelen van Defensie aan dat de huidige privacy- en juridische organisatie niet altijd toereikend is. De voor de uitvoering benodigde kennis en ervaring is zeer gespecialiseerd en kwetsbaar. De FG ontving van meerdere onderdelen signalen over de behoefte aan meer privacybeleid, duidelijke richtlijnen en defensiebrede standpunten. De Onderzoekscommissie LIMC beveelt in hun onderzoeksrapport ook aan om het kennisniveau van privacy- en juridische adviseurs gereed te maken voor de IGO-ontwikkelingen binnen de krijgsmacht. De Auditdienst Rijk (ADR)[4] beveelt in haar onderzoek aan om een privacybeleid op te stellen op basis van de bestaande Regeling Avg Defensie, dit uit te breiden met een explicietere koppeling naar de defensiepraktijk en te voorzien van een nadere uitwerking van beginselen en de aantoonplicht.

Het toezicht op AI en algoritmes is in ontwikkeling. De Europese Unie werkt aan diverse nieuwe verordeningen op het gebied van digitalisering, waaronder een nieuwe verordening voor AI-systemen (de zogeheten AI-Act). In 2023 werkt Defensie aan het uitbreiden en versterken van het toezicht op de ontwikkeling en de inzet van algoritmes die persoonsgegevens gebruiken. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) werkt aan een aantal trajecten op het gebied van algoritmes, zoals het recent gelanceerde Algoritmeregister en een implementatiekader voor overheden. Ook is er door BZK een *impact assessment* (IAMA) voor mensenrechten gepubliceerd bij gebruik van algoritmes.

"De FG ontving van meerdere onderdelen signalen over de behoefte aan meer privacybeleid, duidelijke richtlijnen en defensiebrede standpunten."

Alle defensieonderdelen voerden in 2022 bewustwordingsactiviteiten uit. Daarnaast is naar aanleiding van de bevindingen en conclusies van de FG-onderzoeken en het EIFFEL-onderzoek sprake van een verhoogde bewustwording van de Avg bij Defensie. Aandachtspunten zijn de structurele borging van bewustwordingsactiviteiten en het meten van privacybewustzijn. De aandacht binnen de defensieorganisatie voor de structurele inbedding van *governance* rond gegevensbescherming, de naleving van de Avg en de Wpg en de verdere professionalisering van de Avg- en Wpg-organisatie leidde in 2022 tot verbeteringen. Tegelijkertijd behoeft de naleving van de Avg en de Wpg nog altijd verdere verbetering.

Het toezicht in 2023 vindt plaats op basis van een risicoafweging en de ontwikkelingen binnen Defensie[5].

[4] Nota ADR-deelonderzoek beheersing algoritme. BS2022014990, 8 juli 2022.
[5] Zie het Toezichtjaarplan 2023. Functionaris voor Gegevensbescherming. 852022029078.

1.1 Aanbevelingen

De privacyontwikkelingen vragen om vaardige Avg-coördinatoren, die multidisciplinair inzetbaar zijn. Het vraagt ook om een structurele samenwerking met de operationele- en de juridische lijn, en om een duidelijk privacybeleid met en kaders en tools ter ondersteuning van de werkzaamheden.

Aan de hand van de huidige stand van de privacyorganisatie doet de FG de volgende aanbevelingen:

Aanbeveling 1
Versterk en professionaliseer de positie en functie van de Avg-coördinator.

Aanbeveling 2
Verhoog het volwassenheidsniveau van de gehele privacyorganisatie[6].

Aanbeveling 3
Verhoog de kwaliteit van DPIA's en registraties in het register van verwerkingsactiviteiten.

Aanbeveling 4
Stel privacybeleid op en duidelijke privacy- en juridische kaders.

Aanbeveling 5
Verbeter de beveiliging en het bewustzijn van risico's bij de uitwisseling van gegevens met externe partijen.

[6] Zie ook TK 2022-2023 32761 nr.258 Kamerbrief 13 januari 2023, Rapport en beleidsreactie Onderzoekscommissie Brouwer naar het LIMC inclusief bijlage: Rapport Grondslag gezocht, Onderzoekscommissie Land Information Manoeuvre Centre (LIMC).

2 Uitgevoerde onderzoeken

De FG genereert door middel van toezichtbezoeken, documentanalyse en waarnemingen een beeld van de naleving van wet- en regelgeving rond de bescherming van persoonsgegevens. Behalve gepland toezicht conform het Toezichtjaarplan 2022[7], legde de FG ook ad hoc-toezichtbezoeken af naar aanleiding van incidenten of adviesvragen.

2.1 Nalevingstoezicht

BS/ABP/APG: een gezamenlijk toezichtonderzoek van de Beveiligingsautoriteit (BA), de Documentaire Informatievoorziening (DI) en de FG naar de uitvoering van het mandaatbesluit Defensie specifieke uitkeringsregelingen door het Algemeen Burgerlijk Pensioenfonds (ABP)/Algemene Pensioen Groep (APG) en de archieflocatie 'De Beitel'[8]. De FG, BA en DI constateerden dat verbetering noodzakelijk is met betrekking tot dataminimalisatie, de overdracht van gegevens aan het ABP/APG en het verhogen van het bewustzijn rond privacy en beveiliging. Hoofddirectie Personeel (HDP) stelde een eerste concept verbeterplan op. De HDP werkt het verbeterplan nog verder uit. Een vervolgonderzoek naar de realisatie van de verbetermaatregelen vindt plaats in 2023.

DOSCO/DPOD/DCPL[9]: een gezamenlijk toezichtonderzoek van de FG en de DI naar de naleving van de Avg en het bewaren, vernietigen en anonimiseren van informatie bij het Dienstencentrum Personeelslogistiek (DCPL)[10]. DCPL verwerkt veel persoonsgegevens, waaronder bijzondere persoonsgegevens, bij het uitvoeren van haar werkzaamheden (onder andere op het gebied van arbeidsmarktcommunicatie, recruitment, selectie & keuring en *employability*). Geconstateerd is dat de Rijksbrede DPIA Werving en Selectie en de DPIA Instroom Personeel Defensie zijn vastgesteld. Daarnaast bleek dat het fysieke archief in een goede, geordende en toegankelijke staat verkeert en dat het register van verwerkingsactiviteiten geactualiseerd wordt. De FG constateerde ook dat voor de verwerkingen van DCPL nog een drietal DPIA's (namelijk 'medische keuringen', '*employability*' en 'reservisten') nog opgesteld moeten worden. De FG beveelt onder andere aan om zorg te dragen dat het datalek-register volledig wordt ingevuld en meer structurele aandacht te geven aan bewustwordingssessies. C-DCPL stelde een verbeterplan op en een vervolgonderzoek staat gepland voor 2023.

DOSCO/DGO/EGB: een gezamenlijk toezichtbezoek van de Inspectie Militaire Gezondheidszorg (IMG), de DI en de FG aan de medische archieven in het gezondheidscentrum Garderen (Nieuw-Millingen) en Ermelo. Aandachtspunten waren vooral het beleid over de opslag van papieren dossiers en het bewaren, afstoten en vernietigen daarvan na het inscannen door de Defensie Gezondheidszorg Organisatie (DGO)/Eerstelijns Gezondheidszorg Bedrijf (EGB). Daarnaast vraagt de FG aandacht voor de methode van verzending van dossiers, vanwege het aantal datalekken dat zich voordoet.

CLAS/BIDKL: de Bergings- en Identificatiedienst Koninklijke Landmacht (BIDKL) is verantwoordelijk voor het opsporen, bergen en identificeren van slachtoffers uit de Tweede Wereldoorlog. De FG voerde in 2022 een voorverkenning uit ter voorbereiding op een toezichtbezoek. De Commando Landstrijdkrachten (CLAS) zette diverse (verbeter)acties in gang naar aanleiding van de voorverkenning. Het uitvoeren van het initieel in 2022 geplande toezichtbezoek is daardoor beoordeeld als 'niet opportuun'. Een vervolgonderzoek naar de realisatie van de acties vindt plaats in 2023.

[7] Functionaris voor Gegevensbescherming Toezichtjaarplan 2022, november 2021, BS2021025403.
[8] Nota Gezamenlijk toezichtbezoek BA/DI/FG aan ABP/APG. 29 april 2022. BS2022010726.
[9] Defensie Ondersteuningscommando (DOSCO)/Divisie Personeel en Organisatie Defensie/ Dienstencentrum Personeelslogistiek (DCPL).
[10] Nota 'Toezichtbezoek DCPL'. 10 oktober 2022. BS2022024180.

KMar & Bestuursstaf Gegevensuitwisseling Carib-NL: de FG voerde in 2022 een voorverkenning uit ter voorbereiding van een toezichtbezoek. Het betrof een inventarisatie om de wettelijke kaders, gezagsrelaties en relevante informatiesystemen in kaart te brengen rond de activiteiten van de Koninklijke Marechaussee (KMar) in het Caribisch gebied. Dergelijk inzicht is essentieel voor een goede uitvoering van de KMar-taken en voor de adequate inrichting en het beheer van de organisatie. Dit is ook een noodzakelijke randvoorwaarde voor de uitvoering van de toezichtstaak van de FG. C-KMar is verzocht[11] aan te geven welke interne verbetermaatregelen de KMar van plan is te nemen om de gesignaleerde knelpunten te verbeteren met betrekking tot het benodigde inzicht. Een vervolgonderzoek naar de realisatie van de verbetermaatregelen vindt plaats in 2023.

KMar/PI-NL: een toezichtbezoek vond plaats bij het *Frontoffice* van de *Passenger Information Unit* Nederland (Pi-NL) om een beeld te krijgen van de processen bij het *Frontoffice* en welke vraagstukken of knelpunten er zijn rond de inrichting en de werking van de Pi-NL als geheel en de *Frontoffice* in het bijzonder[12]. De aanbevelingen moeten met name de besluitvorming over de toekomstige inrichting van de organisatie en de processen van de *Frontoffice* ondersteunen. De FG beveelt onder andere aan om, in samenwerking met de beheers- en gezagsverantwoordelijken, de *pilot Frontoffice* te evalueren en aan de hand van de uitkomsten een visie op te stellen voor de definitieve inrichting.

DOSCO/DCIOD: uit een door de FG uitgevoerde voorverkenning blijkt dat de DPIA nog niet gereed is voor het ondersteuningssysteem (G-Module) ten behoeve van de (geautomatiseerde) processen van het Dienstencentrum Internationale Ondersteuning Defensie. Een toezichtbezoek is uitgesteld totdat de DPIA geapprecieerd en vastgesteld is.

Veteranen: voor het geplande onderzoek naar de verwerking van gegevens van veteranen voerde de FG in 2022 een voorverkenning uit. Vanwege capaciteitstekort en andere prioriteiten kon het onderzoek niet meer in 2022 gerealiseerd worden. In 2023 wordt dit onderzoek vervolgd.

2.2 Thematisch onderzoek

De FG besteedde gedurende het jaar aandacht aan en gaf advies over de prioritaire thema's uit het Toezichtjaarplan FG 2022, zoals IGO, *Open Source Intelligence* (OSINT), het gebruik van biometrie, Defensie Cyber Security Center (DCSC) en andere technologische ontwikkelingen.

Onderzoek gebruik social media monitoring en -scraping tools bij Defensie: naar aanleiding van de zorgpunten en de aanbevelingen uit het LIMC-rapport onderzocht de FG de naleving van de gegevensbeschermings-wetgeving (Avg/Wpg) bij het gebruik van tools voor monitoring of *scraping* van *social media* [13]. De uitvoering van dit onderzoek vroeg de eerste helft van 2022 veel tijd en capaciteit. De FG constateerde dat Defensie diverse *social media monitoring* en *-scraping tools* (heeft) gebruikt, waarbij sprake is van een aantal tekortko-mingen in de naleving van de Avg. De FG beveelt onder andere aan om zorg te dragen voor aanvullend beleid en richtlijnen, alsmede voldoende maatregelen om een rechtmatig gebruik van *social media* monitoring te waarborgen. Als de behoefte om *social media monitoring* en *-scraping* toe te passen groter is dan de huidige juridische kaders toelaten, adviseert de FG te onderzoeken of dit binnen de bestaande taakstelling en bevoegdheden van Defensie past, of dat aanvullende bevoegdheden nodig zijn. Ook is aanbevolen verder te investeren in de Avg- en Wpg-organisatie.

[11] Nota Gegevensverwerkingen KMar Carib. 8 december 2022. BS2022031914.
[12] Verslag Toezichtbezoek Frontoffice PI-NL, BS2023000815, versie 1.3 definitief, 12 januari 2023.
[13] Nota FG Onderzoek naar *social media monitoring* bij het Ministerie van Defensie. 29 augustus 2022. BS20220020402 en zie ook TK 2022-2023 32761 nr.51 Kamerbrief 25 november 2022, Voortgang gegevensbescherming binnen Defensie, inclusief bijlage FG-rapport 'Onderzoek naar social media monitoring bij het Ministerie van Defensie'.

Naar aanleiding van het onderzoek zette Defensie diverse acties in gang, waaronder het stopzetten van diverse activiteiten. De minister heeft in de Kamerbrief 'Voortgang-gegevensbescherming binnen Defensie'[14] aangegeven welke maatregelen ter verbetering Defensie treft, zoals het aanpassen van het register van verwerkingsactiviteiten en het opstellen van DPIA's.

2.3 Externe onderzoeken op naleving Avg en Wpg

EIFFEL-onderzoek: naar aanleiding van de bevindingen en aanbevelingen uit het LIMC-rapport en de Kamervragen[15] heeft de Minister van Defensie een extern onderzoek laten uitvoeren door juridisch adviesbureau EIFFEL. Zij onderzocht bij een aantal onderdelen/eenheden in hoeverre de Avg daar wordt nageleefd[16]. In totaal heeft EIFFEL 26 verwerkingen beoordeeld die als 'risicovol' waren bestempeld. Daarvan voldeden vijf activiteiten aan de Avg, zeven activiteiten voldeden grotendeels aan de Avg waarvoor vervolgstappen noodzakelijk waren, en zeven activiteiten voldeden niet aan de Avg, waarbij de geconstateerde tekortkomingen de doorgang van de activiteit blokkeerden. Op zeven activiteiten was de Avg niet van toepassing of lag de verantwoordelijkheid voor de activiteit niet bij Defensie. Naar aanleiding van het onderzoek heeft Defensie diverse acties ter verbetering in gang gezet. Gedurende de eerste helft van 2022 zette de FG haar capaciteit in voor de begeleidingscommissie van dit onderzoek.

Rijksbreed Avg-onderzoek: de Auditdienst Rijk (ADR) onderzocht de verantwoordingsverplichting, de regie en toezicht op de naleving van verwerkersovereenkomsten en welke privacycriteria gehanteerd worden in de departementale *cloud*-strategie. De Avg-beheerders rapporteren jaarlijks aan de FG over de naleving van de Avg. De ADR beschouwt de manier waarop Defensie dit vormgeeft als een *best practice*. De ADR constateerde dat de privacy-uitgangspunten aanwezig zijn in verschillende defensiespecifieke of Rijksbrede documenten. Zij beveelt aan om, conform het advies van de AP, een privacybeleid te overwegen. De ADR constateerde ook dat de taken, verantwoordelijkheden en bevoegdheden rond het opstellen van de verwerkersovereenkomsten belegd zijn. Bij het afsluiten van een verwerkersovereenkomst moeten in beginsel de Rijksbrede formats gehanteerd worden. Wanneer er bijzondere informatie wordt verwerkt, wordt de Algemene Beveiligingseisen Defensieopdrachten (ABDO) bedongen en onderzoekt de MIVD of de dienstverlener aan de normen van de ABDO voldoet. De ADR constateerde verder dat nog niet alle defensieonderdelen een goed overzicht hebben van verwerkersovereenkomsten die nog afgesloten of geactualiseerd moeten worden. Tijdige en betrouwbare (volledige en juiste) registratie van verwerkersovereenkomsten is een bekend aandachtspunt en *key control* van de inkooporganisatie. De ADR constateerde dat er geen proces is ingericht dat erop toeziet dat de ontvangen rapportages van verwerkers worden beoordeeld, waarna, indien noodzakelijk, mitigerende maatregelen worden genomen om de naleving van de Avg te borgen. Defensie beschikt niet over een centraal overzicht van alle *cloud*-diensten die binnen het departement worden afgenomen. Defensie heeft een routekaart opgesteld met hoe zij wil omgaan met het gebruik van *cloud*-diensten en gaat een aanvullende instructie opstellen. De ADR beschouwt de routekaart en het bijgevoegde besluitvormingsraamwerk als een *best practice*.

[14] Nota 'Voortgang gegevensbescherming binnen Defensie', 25 november 2022, BS2022023235.
[15] Kamervragen 9 april 2021 (Kenmerk 2021D12460 #3218542).
[16] Zie TK 2022-2023 32761 nr.51 Kamerbrief 25 november 2022, Voortgang gegevensbescherming binnen Defensie, inclusief bijlage Eiffel-rapport Onderzoek Avg bij het Ministerie van Defensie.

ADR deelonderzoek 'Beheersing algoritme' & Algemene Rekenkamer (AR) onderzoek 'Algoritmes getoetst'[17]: de ADR voerde een Rijksbreed onderzoek uit naar de huidige wijze van beheersing van algoritmes. Daarnaast voerde de AR onderzoek uit naar de inzet van algoritmes bij de Rijksoverheid. Zij adviseerden onder andere verbetermaatregelen voor het uitvoeren van DPIA's, het vastleggen van waar informatie naartoe gaat, het zorgdragen van formele validatie en het inrichten van toezicht op algoritmes. Defensie stelde verbetermaatregelen[18] op om de aandachtspunten te adresseren. Door een samenwerkingsverband tussen de Directoraat-Generaal Beleid (DGB), de Chief Information Office (CIO) en de FG zijn in 2022 de eerste stappen gezet om het toezicht op algoritmes structureel in te richten.

Externe audit Wpg: de ADR voerde bij de KMar de vierjaarlijkse verplichte externe (privacy-)*audit* uit. De ADR beoordeelde of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven. De ADR concludeerde dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen, naar de stand van ultimo december 2018, in opzet, bestaan en werking niet of niet geheel heeft voldaan aan de vereisten zoals genoemd in de Wpg. De verwerkingsverantwoordelijke moet binnen drie maanden een verbeterrapport opstellen. De KMar heeft aangegeven dat een werkgroep de geconstateerde tekortkomingen gaat aanpakken. De werkgroep richt zich op de herinrichting van de opzet en het bestaan van het Wpg-proces. Ook wordt extra geïnvesteerd in de verbetering van de Wpg-compliance. Een vervolgonderzoek van de FG naar de realisatie van een verbeterplan en de verbetermaatregelen vindt door de FG plaats in 2023.

Onderzoekscommissie LIMC[19]: de Onderzoekscommissie LIMC onderzocht de besluitvorming omtrent de oprichting en de uitvoering van de taken van het LIMC. Het onderzoek bevatte ook twee deelonderzoeken. Het eerste deelonderzoek betrof de juridische context waarbinnen het LIMC functioneerde. Het tweede deelonderzoek betrof de juridische kaders van de Avg in relatie tot de verwerking van persoonsgegevens binnen het LIMC. In het rapport van de Onderzoekscommissie wordt onder andere geconcludeerd dat "de gestelde nieuwe dreigingen van hybride conflictvoering raken aan de kern van de hoofdtaken van de krijgsmacht en vragen om aanpassing van de bestaande juridische en beleidsmatige kaders. De aanpassing van deze kaders komt (in de door ons onderzochte periode) nog niet goed van de grond"[20]. Tevens deed de Onderzoekscommissie een aantal aanbevelingen bij het deelonderzoek gegevensbescherming, zoals het in kaart en omhoog brengen van het volwassenheidsniveau van de privacyorganisatie, het kennisniveau van privacy- en juridische adviseurs gereed maken voor de IGO-ontwikkelingen, het opstellen van duidelijke privacy- en juridische kaders voor IGO en het opstellen van kaders voor de wenselijkheid en rechtmatigheid van inzet van *social media monitoring* binnen de Rijksoverheid.

[17] Algoritmes getoetst. De inzet van 9 algoritmes bij de overheid. Algemene Rekenkamer 2022.
[18] Nota ADR-deelonderzoek 'Beheersing algoritme'. BS2022014990. 8 juli 2022.
[19] Zie TK 2022-2023 32761 nr.258 Kamerbrief 13 januari 2023, Rapport en beleidsreactie Onderzoekscommissie Brouwer naar het LIMC inclusief bijlage: Rapport 'Grondslag gezocht', Onderzoekscommissie Land Information Manoeuvre Centre (LIMC).
[20] Rapport 'Grondslag gezocht', Onderzoekscommissie Land Information Manoeuvre Centre (LIMC). Pg. 7.

2.4 Systeemgericht toezicht

Het register van verwerkingsactiviteiten dient inzicht te geven in de gegevensverwerkingen binnen de defensieorganisatie, inclusief relevante beleidsontwikkelingen en de inzet van nieuwe technologieën en toepassingen waarbij de verwerking van persoonsgegevens een rol speelt. De FG monitorde de kwaliteit en de naleving van de verplichting tot het bijhouden van het register van verwerkingsactiviteiten.

De FG houdt toezicht op de uitvoering van de DPIA's. Een DPIA is een wettelijk verplicht instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om deze risico's te verkleinen. Bij het opstellen van een DPIA, alvorens met een hoog risicoverwerking wordt aangevangen, wordt verplicht advies ingewonnen bij de FG. Hierbij wordt een oordeel (appreciatie) gevormd over de kwaliteit van de DPIA en de acceptatie van eventuele restrisico's. Als er ondanks de voorgenomen maatregelen onvoldoende zekerheid kan worden geboden dat de verwerking in overeenstemming met de Avg of de Wpg is, kan de verwerking niet aanvangen (of worden voortgezet).

"Bij het opstellen van een DPIA, alvorens met een hoog risicoverwerking wordt aangevangen, wordt verplicht advies ingewonnen bij de FG."

De FG hield toezicht op de kwaliteit en de naleving van de procedure 'meldplicht datalekken intern Defensie'. 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. Behalve dat een datalek aanleiding kan zijn voor een toezichtbezoek, worden, mede op advies van de FG, maatregelen voorgesteld die een herhaling van het datalek in de toekomst moet voorkomen.

3 Hoofdlijnen uit het toezicht

3.1 Verantwoording

In de 'Regeling Avg Defensie' is vastgelegd dat de Avg-beheerder jaarlijks rapporteert over de naleving van de Avg en de wet binnen zijn onderdeel. De ADR[21] benoemde in haar onderzoek de manier waarop Defensie dit vormgeeft een *best practice*.

Alle Avg-beheerders en de Wpg-beheerder hebben een (concept) jaarrapportage aangeleverd. De meeste onderdelen geven wel aan problemen te ondervinden met het tijdig (voor 1 januari) aanleveren van een vastgestelde jaarrapportage. In 2023 kijkt de FG samen met de Avg-coördinatoren naar verbetermogelijkheden van het rapportageproces.

3.2 Avg- en Wpg-organisatie

Organisatorische ontwikkelingen toezicht en beleid

Ter versterking van het toezicht op gegevensbescherming voor een betere borging van de onafhankelijke positie van de FG is de onafhankelijke toezichtcapaciteit (FG-unit) eind 2022 administratief ondergebracht bij de Inspectie Veiligheid Defensie (IVD). In 2022 is de FG-unit bestaande uit de FG Avg en de FG Wpg versterkt met een functie voor onderzoekscapaciteit. Medio 2023 wordt de FG-unit versterkt met twee aanvullende functies.

De beleidstaak voor gegevensbescherming blijft belegd bij het DGB en is eveneens versterkt met extra personele capaciteit, waaronder een *Chief Privacy Officer* (CPO). Eind 2022 is de formatie van het (beleids) cluster gegevensbescherming uitgebreid met twee functies en zijn tijdelijke adviseursfuncties omgezet naar vaste personele capaciteit. Met de komst van de CPO bestaat het cluster nu uit vijf VTE.

Avg-coördinatoren en Wpg-privacyfunctionaris

Conform de Regeling Avg Defensie hebben alle Avg-beheerders een Avg-coördinator aangewezen. Directie Operaties (DOPS) heeft een Avg-coördinator Militaire Operaties. Conform artikel 34 van de Wpg heeft C-KMar een privacyfunctionaris aangewezen. De Avg-coördinatoren en de privacyfunctionarissen hebben een cruciale rol bij de naleving van de Avg en de Wpg in de praktijk bij Defensie.

In het Toezichtjaarverslag FG 2021 staat de aanbeveling om de privacyorganisatie te versterken en te professionaliseren. In verschillende rapporten uit 2022 staat ook de aanbeveling om de Avg- en Wpg-organisatie te versterken en (verder) te professionaliseren. Dit betreft naast het kennisniveau en de samenwerking met de operationele en juridische lijn ook het zorgdragen voor een duidelijke privacybeleid en -kaders en het zorgdragen voor tools ter ondersteuning van de werkzaamheden.

In 2022 hebben enkele personele ontwikkelingen plaatsgevonden bij de CLAS en de KMar om bij deze onderdelen de privacyorganisatie (tijdelijk) te versterken. Ook is aandacht besteed aan het vergroten van de kennis van de privacyorganisatie. Zo zijn CIPP/E-trainingen[22] voor de Avg-coördinatoren beschikbaar gesteld en volgden zij andere specialistische trainingen en *webinars*. Desondanks geven meerdere onderdelen aan een capaciteitstekort te hebben om de privacytaken naar behoren uit te kunnen voeren. De voor de uitvoering benodigde kennis en ervaring is zeer gespecialiseerd en het gebrek aan *redundancy* bij meerdere onderdelen brengt een zekere kwetsbaarheid met zich mee. Tevens is op dit moment de werklast voor de Avg-coördinatoren en privacyfunctionarissen met betrekking tot de implementatie van de AI-verordening nog onduidelijk maar kan deze aanzienlijk worden.

[21] Nota ADR-deelonderzoek 'Beheersing algoritme'. BS2022014990. 8 juli 2022.
[22] Certified Information Privacy Professional / Europe van The International Association of Privacy Professionals (IAPP).

In 2023 is een toezichtonderzoek naar de positionering, kennis, capaciteit en middelen van de Avg- en Wpg-organisatie gepland.

Zie verder tabel 1, normen a t/m e, in Bijlage 1.

Bewustwording

Alle defensieonderdelen voerden bewustwordingsactiviteiten uit, zoals voorlichting, presentaties en colleges. Daarnaast is er voor alle defensiemedewerkers een intranetsite over beveiliging en privacy beschikbaar. Aandachtspunten zijn het structureel borgen van bewustwordingsactiviteiten, bijvoorbeeld met een awareness-programma, en het meten van de effectiviteit van de bewustwordingsactiviteiten.

Zie verder tabel 1, norm f in Bijlage 1.

3.3 Verwerkersovereenkomsten

Als Defensie gebruik maakt van een verwerker, dan dient een verwerkersovereenkomst (of andere rechtshandeling, zoals een convenant of een verwerkersafspraak) opgesteld te worden.

Het is voor verwervers/inkopers verplicht om de verwerkersovereenkomst te registeren in het contractenregister van SAP M&F. In het contractregister zit een module om te monitoren welke overeenkomsten op korte termijn aflopen. Zoals aangegeven in hoofdstuk 2, heeft de ADR in haar onderzoek geconstateerd dat nog niet alle defensieonderdelen een goed overzicht hebben van verwerkersovereenkomsten die nog afgesloten en geactualiseerd moeten worden en dat er geen expliciet proces is ingericht om erop toe te zien dat de ontvangen rapportages van verwerkers worden beoordeeld. Dit beeld komt overeen met het beeld dat naar voren komt uit de eigen onderzoeken.

Zie ook tabel 1, norm g, in Bijlage 1.

3.4 Register van verwerkingsactiviteiten

De verwerkersverantwoordelijke dient in het kader van zijn verantwoordingsplicht een register bij te houden van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden[23]. Bovendien is doorlopende aandacht nodig voor het onderhouden en actualiseren van het register.

De FG heeft over 2022 bezien of de daadwerkelijk geregistreerde verwerkingen in het register van verwerkingsactiviteiten valide, volledig en *up-to-date* zijn. In 2022 besteedden meerdere defensieonderdelen aandacht aan het verbeteren van de kwaliteit van het register. De Avg-coördinatoren hebben een kwaliteitsslag uitgevoerd op de geregistreerde verwerkingen in het register van verwerkingsactiviteiten van de Bestuursstaf (BS) (apparaat), Commando Luchtstrijdkrachten (CLSK), Commando Zeestrijdkrachten (CZSK), Defensie Materieel Organisatie (DMO), DMO/Joint IV Commando (JIVC) en DOSCO. Hierbij zijn 'dubbelingen' met defensiebrede verwerkingen verwijderd.
Bij CLSK, CZSK, DMO/JIVC, CLAS en KMar vindt een (nadere) kwaliteitsslag en samenvoeging plaats van geregistreerde verwerkingen in 2023. Bij de KMar is gelijktijdig een hernieuwde aanpak en structuur voor het Avg- en de Wpg-registers voorgesteld.

Zie ook tabel 1, normen h t/m j, in Bijlage 1.

Een onderzoek door de FG naar de borging van de volledigheid, de juistheid en de actualiteit van het register van verwerkingsactiviteiten staat gepland voor 2023.

[23] Art.30, lid 1, Avg en art. 31d Wpg.

3.5 Data Protection Impact Assessment

Status DPIA's Avg en Wpg 2022	Defensie
Vastgesteld	20
Gereed voor vaststelling	2
Voorgelegd aan FG ter appreciatie	19
Lopend	45
Voorgenomen	38
Aantal DPIA's geactualiseerd in 2022	4

Er is een sterke toename zichtbaar in het aantal uit te voeren DPIA's en ook de complexiteit neemt toe. 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. Dit onderstreept de noodzaak om het DPIA-proces tijdig op te starten. Uit door de FG uitgevoerde appreciaties blijkt dat er onder meer aandacht nodig is voor het onderkennen van privacyrisico's.

Naast het realiseren van de DPIA's is het van belang dat onder andere de adviezen en maatregelen uit DPIA's ook daadwerkelijk door de organisatie worden opgepakt, zodat zij niet enkel een papieren werkelijkheid blijven. Een onderzoek door de FG naar onder andere de (borging van de) realisatie van openstaande maatregelen om privacyrisico's te mitigeren, staat gepland voor 2023.

3.6 Inbreuken/datalekken

Mogelijke datalekken worden gemeld in het systeem '*PeopleSoft Melden Voorvallen*'(PSMV-systeem). De Avg-coördinator of privacyfunctionaris beoordeelt, conform de procedure, een melding en consulteert de FG. Alle inbreuken in verband met persoonsgegevens neemt de Avg-coördinator op in een datalekregister, ook als niet direct sprake is van een datalek. Daarnaast kan een datalek 'meldingsplichtig'[24] zijn bij de AP.

	2022	2021	2020	2019	2018	2017	2016
Avg-gerelateerde PSMV-meldingen	197	154	156	95	75	51	49
Intern geregistreerde inbreuken	248	169	109				
Bij AP (extern) Avg gemelde datalekken	19	16	15	14	16	18	17
Wpg-gerelateerde PSMV-meldingen	0	1	5	9	n.v.t.	n.v.t.	n.v.t.
Bij AP (extern) Wpg gemelde datalekken	0	1	0	1	n.v.t.	n.v.t.	n.v.t.

De FG ontvangt een afschrift van de in het PSMV-systeem gemelde voorvallen die aangevinkt zijn als een 'Avg-voorval'. In 2022 ontving de FG 197 meldingen. Dit is een toename ten opzichte van voorgaande jaren. Aanpassingen in het PSMV-systeem en het vergroten van de bewustwording over privacy en het belang van het melden van datalekken hebben hier mogelijk aan bijgedragen. In geen van de gevallen leidde de melding tot het instellen van nader toezicht. Wel is met de betreffende defensieonderdelen contact geweest over het treffen van maatregelen ter verbetering van de processen.

[24] In artikel 33 Avg en 33a Wpg wordt een bij de AP meldingsplichtig datalek omschreven als: "een inbreuk in verband met persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen".

In totaal zijn 248 inbreuken in verband met persoonsgegevens geregistreerd in de interne datalekregisters van de defensieonderdelen. Dit is ook een groei ten opzichte van voorgaande jaren. Opvallend is het groot aantal meldingen van foutief gestuurde medische informatie. Dit betreft een medisch dossier, of een deel van een dossier dat wordt aangeleverd aan de verkeerde persoon. In 2022 meldde Defensie in totaal 19 Avg-datalekken en een Wpg-datalek bij de AP. Dit is redelijk constant in vergelijking met de afgelopen jaren. In de medische sector zijn vier datalekken (foutief verzenden van medische informatie) later dan de voorgeschreven 72 uur na de ontdekking gemeld aan de AP. De AP heeft een waarschuwing afgegeven[25] dat de aangedragen reden voor te laat melden, namelijk 'interne doorlooptijden', ongegrond zijn. De AP dringt aan op maatregelen ter verbetering en versnelling van de interne procedures.

De FG ontvangt signalen dat het PSMV-systeem en het proces van melden voorvallen/datalekken verbetering behoeft, ondanks goede aanpassingen om meldingen eenvoudiger te maken. Signalen zijn bijvoorbeeld dat Avg-voorvallen ten onrechte als beveiligingsincident of als integriteitskwestie worden aangemerkt in het PSMV-systeem, of dat de afhandeling door de leidinggevende te lang duurt. Dit kan problemen opleveren voor de naleving van de wettelijke termijn van melden binnen 72 uur aan de AP.

3.7 Rechten van betrokkenen

De Avg en Wpg kent privacyrechten toe aan betrokkenen. Daartoe is een proces 'rechten betrokkenen' ingericht voor zowel de Avg en de Wpg. Externe verzoeken van betrokkenen kunnen via een daartoe ingerichte internetsite van Defensie worden ingediend. Voor medewerkers in werkelijke dienst geldt een vergelijkbaar proces via een intranetpagina van Defensie. Binnen Defensie bestaat een procedure ingericht voor de afhandeling van de verzoeken.

De meeste betrokkenen doen een beroep op het 'recht op inzage' in personeelsdossiers. Van de 2.700 externe verzoeken hebben slechts enkele geleid tot vragen, veroorzaakt door een vertraagde afhandeling of onduidelijke vraagstelling. Deze vragen zijn afgehandeld door de organisatie. De Juridische Dienstverlening Bedrijfsbureau heeft nog twee bezwaarzaken in behandeling. Bij de KMar hebben drie betrokkenen beroep ingesteld tegen het besluit, op grond van artikel 25 Wpg. Het gaat om een besluit over een verzoek tot informatie en inzage in politiegegevens. Van deze beroepen is er een ter zitting gekomen. De andere twee zullen naar verwachting in 2023 ter zitting worden behandeld.

Voor zover bekend zijn er geen verzoeken om bemiddeling of klachten over de afhandeling van verzoeken door betrokkenen ingediend bij de AP.

3.8 Borgen realisatie verbetermaatregelen

In verschillende interne en externe onderzoeken zijn aanbevelingen (zie paragraaf 1.1. Uitgevoerde onderzoeken) gegeven ter verbetering van de naleving van de Avg en de Wpg. Tevens staan in verschillende DPIA's op moment van vaststelling meerdere openstaande maatregelen aangegeven. Dit betreft maatregelen die nodig zijn om de aangegeven risico's van de verwerking te mitigeren. De defensieonderdelen zijn bezig met het realiseren van verbetermaatregelen. Het is onvoldoende inzichtelijk of alle onderdelen het inzicht in en de bewaking van de realisatie van alle relevante verbetermaatregelen structureel geborgd hebben. Dit is een aandachtspunt voor het toezicht in 2023.

[25] BS2023001377, 17 januari 2023. Te laat melden datalekken aan de AP.

3.9 Wet politiegegevens

De hoeveelheid Wpg-werkzaamheden bij de KMar is groter dan door de huidige twee privacyfunctionarissen kon worden uitgevoerd in 2022. Vanwege onvoldoende capaciteit bij het cluster Juridische Zaken konden de privacyfunctionarissen in deze periode minder prioriteit geven aan een aantal taken. Een van deze taken betrof het uitvoeren van toezichtwerkzaamheden op de naleving van de Wpg.

De privacyfunctionarissen krijgen vanuit de KMar-organisatie een groot aantal vragen binnen over de Wpg en daaraan gerelateerde onderwerpen. Gemiddeld 600 vragen op jaarbasis. Het beantwoorden van deze vragen vergt veel tijd. Daarnaast is er een stijging te zien in het aantal inzageverzoeken op basis van de Wpg (+/- 90 in 2022). Het afhandelen hiervan vraagt ook veel van de capaciteit.

De gewijzigde Wpg (ingegaan op 1 januari 2019) bevat een verplichting voor de verwerkingsverantwoordelijke om logbestanden bij te houden van ten minste de volgende activiteiten in systemen voor geautomatiseerde verwerking:

- verzameling;
- wijziging;
- raadpleging;
- verstrekking onder meer in de vorm van doorgiften;
- combineren;
- het vernietigen van politiegegevens.

De logbestanden van raadpleging en bekendmakingen moeten het mogelijk maken de redenen, de datum en het tijdstip van die handelingen en indien mogelijk de identiteit te achterhalen van de persoon die de persoonsgegevens heeft geraadpleegd of heeft bekendgemaakt en de identiteit van de ontvangers van die persoonsgegevens. Deze verplichting dient uiterlijk in 2023 doorgevoerd te zijn in de geautomatiseerde systemen. De stand van zaken van de implementatie van de loggingsplicht is onvoldoende inzichtelijk.

De Wpg kent een *audit*-verplichting op grond van artikel 33 Wpg. Deze verplichting houdt in dat door middel van interne- en externe *audits* de opzet, het bestaan en de werking van de genomen maatregelen en procedures rond de naleving van de Wpg worden beoordeeld. Deze *audits* dienen jaarlijks intern uitgevoerd te worden op deelaspecten van de Wpg en eenmaal per vier jaar dient een volledige en onafhankelijke externe *audit* uitgevoerd te worden. De ADR heeft in 2022 de verplichte externe (privacy-) *audit* van 2019 over de periode 2014-2018 uitgevoerd. De KMar dient de volgende externe audit, over de periode 2019-2022, in 2023 uit te laten uitvoeren. De interne audit over 2021 is in 2022 niet uitgevoerd door de KMar.

3.10 Internationaal verband

Een organisatie mag alleen persoonsgegevens doorgeven aan derde landen met een passend beschermingsniveau. In dit verband worden de overige landen binnen het Koninkrijk der Nederlanden (Curaçao, Aruba, St. Maarten) ook als zodanig beschouwd. Deze regel geldt ook voor in Nederland gevestigde internationale (militaire) organisaties waarmee persoonsgegevens worden uitgewisseld.

In 2022 heeft DGB/DBE/Gegevensbescherming een start gemaakt met het intensiveren van contacten met Duitsland, België, Denemarken, de NAVO en de *European Defence Agency* als het gaat om gegevensbescherming. Op binationaal vlak zijn er gesprekken gevoerd met Duitsland, wat heeft gezorgd voor een concept '*Memorandum of understanding*' (MOU) dat als raamwerk zal dienen voor de gegevensuitwisseling. Met België zijn de eerste verkennende gesprekken gevoerd ten aanzien van het optuigen van een vergelijkbare MOU inzake gegevensbescherming voor de BeNeSam[26]. Daarnaast is er op multinationaal niveau een vergevorderd initiatief om ten aanzien van gegevensbescherming een *Implementing Arrangement* op te leveren voor het *European Air Transport Command*.

In november 2022 vond een evenement plaats met NAVO (HQ en SHAPE), EDA, Duitsland, België en Denemarken, waarbij is gesproken over de uitdagingen bij militaire gegevensuitwisseling. De conclusie is dat dit onderwerp op dit moment te weinig aandacht krijgt en meer urgentie verdient. Daarom zal Nederland begin 2023, samen met België, Duitsland en Denemarken, een brief naar de NAVO en EDA sturen om hiervoor structurele projectcapaciteit te vragen.

[26] Belgisch-Nederlandse Samenwerking.

4 Bijlagen

Bijlage 1: Bevindingen defensieonderdelen

	Avg- en Wpg oganisatie	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS	BS DOPS	Defensie brede processen	DMO/ JIVC	Dosco
A	Avg-beheerders hebben een Avg-coördinator aangewezen. De Wpg-beheerder heeft een privacyfunctionaris aangewezen.										
B	De Avg-coördinatoren en de privacyfunctionaris zijn aangemeld bij de FG.										
C	De Avg-coördinatoren en de privacyfunctionaris zijn formeel bekend gesteld binnen de organisatie.										
D	De taak van Avg-coördinator en privacyfunctionaris is opgenomen in de functieomschrijving van de aangewezen medewerkers.						i	i	i		
E	Geborgd is dat de Avg-coördinator/PF de benodigde tijd, middelen en ruimte krijgt om de taak naar behoren uit te kunnen voeren. Tevens dat ze voldoende opleiding krijgen om de functie uit te kunnen voeren.	ii	iii	iv	v	v	vi	vii	viii		
F	Het defensieonderdeel heeft activiteiten uitgevoerd in het kader van 'Avg- en Wpg-awareness'.										
G	Er is een overzicht van verwerkersovereenkomsten die nog afgesloten of geactualiseerd dienen te worden										
H	De Avg- en Wpg registers zijn geactualiseerd. Opgenomen verwerkingen zijn vastgesteld.	ix	x	xi	xii	xiii	xiv	xv		xvi	xvii
I	Alle vastgestelde DPIA's zijn (als bijlage) in het register van verwerkingsactiviteiten opgenomen.				xii	xiii		xv			
J	Alle verwerkersovereenkomsten zijn (als bijlage) toegevoegd aan het register.				xii	xiii		xv			

Ja/goed	
Verbetering nodig	
Onbekend/geen info	

i. Omdat er wordt gewerkt met generieke functiebeschrijvingen maken de Avg-taken geen onderdeel uit van de generieke functiebeschrijving.

ii. De korte doorlooptijd van Avg-coördinatoren bij CZSK zorgt ervoor dat de Avg-coördinator met een achterstand in netwerk en kennis moeten starten. Vanaf 2023 krijgt de nieuwe Avg-coördinator een langere plaatsingsduur krijgen.

iii. CLAS maakte in 2022 een versterking- en professionaliseringsslag voor de Avg-organisatie door drie fulltime (tijdelijke) Avg-functionarissen aan te stellen. Twee VTE bij Staf CLAS en een VTE bij OOCL. In 2023 wordt de capaciteit binnen Staf CLAS drie vaste functies en OOCL een tijdelijke functie.

iv. De enkele Avg-coördinator CLSK op stafniveau kan de vraag niet aan: er blijven zaken liggen omdat er geprioriteerd moet worden. Dit geldt evenzeer voor de onderdelen, waar de lokale Avg-functionarissen hun werkzaamheden in het beste geval als neventaak uitoefenen.

v. Het aanbod van Avg-werkzaamheden en Wpg-werkzaamheden is hoog, waardoor de afhandeltermijn van (aan)vragen hoger is dan wenselijk. Voorzien wordt dat de werkdruk ook in 2023 blijft voortduren, waardoor bepaalde taken blijven liggen, of later opgepakt kunnen worden dan wenselijk is. Vanwege onvoldoende capaciteit bij het cluster Juridische Zaken, konden de privacyfunctionarissen in deze periode aan een aantal taken minder prioriteit geven. Een van deze taken betrof het uitvoeren van de toezichttaak Wpg. In februari 2022 is een tweede privacyfunctionaris aangesteld.

vi. Er is geen ruimte voor een proactieve invulling van deze rol. De Avg-coördinator heeft wel versterking gekregen binnen AIP. Omdat er vanuit de organisatie steeds meer aandacht is voor de Avg, neemt de hoeveelheid werk geenszins af en is er te weinig tijd.

vii. De functie van Avg-coördinator 'Militaire operaties' is een nevenfunctie en de beschikbare tijd voor de uitvoering ervan is te beperkt. De aanstaande wijziging op de Regeling Gegevensbescherming Militaire Operaties (RGMO), samen met de toenemende bewustwording op de naleving van de Avg vraagt om meer kennis en ervaring bij het hanteren van de Avg en de RGMO. Om vanaf 2023 en daarna de rol Avg-coördinator 'Militaire operaties' op een betere en meer verantwoorde manier in te zetten is meer expertise en capaciteit nodig.

viii. Alle Avg-taken (exclusief toezicht) zijn in 2022 tot oktober uitgevoerd door twee en daarna drie functionarissen. Het uitvoeren van het volledige takenpakket is een uitdaging. De werkzaamheden gerelateerd aan de onderzoeken na LIMC en de beleidsreactie daarop hebben geleid tot verdringing en prioritering van de reguliere Avg-coördinatortaken en andere werkzaamheden.

ix. CZSK heeft, in samenspraak met de Avg-coördinator 'Defensiebrede verwerkingen', de meldingen in het verwerkingenregister geactualiseerd. Het streven is dat het verwerkingsregister CZSK in zijn geheel in Q1 2023 geactualiseerd is. Van de 115 geregistreerde verwerkingen zijn 95 vastgesteld, 18 hebben de status 'in bewerking', twee hebben de status 'vaststelling aangevraagd'.

x. CLAS maakte in 2022 een verbeterslag gemaakt. Van de 139 verwerkingen zijn 77 vastgesteld, 41 zijn in bewerking, 13 hebben de status 'ter review' en 8 de status 'vaststelling aangevraagd'.

xi. CLSK heeft, in samenspraak met de Avg-coördinator 'Defensiebrede verwerkingen', de meldingen in het verwerkingenregister geactualiseerd. Bij CLSK vindt nog een nadere kwaliteitsslag en samenvoeging van geregistreerde verwerkingen plaats. Van de 176 geregistreerde verwerkingen zijn 22 vastgesteld, 63 hebben de status 'in bewerking' en voor 91 verwerkingen is de status 'vaststelling aangevraagd'.

xii. Van de 46 geregistreerde verwerkingen, hebben 38 de status 'vastgesteld', zeven verwerkingen zijn 'in bewerking' en een de status 'vaststelling aangevraagd'. In 2022 is een hernieuwde aanpak gehanteerd voor het verder aanvullen van het Avg-register. Hierbij wordt een toepassingslijst gebruikt, waarin de verschillende systemen van de KMar staan. Deze lijst wordt als aanknopingspunt gebruikt om de verwerkingsactiviteiten in het register verder toe te voegen.

xiii. Het Wpg-register is nog niet gevuld. Zes verwerkingen zijn geregistreerd. Door capaciteitsgebrek is de noodzakelijke inventarisatie nog niet afgerond en zijn de KMar-verwerkingen nog niet (volledig) opgenomen in het register. In 2022 is een hernieuwde aanpak uitgewerkt, naar waarschijnlijkheid zal in 2023 het Wpg-register van verwerkingen verder aangevuld worden.

xiv. De BS (apparaat) heeft, in samenspraak met de Avg-coördinator 'Defensiebrede verwerkingen', de meldingen in het register van verwerkingsactiviteiten geactualiseerd. De BS heeft 30 vastgestelde verwerkingen in het register. Negen verwerkingen zijn in bewerking, een ligt ter review en vier hebben de status 'vaststelling aangevraagd'.

xv. Een RGMO-verwerkingsregister is opgesteld, waarin zowel de 'normale' verwerkingen als de 'uitzonderingsverwerkingen' voor militaire operaties zijn opgenomen. De FG heeft in 2022 het register van de DOPS niet onderzocht. Een onderzoek staat gepland voor 2023.

xvi. DMO heeft, in samenspraak met de Avg-coördinator 'Defensiebrede verwerkingen', de meldingen in het verwerkingenregister geactualiseerd. Bij DMO vindt nog een nadere kwaliteitsslag en samenvoeging van geregistreerde verwerkingen plaats voor publicatie op het internet. DMO heeft van de 44 geregistreerde verwerkingen er 35 vastgesteld, zeven zijn in bewerking, een ligt ter review en voor een is vaststelling aangevraagd.

xvii. DOSCO heeft, in samenspraak met de Avg-coördinator 'Defensiebrede verwerkingen', de meldingen in het verwerkingenregister geactualiseerd. 83 van de 124 verwerkingen zijn vastgesteld, 35 hebben de status 'in bewerking', vijf liggen ter review en voor een is vaststelling aangevraagd.

Bijlage 2: Afkortingen

ABP	Algemeen Burgerlijk Pensioenfonds
ADR	Auditdienst Rijk
AP	Autoriteit Persoonsgegevens
APG	Algemene Pensioen Groep
Avg	Algemene verordening gegevensbescherming
BA	Beveiligingsautoriteit
BIDKL	Bergings- en Identificatiedienst Koninklijke Landmacht
BS	Bestuursstaf
CLAS	Commando Landstrijdkrachten
CLSK	Commando Luchtstrijdkrachten
CZSK	Commando Zeestrijdkrachten
DCIOD	Dienstencentrum Internationale Ondersteuning Defensie
DCPL	Dienstencentrum Personeelslogistiek
DCSC	Defensie Cyber Security Center
DI	Documentaire Informatievoorziening
DMO	Defensie Materieel Organisatie
DOPS	Directie Operaties
DOSCO	Defensie Ondersteuningscommando
DPIA	Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling)
DPO	Data Protection Officer
EGB	Eerstelijns Gezondheidszorg Bedrijf
FG	Functionaris voor Gegevensbescherming
HDP	Hoofddirectie Personeel
IMG	Inspectie Militaire Gezondheidszorg
IGO	Informatiegestuurd optreden
IVD	Inspectie Veiligheid Defensie
JIVC	Joint IV Commando
LIMC	Land Information Manoeuvre Centre
OSINT	Open Source Intelligence
Pi-NL	Passenger Information Unit Nederland
UAvg	Uitvoeringswet Avg
Wpg	Wet politiegegevens

Bijlage 3: Begrippenkader

Begrippen	Toelichting
Avg-beheerder	Het diensthoofd dat namens de Minister van Defensie belast is met de zorg voor de naleving van de Avg en de wet ten aanzien van verwerkingen die gevoerd worden binnen het dienstonderdeel. De operationele commandanten van de krijgsmachtonderdelen, de commandant DOSCO, de directeur van de DMO en de plaatsvervangend Secretaris-generaal voor de Bestuursstaf zijn aangewezen als Avg-beheerder.
Avg-coördinator	Functionaris, aangewezen door de Avg-beheerder, die de uitvoering van de Avg en de wet, en de feitelijke handelingen die daarvoor nodig zijn, binnen het betreffende dienstonderdeel coördineert.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Datalek ('inbreuk in verband met persoonsgegevens')	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
GEB/DPIA	Een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken.
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een *identificator* zoals een naam, een identificatienummer, locatiegegevens, een online *identificator* of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Politiegegeven	Een politiegegeven is elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012 (met uitzondering van de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften en de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012).

Begrippen	Toelichting
Register van verwerkingsactiviteiten	Register waarin alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens worden bijgehouden. Met dit centrale register wordt weergegeven welke processen en activiteiten er met persoonsgegevens plaatsvinden inclusief de verwerkingsdoelen en wettelijke grondslagen.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerken van politiegegevens	Elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Wpg-beheerder	De Wpg-beheerder draagt zorg voor naleving van de regelgeving omtrent verwerking van politiegegevens door de KMar. De C-KMar is Wpg-beheerder namens de Minister van Defensie.